R&D

SECURITY TARGET

"Valid eUICC IoT v1.0"

V1.6

VALID

www.valid.com

History

Revision	Date	Changes	Author	Approved
1.0	16/01/2025	Initial Version	R&D	Rafael Gómez (R&D Manager)
1.1	27/01/2026	Minor changes	R&D	Rafael Gómez (R&D Manager)
1.2	29/01/2026	Minor changes	R&D	Rafael Gómez (R&D Manager)
1.3	29/01/2026	Minor changes	R&D	Rafael Gómez (R&D Manager)
1.4	02/02/2026	Minor changes	R&D	Rafael Gómez (R&D Manager)
1.5	15/07/2026	Updates addressing comments raised by the evaluation laboratory.	R&D	Rafael Gómez (R&D Manager)
1.6	24/07/2026	Updates addressing comments raised by the evaluation laboratory.	R&D	Rafael Gómez (R&D Manager)

Table of Contents

Document overview

This document offers guidance based on VALID's current understanding and expertise. Please note that this information may evolve as product features and characteristics change.

The recommendations outlined here are designed to help you achieve the security objectives specified in the Target of Evaluation (TOE).

VALID strongly encourages you to follow these recommendations for secure product deployment.

VALID will not be liable for any adverse outcomes resulting from the failure to implement these recommendations.

1. ST Introduction

1.1 ST Reference

The ST identification is the following:

Title:	**Security Target "Valid eUICC IoT v1.0"**
Version:	**1.6**
Author:	**VALID**
Reference:	**Security Target "Valid eUICC IoT v1.0"**
Publication date:	**24/07/2026**

1.2 TOE Reference

Product Name:	**Valid eUICC IoT v1.0**
Developer:	**VALID**
TOE Name:	**Valid eUICC IoT v1.0**
TOE Version:	**1.3**
TOE Documentation:	Guidance [**GUIDES**]
TOE Hardware:	**SLx22 (IFX_CCI_00007Ah A11/R11/M11)**

2. TOE Overview

This section describes the Target of Evaluation (TOE) architecture, its type and common usages, life cycle, and physical and logical scope.

2.1 TOE Description

The TOE **Valid eUICC IoT v1.0** is an eUICC (embedded UICC) for Internet of Things (IoT) Devices.

The TOE is an eUICC open platform with multi-application support, such as Java Card, Global Platform, that implements the GSMA Remote SIM Provisioning (RSP) Architecture for IoT Devices compliant with the GSMA specifications SGP.31, SGP.32 and SGP.33 and the Trusted Connectivity Alliance eUICC Profile Package implementing [EUPP].

To enable updates and already installed embedded OS, the TOE contains the OSU (Operating System Update) software.

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

The TOE is composed of:

- A hardware Infineon SLx22 chip based on a 32-bit secure CPU with ROM, up to 1.8M NVM and up to 96kB RAM. The hardware also incorporates communication peripherals and cryptographic coprocessors for execution and acceleration of symmetric and asymmetric cryptographic algorithms from Infineon Technologies.
    - Certification ID: **IFX_CCI_00007Ah A11/R11/M11**
    - Cert Report Number: **BSI-DSZ-CC-1272**
- The embedded eUICC OS over the secure IC platform.
- The Runtime Environment (Java Card System).
- The OSU (OS Update) which is a module that enables a full Operating System update.
- The IPAe module integrated in the eUICC operating system.

2.2 TOE type and usage

The TOE type is a composite system composed of the eUICC software, JCS and OS on top of the certified IC hardware Infineon SLx22.

It consists of secure software running on a secure integrated circuit (IC). The embedded Universal Subscriber Identity Module (eUICC) is integrated into an IoT device. The eUICC connects to a specific mobile network using its currently active Mobile Network Operator (MNO) profile.

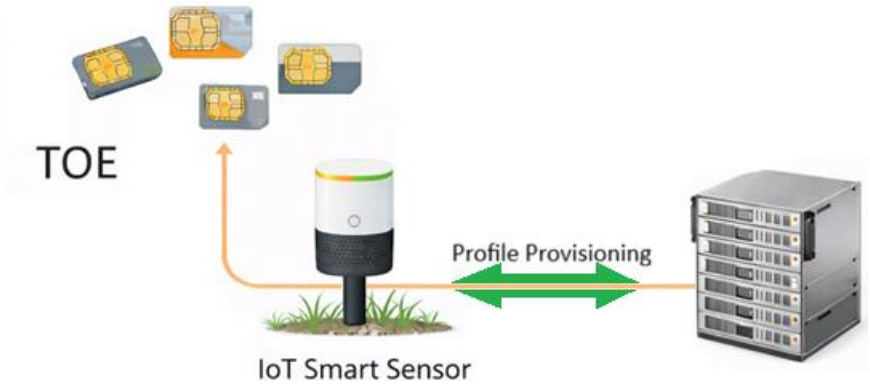

Figure 1 – Product environment

The TOE requires an IoT Profile Assistant (IPA) component. It can either be implemented at the application level as IPAe (the case covered by the IPA PP-Module), or in can be implemented as a non-TOE on-device unit called IPAd.

In this TOE, the OS implements the IoT Profile Assistant embedded in the eUICC (IPAe) as defined in GSMA SGP.25, while also supporting the implementation of an IPAd as a non-TOE on device unit. IPAe enables secure interaction with remote RSP entities (SM-DP+ and SM-DS) for triggering and managing profile download and lifecycle operations in unattended IoT devices.

The **OSU** (OS Update) capability is available to correct existing features as required by the GSMA specifications.

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

The TOE architecture for ST product is represented in the next figure, that represents the eUICC in three layers:

- Hardware.
- eSIM Operating System.
- eSIM data.

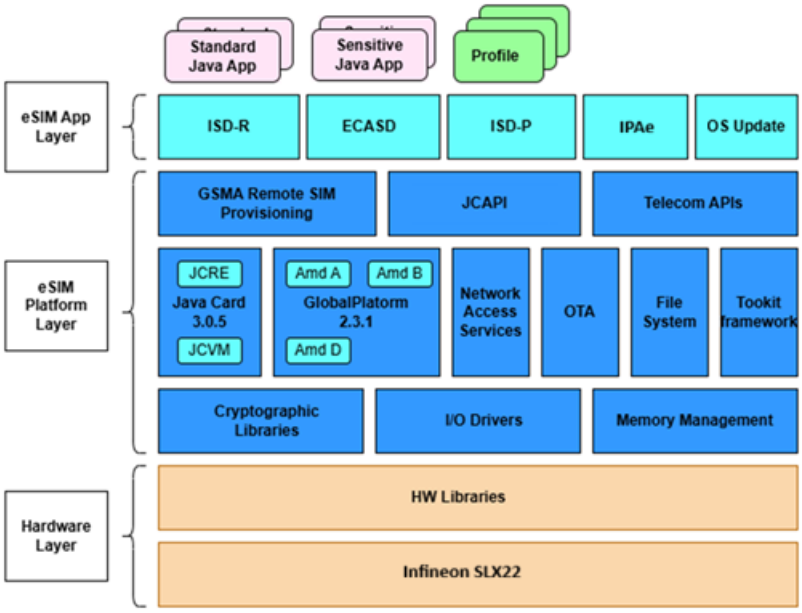

Figure 2 – Valid eUICC IoT v1.0 architecture overview

The TOE includes:

- The Hardware layer is the IC providing support to the platform layer.
- The eSIM platform layer is composed of a set of functions providing support to the application layer.
- The eSIM application layer is composed of privileged applications providing remote provisioning and administration functionality.

The scope of the TOE is shown in the next figure.

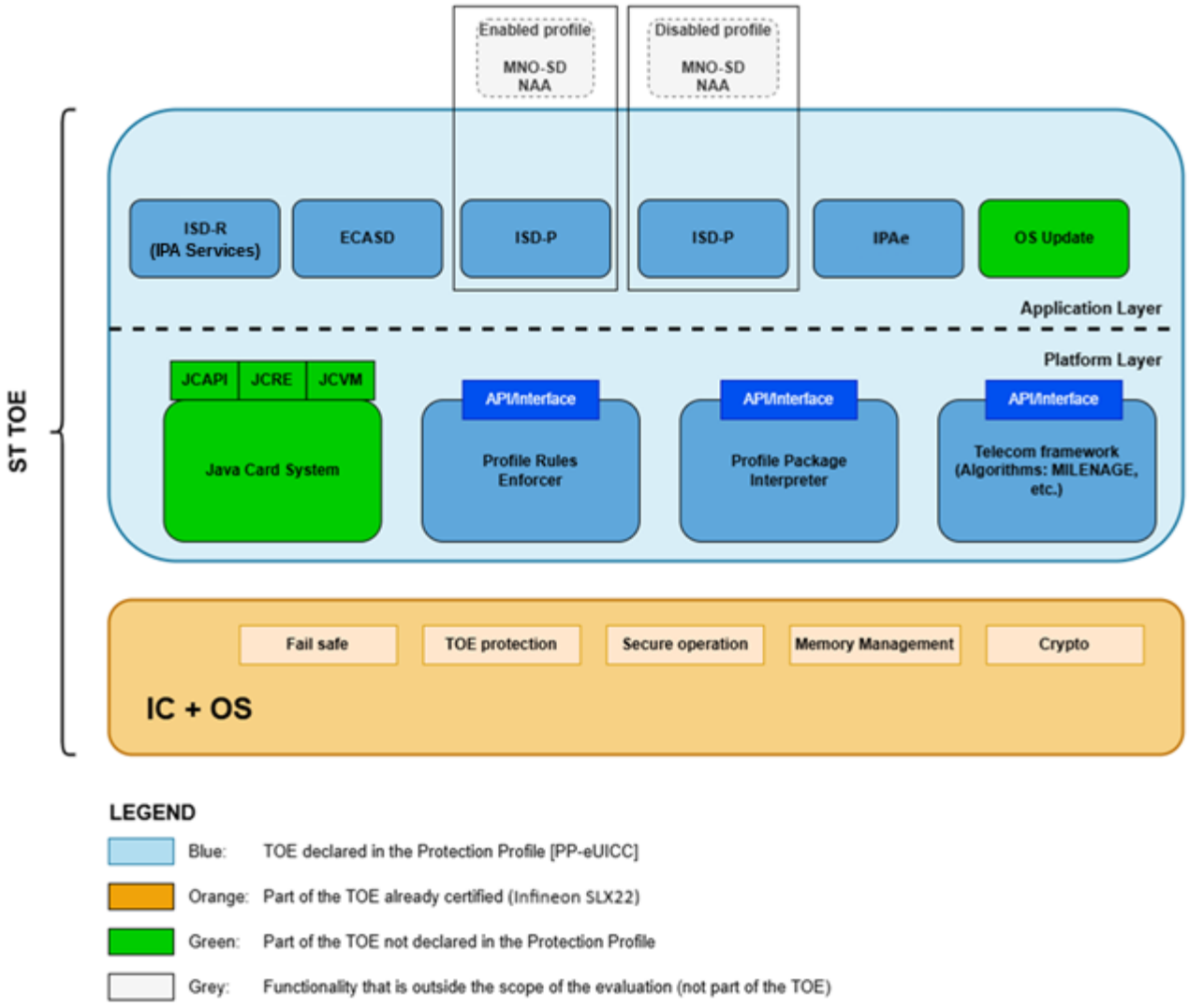

Figure 3 – TOE scope

2.3 TOE life cycle

The life cycle of the TOE is as described in [PP-eUICC]. It's composed of 5 phases (from phase 'a' to phase 'e') which are described in current ST section.

Actors involved in each phase are mentioned below and the associated locations as well.

The delivery of the self-protected TOE takes place before phase 'd' as shown in the next figure.

Phase 'e': operational usage of the TOE includes the activities related with OSU in addition to those listed in next figure.

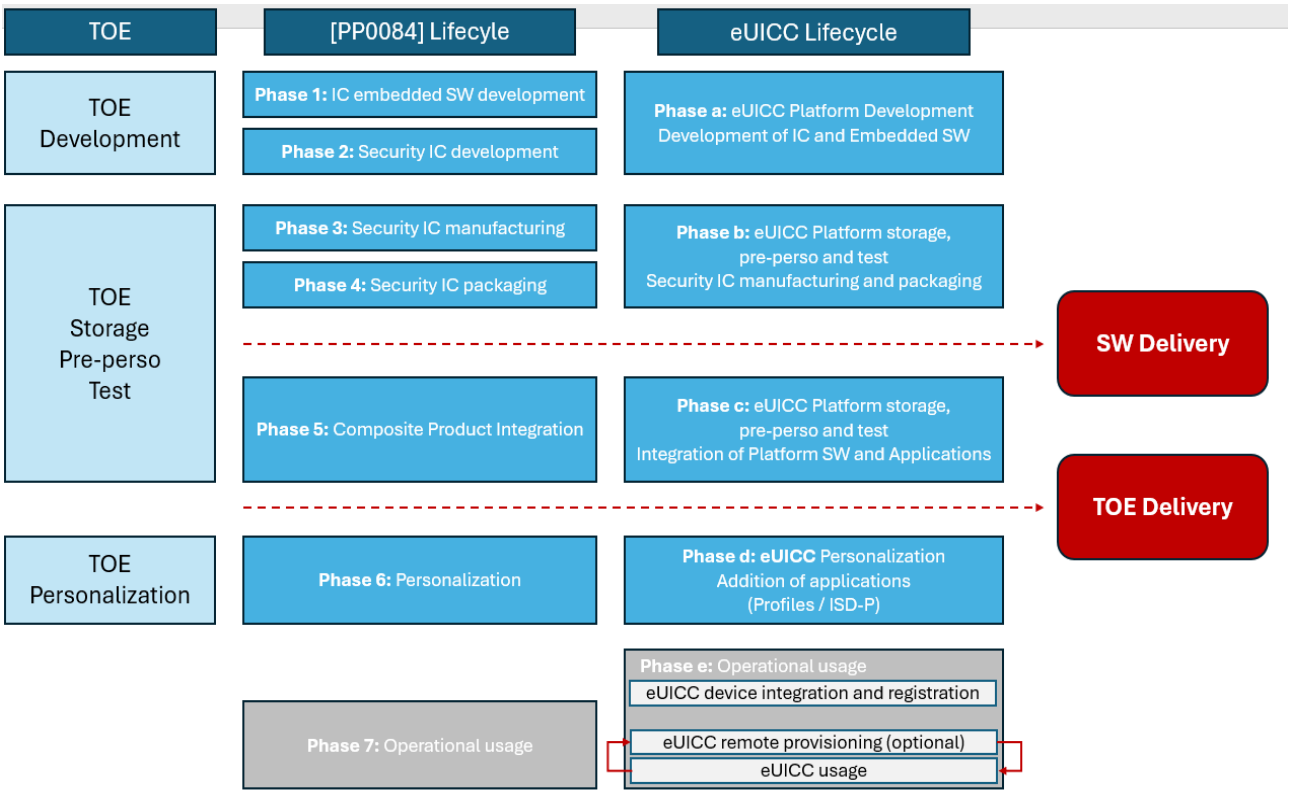

Figure 4 – TOE life cycle and actors

The following table provides an overview of the TOE life cycle:

Phase	Phase description	Actor	Location
a	OS and eSIM development	Valid	Valid's R&D site (EMVCo site audit)
	Development of IC and Embedded Software	Infineon	Sites covered by the IC certificate
b	Security IC manufacturing and packaging	Infineon	Infineon's factories (CC site audit)
c	Integration of Platform Software and Applications	Valid	Valid's Factory site (EMVCo site audit)
--- TOE DELIVERY ---			

d	Dynamic images generation and eSIM OS personalization loading Secure Application	Valid	Valid's Factory site (SAS-UP site audits).
e	Profile loading and activation	Device manufacturer/eIM	On the field, remote access to device manufacturer server

Table 1 - TOE life cycle

The Actors:

- The eUICC Manufacturer (EUM) develops the secure eUICC secure application (VALID).
- The IC Manufacturer designs and produces the integrated circuit (IC) (Infineon)
- The OEM is the original equipment manufacturer of the device.
- The profile issuer is the mobile network operator (MNO) that has the authority to perform remote card content management (CCM) operations on its own profile (ISD-P) using its over-the-air (OTA) server. Although it can also provide profiles to the end user through its RSP servers, it requires the end user's consent to manage profiles remotely.
- The Application Providers (AP) are entities or institutions responsible for their applications and associated services. Examples include financial institutions (banks) and transportation operators.
- The eIM is the RSP entity that manages the profile operations in the eUICC.

The manufacturing flow is described below:

- Phase a:
    - Development and testing of the eUICC Platform development and its associated security features. The eUICC product, specifically the "Static Data" (OS + Pre-Personalization) is generated.
        - Actor: **VALID**
    - Development of IC
        - Actor: **Infineon**
- Phase b:
    - IC's manufacturing, test and sensitive assets management.
        - Actor: **Infineon**
- Phase c:
    - Setting IC embedded bootloader-specific VALID keys for loading application firmware onto flash memory. Performing IC Wafer Testing. Loading the "Static Data" (OS software + Pre-Personalization) onto the eUICC through the IC embedded Bootloader.
        - Actor: **VALID**
- Phase d:

- Development and testing of "Dynamic Data" (Personalization data, carry out by VALID).
- Loading of the "Dynamic Data" (Personalization data, carry out by VALID).
  - Actors: **VALID**

Previous Phases are carried out in secure environments and sites are covered by **CC/EMVCo** or **GSMA SAS-UP** site audit.

TOE delivery to point of sales:

The device has arrived at the points of sale and is ready for purchase.

- Phase e:
  - The Device Manufacturer is responsible for receiving the final eUICC and integrating it into an IoT device, ensuring proper functionality.
  - The eIM interacts with the eUICC remotely though a secure communication channel manage Operator profiles and eIM Configuration Data.
    - Actors: **Manufacturer/eIM**

The OS Update flow is described below:

An OS update is triggered when the eUICC Secure Application (eSIM OS) exhibits security vulnerabilities, functional issues, or the need for additional features.

- Phase a:
  - eUICC Secure Application (eSIM OS) update development / Validation
    - Actor: **VALID**

TOE delivery:

Secure delivery of eSIM OS (patch) to Device OEM.

- Phase e:
  - RSP process (Profile loading and activation)
    - Actor: **Manufacturer/eIM**

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

Non-TOE is same as the ones mentioned in the [PP-eUICC] except for IC, including its Embedded Software (ES), and RE, which are in scope of the TOE.

Bytecode verifier (BCV) must be used before loading a new applet (developed following the rules defined in [GP SG]) 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.

2.4 TOE scope

2.4.1 Physical scope

The physical boundaries define the area within the IC's hardware where the eSIM software operates. Other components are not included in this evaluation.

The TOE consists of the following components:

- **Hardware:**
  - Developer: Infineon Technologies
  - Item: IFX_CCI_00007Ah A11/R11/M11
    - Certification ID: **IFX_CCI_00007Ah A11/R11/M11**
    - Cert Report Number: **BSI-DSZ-CC-1272**
  - Form of delivery: IC module.
  - Delivery method: Delivered physically to Valid's Factory.
- **eUICC OS:**
  - Developer: VALID
  - Item: **Valid eUICC IoT v1.0**
  - Form of delivery: Software (binary in memory).
  - Delivery method: Delivered embedded on the IC.
- **eUICC guidance's:**
  - Developer: VALID.
  - Item: Guides for **Valid eUICC IoT v1.0**
    - [EN] AGD_OPE - Valid eUICC IoT v1.0 - Operational User Guidance - v1.2
    - [EN] AGD_OPE - Valid eUICC IoT v1.0 - Operational User Guidance - Basic Applet Guidelines - v1.1
    - [EN] AGD_OPE - Valid eUICC IoT v1.0 - Operational User Guidance - Sensitive Applet Guidelines - v1.0
    - [EN] AGD_PRE - Valid eUICC IoT V1.0 - Preparative Procedures - v1.2

- Form of delivery: Documents (.pdf)
- Delivery method: Electronic document (PDF) protected with PGP by mail

2.4.2 Logical scope

The eUICC OS provides (at least) the following services:

- Enabling Remote SIM Provisioning.
- Managing communications between the OS and external entities.
- OS Security services as:
  - Providing secure cryptographic primitives, algorithms and services.
  - Ensure the security assets.
  - Generating random numbers.
- Enforcing the Javacard Runtime and Firewall mechanism.
- Standard APIs like Telecom APIs and GP APIs.
- Special services:
  - OSU (OS Update).
  - IPAe

Note: The Java Card included within the scope of the evaluation is limited to the functionalities required by the eUICC. Furthermore, the JC API is considered outside the scope of this evaluation as a service for third party applets.

The TOE also includes the certified Security IC and any embedded software within the IC that provides security-enforcing services used by the TOE. In particular, the IC contributes to the TOE logical scope by providing mechanisms supporting O.IC.SUPPORT and O.IC.RECOVERY, including:

- protection against bypass or alteration of TSFs and restriction of low-level access to TOE API mechanisms;
- protection of code and data stored in IC memory against disclosure/modification;
- support for secure low-level cryptographic processing and RNG services used by TOE components;
- support for atomic operations / transaction mechanisms and secure recovery to a consistent state after interruption.

3. Conformance Claims

Evaluation type:

- This is a composite evaluation, which relies on the IC Infineon SLx22:
  - Certification done under **Bundesamt für Sicherheit in der Informationstechnik (BSI)**.
  - Security Target of IC [ST/IC] conformance to **[PP-0084]**.
  - Assurance level: **EAL6+ (ALC_FLR.1 and ATE_SDP.1)**.

3.1 Common Criteria version and Conformance claims

The Security Target claims conformance to Common Criteria 2022 release 1: [CC-1], [CC-2], [CC-3] and [CC-5].

The Security Target also claims the CC:2022 and CEM:2022 Errata and Interpretation document [CC-ERRATA].

The Security Target is CC Part 2 [CC-2] extended and CC Part 3 [CC-3] conformant of CC:2022 release 1.

3.2 Package Conformance claim - Assurance Package

The Security Target meets the requirements of the EAL4+ augmented with ALC_DVS.2 and AVA_VAN.5 and the composite product package (COMP) defined in [CC-5].

The ADV_ARC defined in [PP-eUICC] is refined to include specific verifications beyond the existing criteria.

3.3 Protection Profile Conformance claim

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

The TOE claims conformance to the OS Update PP-module and IPAe PP-module, extracted from [PP-eUICC] protection profile.

3.4 Conformance claim rationale

The Security Target is conformant to the claimed Protection Profile.

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

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.

The Security Functional Requirements in this ST have been taken directly from the [PP-eUICC] (chapter 6 and chapter 9.7.1) and operations as appropriate have been performed.

Conformance rationale of the Security Target 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 in 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. Additions are from [PP-JCS], [PP-GP] or [CC-2].
- (X): The element is present in [PP-eUICC].

3.4.1 Conformity of the TOE Type

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

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

This is a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

3.4.2 SPD Consistency

3.4.2.1 Assets consistency

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

Assets	PP-eUICC	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)

D.PROFILE_IDENTITY	X	(E)
D.PROFILE_RULES	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.UPDATE_IMAGE	X	(E): as part of OS Update PP-module
D.TOE_IDENTIFIER	X	(E): as part of OS Update PP-module
D.IPAe_TSF_CODE	X	(E): as part of IPAe PP-Module.
D.IPAe_DEVICE_INFO	X	(E): as part of IPAe PP-Module.
D.IPAe_KEYS	X	(E): as part of IPAe PP-Module.
D.OS-UPDATE_KEY(S)	X	(E): as part of OS Update PP-module
D.APP_CODE		(A): Added from [PP-JCS].
D.APP_C_DATA		(A): Added from [PP-JCS]
D.APP_I_DATA		(A): Added from [PP-JCS].

D.APP_KEYS		(A): Added from [PP-JCS].
D.PIN		(A): Added from [PP-JCS].
D.API_DATA		(A): Added from [PP-JCS].
D.CRYPTO		(A): Added from [PP-JCS].
D.JCS_CODE		(A): Added from [PP-JCS].
D.JCS_DATA		(A): Added from [PP-JCS].
D.SEC_DATA		(A): Added from [PP-JCS].

Table 2 - Assets Consistency

3.4.2.2 Users and Subjects consistency

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

User	PP-eUICC	Security Target
U.SM-DP+	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.EIM (SGP.32)	X	(E)

Table 3 - Users Consistency

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

Subjects	PP-eUICC	Security Target
S.ISD-R	X	(E)
S.ISD-P	X	(E)

S.ECASD	X	(E)
S.PPI	X	(E)
S.PRE	X	(E)
S.TELECOM	X	(E)
S.OSU	X	(E): as part of OS Update PP-module
S.UpdateImageCreator	X	(E): as part of OS Update PP-module
S.IPAe	X	(E): as part of IPAe PP-Module
S.ADEL		(A): Added from [PP-JCS].
S.APPLET		(A): Added from [PP-JCS].
S.BCV		(A): Added from [PP-JCS].
S.CAD		(A): Added from [PP-JCS].
S.INSTALLER		(A): Added from [PP-JCS].
S.JCRE		(A): Added from [PP-JCS].
S.JCVM		(A): Added from [PP-JCS].
S.LOCAL		(A): Added from [PP-JCS].
S.MEMBER		(A): Added from [PP-JCS].
S.CAP_FILE		(A): Added from [PP-JCS].
S.SD		(A): Added from [PP-GP].
S.OPEN		(A): Added from [PP-GP].

Table 4 - 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 and the additions from [PP-JCS].

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	(R)
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	(R): Assets added from [PP-JCS] are mapped as threatened assets.
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.
T.PLATFORM-MNG-INTERCEPTION-IPAe	X	(E): as part of IPAe PP-Module.
T.UNAUTHORIZED-PLATFORM-MNG-IPAe	X	(E): as part of IPAe PP-Module.
T.PROFILE-MNG-ELIGIBILITY-IPAe	X	(E): as part of IPAe PP-Module.
T.LOGICAL-ATTACK-IPAe	X	(E): as part of IPAe PP-Module.
T.PHYSICAL-ATTACK-IPAe	X	(E): as part of IPAe PP-Module.

Table 5 – 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 and the additions from [PP-JCS].

OSPs	PP-eUICC	Security Target
OSP.LIFE-CYCLE	X	(E)
OSP.VERIFICATION		(A): Added from [PP-JCS].

Table 6 – 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 and the additions from [PP-JCS].

Assumptions	PP-eUICC	Security Target
A.TRUSTED-PATHS-LPAd-IPAd	X	(R)
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.ACTORS-IPAe	X	(E): as part of IPAe PP-Module.
A.CAP_FILE		(A): Added from [PP-JCS].
A.VERIFICATION		(A): Added from [PP-JCS].
A.Process-Sec-IC		(A): Added from [PP-0084]

Table 7 - Assumptions Consistency

3.4.2.6 Security Aspects consistency

Security aspects (SA) introduced by the OS Update PP-module are also within the scope of evaluation; in particular SA.CONFID-UPDATE-IMAGE and SA.INTEG-UPDATE-IMAGE are included.

Security Aspects	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

3.4.3 Security Objectives Consistency

3.4.3.1 Objective for the TOE consistency

All Security Objectives defined in [PP-eUICC] are relevant to 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.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.
O.SECURE-CHANNELS-IPAe	X	(E): as part of IPAe PP-Module.
O.INTERNAL-SECURE-CHANNELS-IPAe	X	(E): as part of IPAe PP-Module.
O.DATA-CONFIDENTIALITY-IPAe	X	(E): as part of IPAe PP-Module.
O.DATA-INTEGRITY-IPAe	X	(E): as part of IPAe PP-Module.
O.IC.PROOF_OF_IDENTITY		(A): Added and replace OE.IC.PROOF_OF_IDENTITY from [PP-eUICC].

O.IC.SUPPORT		(A): Added and replace OE.IC.SUPPORT from [PP-eUICC].
O.IC.RECOVERY		(A): Added and replace OE.IC.RECOVERY from [PP-eUICC].
O.RE.PRE-PPI		(A): Added and replace OE.RE.PRE-PPI from [PP-eUICC].
O.RE.SECURE-COMM		(A): Added and replace OE.RE.SECURE-COMM from [PP-eUICC].
O.RE.API		(A): Added and replace OE.RE.API from [PP-eUICC].
O.RE.DATA-CONFIDENTIALITY		(A): Added and replace OE.RE.DATA-CONFIDENTIALITY from [PP-eUICC].
O.RE.DATA-INTEGRITY		(A): Added and replace OE.RE.DATA-INTEGRITY from [PP-eUICC].
O.RE.IDENTITY		(A): Added and replace OE.RE.INTEGRITY from [PP-eUICC].
O.RE.CODE-EXE		(A): Added and replace OE.RE.CODE-EXE from [PP-eUICC].
O.LOAD		(A): Added from [PP-JCS].

Table 9 - Security Objectives for the TOE Consistency

3.4.3.2 Objective for Operational Environment consistency

O.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.EIM	X	(E)
OE.MNO	X	(E)

OE.TRUSTED-PATHS-LPAd-IPAd	X	(R)
OE.APPLICATIONS	X	(E): Security Guidelines from [GP SG]
OE.CAP_FILE	X	(A): Added from [PP-JCS].
OE.VERIFICATION	X	(A): Added from [PP-JCS].
OE.CODE-EVIDENCE	X	(A): Added from [PP-JCS].
OE.MNO-SD	X	(E)
OE.CONFID_UPDATE_IMAGE.CREATE	X	(E): as part of OS Update PP-module
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF_IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PRE-PPI	X	Removed and replaced by O.RE.PRE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY.
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY.
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE.
OE.Process-Sec-IC		A: Added from [PP-0084].

Table 10 - Security Objectives for the Operational Environment Consistency

3.4.4 Conformity of the Requirement (SFR / SAR)

3.4.4.1 SFR consistency

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

SFR	PP-eUICC	Security Target
FIA_UID.1/EXT	X	(E)
FIA_UAU.1/EXT	X	(E)
FIA_USB.1/EXT	X	(E)
FIA_UAU.4/EXT	X	(E)
FIA_UID.1/MNO-SD	X	(E)
FIA_USB.1/MNO-SD	X	(E)
FIA_ATD.1/Base	X	(E)
FIA_API.1	X	(E)
FDP_IFC.1/SCP	X	(E)
FDP_IFF.1/SCP	X	(E)
FTP_ITC.1/SCP	X	(E)
FDP_ITC.2/SCP	X	(E)
FPT_TDC.1/SCP	X	(E)
FDP_UCT.1/SCP	X	(E)
FDP_UIT.1/SCP	X	(E)
FCS_CKM.1/SCP-SM	X	(E)
FCS_CKM.2/SCP-MNO	X	(E)
FCS_CKM.6/SCP-SM	X	(E)
FCS_CKM.6/SCP-MNO	X	(E)

FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	(E)
FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
FCS_RNG.1	X	(E)
FPT_EMS.1/Base	X	(E)
FDP_SDI.1/Base	X	(E)
FDP_RIP.1/Base	X	(E)
FPT_FLS.1/Base	X	(E)
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/RULES	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1/Base	X	(E)
FMT_SMR.1/Base	X	(E)
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.6/Mobile_network	X	(E)
FIA_UID.1/IPAe	X	(E): as part of IPAe PP-Module.
FIA_UAU.1/IPAe	X	(E): as part of IPAe PP-Module.

FIA_USB.1/IPAe	X	(E): as part of IPAe PP-Module.
FIA_UAU.4/IPAe	X	(E): as part of IPAe PP-Module.
FIA_ATD.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_IFC.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_IFF.1/IPAe	X	(E): as part of IPAe PP-Module.
FTP_ITC.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_ITC.2/IPAe	X	(E): as part of IPAe PP-Module.
FPT_TDC.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_UCT.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_UIT.1/IPAe	X	(E): as part of IPAe PP-Module.
FCS_CKM.1/IPAe	X	(E): as part of IPAe PP-Module.
FCS_CKM.6/IPAe	X	(E): as part of IPAe PP-Module.
FPT_EMS.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_SDI.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_RIP.1/IPAe	X	(E): as part of IPAe PP-Module.
FMT_SMF.1/IPAe	X	(E): as part of IPAe PP-Module.
FMT_SMR.1/IPAe	X	(E): as part of IPAe PP-Module.
FDP_ACC.2/FIREWALL		(A): Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A): Added from [PP-JCS]. Refined.
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]. Refined.
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/EC **FCS_CKM.1/GP-SCP**		(A): Added from [PP-JCS]. Refined with iteration. (A): Added from [PP-GP].
FCS_CKM.3		(A): Added from [CC-2].
FCS_CKM.6/RE		(A): Added from [CC-2]. Refined with iteration.
FCS_COP.1/TDES_MAC **FCS_COP.1/AES_MAC** **FCS_COP.1/ECDH** **FCS_COP.1/CRC** **FCS_COP.1/ECDSA_SIGN** **FCS_COP.1/GP-SCP** **FCS_COP.1/TDES_CIPHER** **FCS_COP.1/AES_CIPHER** **FCS_COP.1/Hash** **FCS_COP.1/HMAC**		(A): Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A): Added from [PP-JCS].

FDP_RIP.1/APDU		(A): Added from [PP-JCS].
FDP_RIP.1/bArray		(A): Added from [PP-JCS].
FDP_RIP.1/GlobalArray		(A): Added from [PP-JCS].
FDP_RIP.1/KEYS		(A): Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A): Added from [PP-JCS].
FAU_ARP.1		(A): Added from [PP-JCS].
FDP_SDI.2/DATA		(A): Added from [PP-JCS].
FPR_UNO.1		(A): Added from [PP-JCS].
FPT_FLS.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FPT_TDC.1		(A): Added from [PP-JCS].
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ITC.2/Installer		(A): Added from [PP-JCS].
FMT_SMR.1/Installer		(A): Added from [PP-JCS].
FPT_FLS.1/Installer		(A): Added from [PP-JCS].
FPT_RCV.3/Installer		(A): Added from [PP-JCS].
FDP_ACC.2/ADEL		(A): Added from [PP-JCS].
FDP_ACF.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ADEL		(A): Added from [PP-JCS].

FMT_MSA.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].
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]. Refined.
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]. Refined.
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].
FPT_FLS.1/GP		(A): Added from [PP-GP].
FDP_ROL.1/GP		(A): Added from [PP-GP].
FCO_NRO.2/GP		(A): Added from [PP-GP].
FMT_SMF.1/GP		(A): Added from [PP-GP].
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP].

FDP_ITC.2/GP-KL		(A): Added from [PP-GP].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FTP_ITC.1/GP		(A): Added from [PP-GP].
FPR_UNO.1/GP		(A): Added from [PP-GP].
FPT_TDC.1/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-KL		(A): Added from [PP-GP].
FDP_IFF.1/GP-KL		(A): Added from [PP-GP].
FMT_MSA.3/GP		(A): Added from [PP-GP].
FAU_SAS.1		(A): Added from [PP-0084] to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added from [CC-2] to cover O.IC.RECOVERY. Refined with iteration.
FPT_RCV.4		(A): Added from [CC-2] to cover O.IC.SUPPORT.
FDP_ACC.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.
FDP_ACF.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.
FMT_MSA.3/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.

FMT_SMR.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.
FMT_SMF.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.
FIA_ATD.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.
FTP_TRP.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.
FCS_COP.1/OS-UPDATE-DEC		(A): Added from [PP-GP] to cover OS Update PP-Module. Refined.
FCS_COP.1/OS-UPDATE-VER		(A): Added from [PP-GP] to cover OS Update PP-Module.
FPT_FLS.1/OS-UPDATE		(A): Added from [PP-GP] to cover OS Update PP-Module.

Table 11 - Security Functional Requirement consistency

3.4.4.2 SAR consistency

This Security Target claims the same evaluation assurance level as [PP-eUICC], i.e., EAL4+ augmented with ALC_DVS.2 and AVA_VAN.5, including the composite product package (COMP) defined in [CC-5].

4. Security Problem Definition

This section outlines the security challenges facing the TOE and its operational context. It includes potential threats, environmental assumptions, and necessary organizational policies.

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

The TOE is exclusively intended for IoT devices; therefore, aspects related to consumer devices (SGP.22), such as U.End-User (SGP.22) or D.PROFILE_USER_CODES (SGP.22) do not apply to this security target.

4.1 Assets

All assets defined in [PP-eUICC] are relevant for the TOE of this Security Target, including the assets related to OS Update PP-module.

The definition of the Assets from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here. The list of the assets has been set in previous sections.

Assets	Refined/Added assets description
D.MNO_KEYS	
D.PROFILE_NAA_PARAMS	
D.PROFILE_IDENTITY	
D.PROFILE_RULES	Data describing the profile policy rules (PPRs) of a profile. These rules are loaded during provisioning, stored under the control of the ISD-P, and managed by the MNO OTA Platform. PPRs and Enterprise Rules are protected against unauthorized modification.
D.PROFILE_CODE	
D.TSF_CODE	
D.PLATFORM_DATA	
D.DEVICE_INFO	
D.PLATFORM_RAT	
D.SK.EUICC.ECDSA	

D.CERT.EUICC.ECDSA	
D.PK.CI.ECDSA	
D.PK.EIM.ECDSA (SGP.32)	
D.EID	
D.SECRETS	
D.CERT.EUM.ECDSA	
D.CRLs	
D.UPDATE_IMAGE	Encrypted and signed. An update can be an OS update, a patch, a complete OS replacement, or a separate bootloader. It's sent to the TOE and may include executable code, configuration data, or image type information. To ensure security, it must be protected from unauthorized disclosure and modification. It's also known as Additional Code.
D.TOE_IDENTIFIER	Identification data is used to uniquely identify the TOE. It must be protected from unauthorized modification.
D.OS-UPDATE_KEY(S)	
D.IPAe_TSF_CODE	IPAe code is an asset that has to be protected from unauthorized disclosure and modification. Knowledge of this code may allow bypassing the TSF. This concerns logical attacks at runtime in order to gain a read access to executable code, typically by executing an application that tries to read the memory area where a piece of code is stored.
D.IPAe_DEVICE_INFO	This asset includes the security-sensitive elements of Device Information data, such as the device type allocation code (TAC) or the device capabilities (ex. support for updating of certificate revocation lists (CRLs)), that is provided to the eUICC by the IPAe. To be protected from unauthorized modification.

D.IPAe_KEYS	This asset contains the secret keys (corresponding to the asset D.SECRETS of Base-PP) used by the IPAe to perform platform management functions: • session keys for the TLS connection (version 1.2 or greater) of IPAe to SM-DP+ along the interface ES9+; • session keys for the TLS connection (version 1.2 or greater) of IPAe to SM-DS along the interface ES11. • session keys for the TLS or DTLS connection (version 1.2 or 1.3) of IPAe to eIM along the interface ESipa. All of these assets are to be protected from unauthorised disclosure and modification.
D.APP_CODE	
D.APP_C_DATA	
D.APP_I_DATA	
D.APP_KEYs	
D.PIN	
D.API_DATA	
D.CRYPTO	
D.JCS_CODE	
D.JCS_DATA	
D.SEC_DATA	

Table 12 - Security Problem Definition assets

4.2 Users and Subjects

All Users and Subjects defined in [PP-eUICC] are relevant for the TOE of this Security Target, including those related to OS Update PP-module.

The definition of users and subjects from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here. The list of the users and subjects has been set in previous sections.

User
U.SM-DP+
U.SM-DS
U.EIM
U.MNO-OTA
U.MNO-SD

Table 13 - Security Problem Definition users

Subjects	Refined/Added assets description
S.ISD-R	
S.ISD-P	
S.ECASD	
S.PPI	
S.PRE	
S.TELECOM	
S.OSU	
S.UpdateImageCreator	
S.ADEL	
S.APPLET	
S.BCV	
S.CAD	
S.INSTALLER	
S.JCRE	
S.JCVM	
S.LOCAL	

S.MEMBER	
S.CAP_FILE	
S.OSU	The OS Update feature provides a secure mechanism to update the TOE's operating system with an image created by a trusted external entity, the S.UpdateImageCreator.
S.UpdateImageCreator	The off card Update Image Creator guarantees that confidentiality and integrity requirements are met.
S.IPAe	The IPAe is a functional element within the TOE that provides profile download and discovery services features.
S.SD	Represents a Security Domain; performs Secure Channel processing (e.g., unwrap/wrap), enforces required security levels and privileges for GP operations.
S.OPEN	Dispatches and controls GP card management operations and mediates forwarding to SDs/Applications.

Table 14 - Security Problem Definition subjects

4.3 Threats

All threats defined in the [PP-eUICC] are relevant for the TOE of this Security Target, including the threats related to OS Update PP-module.

They have been refined by extending the list of directly threatened assets shown in previous sections.

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

Threats	Refined/Added assets description
T.UNAUTHORIZED-PROFILE-MNG	Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_NAA_PARAMS, D.PROFILE_IDENTITY,

	D.PROFILE_RULES, D.PROFILE_CODE, **D.APP_C_DATA, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_CODE**.
T.UNAUTHORIZED-PLATFORM-MNG	Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behavior of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.
T.PROFILE-MNG-INTERCEPTION	Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_NAA_PARAMS, D.PROFILE_IDENTITY, D.PROFILE_RULES, D.PROFILE_CODE, **D.APP_C_DATA, D.PIN and D.APP_KEYs**.
T.PROFILE-MNG-ELIGIBILITY	Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, **D.APP_C_DATA, D.PIN, D.APP_KEYs, D.APP_CODE and D.APP_I_DATA**.
T.UNAUTHORIZED-IDENTITY-MNG	Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, **D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA, D.PK.EIM.ECDSA (SGP.32)**.
T.IDENTITY-INTERCEPTION	Directly threatens the assets: D.SECRETS, D.EID, **D.APP_C_DATA, D.PIN and D.APP_KEYs**.
T.UNAUTHORIZED-eUICC	
T.LPAd-INTERFACE-EXPLOIT	Refinement: For this TOE, the SGP.22 and LPAd functionalities referenced by this threat are excluded from the scope of evaluation. The threat is retained only for the relevant interfaces applicable to the IoT architecture supported by this TOE. Therefore, references to LPAd functionality shall be understood as not applicable to this TOE.

T.UNAUTHORIZED-MOBILE-ACCESS	
T.LOGICAL-ATTACK	Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, **D.JCS_CODE, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYS, D.OS-UPDATE_KEY(S) and D.APP_C_DATA**.
T.PHYSICAL-ATTACK	All assets
T.CONFID-UPDATE-IMAGE.LOAD	Confidentiality of Update Image –Load: The attacker discloses (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the eUICC for installation. See SA.CONFID-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, **D.JCS_CODE, D.JCS_DATA.**
T.INTEG-UPDATE-IMAGE.LOAD	Integrity of update Image –Load: The attacker modifies (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the card for installation. See SA.INTEG-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, **D.JCS_CODE, D.JCS_DATA.**
T.UNAUTH-UPDATE-IMAGE.LOAD	Load an unauthorized update. The attacker tries to upload an unauthorized update image. See SA.INTEG-UPDATEIMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, **D.JCS_CODE, D.JCS_DATA.**
T.INTERRUPT_OSU	OS Update procedure interrupted. The attacker tries to interrupt the OS update procedure (Load Phase through activation of Additional Code) leaving the TOE in a partially functional state.

	Directly threatened asset(s): D.TOE_IDENTIFIER, D.UPDATE_IMAGE.

Table 15 - Security Problem Definition threats

Security aspects added to cover OS update:

Security aspects	Description
SA.CONFID-UPDATE-IMAGE	Confidentiality of Update Image. The update image must be kept confidential. This concerns the non disclosure of the update image in the transit to the eUICC.
SA.INTEG-UPDATE-IMAGE	Integrity of Update Image. The update image must be protected against unauthorized modification. This concerns the modification of the image in transit to the eUICC.
T.PLATFORM-MNG-INTERCEPTION-IPAe	An attacker alters or eavesdrops the transmission between the SM-DP+, SM-DS and eIM and the IPAe on respective interfaces ES9+, ES11 and ESipa, in order to compromise the platform management process: • the delivery and the binding of a Profile Package for the eUICC; • or, the event retrieval process between the IPAe and an SM-DS (Alternative SM-DS or Root SM-DS). • or, the retrieval of profiles from the eIM, • or, delivery of Notifications. NOTE: the attacker may be an on-card application intercepting transmissions to the IPAe, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device. Directly threatened assets: D.IPAe_KEYS.
T.UNAUTHORIZED-PLATFORM-MNG-IPAe	An on-card application: • modifies or discloses IPAe data; • executes or modifies operations from IPAe. In particular, the following cases 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 Card objects • exploitation of the APDU buffer and global byte array Directly threatens the assets: D.IPAe_TSF_CODE.
T.PROFILE-MNG-ELIGIBILITY-IPAe	An attacker alters the Device Information when provided from the IPAe to the eUICC, in order to compromise the eligibility of the eUICC, for example: • obtain an unauthorized profile by modifying the Device Info. NOTE: the attacker may be an on-card application intercepting transmissions to the security domains. Directly threatens the assets: D.IPAe_TSF_CODE, D.IPAe_DEVICE_INFO.
T.LOGICAL-ATTACK-IPAe	An on-card malicious application bypasses the Platform security measures by logical means, in order to disclose or modify sensitive data when they are processed by the IPAe. An example of such a threat would consist of using buffer overflows to access confidential data manipulated by native libraries. This threat also includes cases of unauthorized code execution by applications. Directly threatens the asset: D.IPAe_TSF_CODE, D.IPAe_DEVICE_INFO, D.IPAe_IPAe_KEYS.
T.PHYSICAL-ATTACK-IPAe	An off-card actor discloses or modifies the design of the IPAe, its sensitive data or application code by physical (as opposed to logical) tampering means. This threat includes environmental stress, IC failure analysis, electrical probing, unexpected tearing, and side channels. That also includes the modification of the TOE runtime execution through alteration of the intended execution order of (set of) instructions through physical tampering techniques. The off-card actor has high attack potential. The off-card actor may be any actor using the external interfaces of the eUICC, whether they are intended to be used or not. Directly threatens the assets: D.IPAe_TSF_CODE, D.IPAe_DEVICE_INFO, D.IPAe_IPAe_KEYS.

Table 16 - Security Problem Definition security aspects

4.4 Organizational Security Policies

The TOE complies with all Organizational Security Policies defined in [PP-eUICC] and [PP-JCS].

The definition of Organizational Security Policies from [PP-eUICC] and [PP-JCS] are available in the table below. The complete list of Organizational Security Policies is available in previous sections.

OSPs	Refined/Added assets description

OSP.LIFE-CYCLE	From [PP-eUICC].
	
	The TOE must enforce the eUICC life-cycle defined in SGP.22.
	
	- There is a limit on the number of ISD-Ps enabled at a time:
	  o if the eUICC supports MEP, the limit is greater than one
	  o otherwise, the limit is one
	- The eUICC must enforce the profile policy rules (PPR) in case a profile state change is attempted (installation, disabling or deletion of a profile), except during the memory reset or test memory reset functions: in this case, the eUICC may disable and delete the currently enabled profile, even if a PPR states that the profile cannot be disabled or deleted;
	- The eUICC must enforce the rules authorisation table (RAT) before a profile containing PPRs is authorized to be installed on the eUICC.

OSP.VERIFICATION	From [PP-JCS]. The TOE shall ensure the consistency between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed in between its verification and the signing by the verification authority. See #.VERIFICATION for details. If the application development guidance provided by the platform developer contains recommendations related to the isolation property of the platform, this policy shall also ensure that the verification authority checks that these recommendations are applied in the application code.

Table 17 - Security Problem Definition OSPs

4.5 Assumptions

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

The definition of assumptions from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated in this section. Additionally, the assumption A.Process-Sec-IC is defined as in section 3.4 of [PP-0084].

The complete list of Assumptions is available in previous sections.

Assumptions
A.TRUSTED-PATHS-LPAd-IPAd. Refinement: For this TOE, the SGP.22 and LPAd parts of this assumption are excluded from the scope of evaluation. The assumption is retained only for the trusted paths applicable to the IoT architecture supported by this TOE. Therefore, references to LPAd functionality shall be understood as not applicable to this TOE.
A.ACTORS
A.APPLICATIONS
A.ACTORS-IPAe
A.CAP_FILE
A.VERIFICATION
A.Process-Sec-IC

Table 18 - Security Problem Definition assumptions

5. Security Objectives

This section introduces the Security Objectives for the TOE.

5.1 Security Objectives for the TOE

All the Security Objectives defined in the [PP-eUICC] are included in this Security Target, including the objectives related to OS Update PP-module.

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] where no refinements are made are not repeated here. The complete list of the Security Objectives for the TOE is available in previous sections.

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

O.TOE	Refined/Added assets description
O.PRE-PPI	
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
O.IC.PROOF_OF_IDENTITY	The IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The embedded software in the IC must support the following functionalities: (1) Prevent unauthorized bypass or alteration of TSFs and restrict access to low-level functions to those provided by the

	API packages. Protect private data and code from disclosure or modification. (2) Provide secure low-level cryptographic processing to the Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PRE, S.PPI, and S.TELECOM). (3) Allow the Profile Policy Enabler (S.PRE), Profile Package Interpreter (S.PPI), and Telecom Framework (S.TELECOM) to store data in persistent technology memory or volatile memory, as needed. The memory model should be structured and allow for low-level control accesses (segmentation fault detection). (4) Provide a mechanism for atomic memory operations for the Profile Policy Enabler (S.PRE), Profile Package Interpreter (S.PPI), and Telecom Framework (S.TELECOM).
O.IC.RECOVERY	In the event of a power outage during an operation, the IC must enable the TOE to successfully complete the interrupted operation or recover to a consistent and secure state.
O.RE.PRE-PPI	The Runtime Environment shall provide secure means for card management activities, including: - Load of a package file. - Installation of a package file. - Extradition of a package file or an application. - Personalization of an application or a Security Domain. - Deletion of a package file or an application. - Privileges update of an application or a Security Domain. - Access to an application outside of its expected availability.
O.RE.SECURE-COMM	The Runtime Environment must provide mechanisms to protect the confidentiality and integrity of application communications.
O.RE.API	The Runtime Environment must ensure that native code can only be invoked through an API.

O.RE.DATA-CONFIDENTIALITY	The Runtime Environment must ensure the confidentiality of all sensitive TOE data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment must ensure the integrity of all sensitive TOE data it processes.
O.RE.IDENTITY	The Runtime Environment must ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.
O.SECURE_LOAD_ACODE	The Loader of the Initial TOE must verify the authenticity and integrity of the loaded Additional Code. Only the allowed version of the Additional Code can be loaded onto the Initial TOE. The Loader must prevent the loading of Additional Code that is not intended for assembly with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure.
O.SECURE_AC_ACTIVATION	The activation of the Additional Code and the update of the Identification Data must be performed simultaneously in an atomic operation. All necessary operations for the code to function as in the Final TOE must be completed before activation. If the Atomic Activation is successful, the resulting product is the Final TOE. Otherwise, in case of interruption or an incident that prevents the formation of the Final TOE (such as tearing, integrity violation, or an error), the Initial TOE must remain in its initial state or fail securely.
O.TOE_IDENTIFICATION	The Identification Data uniquely identifies the Initial TOE and Additional Code. The TOE stores Identification Data in its non-volatile memory and ensures its integrity.

	After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows the identification of the Initial TOE and Additional Code. Users can uniquely identify the Initial TOE and Additional Code(s) embedded in the Final TOE.
O.CONFID-UPDATE-IMAGE.LOAD	The TOE shall ensure that the D.UPDATE_IMAGE transferred to the device is not disclosed during the installation.
O.AUTH-LOAD-UPDATE-IMAGE	The TOE shall ensure that it is only possible to load an authorized image.
O.LOAD	
O.SECURE-CHANNELS-IPAe	The TOE shall maintain secure channels between: • IPAe and SM-DP+. • IPAe and SM-DS. • IPAe and eIM. The TOE shall ensure at any time: • that incoming messages are properly provided unaltered to the IPAe; • that any response messages are properly returned to the off-card entity. Communications shall be protected from unauthorized disclosure, modification and replay. This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment and the PRE/PPI (see O.PRE-PPI).
O.INTERNAL-SECURE-CHANNELS-IPAe	The TOE ensures that the communication shared secrets transmitted from the ECASD to the IPAe are protected from unauthorized disclosure or modification. This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment.

O.DATA-CONFIDENTIALITY-IPAe	The TOE shall avoid unauthorised disclosure of the secret keys which are part of the keyset D.IPAe_KEYS.
O.DATA-INTEGRITY-IPAe	The TOE shall avoid unauthorised modification of the following data when managed or manipulated by the TOE.

Table 19 - Security Objects for the TOE

5.2 Security Objectives for the operational environment

The complete list of Security Objectives for the Operational Environment of this TOE is available in previous sections of this Security Target.

The list and definitions of the Security Objectives for the Operational Environment from [PP-eUICC] and [PP-JCS] where no refinements are made are not repeated in this section.

Additionally, OE.Process-Sec-IC is defined in the same way as in section 4.3 of [PP-0084], as it is required to ensure protection during the composite product manufacturing, specifically up to the Phase 6, as well as during the delivery to Phase 7 (phases stated in [PP-0084]).

O.ENV	Refined/Added assets description
OE.CI	
OE.SM-DP+	
OE.EIM	
OE.MNO	
OE.TRUSTED-PATHS-LPAd-IPAd	The operational environment shall provide and protect trusted communication paths between the LPAd and IPAd (including the relevant local interface as specified by the applicable GSMA specifications) such that endpoints are authenticated and communications are protected against disclosure, modification, replay, and spoofing.
OE.APPLICATIONS	
OE.CAP_FILE	

OE.VERIFICATION	
OE.CODE-EVIDENCE	
OE.MNO-SD	
OE.CONFID_UPDATE_IMAGE.CREATE	Confidentiality of Update Image – CREATE. The off-card Update Image Creator guarantees that confidentiality and integrity requirements are met.
OE.Process-Sec-IC	

Table 20 - Security Objectives for the operational environment

5.3 Security Objectives Rationale

5.3.1 Threats

5.3.1.1 Unauthorized Profile and Platform management

T.UNAUTHORIZED-PROFILE-MNG:

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

- O.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-CHANNEL 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 communication (O.RE.SECURE-COMM).

Since the MNO-SD Security Domain is not part of the TOE, the operational environment must guarantee that it will use securely SCP80/81 secure channel provided by the TOE (OE.MNO-SD). 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.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 Domain 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 or compliance to security guidelines for applications (OE.APPLICATIONS).

T.PROFILE-MNG-INTERCEPTION

Commands and profiles are transmitted by the SM-DP+ to its on-card representative (ISD-P), while profile data (including meta-data such as PPRs) is also transmitted by the MNO OTA Platform to its on-card representative (MNO-SD) by means of RPM requests from Profile owner to ISD-R (UpdateMetadataRequest), or by means of PSMO commands from eIM to ISD-R (SGP.32).

Consequently, the TSF ensures:

- Security of the transmission to the Security Domain (O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS) by requiring authentication from SM-DP+ and MNO OTA Platforms, and protecting the transmission from unauthorized disclosure, modification or 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 user 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-cards actors.OE.SM-DP+

T.PROFILE-MNG-ELIGIBILITY

Device Info and eUICCInfo2 transmitted by the eUICC to the SM-DP+ are used by the SM-DP+ to perform 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).

O.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 eUICCIndo2 is protected at the eUICC level.

T.PLATFORM-MNG-INTERCEPTION-IPAe

The SM-DP+ transmits Profiles (Bound Profile Packages) to the IPAe, the SM-DS transmits Events to the IPAe.
Consequently, the TSF ensures:

- Security of the transmission to the IPAe (O.SECURE-CHANNELS-IPAe and O.INTERNAL-SECURE-CHANNELS-IPAe) 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-IPAe

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-IPAe

Device Info, transmitted by the IPAe 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 IPAe and other security domains of the TOE (O.INTERNAL-SECURE-CHANNELS-IPAe) 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-IPAe 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.UNATHORIZED-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 others 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 applications communications (O.RE.SECURE-COMM).

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

5.3.1.3 eUICC cloning

T.UNATHORIZED-eUICC

O.PROOF_OF_IDENTITY guarantees that the off-card actor can be provided with 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 are trusted paths to the LPAd/IPA.

5.3.1.5 Unauthorized access to the mobile network

T.UNATHORIZED-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 PRE, PPI, the Telecom Framework or any native/OS part of the TOE As such is covered:

- by the APIs provided by the Runtime Environment (O.RE.API);
- by the APIs of the TSF (O.API); the APIs of the Telecom Framework, PRE and PPI shall ensure atomic transactions (O.IC.SUPPORT).

Whenever sensitive data of the TOE are processed by applications, confidentiality and integrity must be always protected by the Runtime Environment (O.RE.DATA-CONFIDENTIALITY and 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 PRE, PPI and Telecom Framework (O.OPERATE);
- PRE, PPI and Telecom Framework must protect the confidentiality and integrity of the sensitive data they process (O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY).

This threat is covered by:

- Prevention of unauthorized code execution by applications (O.RE.CODE-EXE).

The following objectives for the operational environment are also required:

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

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 channel (O.DATA-CONFIDENTIALITY). For the same season, the Runtime Environment (to which Java Card System can be an implementation) security architecture must cover side channels (O.RE.DATA-CONFIDENTIALITY).

T.LOGICAL-ATTACK-IPAe

This threat is covered by controlling the information flow between the IPAe 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 IPAe shall ensure atomic transactions (O.IC.SUPPORT).

Whenever sensitive data of the TOE are processed by IPAe, 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).

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). For the same reason, the Runtime Environment (to which Java Card System can be an implementation) security architecture must cover side channels (O.RE.DATA-CONFIDENTIALITY).

5.3.1.7 eUICC OS Update capability

T.CONFID-UPDATE-IMAGE.LOAD

O.CONFID-UPDATE-IMAGE.LOAD ensures the confidentiality of D.UPDATE_IMAGE during installing it on the TOE.

OE.CONFID_UPDATE_IMAGE.CREATE ensures that the D.UPDATE_IMAGE is not transferred in plain and that the keys are kept secret.

T.INTEG-UPDATE-IMAGE.LOAD

O.SECURE_LOAD_ACODE ensures the authenticity and integrity of D.UPDATE_IMAGE.

T.UNAUTH-UPDATE-IMAGE.LOAD

O.SECURE_LOAD_ACODE ensures that only authorized (allowed version) images can be installed.

O.AUTH-LOAD-UPDATE-IMAGE ensures that only authorized (allowed version) images can be loaded.

T.INTERRUPT_OSU

O.SECURE_LOAD_ACODE ensures that the TOE remains in a secure state after interrupt of the OS Update procedure (Load phase).

O.TOE_IDENTIFICATION ensures that D.TOE_IDENTIFIER is only updated after successful OS Update procedure.

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

5.3.2 Organizational Security Policies

OSP.LIFE-CYCLE

O.PRE-PPI ensures that there is a single ISD-P enabled at a time if the eUICC supports only SEP (Single Enabled Profile). The profile deletion capability relies on the secure application deletion mechanisms provided by O.RE.PRE-PPI.

O.OPERATE contributes to this OSP by ensuring that the Platform security functions are always enforced.

OSP.VERIFICATION

It is upheld by the security objective of the environment OE.VERIFICATION which guarantees that all the bytecode shall be verified at least once, before the loading, before the installation or before the execution in order to ensure that each bytecode is valid at execution time.

This policy is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that evidences exist that the application code has been verified and not changed after certification, and by the security objective for the TOE O.LOAD which shall ensure that the loading of CAP file into the card is safe.

5.3.3 Assumptions

A.TRUSTED-PATHS-LPAd-IPAd

This assumption is upheld by OE.TRUSTED-PATHS-LPAd-IPAd.

A.ACTORS

This assumption is upheld by objectives OE.CI, OE.SM-DP+, OE.MNO, OE.SM-DS and OE.EIM (SGP.32) which ensure that credentials and otherwise sensitive data will be managed correctly by each actor of the infrastructure.

A.APPLICATIONS

This assumption is directly upheld by objective OE.APPLICATIONS.

A.CAP_FILE

This assumption is upheld by the security objective for the operational environment OE.CAP_FILE which ensures that no CAP file loaded port-issuance shall contain native methods.

A.VERIFICATION

This assumption is upheld by the security objective on the operational environment OE.VERIFICATION which guarantees that all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution in order to ensure that each byte code is valid in execution time.

This assumption is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that evidences exist that the application code has been verified and not changed after verification.

The assumption A.Process-Sec-IC is defined as in Section 3.4 of [PP-0084].

A.ACTORS-IPAe

This assumption is upheld by objective OE.SM-DS, OE.SM-DP+ and OE.EIM which ensures that credentials and otherwise sensitive data will be managed correctly by this actor of the infrastructure.

5.3.4 Rationale Tables

5.3.4.1 Threats and Security Objectives 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 O.INTERNAL-SECURE-CHANNELS O.RE.SECURE-COMM O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY OE.MNO-SD	Section 5.3.1.1
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS O.PRE-PPI OE.APPLICATIONS O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY OE.SM-DP+ OE.EIM (SGP.32)	Section 5.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+ OE.MNO O.SECURE-CHANNELS O.INTERNAL-SECURE-CHANNELS O.RE.SECURE-COMM OE.MNO-SD OE.EIM (SGP.32)	Section 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+ O.RE.SECURE-COMM O.SECURE-CHANNELS O.INTERNAL-SECURE-CHANNELS O.RE.DATA-INTEGRITY	Section 5.3.1.1

	O.DATA-INTEGRITY	
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS O.PRE-PPI O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY O.RE.IDENTITY	Section 5.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI O.INTERNAL-SECURE-CHANNELS O.RE.SECURE-COMM	Section 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY O.IC.PROOF_OF_IDENTITY	Section 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 5.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY O.DATA-INTEGRITY O.API OE.APPLICATIONS O.OPERATE O.RE.API O.RE.CODE-EXE O.IC.SUPPORT O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY	Section 5.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT O.IC.RECOVERY O.DATA-CONFIDENTIALITY O.RE.DATA-CONFIDENTIALITY	Section 5.3.1.6
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATEIMAGE.LOAD OE.CONFID_UPDATE_IMAGE.CREATE	Section 5.3.1.7
T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE	Section 5.3.1.7
T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE O.AUTH-LOAD-UPDATE-IMAGE	Section 5.3.1.7

T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE O.TOE_IDENTIFICATION O.SECURE_AC_ACTIVATION	section 5.3.1.7
T.PLATFORM-MNG- INTERCEPTION-IPAe	O.RE.SECURE-COMM OE.SM-DS O.SECURE-CHANNELS-IPAe O.INTERNAL-SECURE-CHANNELS-IPAe	Section 5.3.1.1
T.UNAUTHORIZED-PLATFORM-MNG-IPAe	OE.APPLICATIONS O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY	Section 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY-IPAe	O.RE.SECURE-COMM O.INTERNAL-SECURE-CHANNELS-IPAe O.DATA-INTEGRITY-IPAe OE.SM-DP+ O.RE.DATA-INTEGRITY	Section 5.3.1.1
T.LOGICAL-ATTACK-IPAe	O.OPERATE O.API O.RE.API O.RE.CODE-EXE OE.APPLICATIONS O.DATA-CONFIDENTIALITY-IPAe O.DATA-INTEGRITY-IPAe O.IC.SUPPORT O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY	Section 5.3.1.6
T.PHYSICAL-ATTACK-IPAe	O.DATA-CONFIDENTIALITY-IPAe, O.IC.SUPPORT, O.IC.RECOVERY, O.RE.DATA-CONFIDENTIALITY	Section 5.3.1.6

Table 21 - Threats and Security Objectives - Coverage

5.3.4.2 Organizational Security Policies Rationale

Organizational Security Rationale	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PRE-PPI O.RE.PRE-PPI	Section 5.3.2

	O.OPERATE	
OSP.VERIFICATION	OE.VERIFICATION O.LOAD OE.CODE-EVIDENCE	Section 5.3.2

Table 22 - Organizational Security Policies and Security Objectives coverage

5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.3
A.ACTORS	OE.CI OE.SM-DP+ OE.MNO OE.EIM (SGP.32) OE.SM-DS	Section 5.3.3
A.APPLICATIONS	OE.APPLICATIONS	Section 5.3.3
A.VERIFICATION	OE.VERIFICATION OE.CODE-EVIDENCE	Section 5.3.3
A.CAP_FILE	OE.CAP_FILE	Section 5.3.3
A.Process-Sec-IC	OE.Process-Sec-IC	Section 5.3.3
A.ACTORS-IPAe	OE.SM-DS OE.SM-DP+ OE.EIM	Section 9.5.3

Table 23 - Assumptions and Security Objectives for the Operation Environment coverage

6. Extended Components Definition

The extended component definition for FAU_SAS.1 [PP 0084] (section 5.3) has been taken with no modification.

7. Security Requirements

The following SFRs are relevant for this TOE.

SFR	Included in this ST
[PP-eUICC] SFRs	All SFRs.
[PP-JCS] SFRs	All SFRs listed in section 3.4.4.1 from [PP-JCS].
[PP-GP] SFRs	The GlobalPlatform-related SFRs claimed by this ST are those instantiated in this document (see section 7.2.7 and OS Update sections). The [PP-GP] components FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FIA_UID.1/GP, FMT_MSA.1/GP and FPT_RCV.3/GP are not claimed as separate SFRs because their security functionality is already covered by SFRs claimed in this ST (see section 7.3.2).
[PP-0084] SFRs	FAU_SAS.1.
[CC-2] SFRs	FPT_RCV.3/OS, FPT_RCV.4.

Table 24 - SFRs of the TOE of this Security Target

7.1 eUICC Security Functional Requirements

The TOE of this Security Target includes all SFRs contained in sections 6.1 and 9.7.1 of [PP-eUICC] for the eUICC component in compliance with the Security Problem Definition state in the [PP-eUICC]. The introduction and security attribute definitions from sections 6.1 and 9.7.1 of [PP-eUICC] are not repeated here.

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

- Selections and assignments previously made in [PP-eUICC], [PP-JCS], or [PP-GP] are in **bold**, and the original test is not referenced.
- Selections and assignments made in this ST are in *italics*.
- ~~Text~~ means item (e.g. CARD_LOCKED and CARD_TERMINATE states) not applicable to eUICC.
- Refinements are in *italics*.

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:** *none*]

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

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

Application note:

- This SFR is related to the identification of the following external (remote) users of the TOE:
  - U.SM-DP+;
  - U.MNO-OTA;
  - U.EIM (SGP.32).
- The identification of the only local user (U.MNO-SD) is addressed by the FIA_UID.1/MNO-SD SFR.
- Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote 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:** *none*]

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

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

Application note:

- This SFR is related to the authentication of the following external (remote) users of the TOE:
  - U.SM-DP+;
  - U.MNO-OTA;
  - U.EIM (SGP.32).
- As the cryptographic mechanisms used for the authentication may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFRs.
- The ST include FCS_COP.1 requirements stated by SGP.22:

- A U.SM-DP+ must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.Dpauth.ECDSA and CERT.DPpb.ECDSA), as well as the public key of the CI (D.PK.ECDSA).
- U.MNO-OTA must be authenticated using a SCP80 secure channel according to SCP80 protocol using the parameters defined in SGP.02, section 2.4.3, or optionally SCP81 according to SCP81 protocol using the parameters defined in SGP.02 section 2.4.4 (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO).
- U.EIM must be authenticated by verifying its ECDSA signature using the public key PK.EIM.ECDSA included in its certificate (CERT.EIM.ECDSA).

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with at least one of the elliptic curves referenced for that purpose in SGP.22 and/or SGP.32.

FIA_USB.1/EXT User-Subject binding

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

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

FIA_USB.1.2/EXT The TSF shall enforce the following rules on the initial association of the 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).***]**

Application note:

- This SFR is related to the binding of external (remote) users to local subjects or users of the TOE:
  - U.SM-DP+ binds to a subject (S.ISD-R);
  - U.SM-DS binds to a subject (S.ISD-R);
  - U.MNO-OTA binds to an on-card user (U.MNO-SD);
  - U.EIM binds to a subject (S.ISD-R).
- This SFR is related to the following commands:
  - Initial association of the D.MNO_KEYS keyset is performed by the ES8+.ConfigureISDP command.

FIA_UAU.4/EXT Single-use authentication mechanism

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)***]**

Application note:

- This SFR is related to the authentication of external (remote) users of the TOE:
  - U.SM-DP+;
  - U.MNO-OTA;

FIA_UID.1/MNO-SD Timing of identification

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

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

Application note:

- This SFR is related to the identification of the local user U.MNO-SD only. The identification of remote users is addressed by the FIA_UID.1/EXT SFR.
- It should be noted that the U.MNO-SD is identified but not authenticated. However, U.MNO-SD is installed on the TOE by the U.SM-DP+ via the subject S.ISD-R (see FDP_ACF.1/ISDR), and the binding between U.SM-DP+ and S.ISD-R requires authentication of U.SM-DP+, as described in FIA_USB.1/EXT.

FIA_USB.1/MNO-SD User-Subject binding

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

- **The AID is associated to the S.ISD-P acting on behalf of U.MNO-SD.**

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

- **Initial association of AID requires U.SM-DP+ to be authenticated via CERT.DPauth.ECDSA.**

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

- **No change of AID is allowed.**

Application note:

- This SFR is related to the identification of the local user U.MNO-SD.
- Being a local but external user of the TOE, the U.MNO-SD is bound to the S.ISD-R which is responsible for its installation during the "Profile download and install". This profile installation is controlled by the ISD-R content access control SFP (see FDP_ACC.1/ISDR). Being performed by the S.ISD-R, it requires authentication of the U.SM-DP+.
- In order to perform operations such as PPR update, U.MNO-OTA authenticates, then sends a command to U.MNO-SD, which transmits it to S.ISD-P.
- The identification does not depend on direct authentication of the MNO OTA Platform, but on the authentication of the S.ISD-R: The S.ISD-R installs a profile which includes a U.MNO-SD and associated keyset.

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

FIA_API.1.1 The TSF shall provide a **cryptographic authentication mechanism based on the EID of the eUICC** to prove the identity of the **TOE** by including the following properties **the EID value in the eUICC certificate** to an external entity.

Application note:

- This proof is obtained by including the EID value in the eUICC certificate, which is signed by the eUICC Manufacturer.

FIA_UID.1/IPAe Timing of identification

FIA_UID.1.1/IPAe The TSF shall allow

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

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

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

Application Note 75:

This SFR is related to the identification of the following external (remote) user of the TOE:

- U.SM-DP+
- U.SM-DS
- U.EIM

Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user.

FIA_UAU.1/IPAe Timing of authentication

FIA_UAU.1.1/IPAe The TSF shall allow

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

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

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

Application Note 76:

This SFR is related to the authentication of the following external (remote) user of the TOE:

- U.SM-DP+
- U.SM-DS
- U.EIM
- A U.SM-DP+ must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.DPauth.ECDSA, CERT.DPpb.ECDSA and CERT.DP.TLS), as well as the public key of the CI (D.PK.CI.ECDSA).
- A U.SM-DS must be authenticated by verifying its ECDSA signature, using the public keys included in its certificates (CERT.DSauth.ECDSA and CERT.DS.TLS), as well as the public key of the eSIM CA (D.PK.CI.ECDSA).A U.EIM must be authenticated by verifying its ECDSA signature, using the public keys included in its certificates (CERT.EIM.ECDSA, and CERT.EIM.TLS).

FIA_USB.1/IPAe User-subject binding

FIA_USB.1.1/IPAe 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.IPAe, acting on behalf of U.SM-DP+**
- **SM-DS OID is associated to S.IPAe, acting on behalf of U.SM-DS.**
- **eIM ID is associated to S.IPAe, acting on behalf of U.EIM.**

FIA_USB.1.2/IPAe 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 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".**
- **Initial association of eIM ID requires U.EIM to be authenticated via "CERT.EIM.ECDSA".**

FIA_USB.1.3/IPAe

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 SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA".**
- **change of EIM ID requires U.EIM to be authenticated via "CERT.EIM.ECDSA".**

Application Note 77:

This SFR is related to the binding of external (remote) users to local subjects or users of the TOE:

- U.SM-DP+ binds to a subject (S.IPAe)
- U.SM-DS binds to a subject (S.IPAe)
- U.EIM binds to a subject (S.IPAe)

FIA_UAU.4/IPAe Single-use authentication mechanisms

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

- **U.SM-DP+**
- **U.SM-DS**
- **U.EIM**

Application Note 78:

This SFR is related to the authentication of external (remote) users of the TOE:

- U.SM-DP+
- U.SM-DS
- U.EIM

FIA_ATD.1/IPAe User attribute definition

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

- **CERT.DP.TLS belonging to U.SM-DP+,**
- **CERT.DS.TLS belonging to U.SM- DS,**
- **CERT.EIM.TLS belonging to U.EIM.**

7.1.2 Communication

FDP_IFC.1/SCP Subset information flow control

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

- **Users/subjects/objects:**
  - **U.SM-DP+ and SO.ISD-R, SO.ISD-P**
  - **U.MNO-OTA and U.MNO-SD**
- **Information: transmission of commands**.

FDP_IFF.1/SCP Simple security attributes

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

- **Users/subjects/objects:**
  - **U.SM-DP+, SO.ISD-P and SO.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.MNO-SD in a SCP80 or SCP81 secure channel.**

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

FDP_IFF.1.4/SCP The TSF shall explicitly 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.**

Application note:

- More details on the secure channels can be found in SGP.22:
  - For SM-DP+: Section 5.5
  - For MNO-SD: Section 5.4

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 communications 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 a communication via the trusted channel.

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

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

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

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

- *ES10b.SetDefaultDpAddress (SGP.32)*
- *ES10b.PrepareDownload*
- *ES10b.LoadBoundProfilePackage*
- *ES10b.GetEUICCChallenge*
- *ES10b.GetEUICCInfo*
- *ES10b.ListNotification*
- *ES10b.RetrieveNotificationsList*
- *ES10b.RemoveNotificationFromList*
- *ES10b.AuthenticateServer*
- *ES10b.CancelSession*
- *ES10b.LoadEuiccPackage (SGP.32)*
- *ES10b.AddInitialEim (SGP.32)*
- *ES10b.GetCerts (SGP.32)*
- *ES10b.ImmediateEnable (SGP.32)*
- *ES10b.ProfileRollback (SGP.32)*
- *ES10b.ConfigureImmediateProfileEnabling (SGP.32)*
- *ES10b.GetEimConfigurationData (SGP.32)*
- *ES10b.GetProfilesInfo (SGP.32)*
- *ES10b.GetEID (SGP.32)*

- *ES10b.GetRAT*

The TSF may permit the IPAd to transmit the following operation:

- *ES10b.eUICCMemoryReset (SGP.32)*
- *ES10b.ExecuteFallbackMechanism (SGP.32)*
- *ES10b.ReturnFromFallback (SGP.32)*
- *ES10b.EnableEmergencyProfile (SGP.32)*
- *ES10b.DisableEmergencyProfile (SGP.32)*
- *ES10b.GetConnectivityParameters (SGP.32)*

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

- *ES6.UpdateMetadata.*

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

FDP_ITC.2.1/SCP The TSF shall enforce the **Secure Channel Protocol Information flow control SFP** when import 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.

Application note:

- The commands related to the SFRs FPT_TDC.1/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP and the Downloaded objects related to this SFR FPT_TDC.1/SCP are listed below:
    - SM-DP+ commands:
        - ES8+.InitialiseSecureChannel
        - ES8+.ConfigureISDP
        - ES8+.StoreMetadata
        - ES8+.ReplaceSessionKeys
        - ES8+.LoadProfileElements.
    - IPAd commands:
        - *ES10b.SetDefaultDpAddress (SGP.32)*
        - *ES10b.PrepareDownload*
        - *ES10b.LoadBoundProfilePackage*
        - *ES10b.GetEUICCChallenge*
        - *ES10b.GetEUICCInfo*
        - *ES10b.ListNotification*
        - *ES10b.RetrieveNotificationsList*
        - *ES10b.RemoveNotificationFromList*
        - *ES10b.AuthenticateServer*
        - *ES10b.CancelSession*
        - *ES10b.LoadEuiccPackage (SGP.32)*
        - *ES10b.AddInitialEim (SGP.32)*
        - *ES10b.GetCerts (SGP.32)*
        - *ES10b.ImmediateEnable (SGP.32)*
        - *ES10b.ProfileRollback (SGP.32)*
        - *ES10b.ConfigureImmediateProfileEnabling (SGP.32)*
        - *ES10b.GetEimConfigurationData (SGP.32)*
        - *ES10b.GetProfilesInfo (SGP.32)*
        - *ES10b.GetEID (SGP.32)*
        - *ES10b.GetRAT*
        - *ES10b.eUICCMemoryReset (SGP.32)*
        - *ES10b.ExecuteFallbackMechanism (SGP.32)*
        - *ES10b.ReturnFromFallback (SGP.32)*

- *ES10b.EnableEmergencyProfile (SGP.32)*
- *ES10b.DisableEmergencyProfile (SGP.32)*
- *ES10b.GetConnectivityParameters (SGP.32)*

- Download objects from SM-DP+:
  - Session keys
  - Profile Metadata (including PPR data)
- MNO commands
  - ES6.UpdateMetadata
- Download objects from MNO OTA Platform
  - Profile Metadata (including PPR data and Enterprise Rules (optional)).

FDP_UCT.1/SCP Basic data exchange confidentiality

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

Application note:

- This SFR is related to the protection of:
  - Profiles downloaded from SM-DP+.
- Cryptographic mechanisms used for the trusted channel are provided by the underlying Platform.
- Related keys are:
  - Either generated on-card (D.SECRETS): see FCS_CKM.1/SCP-SM for further details
  - Distributed along with the Profile (D.MNO_KEYS): see FCS_CKM.2/SCP-MNO for further details.

FDP_UIT.1/SCP Data exchange integrity

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

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

Application note:

- This SFR is related to the protection of:
  - Profiles downloaded from SM-DP+;
  - Commands received from SM-DP+ and MNO OTA Platform;
  - PPR received from MNO OTA Platform.
- Related keys are:

- Either generated on-card (D.SECRETS): see FCS_CKM.1/SCP-SM for further details
- Distributed along with the Profile (D.MNO_KEYS): see FCS_CKM.2/SCP-MNO for further details.

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, BrainpoolP256r1*]

Application note:

- This key generation mechanism is used to generate:
  - D.SECRETS keyset via the ES8+.InitialiseSecureChannel command, using the U.SM-DP+ public key otPK.DP.ECKA.
- The Elliptic Curve cryptographic mechanisms used for the key agreement are provided by the underlying Platform.

FCS_CKM.2/SCP-MNO Cryptographic key distribution

FCS_CKM.2.1/SCP-MNO The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *distribution method from SCP-SGP22 (SCP03t)*] that meets the following: [assignment: *SGP.32 standard*].

Application note:

- This SFR is related to the distribution of:
  - D.MNO_KEYS during profile download.
- Note: This SFR does not apply to the private keys loaded pre-issuance of the TOE (D.SK.EUICC.ECDSA).

FCS_CKM.6/SCP-SM Cryptographic key destruction

FCS_CKM.6.1/SCP-SM The TSF shall destroy **D.SECRETS, CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DSauth.ECDSA, D.CERT.EUICC.ECDSA, D.SK.EUICC.ECDSA, D.PK.CI.ECDSA** 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: *wipe the buffer with random bytes*] 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-MNO in accordance with a specified cryptographic key destruction method [assignment: *invalidating memory containing the key in masked value*] that meets the following:

- [assignment: *none*].

Application note:

- This SFR is related to the destruction of the following keys:
  - D.MNO_KEYS.

FDP_IFC.1/IPAe Subset information flow control

FDP_IFC.1.1/IPAe The TSF shall enforce the **IPAe information flow control SFP** on

- **users/subjects:**
  - **U.SM-DP+ and S.IPAe**
  - **U.SM-DS and S.IPAe**
  - **U.EIM and S.IPAe**
- **information: transmission of commands.**

FDP_IFF.1/IPAe Simple security attributes

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

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

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

[assignment:

- *The IPA SHALL communicate with the SM-DP+ secured by HTTPS in server authentication mode with TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (ES9+),*
- *The IPA SHALL communicate with the SM-DS secured by TLS in server authentication mode with the Protocol for Profile Protection signatures based on ECDSA (ES11),*
- *The IPA SHALL communicate with the eIM secured by TLS/DTLS in server authentication mode with the Protocol for Profile Protection signatures based on ECDSA (ESipa).***]**

FDP_IFF.1.3/IPAe The TSF shall not enforce the **[assignment:** *none***]**.

FDP_IFF.1.4/IPAe The TSF shall explicitly authorise an information flow based on the following rules: **[assignment:** *rules defined in section 3.2 of SGP.32 [36] and 3.2.1 of SGP.22 [24].*]

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

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

Application Note 79:

More details on the secure channels can be found in the following sections of SGP.32 [36]:

- For SM-DP+: Section 5.6
- For SM-DS: Section 5.10
- For eIM: Section 5.14

FTP_ITC.1/IPAe Inter-TSF trusted channel

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

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

[assignment:

- *ES9+.InitiateAuthentication*
- *ES9+.GetBoundProfilePackage*
- *ES9+.AuthenticateClient*
- *ES9+.HandeNotification*
- *ES9+.CancelSession*
- *ESipa.InitiateAuthentication*
- *ESipa.GetBoundProfilePackage*
- *ESipa.AuthenticateClient*
- *ESipa.HandleNotification*
- *ESipa.CancelSession*
- *ESipa.GetEimPackage*
- *ESipa.ProvideEimPackageResult*]

Application Note 80:

- The secure channels from the IPAe to eIM, SM-DP+ and SM-DS must be TLS with server authentication.

Related keys are generated on-card (D.IPAe_KEYS); see FCS_CKM.1/IPAe.

In terms of commands, the TSF shall permit remote actors to initiate communication via a trusted channel in the following cases:

- The TSF shall permit the IPAe 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 IPAe to open a TLS secure channel to SM-DS and transmit the following operations:
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient

- The TSF shall permite the IPAe 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.ProvideEimPackageResult

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

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

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

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

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

FPT_TDC.1.1/IPAe 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/IPAe The TSF shall use the rules defined in [GP-PP] [11] when interpreting the TSF data from another trusted IT product.

Application Note 81:

The commands related to the SFRs FPT_TDC.1/IPAe, FDP_IFC.1/IPAe, FDP_IFF.1/IPAe and the Downloaded objects related to this SFR FPT_TDC.1/IPAe are listed below:

- SM-DP+ commands

  - ES9+.InitiateAuthentication
  - ES9+.GetBoundProfilePackage
  - ES9+.AuthenticateClient
  - ES9+.HandeNotification
  - ES9+.CancelSession
  - ES9+.ConfirmDeviceChange
- eIM commands
  - ESipa.InitiateAuthentication
  - ESipa.GetBoundProfilePackage
  - ESipa.AuthenticateClient
  - ESipa.HandleNotification
  - ESipa.CancelSession
  - ESipa.GetEimPackage
  - ESipa.TransferEimPackage
  - ESipa.ProvideEimPackageResult
- Downloaded objects from SM-DP+ and eIM
  - Session keys
  - Bound Profile Package
- SM-DS commands
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient
  - ES11.CheckEvent

FDP_UCT.1/IPAe Basic data exchange confidentiality

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

Application Note 82:

This SFR is related to the protection of:

- Bound Profile Packages downloaded from SM-DP+ and eIM.

Confidentiality of communication must be addressed by the use of AES in CBC mode with a minimum key size of 128 bits.

Related keys are generated on-card (D.IPAe_KEYS); see FCS_CKM.1/IPAe for further details.

FDP_UIT.1/IPAe Data exchange integrity

FDP_UIT.1.1/IPAe The TSF shall enforce the **IPAe information flow control SFP** to receive user data in a manner protected from modification, deletion, insertion and replay errors.

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

Application Note 83:

This SFR is related to the protection of:

- Bound Profile Packages downloaded from SM-DP+ and eIM;
- Commands received from to SM-DP+, eIM and SM-DS.

Integrity of communication must be addressed by the use of AES in CMAC mode with a minimum key size of 128 bits and a MAC length of 64 bits.

Related keys are generated on-card (D.IPAe_KEYS); see FCS_CKM.1/IPAe for further details.

FCS_CKM.1/IPAe Cryptographic key generation

FCS_CKM.1.1/IPAe 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, BrainpoolP256r1.*]

Application Note 84:

This key generation mechanism is used to generate:

- D.IPAe_KEYS keys.

The Elliptic Curve cryptography used for this key agreement may be provided by the underlying Platform. Consequently this PP does not include the corresponding FCS_COP.1 SFR.

FCS_CKM.6/IPAe Cryptographic key destruction

FCS_CKM.6.1/IPAe The TSF shall destroy D.IPAe_KEYS when **[assignment:** *no longer needed*]**.**

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

7.1.3 Security Domains

FDP_ACC.1/ISDR Subset access control

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

- **Subjects: S.ISD-R**
- **Objects: SO.ISD-P**
- **Operations:**
  - **Create and configure profile**
  - **Store profile metadata**
  - **Enable profile**
  - **Disable profile**
  - **Delete profile**
  - **Perform a Memory reset**

FDP_ACF.1/ISDR Security attribute-based access control

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

- **Subjects: S.ISD-R**
- **Objects:**
  - **SO.ISD-P with security attributes "state" "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 enable 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 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 rules:

- [Assignment: *none*]

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

- [Assignment: *none*]

FDP_ACC.1/ECASD Subset access control

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

- **Subjects: S.ISD-R, S.ECASD**
- **Objects: data and attributes of ECASD,**
- **Operations:**
  - **Execution of a ECASD function**
  - **Access to output data of these functions.**
- [**Assignment**: *none*]

FDP_ACF.1/ECASD Security attribute based access control

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

- **Subjects: S.ISD-R, with security attribute "AID", 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 eSIM CA public key (D.PK.CI.ECDSA)**
    - **Creation of an eUICC signature on material provided by an ISD-R.**
  - **Access to output data of these functions.**
- **[assignment:** *none***].**

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

- **Authorized users: only S.ISD-R, identified by its AID, shall be authorized to execute the following S.ECASD functions:**
  - **Verification of a certificate CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DP.TLS, CERT.Dsauth.ECDSA or CERT.DS.TLS, provided by an ISD-R, with the CI public key (PK.CI.ECDSA).**
  - **Creation of an eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R.**
- [**Assignment**: *none*].

FDP_ACF.1.3/ECASD The TSF shall explicitly authorize access of subjects to objects based on the following rules:

- [Assignment: *none*]

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

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: *none*].

Application note:

- This SFR aims to control which subject is able to transmit Profile Policy Rules, Rules Authorization Table or network authentication keys to the PPE, PPI, and Telecom Framework.

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

FCS_RNG.1.1 The TSF shall provide a [selection: *physical*] random number generator that implements:

[Assignment:

- *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.*
- *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.*
- *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.*
- *The online test procedure shall be effective to detect non-tolerable weakness of the random numbers soon.*
- *The online test procedure checks the quality of the raw random number sequence. It is triggered applied upon specified internal events. 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 random words*]] that meet [assignment:

- *Test procedure A and no other test suites does not distinguish the internal random numbers from output sequences of an ideal RNG.*
- *The average Shannon entropy per internal random bit exceeds 0.997*].

Refinement:

Random number generator class used is PTG.2 as defined in AIS31 [AIS31].

FPT_EMS.1/Base TOE Emanation of TSF and User data

FPT_EMS.1.1/Base The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in table 24:

ID	Emission	Attack surface	TSF data	User data
1	[assignment: *power consumptions and electromagnetic fluctuations*]	**Any**	**-**	- **D.SECRETS;** - **D.SK.EUICC.ECDSA** **and the secret keys which are part of the following keysets:** - **D.MNO_KEYS,** - **D.PROFILE_NAA_PARAMS.**

Table 25 - FPT_EMS.1.1/Base

Application note:

- The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate from internal operation of the TOE or may originate from an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE.
- Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, and so on.

FDP_SDI.1/Base Stored data integrity monitoring

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

Refinement:

The notion of integrity-sensitive data covers the assets of the Security Target TOE that require to be protected against unauthorized modification, including but not limited the assets of this PP that require to be protected against unauthorized modification:

- *D.MNO_KEYS*
- *Profile data:*
  - *D.PROFILE_NAA_PARAMS*
  - *D.PROFILE_IDENTITY*
  - *D.PROFILE_RULES*
- *Management data:*
  - *D.PLATFORM_DATA*
  - *D.DEVICE_INFO*
  - *D.PLATFORM_RAT*
- *Identity management data:*
  - *D.SK.EUICC.ECDSA*
  - *D.CERT.EUICC.ECDSA*
  - *D.PK.CI.ECDSA*
  - *D.PK.EIM.ECDSA (SGP.32)*
  - *D.EID*
  - *D.SECRETS*
  - *D.CERT.EUM.ECDSA*
  - *D.CRLs if existing*

FDP_RIP.1/Base Subset residual information protection

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

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

FPT_FLS.1/Base Failure with preservation of secure state

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

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

FMT_MSA.1/PLATFORM_DATA Management on security attributes

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

- **ISD-P state**

to

- **Modify ISD-P state:**
  - **from "INSTALLED" to "SELECTABLE" (during ISD-P creation).**
  - **from "ENABLED" to "DISABLED" (during profile disabling).**
- **Modify ISD-P state:**
  - **from "DISABLED" to "ENABLED" (during profile enabling).**

Application note:

- In case of part of the Platform functionality is performed by GlobalPlatform packages, the role of S.PRE may for instance be partly attributed to the OPEN.

FMT_MSA.1/RULES Management of security attributes

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

- **D.PROFILE_RULES**

to

- **S.ISD-R for change default, via function "ES8+.ConfigureISDP"**
- **S.ISD-R for query**
- **S.ISD-P for modify, via function "ES6.UpdateMetadata"**
- **[selection: *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:

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

to

- **S.ISD-R for:**
  - **Query D.PK.CI.ECDSA**
  - **Delete D.MNO_KEYS, via function** [**selection**: ***ESep.Delete (SGP.32)]***
- **No actor for other operations.**

Application note:

- The modification of D.MNO_KEYS keysets is forbidden. To modify the keysets, one must delete the profile and load another profile.

FMT_SMF.1/Base Specification of Management Functions

FMT_SMF.1.1/Base The TSF shall be capable of performing the following management functions:

- [assignment: *following list of management functions*].

List of management functions:

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

FMT_SMR.1/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.ECASD**
  - **S.PPI**
  - **S.PRE**
  - **S.TELECOM**

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

Application note:

- The roles defined here correspond to the users and subjects defined in chapter 4.2.

FMT_MSA.1/RAT Management of security attributes

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

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

to

- **S.ISD-R for query.**
- **S.PRE for query.**

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **Secure Channel Protocol information flow control SFP, ISD-R content access control SFP, ECASD access control SFP and Platform services information flow control SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

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

FPT_EMS.1/IPAe TOE Emanation

FPT_EMS.1.1/IPAe 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: *power consumptions and electromagnetic fluctuations*]	**Any**	**D.IPAe_KEYS**	- **D.SECRETS;** - **D.SK.EUICC.ECDSA** **and the secret keys which are part of the following keysets:** - **D.MNO_KEYS,** - **D.PROFILE_NAA_PARAMS.**

Table 26 - FPT_EMS.1.1/IPAe

Application Note 86:

The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate from internal operation of the TOE or may originate from an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE.

Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, and so on.

FDP_SDI.1/IPAe Stored data integrity monitoring

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

Refinement:

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

- Management data
  - D.IPAe_DEVICE_INFO
- Keys
  - D.IPAe_KEYS

FDP_RIP.1/IPAe Subset residual information protection

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

- **D.IPAe_KEYS.**

FMT_SMF.1/IPAe Specification of Management Functions

FMT_SMF.1.1/IPAe The TSF shall be capable of performing the following management functions:

[assignment:

- *Manage authentication state*
- *Enable profile*
- *Disable profile*
- *Delete profile*
- *Add an Associated eIM*
- *Update an Associated eIM*
- *Delete an Associated eIM*
- *Retrieve a single eIM Package***]**

FMT_SMR.1/IPAe Security roles

FMT_SMR.1.1/IPAe The TSF shall maintain the roles

- **External users:**
  - **U.SM-DS**
  - **U.SM-DP+**
  - **U.EIM**
- **Subjects:**
  - **S.IPAe.**

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

Application Note 87:

The roles defined here correspond to the users and subjects defined in Section 4.2

7.1.6 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, TUAK, [selection:** *no other algorithm***]** and cryptographic key size **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 constant 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 support sizes for RES, MAC, CK and IK to those currently support in 3GPP standards.**
- **[selection:** *no additional standards.***]**

Application note:

- The keys used by these algorithms are distributed within the profiles during provisioning (see FCS_CKM.2/Mobile_network) and must be securely deleted (FCS_CKM.6/Mobile_network).

FCS_CKM.2/Mobile_network Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *following key distribution methods*] that meets the following:

- [assignment: *following standards*]
  - *MILENAGE: Distribution method from SCP-SGP22 (SCP03t) – [SGP.22]*
  - *TUAK: Distribution method from SCP-SGP22 (SCP03t) – [SGP.22]*

Application note:

- The keys in this SFR are the Mobile Network authentications keys included in the asset D.PROFILE_NAA_PARAMS. These keys are distributed as a part of the MNO profile during profile download.

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: *physically overwriting key with random values*] that meets the following: [assignment: *none*].

7.2 Runtime Environment Security Requirements

In the Protection Profile [PP-eUICC] the objectives for the Runtime Environment are defined as objectives for the environment (OE.RE.*).

Since the IC and the RE are part of the TOE of this Security Target, the objectives for the environment were translated into objectives for the TOE. They subsequently must be covered by SFRs that have been imported from Java Card Protection Profile [PP-JCS].

- The Subjects: Prefixed with an "S".
- The Objects: Prefixed with an "O".
- Information: Prefixed with an "I".
- Operations: Prefixed with "OP"

Subjects, Objects and Information are defined and described in [PP-JCS]. Security Attributes linked to these subjects, objects and information are also defined in [PP-JCS]. Finally, Operations definition and description are also present in [PP-JCS].

7.2.1 CoreLG Security Functional requirements

This group is focused on the main security policy of the Java Card System, known as the firewall.

7.2.1.1 Firewall Policy

FDP_ACC.2/FIREWALL Complete access control

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

Refinement:

The oration involved in the policy are:

- *OP.CREATE*
- *OP.INVK_INTERFACE*
- *OP.INVK_VIRTUAL*
- *OP.JAVA*
- *OP.THROW*
- *OP.TYPE_ACCESS*

- *OP.ARRAY_LENGTH*
- *OP.ARRAY_T_ALOAD*
- *OP.ARRAY_T_ASTORE*
- *OP.ARRAY_AASOTRE*

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

Application note:

- It should be noticed that accessing array's components of a static array, and more generally fields and methods of static objects, is an access to the corresponding O.JAVAOBJECT.

FDP_ACF.1/FIREWALL Security attribute-based access control

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

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

Table 27 - FDP_ACF.1.1/FIREWALL

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

- **R.JAVA.1: S.CAP_FILE may freely perform, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS upon any O.JAVAOBJECT whose Sharing attribute has value "JCRE entry point" or "global array".**
- **R.JAVA.2: S.CAP_FILE may freely perform OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE or OP.THROW upon any O.JAVAOBJECT whose Sharing attribute has value "Standard" and whose Lifetime attribute has value "PERSISTENT" only if O.JAVAOBJECT's Context attribute has the same value as the active context.**
- **R.JAVA.3: S.CAP_FILE may perform OP.TYPE_ACCESS upon an O.JAVAOBJECT with Context attribute different from the currently active context, whose Sharing attribute has**

value "SIO" only if O.JAVAOBJECT is being cast into (checkcast) or is being verified as being an instance of (instanceof) an interface that extends the Shareable interface.

- **R.JAVA.4: S.CAP_FILE may perform OP.INVK_INTERFACE upon an O.JAVAOBJECT with Context attribute different from the currently active context, whose Sharing attribute has the value "SIO", and whose Context attribute has the value "CAP File AID", only if the invoked interface method extends the Shareable interface and one of the following conditions applies:**
  - **The value of the attribute Selection Status of the CAP file whose AID is "CAP File AID" is "Multiselectable"**
  - **The value of the attribute Selection Status of the CAP file whose AID is "CAP File AID" is "Non-multiselectable", and either "CAP File AID" is the value of the currently selected applet or otherwise "CAP File AID" does not occur in the attribute Active Applets**
- **R.JAVA.5: S.CAP_FILE may perform OP.CREATE upon O.JAVAOBJECT only if the value of the Sharing parameter is "Standard" or "SIO".**
- **R.JAVA.6: S.CAP_FILE may freely perform OP.ARRAY_ACCESS or OP.ARRAY_LENGTH upon any O.JAVAOBJECT whose Sharing attribute has value "global array".**

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

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

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

1. **Any subject with OP.JAVA upon an O.JAVAOBJECT whose LifeTime attribute has value "CLEAR_ONDESELECT" if O.JAVAOBJECTs Context is not the same as the Selected Applet Context.**
2. **Any subject attempting to create an object by the means of OP.CREATE and a "CLEAR_ON_DESEECT" LifeTime parameter if the active context is no the same as the Selected Applet Context.**
3. **S.CAP_FILE performing OP.ARRAY_AASTORE of the reference of an O.JAVAOBJECT whose sharing attribute has value "global array" or "Temporary".**
4. **S.CAP_FILE performing OP.PUTFIELD or O.PUTSTATIC of the reference of an O.JAVAOBJECT whose sharing attribute has value "global array" or "Temporary".**

5. **R.JAVA.7: S.CAP_FILE performing OP.ARRAY_T_ASTORE into an array view without ATTR_WRITABLE_VIEW access attribute.**
6. **R.JAVA.8: S.CAP_FILE performing OP.ARRAY_T_ALOAD into an array view without ATTR_READABLE_VIEW access attribute.**

Application note:

- The deletion of applets may render some O.JAVAOBJECT inaccessible, and the Java Card RE may be in charge of this aspect. This can be done, for instance, by ensuring that references to objects belonging to a deleted application are considered as a null reference. Such a mechanisms is implementation-dependent.
- In the case of an array type, fields are components of the array ([JVM]), as well as the length; the only methods of an array object are those inherited from the Object class.
- The Sharing attribute defines five categories of objects:
    - Standard ones, whose both fields and methods are under the firewall policy.
    - Shareable interface Objects (SIO), which provide a secure mechanism for inter-applet communication.
    - JCRE entry points (Temporary or Permanent), who have freely accessible methods but protected fields.
    - Global arrays, having both unprotected fields (including components; refer to JavaCardClass) and methods.
    - Array Views, having fields/elements access controlled by access control attributes, ATTR_READABLE_VIEW and ATTR_WRITABLE_VIEW and methods.
- When a new object is created, it is associated with the Currently Active Context. But the object is owned by the applet instance within the Currently Active Context when the object is instantiated ([JCRE3]). An object is owned by an applet instance, by the JCRE or by the library where is has been defined (these latter objects can only be arrays that initialize static fields of CAP files).
- ([JCRE3], Glossary) Selected Applet Context: The Java Card RE keeps track of the currently selected Java Card applet. Upon receiving a SELECT command with the applet's AID, the Java Card RE makes this applet the Selected Applet Context. The Java Card RE sends all APDU commands to the Selected Applet Context.
- While the expression "Selected Applet Context" refers to a specificinstalled applet, the relevant aspect to the policy is the context (CAP file AID) of the selected applet. In this policy, the "Selecteed Applet Context" is the AID of the selected CAP file.
- ([JCRE3]) At any point in time, there is only one active context within the Java Card VM (this is called the Currently Active Context).

- It should be noticed that the invocation of a static methods (or access to a static field) is not considered by this policy, as there are no firewall rules. They have no effect on the active context as well and the "acting CAP File" is not the one to which the static method belongs to in this case.
- It should be noticed that the Java Card Platform, version 2.2x and version 3.x.x Classic Edition, introduces the possibility to an applet instance to be selected on multiple logical channels at the same time, or accessing other applets belonging to the same CAP file being selected simultaneously. These applets are referred to as multiselectable applets. Applets that belong to a same CAP file are either all multiselectable or not ([JCVM3]). Therefore, the selection mode can be regarded as an attribute of CAP files. No selection mode is defined for the library CAP file.
- An applet instance will be considered an active applet instance if it is currently selected in at least one logical channel. An applet instance is the currently selected applet instance only if it is processing the current command. There can only be one currently selected applet instance at a given time ([JCRE3]).

FDP_IFC.1/JCVM Subset information flow control

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

Application note:

- It should be noticed that references of temporary Java Card RE entry points, which cannot be stored in class variables, instance variables or array components, are transferred from the internal memory of the Java Card RE (TSF data) to some stack through specific APIs (Java Card RE owned exceptions) or Java Card RE invoked methods (such as the process (APDU apdu)); these are causes of OP:PUT (S1, S2, I) operations as well.

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 and information security attributes:

- **Subject:** S.JCVM
- **Security attributes:** 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: *none*].

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*].

Application note:

- The storage of temporary Java Card RE-owned objects references in runtime-enforced ([JCRE3]).
- It should be noticed that this policy essentially applies to the execution of bytecode. Native methods, the Java Card RE itself and possibly some API methods can be granted specific rights or limitations through the FDP_IF.1.3/JCVM to FDP_IFF.1.5/JCVM elements. The way the Java Card virtual machine manages the transfer of values on the stack and local variables (returned values, uncaught exceptions) from and to internal registers is implementation-dependent. For instance, a returned reference, depending on the implementation of the stack frame, may transit through an internal register prior to being pushed on the stack of the invoker. The returned bytecode would cause more than one OP.PUT operation under this scheme.

FDP_RIP.1/OBJECTS Subset residual information protection

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

Application note:

- The semantics of the Java programming language requires for any object field and array position to be initialized with default values when the resource is allocated ([JVM]).

FMT_MSA.1/JCRE Management of security attributes

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

Application note:

- The modification of the Selected Applet Context should be performed in accordance with the rules given in [JCRE3] and [JCVM3].

FMT_MSA.1/JCVM Management of security attributes

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

Application note:

- The modification of the Selected Applet Context should be performed in accordance with the rules given in [JCRE3] and [JCVM3].

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

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

Application note:

- The following rules are given as examples only. Future versions may allow the creation of transient objects belonging to arbitrary classed; such evolution will naturally change the range of "secure values" for this component.
    - The Context attribute of an O.JAVAOBJECT must correspond to that of an installed applet or be "Java Card RE".
    - An O.JAVAOBJECT whose Sharing attribute is a Java Card RE entry point or a global array necessary has "Java Card RE" as the value for its Context security attribute.
    - Any O.JAVAOBJECT whose Sharing attribute is not "Standard" has a PERSISTENT-LifeTime attribute's value.
    - Any O.JAVAOBJECT whose LifeTime attribute value is no PERSISTENT has an array type as JavaCardClass attribute's value.

FMT_MSA.3/FIREWALL Static attribute initialization

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

Application note:

- Objects' security attributes of the access control policy are created and initialized at the creation of the object or the subject. Afterwards, these attributes are no longer mutable (FMT_MSA.1/JCRE). At the creation of an object (OP.CREATE), the newly created object, assuming that the FIREWALL access control SFP permits the operation, gest its Lifetime and Sharing attributes from the parameters of the operation; on the contrary, its Context attribute has a default value, which is its creator's Context attribute and AID respectively ([JCRE3]). There is one default value for the Selected Applet Context that is the default applet identifier's Context, and one default value for the Currently Active Context that is "Java Card RE".

- The knowledge of which reference corresponds to a temporary entry point object or a global array and which does not is solely available to the Java Card RE (and the Java Card virtual machine).

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

Application note:

- The intent is that none of the identified roles has privileges with regard to the default values of the security attributes. It should be noticed that creation of objects is an operation controlled by the FIREWALL access control SFP. The operation shall fail anyway if the created object would have had security attributes whose value violates FMT_MSA.2.1/FIREWALL_JCVM .

FMT_MSA.3/JCVM Static attribute initialization

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

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

FMT_SMF.1/JC Specification of Management Functions

FMT_SMF.1.1/JC The TSF shall be capable of performing the following management functions:

- Modify the Currently Active Context.
- Modify the Selected Applet Context.
- Modify the Active Applets.

FMT_SMR.1/JC Security roles

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

- **JavaCard RE (JCRE)**
- **JavaCard VM (JCVM)**

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

7.2.1.2 Application Programming Interface

FCS_CKM.1/EC Cryptographic key generation

FCS_CKM.1.1/EC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *EC Key Pair Generation*] and specified cryptographic key sizes [assignment: *P ranging from 224 to 521 bits*] that meet the following:

- [Assignment: *TR-03111 (BSI) and RFC 5639*]

FCS_CKM.1/GP-SCP Cryptographic key Generation

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

SCP Protocol	Cryptographic algorithm	Cryptographic Key Size	Cryptographic Standard
SCP02	*TDES 2-Keys*	*112 bits*	*[GPCS]*
SCp03	*AES*	*128, 192, 256 bits*	*[GPCS] (Amd D)*
SCP81	*TDES 3-Keys*	*168 bits*	*[GPCS] (Amd B)*
SCP81	*AES*	*128 bits*	*[GPCS] (Amd B)*

Table 28 - FCS_CKM.1/GP-SCP

FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [assignment: cryptographic key access to TSF-managed cryptographic keys for cryptographic services and secure channel processing] in accordance with a specified cryptographic key access method [assignment: controlled access through JCS.KeyManagement services and GP Secure Channel mechanisms using internal key representations] that meets the following: [assignment: none].

FCS_CKM.6/RE Timing and event of cryptographic key destruction

FCS_CKM.6.1/RE The TSF shall destroy [assignment: *all cryptographic keys*] 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 in accordance with a specified cryptographic key destruction method [assignment: *physically overwriting the keys with zero values*] that meets the following: [assignment: *none*].

FCS_COP.1/TDES_MAC Cryptographic operation

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

MAC length	MAC Algorithm

4 bytes	*ISO9797-1 MAC algorithm 3*
4 bytes	*3DES in outer CBC mode*
8 bytes	*ISO9797-1 MAC algorithm 3*
8 bytes	*3DES in outer CBC mode*

Table 29 - FCS_COP.1/TDES_MAC

FCS_COP.1/AES_MAC Cryptographic operation

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

MAC length	MAC Algorithm
16 bytes	*AES in CBC mode, block size 128 bits*
24 bytes	*AES in CBC mode, block size 192 bits*
32 bytes	*AES in CBC mode, block size 256 bits*

Table 30 - FCS_COP.1/AES_MAC

FCS_COP.1/ECDH Cryptographic operation

FCS_COP.1.1/ECDH The TSF shall perform [assignment: *secret key agreement*] in accordance with a specified cryptographic algorithm [assignment: *Elliptic Curve Diffie-Herrman (ECDH)*] and cryptographic key sizes [assignment: *P ranging from 224 to 521 bits*] that meet the following: [assignment:[*ANSI X9.62], [ANSI X9.63] and [BSI TR 03111]*].

FCS_COP.1/CRC Cryptographic operation

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

Application note:

- *The algorithm "CRC16" and "CRC32" are not claimed as security functions.*

FCS_COP.1/ECDSA_SIGN Cryptographic operation

FCS_COP.1.1/ECDSA_SIGN The TSF shall perform [assignment: *Signature generation and verification*] in accordance with a specified cryptographic algorithm [assignment: *ECDSA*] and cryptographic key sizes [assignment: *from 224 to 521 bits*] that meet the following: [assignment: *ANSI X9.62-2005 and BSI TR-03111*].

FCS_COP.1/GP-SCP Cryptographic operation

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

SCP Protocol	Cryptographic Operation	Cryptographic algorithm	Cryptographic Key size	Cryptographic Standard
SCP02	*MAC Generation/Verification*	*HMAC, CMAC using TDES*	*112 bits*	*FIPS 198*
SCP02	*Symmetric Encryption/Decryption*	*TDES in CBC mode*	*112 bits*	*NIST 800 67* *NIST 800 38A*
SCP02	*Key Derivation*	*HMAC-based KDF, CMAC-based KDF using TDES*	*112 bits*	*NIST 800 108* *FIPS 198*
SCP03	*Symmetric Encryption/Decryption*	*AES in CBC mode*	*128, 192, or 256 bits*	*FIPS 197* *NIST 800 38A*
SCP03	*MAC Generation/Verification*	*CMAC AES*	*128, 192, or 256 bits*	*NIST 800 38B*
SCP03	*Key Derivation*	*CMAC-based KDF using AES*	*128, 192, or 256 bits*	*NIST 800 108* *NIST 800 38B*
SCP81	*Secure communication channel with the Remote Administration Server*	*TLS_PSK_WITH_AES_128_CBC_SHA256* *TLS_PSK_WITH_NULL_SHA256*		*[GPCS] (Amd B, section 3.3.2)*
SCP-SGP22 (SCP03t)	*Secure communication channel with the SM-DP+ for profile download*	*AES in CBC and CMAC modes*	*AES: 128*	*SGP.02*

Table 31 - FCS_COP.1/GP-SCP

FCS_COP.1/TDES_CIPHER Cryptographic operation

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

FCS_COP.1/AES_CIPHER Cryptographic operation

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

FCS_COP.1/Hash Cryptographic operation

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

Implemented Algorithm	Standard
SHA-256	FIPS 180-4

Table 32 FCS_COP.1/Hash

FCS_COP.1/HMAC Cryptographic operation

FCS_COP.1.1/HMAC The TSF shall perform [assignment: *computation of a HMAC value*] in accordance with a specified cryptographic algorithm [assignment: *see cryptographic algorithms in the table below*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *RFC2104*].

Implemented Algorithm
HMAC_SHA_256

Table 33 - FCS_COP.1/HMAC

FDP_RIP.1/ABORT Subset residual information protection

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

Application note:

- The events that provoke the de-allocation of a transient object are described in [JCRE3].

FDP_RIP.1/APDU Subset residual information protection

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

Application note:

- The allocation of a resource to the APDU buffer is typically performed as the result of a call to the process() method of an applet.

FDP_RIP.1/bArray Subset residual information protection

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

Application note:

- A resource is allocated to the bArray object when a call to an applet's install() method is performed. There is no conflict with FDP_ROL.1 here because of the bounds on the rollback mechanism (FDP_ROL.1.2/FIREWALL): the scope of the rollback does not extend outside the execution of the install() method, and the de-allocation occurs precisely right after the return of it.

FDP_RIP.1/GlobalArray Subset residual information protection

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

FDP_RIP.1/KEYS Subset residual information protection

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

FDP_RIP.1/TRANSIENT Subset residual information protection

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

Application note:

- The events that provoke the de-allocation of any transient object are described in [JCRE3].
- The clearing of CLEAR_ON_DESELECT objects is not necessarily performed when the owner of the objects is deselected. In the presence of multiselectable applet instances, CLEAR_ON_DESELECT memory segments may be attached to applets that are active in different logical channels. Multiselectable applet instances within the same CAP file must share the transient memory segment if they are concurrently active ([JCRE3]).

FDP_ROL.1/FIREWALL Basic rollback

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

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

7.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take one of the following actions Upon detection of a potential security violation.

- **Throw an exception**
- **Lock the card session**
- **Reinitialize the Java Card System and its data**
- **[assignment:** *none***]**

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.*

- *Unavailable of resources.*
- *Array overflow*
- *[Assignment: Global Platform card state inconsistency].*

Application note:

- The developer shall provide the exhaustive list of actual potential security violations the TOE reacts to. For instance, other runtime errors related to applet's failure like uncaught exceptions.
- The bytecode verification defines a large set of rules used to detect a "potential security violation". The actual monitoring of these "events" within the TOE only makes sense when the bytecode verification is performed on-card.
- Depending on the context of use and the required security level, there are cases where the card manager and the TOE must work in cooperation to detect and appropriately react in case of potential security violation. This behavior must be described in this component. It shall detail the nature of the feedback information provided to the card manager (like the identity of the offending application) and the conditions under which the feedback will occur (any occurrence of the java.lang.SecurityException exception).
- The "locking of the card session" may not appear in the policy of the card manager. Such measure should only be taken in case of severe violation detection; the same holds for the re-initialization of the Java Card System. Moreover, the locking should occur when "clean" re-initialization seems to be impossible.
- The locking may be implemented at the level of the Java Card System as a denial of service (through some systematic "fatal error" message or return value) that lasts up to the next "RESET" event, without affecting other components of the card (such as the card manager). Finally, because the installation of applets is a sensitive process, security alerts in this case should also be carefully considered herein.

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 check data*].

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

Application note:

- The following data persistently stored by TOE have an integrity check data security attribute:
    - Key.
    - PIN.
    - CAP File.

  - GlobalPlatform card state (OP_READY, SECURED).
- The card states CARD_LOCKED and TERMINATE are not applicable to eUICC.

FPR_UNO.1 Unobservability

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

Application note:

- The non-observability of operations on sensitive information such as keys appears as impossible to circumvent in the smart card world. The precise list of operations and objects is left unspecified, but should at least concern secret keys and PIN values when they exist on the card, as well as the cryptographic operations and comparisons performed on them.

FPT_FLS.1/JC Failure with preservation of secure state

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

Application note:

- The Java Card RE Context is the Current context when the Java Card VM begins running after a card reset ([JCRE3]) or after a proximity card (PICC) activation sequence ([JCRE3]). Behavior of the TOE on power loss and reset is described in [JCRE3]. Behavior of the TOE on RF signal loss is described in [JCRE3].

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use:

- **The rules defined in [JCVM3] specification**
- **The API tokens defined in the export files of the reference implementation.**
- [assignment: *none*]

when interpreting the TSF data from another trusted IT product.

Application note:

- Concerning the interpretation of data between the TOE and the underlying Java Card platform, it is assumed that the TOE is developed consistently with the SCP functions, including memory management, I/O functions and cryptographic functions.

7.2.1.4 AID Management

FIA_ATD.1/AID User attribute definition

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

- **CAP file AID.**
- **Package AID.**
- **Applet version number.**
- **Registered Applet AID.**
- **Applet Selection Status.**

Application note:

- ***JC3.0.5 CAP File extended format is not supported by the TOE, therefore CAP File AID is equivalent to Package AID.***

Refinement: "Individual users" stand for applets.

FIA_UID.2/AID User identification before any action

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

Application note:

- By users here it must be understood the ones associated to the CAP files (or applets) that act as subjects of policies. In the Java Card System, every action is always performed by an identified user interpreted here as the currently selected applet or the CAP file that is the subject's owner. Means of identification are provided during the loading procedure of the CAP file and the registration of applet instances
- The role Java Card RE defined in FMT_SMR.1/JC is attached to an IT security function rather than to a "user" of the CC terminology. The Java Card RE does not "identify" itself to the TOE, but it is part of it.

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: *CAP File AID is defined with associated value during loading and with context identifier*].

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

Application note:

- *JC3.0.5 CAP File extended format is not supported by the TOE, therefore CAP File AID is equivalent to Package AID*.

FMT_MTD.1/JCRE Management of TSF data

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

Application note:

- The installer and the Java Card RE manage other TSF data such as the applet life cycle or CAP files, but this management is implementation specific. Objects in the Java programming language may also try to query AIDs of installed applets through the lookupAID(...) API method
- The installer, applet deletion manager or even the card manager may be granted the right to modify the list of registered applets' AIDs in specific implementations (possibly needed for installation and deletion; see #.DELETION and #.INSTALL).

FMT_MTD.3/JCRE Secure TSF data

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

7.2.2 INSTG Security Functional requirements

This group consists of SFRs related to the installation of Boolean applets, addressing security aspects outside the runtime.

The installation of applets is a critical phase that partially extends beyond the firewall boundaries and requires specific treatment.

In this PP, loading a package or installing an applet is modeled as importing user data with its security attributes, such as the applet parameters used in the firewall rules.

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

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

Application note:

- The most common importation of user data is CAP file loading and applet installation on the behalf of the installer. Security attributes consist of the shareable flag of the class component, AID and version numbers of the CAP file and the package or packages contained within the CAP file, maximal operand stack size and number of local variables for each method, and export and import components (accessibility).

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

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

Application note:

- The format of the CAP file is precisely defined in [JCVM3] specifications; it contains the user data (like applet's code and data) and the security attributes altogether. Therefore, there is no association to be carried out elsewhere.

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

Application note:

- Each CAP file and all the packages contained within a CAP file contain a Version attribute, which is a pair of major and minor version numbers ([JCVM3]). With the AID, it describes the package defined in the CAP file. When an export file is used during preparation of a CAP file, the version numbers and AIDs of imported packages indicated in the export file are recorded in the CAP files ([JCVM3]): the dependent packages' Version and AID attributes allow the retrieval of these identifications. Implementation-dependent checks may occur on a case-by-case basis to check that packages are binary compatible. Packages have "package Version Numbers" ([JCVM3]) that indicate binary compatibility or incompatibility between successive implementations of a package, which directly concern this requirement.

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

CAP file loading is allowed only if, for each dependent package, its AID attribute is equal to a resident package AID attribute, the major version attribute associated to the

dependent package file is equal to the major version attribute of the resident package and the minor version attribute is equal to or less than the minor version attribute associated to the resident package ([JCVM3]).

Application note:

- A package may depend on (import or use data from) other packages already installed. This dependency is explicitly stated in the loaded package in the form of a list of package AIDs.
- The intent of this rule is to ensure the binary compatibility of the package with those already on the card ([JCVM3]).
- The installation (the invocation of an applet's install method by the installer) is implementation dependent ([JCRE3]).
- Other rules governing the installation of an applet, that is, its registration to make it SELECTable by giving it a unique AID, are also implementation dependent (see, for example, [JCRE3]).

JC3.0.5 CAP File extended format is not supported by the TOE, therefore CAP File AID is equivalent to Package AID.

FMT_SMR.1/Installer Security roles

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

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

FPT_FLS.1/Installer Failure with preservation of secure state

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

Application note:

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

FPT_RCV.3/Installer Automated recovery without undue loss

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.

Application Note:

- This element is not within the scope of the Java Card specification, which only mandates the behavior of the Java Card System in good working order. Further details on the "maintenance mode" shall be provided in specific implementations. The following is an excerpt from [CC2]: In this maintenance

mode normal operation might be impossible or severely restricted, as otherwise insecure situations might occur. Typically, only authorized users should be allowed access to this mode but the real details of who can access this mode is a function of FMT: Security management. If FMT: Security management does not put any controls on who can access this mode, then it may be acceptable to allow any user to restore the system if the TOE enters such a state. However, in practice, this is probably not desirable as the user restoring the system has an opportunity to configure the TOE in such a way as to violate the SFRs

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

Application Note:

- Should the installer fail during loading/installation of a CAP file/applet, it has to revert to a "consistent and secure state". The Java Card RE has some clean up duties as well; see [JCRE3], for possible scenarios. Precise behavior is left to implementers. This component shall include among the listed failures the deletion of a CAP file/applet. See ([JCRE3]) for possible scenarios. Precise behavior is left to implementers.
- Other events such as the unexpected tearing of the card, power loss, and so on, are partially handled by the underlying hardware platform (see [PP0084b]) and, from the TOE's side, by events "that clear transient objects" and transactional features. See FPT_FLS.1.1/Base, FDP_RIP.1/TRANSIENT, FDP_RIP.1/ABORT and FDP_ROL.1/FIREWALL

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**:** *The loading or installation of the Executable Load File is at 0%*] for loss of TSF data or objects under the control of the TSF.

Application Note:

- The quantification is implementation dependent, but some facts can be recalled here. First, the SCP ensures the atomicity of updates for fields and objects, and a power-failure during a transaction or the normal runtime does not create the loss of otherwise-permanent data, in the sense that memory on a smart card is essentially persistent with this respect (EEPROM). Data stored on the RAM and subject to such failure is intended to have a limited lifetime anyway (runtime data on the stack, transient objects' contents). According to this, the loss of data within the TSF scope should be limited to the same restrictions of the transaction mechanism

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

7.2.3 ADELG Security Functional Requirements

This group consists of 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 serves as a framework to be implemented by ST.

FDP_ACC.2/ADEL Complete access control

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

Refinement:

The operations involved in the policy are:

- *OP.DELETE_APPLET.*
- *OP.DELETE_CAP_FILE.*
- *OP.DELETE_CAP_FILE_APPLET.*

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

FDP_ACF.1/ADEL Security attribute-based access control

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

Subject/Object	Attributes
S.JCVM	Active Applets
S.JCRE	Selected Applet Context Registered Applets Resident Packages
O.CODE_CAP_FILE	CAP file AID AIDs of packages within a CAP file Dependent Package AID Static References
O.APPLET	Applet Selection Status

O.JAVAOBJECT	Owner Remote

Table 34 - FDP_ACF.1.1/ADEL

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

In the context of this policy, an object O is reachable if and only one of the following conditions hold:

1. **The owner of O is a registered applet instance A (O is reachable from A).**
2. **A static field of a resident package P contains a reference to O (O is a reachable from P).**
3. **There exists a valid remote reference to O (O is remote reachable).**
4. **There exist an object O' that is reachable according the either (1) or (2) or (3) above and O' contains a reference to O (the reachability status of O is that of O').**

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

- **R.JAVA.14 ([JCRE3] Applet Instance Deletion): S:ADEL may perform OP.DELETE_APPLET upon an O.APPLET only if:**
  1. **S.ADEL is currently selected.**
  2. **There is no instance in the context of O.APPLET that is active in any logical channel.**
  3. **There is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from the applet instance distinct from O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3]) O.JAVAOBJECT is remote reachable.**
- **R.JAVA.15 ([JCRE3] Multiple Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon several O.APPLET only if:**
  1. **S.ADEL is currently selected.**
  2. **There is no instance of any of the O.APPLET being deleted that is active in any logical channel.**
  3. **There is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3]) O.JAVAOBJECT is remote reachable.**

- **R.JAVA.16 ([JCRE3] Applet/Library CAP file deletion): S.ADEL may perform OP.DELETE_CAP_FILE upon an O.CODE_CAP_FILE only if:**
  1. **S.ADEL is currently selected.**
  2. **No reachable O.JAVAOBJECT, from a CAP file distinct from O.CODE_CAP_FILE that is an instance of a class that belongs to O.CODE_CAP_FILE, exists on the card.**
  3. **There is no resident package on the card that depends on O.CODE_CAP_FILE.**
- **R.JAVA.17 ([JCSR3] Applet CAP file and Contained Instances Deletion): S.ADEL may perform OP.DELETE_CAP_FILE_APPLET upon an O.CODE_CAP_FILE only if:**
  1. **S.ADEL is currently selected.**
  2. **No reachable O.JAVAOBJECT, from a CAP file distinct from O.CODE_CAP_FILE, which is an instance of a class that belongs to O.CODE_CAP_FILE exists on the card.**
  3. **There is no CAP file loaded on the card that depends on O.CODE_CAP_FILE.**
  4. **For every O.APPLET of those being deleted it holds that:**
     a. **There is no instance in the context of O.APPLET that is active in any logical channel.**
     b. **There is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance not being deleted, or O.JAVAOBJECT is reachable from a CAP file not being deleted, or ([JCRE3]) O.JAVAOBJECT is remote reachable.**

Application note:

- This policy introduces the notion of reachability, which provides a general means to describe objects that are referenced from a certain applet instance or CAP file.
- S.ADEL calls the "uninstall" method of the applet instance to be deleted, if implemented by the applet, to inform it of the deletion request. The order in which these calls and the dependencies checks are performed are out of the scope of this protection profile.

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

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

FDP_RIP.1/ADEL Subset residual information protection

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

- **Applet instances and/or CAP files when one of the deletion operations in FDP_ACC.2.1/ADEL is performed on them.**

Application note:

- Deleted freed resources (both code and data) may be reused, depending on the way they were deleted (logically or physically). Requirements on de-allocation during applet/CAP file deletion are described in [JCRE3].

FMT_MSA.1/ADEL Management of security attributes

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

FMT_MSA.3/ADEL Static attribute initialization

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

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

FMT_SMF.1/ADEL Specification of Management Functions

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

FMT_SMR.1/ADEL Security roles

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

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

FPT_FLS.1/ADEL Failure with preservation of secure state

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

Application Note:

- The TOE may provide additional feedback information to the card manager in case of potential security violations (see FAU_ARP.1).
- The CAP file/applet instance deletion must be atomic. The "secure state" referred to in the requirement must comply with Java Card specification ([JCRE3]).

7.2.4 RMIG Security Functional Requirements

The product does not support RMI features.

7.2.5 ODELG Security Functional Requirements

FDP_RIP.1/ODEL Subset residual information protection

FDP_RIP.1.1/ODEL [Refined] The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **the objects owned by the context of an applet instance.**

FPT_FLS.1/ODEL Failure with preservation of secure state

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

Application Note:

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

7.2.6 CARG Security Functional Requirements

FCO_NRO.2/CM Enforced proof of origin

FCO_NRO.2.1/CM The TSF shall always enforce the generation of evidence of origin for transmitted **application CAP files**.

Application Note:

- Upon reception of a new application CAP file for installation, the card manager shall first check that it actually comes from the verification authority and represented by the subject S.BCV. The verification authority is indeed the entity responsible for bytecode verification.

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 files contained** in the information to which the evidence applies.

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

Application Note:

- The exact limitations on the evidence of origin are implementation dependent. In most of the implementations, the card manager performs an immediate verification of the origin of the CAP file using an electronic signature mechanism, and no evidence is kept on the card for future verifications.

FDP_IFC.2/CM Complete information flow control

FDP_IFC.2.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** on **S.INSTALLER, S.BCV, S.CAD and I.APDU** and all operations that cause that information to flow to and from subjects covered by the SFP.

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

Application note:

- The subjects covered by this policy are those involved in the loading of an application CAP file by the card through a potentially unsafe communication channel.
- The operations that make information to flow between the subjects are those enabling to send a message through and to receive a message from the communication channel linking the card to the outside world. It is assumed that any message sent through the channel as clear text can be read by an attacker. Moreover, an attacker may capture any message sent through the communication channel and send its own messages to the other subjects.
- The information controlled by the policy is the APDUs exchanged by the subjects through the communication channel linking the card and the CAD. Each of those messages contain part of an application CAP file that is required to be loaded on the card, as well as any control information used by the subjects in the communication protocol.

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

Application note:

- The security attributes used to enforce the CAP FILE LOADING SFP are implementation dependent. More precisely, they depend on the communication protocol enforced between the CAD and the card. For instance, some of the attributes that can be used are: (1) the keys used by the subjects to encrypt/decrypt their messages; (2) the number of pieces the application CAP file has been split into in order to be sent to the card; (3) the ordinal of each piece in the decomposition of the CAP file, etc. See for example Appendix D of [GP].

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

- *S.SD implements one or more Secure Channel Protocols, namely [Selection: SCP02, SCP03], each with a complete Secure Channel Key Set.*
- *S.SD has all the cryptographic keys requires by its privileges.*
- *S.OPEN accepts al ELF only if its integrity and authenticity has been verified.*
- *[Assignment: S.OPEN accepts an ELF only if its AID is not already registered by the TSF***].**

Application note:

- The precise set of rules to be enforced by the function is implementation dependent. The whole exchange of messages shall verify at least the following two rules: (1) the subject S.INSTALLER shall accept a message only if it comes from the subject S.CAD; (2) the subject S.INSTALLER shall accept an application CAP file only if it has received without modification and in the right order all the APDUs sent by the subject S.CAD.

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

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

FDP_IFF.1.5/CM [Refined] 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.**
Refinement:
- *S.OPEN fails to verify the integrity and request verification of the authenticity for CAPs.*
- *S.OPEN fails to verify the Card Life Cycle State.*
- *S.OPEN fails to verify the SD privileges.*
- *S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.*
- *S.SD fails to set the security level (integrity and/or confidentiality) to apply to the next incoming command and/or next outgoing response.*

- *S.SD fails to unwrap INSTALL or LOAD commands.*
- [assignment: *The AID is already registered within the card*].

Application note:

- The verification of the integrity and authenticity evidences can be performed either during loading or during the first installation of an application of the CAP file.

FDP_UIT.1/CM Data exchange integrity

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

FDP_UIT.1.2/CM [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.

Application note:

- Modification errors should be understood as modification, substitution, unrecoverable ordering change of data and any other integrity error that may cause the application CAP file to be installed on the card to be different from the one sent by the CAD.

FIA_UID.1/CM Timing of identification

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

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

Application note:

- The list of TSF-mediated actions is implementation-dependent, but CAP file installation requires the user to be identified. Here by user is meant the one(s) that in the Security Target shall be associated to the role(s) defined in the component FMT_SMR.1/CM.

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: [assignment: *perform the operations listed in table acting on*]] the security attributes [assignment: *mentioned in table*] to [assignment: *the authorized identified roles mentioned in table*].

Legend for tables below:

- ISD: Issuer Security Domain.
- AM SD: Security Domain with Authorized Management privilege.
- DM SD: Security Domain with Delegated management privilege.
- SD: Other Security Domain.
- The card states CARD_LOCKED and TERMINATE are not applicable to eUICC.
- Security Attributes: Minimum Security Level is the minimum-security level requires to run the command.

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

STORE DATA	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, ~~CARD_LOCKED, or TERMINATED~~	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, ~~or CARD_LOCKED~~	ISD, AM SD, DM SD, SD

Table 35 - FMA_MSA.1.1 Operations

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

Table 36 - FMA_MSA.1.1 SCP02 information

Operations: SCP22 Commands	**Security attributes: Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorized Identified Roles with Privileges**
SELECT MF	OP_READY, INITIALIZED, SECURED~~, or CARD_LOCKED~~	None	ISD, AM SD, DM SD, SD
SELECT FILE [by FID] (other than SELECT MF)	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
READ BINARY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
READ RECORD	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD

GENERAL AUTHENTICATE	OP_READY, INITIALIZED, SECURED	AUTHENTICATED or ANY_AUTHENTICATED	ISD, AM SD, DM SD, SD

Table 37 - FMA_MSA.1.1 SCP22 information

Operations: SCP80 Commands	**Security attributes: Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorized Identified Roles with Privileges**
Remote File Management Commands SELECT, UPDATE BINARY, UPDATE RECORD, SEARCH RECORD, INCREASE, VERIFY PIN, CHANGE PIN, DISABLE PIN, ENABLE PIN, UNBLOCK PIN, DEACTIVATE FILE, ACTIVATE FILE, READ BINARY, READ RECORD, CREATE FILE, DELETE FILE, RESIZE FILE, SET DATA, RETRIEVE DATA	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]
Remote Applet Management Commands DELETE, SET STATUS, INSTALL, LOAD, PUT KEY, GET STATUS, GET DATA, STORE DATA	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]

Table 38 - FMA_MSA.1.1 SCP80 information

Operations: SCP81 Commands	**Security attributes: Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorized Identified Roles with Privileges**
PUT KEY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD

STORE DATA	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, ~~CARD_LOCKED, or TERMINATED~~	None	ISD, AM SD, Dm sd, SD

Table 39 - FMA_MSA.1.1 SCP81 information

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: *following management functions*].

The following management functions specified in [GPCS]:

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

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

FMT_SMR.1/CM Security roles

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

[assignment:

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

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

FTP_ITC.1/CM Inter-TSF trusted channel

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

FTP_ITC.1.2/CM [Editorially Refined] The TSF shall permit **the CAD placed in the card issuer secured environment** to initiate communication via the trusted channel.

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

Application note:

- There is no dynamic CAP file loading on the Java Card platform. New CAP files can be installed on the card only on demand of the card issuer.

7.2.7 Global Platform Security Functional Requirements

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

FPT_FLS.1/GP Failure with preservation of secure state

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

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

Application note:

- This SFR extends FPT_FLS.1/Installer of [PP-JC] to include the failures that may occur during the loading of SD/Application keys and data.
- Refer to [JCRE] and [GPCS] for additional details.

FDP_ROL.1/GP Basic rollback

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

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

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

FCO_NRO.2/GP Enforced proof of origin

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

Refinement:

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

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

Refinement:

The TSF must be able to load Executable Load Files, SD/Application data, and keys to the card with associated security attributes (the identity of the originator and the destination) in a way that allows verification of the evidence of origin.

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

Application Note:

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

FMT_SMF.1/GP Specification of Management Functions

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

- **Card and Application Security Management as defined in [GPCS]:**
  - **Life Cycle**
  - **Privileges**
  - **Application/SD Locking and Unlocking**
  - **Card Locking and Unlocking**
  - **Card Termination**
  - **Application Status interrogation**
  - **Card Status interrogation**
  - **Command dispatch**
  - **Operational Velocity Checking**
  - **Tracing and Event logging**
- **Management function (Secure Channel Initiation/Operation/Termination) related to SCPs as defined in [GPCS].**

Application note:

- This SFR corresponds to FMT_SMF.1/CM of [PP-JC], applied to card content management operations (this is why it has been renamed).
- Management functions related to SCPs are defined in [GPCS].

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

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

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

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

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

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

- **Referring to Java Card rules defined in [JCVM] and [JCRE]: ELF loading is allowed only if, for each dependent ELF, its AID attribute is equal to a resident ELF AID attribute, and the major (minor) Version attribute associated with the dependent ELF is less than or equal to the major (minor) Version attribute associated with the resident ELF.**
- **[assignment:** *none***].**

Application note:

- This SFR corresponds to FDP_ITC.2/Installer of [PP-JC].
- Java Card rules are defined in [JCVM] and [JCRE].
- The TSF shall use the INSTALL data format and the LOAD data format when interpreting the user data from outside the TOE.

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

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

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

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

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

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

- **The algorithms and key sizes of the imported keys shall be supported by the SE.**
- **[Assignment: *The key version Number (KVN) and the Key Identifier (Key ID) of the imported keys shall be in an allowed range as specified in section 4 of [CIC]*].**

Application note:

- The algorithms and key sizes of the imported keys shall be supported by the Card as specified in [GPCS] Appendices B and C.
- PUT KEY and STORE DATA are described in [GPCS].

FIA_AFL.1/GP Authentication failure handling

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

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

FIA_UAU.1/GP Timing of authentication

FIA_UAU.1.1/GP The TSF shall allow **the TSF mediated actions listed in FIA_UID.1/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

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

FDP_UIT.1/GP Basic data exchange integrity

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

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

Application note:

- This SFR extends FDP_UIT.1/CM of [PP-JC] to cover the integrity protection of SD/Application data and keys.
- This SFR applies where APDU command and response integrity protection is required. For instance: INSTALL, LOAD, STORE DATA and PUT KEY commands.

FDP_UCT.1/GP Basic data exchange confidentiality

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

Application note:

- This SFR applies where APDU command and response confidentiality protection is required. For example, the sensitive data (e.g. secret keys) shall always be transmitted as confidential data.

FTP_ITC.1/GP Inter-TSF trusted channel

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

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

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

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

Application note:

- This SFR corresponds to FTP_ITC.1/CM of [PP-JC], applied where APDU command and response integrity and/or confidentiality protection through a Secure Channel are required.

FPR_UNO.1/GP Unobservability

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

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

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

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

Application note:

- The list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card are defined in [GPCS].

FDP_IFC.2/GP-KL Complete information flow control

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

- **Subjects: S.SD, S.CAD, S.OPEN and Application**

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

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

Application note:

- GlobalPlatform's card content management APDU commands and API methods are described in [GPCS].

FDP_IFF.1/GP-KL Complete information flow control

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

- *Subjects: S.SD and S.OPEN*
- *GlobalPlatform APDU commands STORE DATA and PUT KEY and GLobalPlatform APIs for loading and storing data and keys.*
- *Security Attributes:*
  - *Card Life Cycle state*
  - *Application and SD Life cycle states*
  - *Secure Channel Security Level*
  - *SD and Application privileges*]

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection:** *SCP02, SCP03, SCP80 and SCP81***], each equipped with a complete Secure Channel Key Set.**
- **S.SD has all the cryptographic keys required by its privileges.**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the S.OPEN checks that the requesting S.SD has no restrictions for personalization.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and priori to the command forwarding to the targeted Application or SD.**
- **[Assignment:** *S.OPEN verifies that the targeted application implements a personalization interface***].**

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

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

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

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

FMT_MSA.3/GP Security attribute initialization

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

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

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**:

- **Subject**: **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 authorized.
- **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 authorize 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*].

Application note:

- Identification data verification is necessary to ensure that the received additional code is targeting the TOE and that its version is compatible with the TOE version.
- Confidentiality protection must be enforced during the transmission of the additional code to the TOE for loading. Direct encryption of the additional code ensures confidentiality.

FMT_MSA.3/OS-UPDATE Security attribute initialization

FMT_MSA.3.1/OS-UPDATE The TSF shall enforce the OS Update Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/OS-UPDATE The TSF shall allow the OS Developer to specify alternative initial values to override the default values when an object or information is created.

Application Note:

- The additional code signature verification status must be set to "Fail" by default. This prevents installation of any additional code until the additional code signature is successfully verified by the TOE.

FMT_SMR.1/OS-UPDATE Security roles

FMT_SMR.1.1/OS-UPDATE The TSF shall maintain the roles **OS Developer, Issuer**.

FMT_SMR.1.2/OS-UPDATE The TSF shall be able to associate users with roles.

FMT_SMF.1/OS-UPDATE Specification of Management Functions

FMT_SMF.1.1/OS-UPDATE The TSF shall be capable of performing the following management functions: **activation of additional code**.

Application Note:

- Once verified and installed, additional code needs "to be activated" to become effective. Activation occurs by verifying the CRC of the loaded information.
- CRC algorithm is implemented by SW in a secure way.

FIA_ATD.1/OS-UPDATE User attribute definition

FIA_ATD.1.1/OS-UPDATE The TSF shall maintain the following list of security attributes belonging to individual users: **additional code ID for each activated additional code.**

Refinement: "Individual users" stands for additional code.

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: *none*].

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**.

Application Note:

- During the transmission of the additional code to the TOE for loading, the confidentiality is ensured through direct encryption of the additional code.

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 in CBC mode*] and cryptographic key sizes [**assignment:** *128 bits*] that meet the following: [**assignment:** *FIPS 197 standard*].

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-CMAC*] and cryptographic key sizes [**assignment**: *128 bits*] that meet the following: [**assignment:** *FIPS 197 and SP800-38B*].

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

FPT_FLS.1.1/OS-UPDATE The TSF shall preserve a secure state when the following types of failures occur: **interruption or incident, which prevents the forming of the Updated TOE**.

Application Note:

- The OS Update operation must either be successful or fail securely. There are 3 steps in an OS Update operation.
    - Step 1: Loading
    - Step 2: Activation
    - Step 3: Update of TOE identification data

  Steps 2 and 3 are performed automatically, so that the TOE active code and identification data always remain consistent.

- If a failure (interruption or incident) occurs during step 1, then the TOE remains in its initial state (no update, neither of code nor of the TOE identification data).
- If a failure (interruption or incident) occurs during the atomic sequence step 2/ step 3, then the enforced behavior depends on the nature of the update.
    - In any case, only two possible secure states are possible at any given time:
        - Either activation is not done, and TOE identification data is not updated.
        - Alternatively, the atomic sequence completes successfully, the OS update is activated, and the TOE identification data is updated accordingly.

7.2.8 Underlying Platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide [assignment: *test process before TOE Delivery*] with the capability to store [assignment: *the Initialization Data, Pre-personalization Data [*assignment: *none]*] in the [assignment: *chip non-volatile memory*].

Application Note:

- Initialization and Pre-personalization data is prepared before TOE delivery but is loaded in Device OEM manufacturer factory. Personalization data consistency and self-test processes are performed at this manufacturing stage.
- The integrity and uniqueness of the unique identification of the TOE must be supported by the development, production and test environment.
- The test process is running under control of the test-personnel.

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**:

- *None of the contents of Java Card static fields, instance fields and array positions that fall under the scope of an open transaction.*
- *None of the Java Card objects that were allocated into the scope of an open transaction.*
- *None of the contents of Java Card transient objects.*
- *None of the 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 Function recovery

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

7.3 Security Functional Requirements Rationale

7.3.1 SFRs for eUICC rationale

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

7.3.2 SFRs for Runtime Environment rationale

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

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

The next table shows the objectives related to [PP-eUICC] runtime environment and its translation according to [PP-eUICC] application note for OE.RE* objectives.

The security functional requirements rationale of O.RE* will be the same that the rationale for the objectives translated from JavaCard PP [PP-JCS] and are not repeated here. In case of O.CARD-MANAGEMENT, the SFR rationale is based on [PP-GP] for the GP-related SFRs included in this ST (see the GP/RE coverage table), and complemented by the PP-JCS (CM) and OS/IC SFR rationales where the TOE uses equivalent mechanisms.

The rationale from [PP-GP] is used as a basis for the GlobalPlatform-related SFRs that are claimed by this ST. [PP-GP] also mentions the components FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FIA_UID.1/GP, FMT_MSA.1/GP and FPT_RCV.3/GP. These components are not claimed as separate SFRs in this ST because their security functionality is already addressed by claimed SFRs, as follows:

• **FDP_IFC.2/GP-ELF and FDP_IFF.1/GP-ELF:** covered by the CAP/ELF loading controls already claimed in **FDP_IFC.2/CM** and **FDP_IFF.1/CM**.

• **FIA_UID.1/GP:** identification timing is already enforced for GP management actions by **FIA_UID.1/CM** (GP operations are mediated through SD selection / secure channel context).

• **FMT_MSA.1/GP:** management of GP-related security attributes is already covered by **FMT_MSA.1/CM** together with GP default/initialisation controls (e.g., **FMT_MSA.3/GP** as claimed).

• **FPT_RCV.3/GP:** recovery/atomicity properties relied on by GP operations are covered by **FPT_RCV.3/OS** and **FPT_RCV.4** (OS atomicity/memory-management support).

RE Objectives	Translation from JavaCard PP [PP-JCS] and GP PP [PP-GP]
O.RE.PRE-PPI	O.INSTALL, O.DELETION, O.LOAD, O.CARD-MANAGEMENT
O.RE.SECURE-COMM	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, OE.VERIFICATION, O.ARRAYS_VIEWS_CONFID, O.ARRAY_VIEWS_INTEG, OE.CODE_EVIDENCE
O.RE.API	O.CARD-MANAGEMENT, O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM, OE.VERIFICATION, OE.CODE_EVIDENCE
O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.ARRAYS_VIEWS_CONFID, OE.VERIFICATION
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE, O.ARRAY_VIEWS_INTEG, OE.CODE_EVIDENCE, OE.VERIFICATION
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT
O.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE, OE.VERIFICATION, OE.CAP_FILE
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
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 (the TOE preserves a secure state when upon interruption or incident, which prevents the forming of the Updated TOE)

O.TOE_IDENTIFICATION	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
O.CONFID-UPDATE-IMAGE.LOAD	FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS-Update Access Control Policy, ensuring that only authorized subjects may request the loading, installation or activation of additional code. FMT_MSA.3/OS-UPDATE guarantees that the security attributes supporting the OS Update Access Control Policy are initialised with safe default values. FMT_SMR.1/OS-UPDATE maintains the OS Developer and Issuer roles, which are permitted to decrypt and verify the signature of an update package before any Load, Install or Activation operation. FMT_SMF.1/OS-UPDATE lists the management functions that control activation of additional code. FTP_TRP.1/OS-UPDATE provides a trusted path for transferring the update image to the TOE. FCS_COP.1/OS-UPDATE-DEC specifies the cryptographic algorithm and key length used to decrypt the update image inside the TOE, ensuring that the code remains confidential until integrity and authenticity check pass.
O.AUTH-LOAD-UPDATE-IMAGE	FDP_ACC.1/OS-UPDATE enforces the OS Update Access Control Policy on the eligibility, loading, installation and activation of additional code. FCS_COP.1/OS-UPDATE-VER requires the TSF to authenticate each update image by validating its digital signature before allowing the image to be loaded.

Table 40 - Runtime Environment objectives conversion for SFR rationale

OS.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.

7.3.3 SFRs for Underlying platform IC rationale

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

O.IC.RECOVERY coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for recovery operations as dealt with in FPT_RCV.3/OS and FPT_RCV.4, for secure state preservation against security violations as in FPT_FLS.1/Platform_services.

O.IC.SUPPORT coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for secure low-level cryptographic processing as in FCS_CKM.1, FCS_CKM.6, FCS_COP.1/TDES_CIPHER, FCS_COP.1/AES_CIPHER, FCS_COP.1/CRC, FCS_COP.1/ECDH, FCS_COP.1/ECDSA_SIGN, FCS_COP.1/HASH and FCS_COP.1/HMAC and random number generation as in FCS_RNG.1.

7.3.4 SFRs dependency rationale

SFRs	CC Dependencies	Satisfied dependencies
FIA_UID.1/EXT	No Dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_UAU.4/EXT	No Dependencies	
FIA_UID.1/MNO-SD	No Dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_ATD.1	No Dependencies	
FIA_API.1	No Dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	No Dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP, FPT_TDC.1/SCP
FPT_TDC.1/SCP	No Dependencies	
FDP_UCT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP

FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1/GP-SCP, FCS_CKM.6/SCP-SM, FCS_RNG.1
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	
FCS_RNG.1	No Dependencies	
FPT_EMS.1/Base	No Dependencies	
FDP_SDI.1/Base	No Dependencies	
FDP_RIP.1/Base	No Dependencies	
FPT_FLS.1/Base	No Dependencies	

FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.1/RULES	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/SCP, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ECASD, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_SMF.1/Base	No Dependencies	
FMT_SMR.1/Base	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Platform_services, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS, FMT_SMR.1/Base, FMT_MSA.1/RAT
FCS_COP.1/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and FCS_CKM.6	FDP_ITC.2/SCP, FCS_CKM.6/Mobile_network
FCS_CKM.2/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or	FDP_ITC.2/SCP

	FDP_ITC.2 or FCS_CKM.5)	
FDP_ACC.2/FIREWALL	(FDP_ACF.1)	FDP_ACF.1/FIREWALL
FDP_ACF.1/FIREWALL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/FIREWALL, FMT_MSA.3/FIREWALL
FDP_IFC.1/JCVM	(FDP_IFF.1)	FDP_IFF.1/JCVM
FDP_IFF.1/JCVM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/JCVM, FMT_MSA.3/JCVM
FDP_RIP.1/OBJECTS	No Dependencies	
FMT_MSA.1/JCRE	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, **See rationale** FMT_SMR.1/JC
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_SMF.1/CM, FMT_SMR.1/JC
FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1/JC
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1/JC
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM, FMT_SMR.1/JC
FMT_SMF.1/JC	No Dependencies	
FMT_SMR.1/JC	(FIA_UID.1)	FIA_UID.2/AID
FCS_CKM.1/EC	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_CKM.3) and (FCS_RBG.1 or	FCS_COP.1/ECDSA_SIGN, FCS_COP.1/ECDH, FCS_CKM.3, FCS_RNG.1, FCS_CKM.6/RE

	FCS_RNG.1) and (FCS_CKM.6)	
FCS_CKM.1/GP-SCP	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_CKM.3) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1/GP-SCP, FCS_CKM.3, FCS_RNG.1, FCS_CKM.6/RE
FCS_CKM.3	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FCS_CKM.1/EC, FCS_CKM.1/GP-SCP
FCS_CKM.6/RE	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1/EC, FCS_CKM.1/GP-SCP
FCS_COP.1/TDES_MAC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE
FCS_COP.1/AES_MAC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE
FCS_COP.1/ECDH	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE

	(FCS_CKM.3) and (FCS_CKM.6)	
FCS_COP.1/CRC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	**See rationale**
FCS_COP.1/ECDSA_SIGN	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE
FCS_COP.1/GP-SCP	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/GP-SCP, FCS_CKM.3, FCS_CKM.6/RE
FCS_COP.1/TDES_CIPHER	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE
FCS_COP.1/AES_CIPHER	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE

FCS_COP.1/Hash	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	**See rationale**
FCS_COP.1/HMAC	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and (FCS_CKM.3) and (FCS_CKM.6)	FCS_CKM.1/EC, FCS_CKM.3, FCS_CKM.6/RE
FDP_RIP.1/ABORT	No Dependencies	
FDP_RIP.1/APDU	No Dependencies	
FDP_RIP.1/bArray	No Dependencies	
FDP_RIP.1/GlobalArray	No Dependencies	
FDP_RIP.1/KEYS	No Dependencies	
FDP_RIP.1/TRANSIENT	No Dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAA.1)	**See rationale**
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPT_FLS.1/JC	No Dependencies	
FPT_TDC.1	No Dependencies	
FIA_ATD.1/AID	No Dependencies	
FIA_UID.2/AID	No Dependencies	
FIA_USB.1/AID	(FIA_ATD.1/AID)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/CM, FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ITC.2/Installer	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and	FDP_IFC.2/CM, FPT_TDC.1/GP,

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

FMT_MSA.3/CM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/CM, FMT_SMR.1/CM
FMT_SMF.1/CM	No Dependencies	
FMT_SMR.1/CM	(FIA_UID.1)	FIA_UID.1/CM
FTP_ITC.1/CM	No Dependencies	
FPT_FLS.1/GP	No Dependencies	
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/CM, FDP_IFC.2/GP-KL
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/CM
FMT_SMF.1/GP	No Dependencies	
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FPT_TDC.1/GP FTP_ITC.1/GP
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL, FPT_TDC.1/GP, FTP_ITC.1/GP
FIA_AFL.1/GP	(FIA_UAU.1)	FIA_UAU.1/GP
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/CM
FIA_UAU.4/GP	No Dependencies	
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FDP_IFC.2/GP-KL, FTP_ITC.1/GP
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/CM, FDP_IFC.2/GP-KL, FTP_ITC.1/GP
FTP_ITC.1/GP	No Dependencies	
FPR_UNO.1/GP	No Dependencies	
FPT_TDC.1/GP	No Dependencies	
FDP_IFC.2/GP-KL	(FDP_IFF.1)	FDP_IFF.1/GP-KL

FDP_IFF.1/GP-KL	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-KL, FMT_MSA.3/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/CM, FMT_SMR.1/CM
FDP_ACC.1/OS-UPDATE	(FDP_ACF.1)	FDP_ACF.1/OS-UPDATE
FDP_ACF.1/OS-UPDATE	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE
FMT_MSA.3/OS-UPDATE	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1/OS-UPDATE **See rationale**
FMT_SMR.1/OS-UPDATE	(FIA_UID.1)	FIA_UID.1/CM
FMT_SMF.1/OS-UPDATE	No Dependencies	
FIA_ATD.1/OS-UPDATE	No Dependencies	
FTP_TRP.1/OS-UPDATE	No Dependencies	
FCS_COP.1/OS-UPDATE-DEC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FDP_ITC.2/GP-ELF, FCS_CKM.6
FCS_COP.1/OS-UPDATE-VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FDP_ITC.2/GP-ELF, FCS_CKM.6
FPT_FLS.1/OS-UPDATE	No dependencies	
FAU_SAS.1	No Dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4	No Dependencies	
FIA_UID.1/IPAe	No Dependencies	
FIA_UAU.1/IPAe	(FIA_UID.1)	FIA_UID.1/IPAe
FIA_USB.1/IPAe	(FIA_ATD.1)	FIA_ATD.1/IPAe
FIA_UAU.4/IPAe	No Dependencies	
FIA_ATD.1/IPAe	No Dependencies	
FDP_IFC.1/IPAe	(FDP_IFF.1)	FDP_IFF.1/IPAe

FDP_IFF.1/IPAe	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/IPAe
FTP_ITC.1/IPAe	No Dependencies	
FDP_ITC.2/IPAe	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/IPAe, FTP_ITC.1/IPAe, FPT_TDC.1/IPAe
FPT_TDC.1/IPAe	No Dependencies	
FDP_UCT.1/IPAe	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/IPAe, FTP_ITC.1/IPAe
FDP_UIT.1/IPAe	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/IPAe, FTP_ITC.1/IPAe
FCS_CKM.1/IPAe	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1, FCS_CKM.6/IPAe, FCS_RNG.1
FCS_CKM.6/IPAe	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/IPAe
FPT_EMS.1/IPAe	No Dependencies	
FDP_SDI.1/IPAe	No Dependencies	
FDP_RIP.1/IPAe	No Dependencies	

FMT_SMF.1/IPAe	No Dependencies	
FMT_SMR.1/IPAe	(FIA_UID.1)	FIA_UID.1/IPAe

Table 41 - SFRs dependencies

Rationale for the exclusion of dependencies:

- **The dependency FMT_SMF.1/Base of FMT_MSA.1/JCRE is unsupported.**
  - The dependency between FMT_MSA.1/JCRE and FMT_SMF.1/Base is not satisfied because no management functions are required for the Java Card RE.
- **The dependencies of FCS_COP.1/Hash are unsupported**
  - Hash operation does not require any key.
- **The dependencies of FCS_COP.1/CRC are unsupported**
  - CRC operations do not require any key.
- **The dependency FAU_SAA.1 of FAU_ARP.1 is unsupported**
  - The dependency of FAU_ARP.1 assumed that a "potential security violation" generates an audit event. On the contrary, the events listed in FAU_ARP.1 are self-contained (arithmetic exception, bad formed bytecodes, access failure) and ask for a straightforward reaction of the TSFs on their occurrence at runtime.
  - The JCVM or other components of the TOE detect these events during their usual working order. Thus, there is no mandatory audit recording in this ST.
- **The dependency FIA_UID.1 of FMT_SMR.1/ADEL is unsupported**
  - This Security Target does not require the identification of the "deletion manager" since it can be considered as part of the TSF.
- **The dependency FMT_MSA.1 of FMT_MSA.3/OS-UPDATE is unsupported.**
  - No history information is managed by the TOE.

7.3.5 SAR Refinement

ADV_ARC – Security Architecture Refinements

The Security Architecture description shall demonstrate how its design and implementation prevent the bypass of Security Functional Requirements (SFRs) against side-channel attacks, in accordance with the O.RE.DATA-CONFIDENTIALITY refinement from [PP-eUICC].

8. TOE Summary Specification

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

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

8.1 eUICC Security Functions

8.1.1 GSMA.Security

This Security Function provides User data and TSF self-protection measures:

- TOE emanation.
- Residual data protection.
- Preservation of secure state.
- Resistance to side channels attacks.
- Detection of physical tampering.

This Security Function provides resistance to side channel attacks by enforcing protection of secret data of the TOE during cryptographic or comparison of secret data of the TOE and against state-of-art attacks that are based on external observable physical phenomenon of the TOE.

The TOE hides information about IC power consumptions and command execution time such that no confidential information can be derived from this data.

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

- Deletion of applet instances and/or CAP files.
- In case of failures of PRE, PPI or Telecom Framework.
- Any reference to an object instance created during an aborted transaction.
- Sensitive temporary buffers (transient object, bArray object, APDU buffer, Cryptographic buffer) are securely cleared after their usage with respect to their life cycle and interface as defined in [JCRE].
- Transient objects and persistent objects are made inaccessible upon deallocation of the object.

The card is muted upon detection of a potential security violation such that the TOE preserves a secure state in the next cases:

- When platform or content management operations fail (i.e.):
    - Failure of creation of a new ISD-P by ISD-R.

  - Failure of installation of a new profile by ISD-R.
  - The installer fails to load/install an applet.
  - The applet deletion manager fails to delete an applet.
  - The object deletion functions fail to delete all the unreferenced objects owned by the applet that requested the execution of the method.
- Failures that lead to a potential security violation during the processing of a O.RE.PRE-PPI or Telecom API specific functions.
- Failures detected during OS updates.
- Detection of a potential security violation.

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

8.1.2 GSMA.ProfileManagement

This security function (SF) implements the controls related to profiles management as defined by [SGP.32] and [EUPP], encompassing the following operations:

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

It also supports everything related to profile data isolation.

8.1.3 GSMA.ECASD

This security function manages the Embedded UICC Controlling Authority Security Domain (ECASD) as defined in [SGP.32]. The ECASD securely stores credentials necessary for supporting the required Security Domains on the eUICC.

This includes ECASD installation, provisioning, eUICC authentication, and credentials management.

8.1.4 GSMA.ISDR

The security function handles the ISD-R management as defined in [SGP.32]. The ISD-R is responsible for the creation of new ISD-Ps and lifecycle management of all ISD-Ps.

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

8.1.5 GSMA.ISDP

This security function manages the ISD-P according to [SGP.32]. The ISD-P is the on-card representative of the SD-DP+ and is a secure container (Security Domain) for hosting a Profile.

The ISD-P collaborates with the Profile Package Interpreter to download and install Profiles, decoding and interpreting the received Profile Package.

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

8.1.6 GSMA.PPR

This security function manages Profile Policy Rules (PPRs) as defined in [SGP.32]. Profile Owners define PPRs, which are set by the SM-DP+ in the Profile Metadata.

When a profile with defined PPRs is downloaded, the eUICC must follow these rules.

This includes secure management and processing of PPRs.

8.1.7 GSMA.AccessControl

This Security Function is responsible for enforcing the following security policies to control the flow of information between subjects and to control the access to objects by subjects listed below:

- ISD-R access control.
- ISD-P content access control.
- ECASD access control.
- FIREWALL access control.
- ADEL access control.
- JCVM access control.
- CAP FILE LOADING information flow control.

The TOE provides security management measures:

- Management of security attributes such as Platform Data with restrictive default values.
- Management of roles and security functions.

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

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

The TOE requires each user to identify itself before allowing Security Function actions on behalf of that user. The Security Function associates user security attributes with subjects acting on behalf of that user. The TSF accepts only secure values for security attributes.

The TOE requires each user to be successfully authenticated before allowing Security Functions actions on behalf of that user. Cryptographic mechanisms used for the authentication are covered. This Security Function prevents reuse of authentication data.

The Security Function ensures that unauthorized actors shall not get access to or change cryptographic keys. Modification of Security Domain is restricted to its corresponding owner. Only legitimate users can access or change its confidential or integrity sensitive data.

This Security Domain separation capability relies upon the Runtime Environment protection applications implemented by the FIREWALL access control and the JCVM information flow control.

8.1.8 GSMA.Integrity

This Security Function provides protection from integrity errors because initializes the checksum of cryptographic keys, PIN values and their associated security attributes and monitors cryptographic keys, PIN values and their associated security attributes stores within the Security Functions for integrity errors by secure verification of the checksum.

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

8.1.9 GSMA.IPAe

This security function implements the IoT Profile Assistant embedded in the eUICC operating system (IPAe) and enables secure interaction with remote RSP entities (SM-DP+ and SM-DS) and the eIM for triggering and managing profile download and lifecycle operations in unattended IoT devices.

This Security Function provides the following security services for IPAe:

Identification and authentication of external (remote) users (U.SM-DP+, U.SM-DS, U.EIM), allowing only limited pre-authentication actions (e.g., application selection and requesting data that identifies the eUICC), and requiring successful identification/authentication before any other TSF-mediated actions.

User-subject binding by associating remote user identities (e.g., SM-DP+ OID, SM-DS OID, eIM ID) to the local IPAe subject (S.IPAe) acting on behalf of these users, and maintaining the corresponding user security attributes (e.g., certificates used for server authentication).

Enforcement of the IPAe information flow control policy for command and data exchanges between U.SM-DP+, U.SM-DS, U.EIM and S.IPAe, including explicit denial of communications that are not protected by the required secure channel.

Provision of trusted channels from IPAe to remote entities using TLS/DTLS (or equivalent) in server authentication mode (including the mandated cipher suite/protocol constraints where applicable), protecting channel data from disclosure and modification, and supporting integrity/replay protection for exchanged commands and downloaded objects (e.g., Bound Profile Packages).

Secure import and consistent interpretation of IPAe-related commands and downloaded objects received from remote entities, ensuring unambiguous association of security attributes with received data and correct interpretation of these attributes.

Cryptographic key management for IPAe channel protection, including generation of IPAe key material (D.IPAe_KEYS) used for session establishment, and secure destruction of IPAe key material when no longer needed (including secure wipe of temporary buffers as appropriate).

Protection of IPAe assets by monitoring integrity-sensitive stored data related to IPAe (e.g., device/management data and IPAe key material), and ensuring residual information protection for IPAe key material upon deallocation.

Support of IPAe management functions, including management of authentication state and authorized IPAe-triggered profile lifecycle operations (enable/disable/delete), as well as management of Associated eIM information and retrieval of an eIM Package.

8.2 Runtime Environment Security Functions

8.2.1 GP.CardContentManagement

This security function provides the capability and a dedicated flow control for loading, installing, extracting, updating the registry, selecting, and removing card content, especially executable files and application instances.

These features are offered to the Card Issuer and its business partners, allowing the Card Issuer to delegate card content management to an Application Provider based on privileges assigned to the various security domains on the card.

The security function supports Delegated management (DM), Authorized management (AM), and can use DAP or Mandated DAP verification and generation of Reception tokens. It also checks that only the card management commands specified and allowed for each state of the smart card's life cycle are accepted, rejecting ill-formed commands with appropriate error responses.

Content changes are permitted based on the privileges assigned to the acting Security Domain, which holds cryptographic keys used for Secure Channel Protocol operations and/or authorized platform management functions. Before performing platform or content management operations, the TOE verifies that the off-card entity has been successfully authenticated and a Secure Channel Session has been initiated.

8.2.2 GP.KeyLoading

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

8.2.3 GP.SecurityDomain

This security function manages security domains, including creation, selection, privilege setting, and deletion within the SD hierarchy.

It enables the association or extradition of an application to or from a security domain to provide services (such as secure channels) to the dedicated application without sharing the related keys stored in the SD.

The function also manages key sets within security domains, including creation, deletion, importation, replacement, and deletion of keys within key sets.

Security Domains are privileged applications as defined in [GPCS], holding cryptographic keys to be used to support Secure Channel Protocol operations and/or to authorize card content management functions.

The are different types of Security Domains with dedicated privileges and associated operations: ISD Security Domain, Supplementary Security Domains and Controlling Authority Security Domains.

8.2.4 GP.SecureChannel

This security function provides a secure communication channel between a card and an off-card entity during an Application Session according to [GPCS], [TS 102.225] and [TS 102.226].

Trusted channels protect against unauthorized disclosure, modification, or replay. The security function ensures that incoming messages are transmitted unaltered to the corresponding Security Domain and that response messages are properly returned to the off-card entity.

Applications may use the Secure Channel Protocols supported by their associated Security Domain to securely exchange information with the off-card entity.

This security function provides APDU flow control, checking command security levels based on the Card Life Cycle and APDU type.

A Secure Channel Session is divided into three sequential phases:

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

The following services are provided by the Secure Channel:

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

The following Secure Channel Protocols are supported by the TOE: SCP02, SCP03, SCP03(t), SCP-SGP.22, SCP80 and SCP81.

8.2.5 GP.GPRegistry

The Security function provides management and access to the GlobalPlatform Registry used for:

- Store card management information.
- Store relevant application management information (AID, associated Security Domain and Privileges).
- Support card resource management data.

- Store Application Life Cycle information.
- Store card Life Cycle information.
- Track any counters associated with logs.

The content of the GlobalPlatform Registry may be accessed by administrative command or by applet using a dedicated GlobalPlatform API.

Only secure values are accepted for the information stored in the GlobalPlatform registry (including Life Cycle states, Security Levels and Privileges).

8.2.6 GP.OSU

This security function implements an OS Update capability using a proprietary mechanism, allowing the eSIM OS to be updated post-issuance.

OS Updates are performed by loading, installing, and activating related ELFs, following the same rules as for any other ELF. DAP verification is mandatory for ELFs containing OS updates, ensuring the authenticity and integrity of the code update. The content of the ELF is directly encrypted with a dedicated encryption key, protecting confidentiality.

Both the DAT signature verification key and the encryption key are proprietary keys, meaning OS updates can only be issued and decrypted by VALID.

The TOE's identification data must be verified before allowing any OS update. The entire OS update operation is performed through an atomic process, ensuring permanent consistency between the eSIM's active code and its identification data.

The OS update operation must either be successful or fail securely. There are 3 steps in an OS Update operation:

- Step 1: Loading
- Step 2: Activation
- Step 3: Update of the TOE Identification data
    - Steps 2 and 3 are performed atomically, so that the TOE active code and identification data always remain consistent.

If a failure (interruption or incident) occurs during step 1 (loading), then the TOE remains in its initial state (no update, neither of code nor of the TOE identification data).

If a failure (interruption or incident) occurs during the atomic sequence step 2/3 (activation and update of TOE identification data), then the enforced behavior depends on the nature of the update:

- In any case, two possible secure states are possible:
    - Either activation in not done and the TOE identification data is not updated.
    - If the atomic sequence is completed successfully, the OS update is activated, and the TOE identification data is updated.

8.2.7 JCS.APDUBuffer

The Security function maintains a byte array buffer accessible from any applet context. This buffer is used to transfer incoming APDU header and data bytes as well as outgoing data.

The APDU class API is designed to be transport protocol independent T=0 (as defined in ISO 7816-3).

APDU buffer is a JCRE temporary entry point object where no associated reference can be stored in a variable or an array component.

8.2.8 JCS.ByteCodeExecution

This security function handles applet bytecode execution.

The JCVM execution involves JCVM interpreter startup, bytecode execution, and the JCVM interpreter loop. The applet bytecode execution loop consists of:

- Fetching the next bytecode to be executed by the applet to make a flow control.
- Decoding the next bytecode.
- Executing the fetched bytecode.

The JCVM manages several types of objects, including persistent objects, transient objects, persistent arrays (Boolean, byte, short, int, or reference), transient arrays (Boolean, byte, short, int, or reference), and static field images.

For each type of object, different types of control are performed.

8.2.9 JCS.Firewall

This Security Function enforces a Firewall access control policy and a JCVM information flow control policy runtime.

It defines how accessing to the following items:

- Static Class Fields.
- Array Objects.
- Class Instance Object Fields.

- Class Instance Object Methods.
- Standard Interface Methods.
- Shareable interface Methods.
- Classes.
- Standard Interfaces.
- Shareable Interfaces.
- Array Objects Methods.

Based on security attributes (Sharing, Context, Lifetime), the JCRE performs access control for object fields between objects, throwing security exceptions when access is denied.

This enforces applet isolation between different packages and controls access to global data containers shared by all applet instances.

The JCRE allocates and manages a context containing applets. The JCRE maintains special system privileges for its own context, allowing it to perform operations that are denied to applet contexts.

8.2.10 JCS.Package

This Security Function manages packages. A package is a structural item defined by a context composed by:

- Naming
- Loading
- Storing
- Execution

There are rules for package identification, structure check and access rules definition.

If inconsistent items are found during checks, an error message is sent or a security exception is triggered.

8.2.11 JCS.CryptoAPI

The Security Function offers the following cryptographic services:

- Generation of random numbers to be used for key values or challenges during external exchanges. The RNG (Random Number Generator) is conformant to [AIS31], providing enhanced backward secrecy & enhanced forward secrecy. It passes [AIS31] test procedure A.
- Encryption and decryption using TDES algorithm. Both TDES 2-keys (112 bits key length) and TDES 3-Keys (168 bits key length) are supported. Encryption and decryption using AES (128, 192 and 256 bits key length) algorithm is also defined.

- Generation of 16, 24 and 32 bytes MAC using AES algorithm (128, 192 and 256 bits key length) in CBC mode.
- Generation of 4 and 8 bytes MAC using TDES algorithm (112 bits key length).
- Computation of checksum CRC16 and CRC32 conformant with ISO3309.
- Data hash computation.
- HMAC computation.
- Generation and verification of ECDSA signatures. Elliptic curve cryptographic over GF(p) is considered here, with P ranging from 224 to 521 bits.
- Secret key agreement according to the ECDH algorithm.

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

8.2.12 JCS.KeyManagement

This Security Function enforces key management for the following associated operations:

- Key building and generation: implemented through ECDSA Key Pair Generation (P ranging from 224 to 521 bits).
- Key importation: is done using method protecting confidentiality and integrity of key.
- Key exportation: is done using method protecting confidentiality and integrity of key.
- Key masking: protects the confidentiality of cryptographic keys from being read out from the memory. It ensures the service of accessing and modifying them.
- Key destruction: disables the use of the key both logically and physically. Reuse is only possible after erasing.

8.2.13 JCS.OwnerPIN

This security function supports the user identification and authentication mechanisms used by the eUICC functionalities within the scope of evaluation.

It enables the creation and secure storage of a PIN in persistent memory. Access to the PIN value is restricted to secure comparisons between the stored PIN and a received parameter.

The method returns a positive result if a valid PIN has been presented during the current session. If the PIN is not blocked and the comparison is successful, the validated flag is set to true, and the try counter is set to its maximum. Otherwise, authentication fails, and the associated try counter is decreased.

When the validated flag is set, it is assumed that the user is authenticated.

If the try counter reaches zero, the PIN is blocked, and further authentication is not possible until the PIN is unblocked.

8.2.14 JCS.EraseResidualData

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

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

Temporary buffers (transient objects, bArray objects, Global Array objects, APDU buffers, and Cryptographic buffers) are securely cleared after their usage, respecting their life cycle and interface as defined in [JCRE3]. Transient objects are erased upon reset or allocation, while persistent objects are erased when space is needed for allocating new objects.

8.2.15 JCS.OutOfLifeDataUndisclosure

This Security Function ensures that sensitive data are locked until postponed erasure on the following operation:

- Deletion of persistent and transient objects according to [JCRE3].

8.2.16 JCS.RunTimeExecution

This Security Function provides a secure run time environment conformant to [JCRE3] and deals with:

- Instance registration or deletion.
- Application selection.
- Applet opcode execution.
- Logical channel management.
- APDU flow control, dispatch and buffer management.
- JCRE memory and context management.
- JCRE reference deletion.
- JCRE access rights.
- JCRE throw exception.
- JCRE security reaction.

8.2.17 JCS.Exception

This Security Function manages throwing of an instance of Exception class in the following cases:

- SecurityException when an illegal access to an object is detected.
- SecurityException with an error code describing the error condition.
- CryptoException in case of algorithm error or illegal use.
- Any exception decided by the applet or the JCRE handled as temporary JCRE entry point object. It also offers a means to applet to handle exceptions and to JCRE to handle uncaught exception by applets.

8.2.18 OS.Atomicity

This security function performs write operations atomically using the JavaCard Transaction and Atomicity mechanism, with commit and rollback capabilities for updating persistent objects in flash memory to prevent incomplete updates.

Update operations either complete successfully or restore the data to its original pre-transaction state if the transaction fails to complete. Before writing, data is stored in an atomic backup area.

A transaction exception is thrown if the commit capacity is exceeded during a transaction. The rollback operation restores the original values of the persistent objects and clears the dedicated transaction area.

8.2.19 OS.MemoryManagement

This security function allocates memory areas and performs access control to prevent unauthorized access.

It manages circular writing to avoid unstable memory states and enforces memory recovery in case of error detection.

It also offers confidentiality services for data storage when required.

8.3 Summary Specifications Rationale (TSS)

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

8.3.1 eUICC SFRs coverage

SFR (Security Functional Requirement)	Coverage by TSS Security Functions
FIA_UID.1/EXT	This SFR is covered by GSMA.ISDR, GSMA.AccessControl, GSMA.ECASD and GP.SecureChannel.

FIA_UAU.1/EXT	This SFR is covered by GSMA.ECASD, GSMA.AccessControl, GP.SecureChannel and GSMA.ISDR.
FIA_USB.1/EXT	This SFR is covered by GSMA.ECASD, GSMA.AccessControl and GP.SecurityDomain.
FIA_UAU.4/EXT	This SFR is covered by GSMA.ECASD, GSMA.AccessControl and GP.SecureChannel.
FIA_UID.1/MNO-SD	This SFR is covered by GP.SecurityDomain and GSMA.AccessControl.
FIA_USB.1/MNO-SD	This SFR is covered by GP.SecurityDomain, GSMA.ISDP, GSMA.ECASD and GSMA.AccessControl.
FIA_ATD.1/Base	This SFR is covered by GP.SecurityDomain, GSMA.AccessControl and GSMA.ECASD.
FIA_API.1.1	This SFR is covered by GSMA.ECASD.
FDP_IFC.1/SCP	This SFR is covered by GSMA.ProfileManagement.
FDP_IFF.1/SCP	This SFR is covered by GSMA.ProfileManagement.
FTP_ITC.1/SCP	This SFR is covered by GSMA.ProfileManagement and GP.SecureChannel.
FDP_ITC.2/SCP	This SFR is covered by GSMA.ProfileManagement.
FPT_TDC.1/SCP	This SFR is covered by GSMA.ProfileManagement and GSMA.AccessControl.
FDP_UCT.1/SCP	This SFR is covered by GSMA.ProfileManagement.
FDP_UIT.1/SCP	This SFR is covered byGSMA.ProfileManagement.
FCS_CKM.1/SCP-SM	This SFR is covered by GSMA.ProfileManagement and JCS.CryptoAPI for ECKA-EG.
FCS_CKM.2/SCP-MNO	This SFR is covered by JCS.CryptoAPI.
FCS_CKM.6/SCP-SM	This SFR is covered by JCS.KeyManagement.
FCS_CKM.6/SCP-MNO	This SFR is covered by JCS.KeyManagement.
FDP_ACC.1/ISDR	This SFR is covered by GSMA.ISDR and GSMA.AccessControl.
FDP_ACF.1/ISDR	This SFR is covered by GSMA.ISDR and GSMA.AccessControl.
FDP_ACC.1/ECASD	This SFR is covered by GSMA.ECASD and GSMA.AccessControl.
FDP_ACF.1/ECASD	This SFR is covered by GSMA.ECASD and GSMA.AccessControl.
FDP_IFC.1/Platform_services	This SFR is covered by GSMA.ProfileManagement.
FDP_IFF.1/Platform_services	This SFR is covered by GSMA.ProfileManagement.

FPT_FLS.1/Platform_services	This SFR is covered by GSMA.Security.
FCS_RNG.1	This SFR is covered by JCS.CryptoAPI providing AIS31 PTG.2 random number generation to applets.
FPT_EMS.1/Base	This SFR is covered by JCS.CryptoAPI, GSMA.Integrity, GSMA.Security and JCS.KeyManagement.
FDP_SDI.1/Base	This SFR is covered by GSMA.ProfileManagement and GSMA.Integrity.
FDP_RIP.1/Base	This SFR is covered by GSMA.ProfileManagement and GSMA.Integrity.
FPT_FLS.1/Base	This SFR is covered by GSMA.ProfileManagement and GSMA.Security.
FMT_MSA.1/PLATFORM_DATA	This SFR is covered by GSMA.ISDR and GSMA.AccessControl.
FMT_MSA.1/RULES	This SFR is covered by GSMA.PPR.
FMT_MSA.1/CERT_KEYS	This SFR is covered by GSMA.ProfileManagement.
FMT_SMF.1/Base	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, GSMA.PPR and GSMA.AccessControl.
FMT_SMR.1/Base	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR.
FMT_MSA.1/RAT	This SFR is covered by GSMA.ISDR, GSMA.AccessControl and GSMA.PPR.
FMT_MSA.3	This SFR is covered by GSMA.ISDR, GSMA.AccessControl and GSMA.ECASD.
FCS_COP.1/Mobile_network	This SFR is covered by JCS.CryptoAPI.
FCS_CKM.2/Mobile_network	This SFR is covered by GP.KeyLoading.
FCS_CKM.6/Mobile_network	This SFR is covered by JCS.KeyManagement.
FIA_UID.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.AccessControl, GSMA.ECASD and JCS.CryptoAPI.
FIA_UAU.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.ECASD, GSMA.AccessControl and JCS.CryptoAPI.
FIA_USB.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.AccessControl and GSMA.ECASD.
FIA_UAU.4/IPAe	This SFR is covered by GSMA.IPAe and JCS.CryptoAPI.
FIA_ATD.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.ECASD and GSMA.AccessControl.

FDP_IFC.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.ProfileManagement and GSMA.AccessControl.
FDP_IFF.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.ProfileManagement and GSMA.AccessControl.
FTP_ITC.1/IPAe	This SFR is covered by GSMA.IPAe and JCS.CryptoAPI.
FDP_ITC.2/IPAe	This SFR is covered by GSMA.IPAe, GSMA.ProfileManagement and GSMA.AccessControl.
FPT_TDC.1/IPAe	This SFR is covered by GSMA.IPAe and GSMA.AccessControl.
FDP_UCT.1/IPAe	This SFR is covered by GSMA.IPAe and JCS.CryptoAPI.
FDP_UIT.1/IPAe	This SFR is covered by GSMA.IPAe and JCS.CryptoAPI.
FCS_CKM.1/IPAe	This SFR is covered by GSMA.IPAe and JCS.CryptoAPI for ECKA key agreement / key material generation.
FCS_CKM.6/IPAe	This SFR is covered by GSMA.IPAe and JCS.KeyManagement.
FPT_EMS.1/IPAe	This SFR is covered by GSMA.Security, GSMA.Integrity, JCS.CryptoAPI, JCS.KeyManagement and GSMA.IPAe.
FDP_SDI.1/IPAe	This SFR is covered by GSMA.IPAe and GSMA.Integrity.
FDP_RIP.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.Security, JCS.OutOfLifeDataUndisclosure and JCS.EraseResidualData.
FMT_SMF.1/IPAe	This SFR is covered by GSMA.IPAe, GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD and GSMA.AccessControl.
FMT_SMR.1/IPAe	This SFR is covered by GSMA.IPAe and GSMA.AccessControl.

Table 42 - eUICC SFRs coverage

8.3.2 Runtime Environment SFRs coverage

SFR (Security Functional Requirement)	Coverage by TSS Security Functions
FDP_ACC.2/FIREWALL	This SFR is covered by JCS.Firewall and GSMA.AccessControl.
FDP_ACF.1/FIREWALL	This SFR is covered by JCS.Firewall and GSMA.AccessControl.
FDP_IFC.1/JCVM	This SFR is covered by JCS.Firewall, GSMA.AccessControl and JCS.APDUBuffer controlling unauthorized access or invalid storage of reference.
FDP_IFF.1/JCVM	This SFR is covered by JCS.Firewall and GSMA.AccessControl.

FDP_RIP.1/OBJECTS	This SFR is covered by JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data) and GSMA.Security.
FMT_MSA.1/JCRE	This SFR is covered by JCS.RunTimeExecution covering context switch and application selection.
FMT_MSA.1/JCVM	This SFR is covered by JCS.ByteCodeExecution requiring context switch for specific code execution and JCS.RunTimeExecution covering context switch and modification of the Currently Active Context according to given rules.
FMT_MSA.2/FIREWALL_JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing, JCS.Firewall and GSMA.AccessControl.
FMT_MSA.3/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering object sharing and GSMA.AccessControl.
FMT_MSA.3/JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing, JCS.Firewall and GSMA.AccessControl.
FMT_SMF.1/JC	This SFR is addressed by JCS.RunTimeExecution covering context management and instance registration.
FMT_SMR.1/JC	This SFR is addressed by JCS.RunTimeExecution and GSMA.AccessControl covering JCVM and JCRE roles.
FCS_CKM.1/EC	This SFR is addressed by JCS.KeyManagement covering key generation.
FCS_CKM.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FCS_CKM.6/RE	This SFR is addressed by JCS.KeyManagement covering key deletion.
FCS_COP.1/TDES_MAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/AES_MAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/ECDH	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.

FCS_COP.1/CRC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/ECDSA_SIGN	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FCS_COP.1/TDES_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/AES_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/Hash	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FCS_COP.1/HMAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services used by the eUICC functionalities within the scope of evaluation.
FDP_RIP.1/ABORT	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/APDU	This SFR is addressed by JCS.EraseResidualData and GSMA.Security covering data erasure.
FDP_RIP.1/bArray	This SFR is addressed by JCS.OutOfLifeDataUndisclosure, GSMA.Security and JCS.EraseResidualData covering data erasure.
FDP_RIP.1/GlobalArray	This SFR is addressed by JCS.EraseResidualData and GSMA.Security covering data erasure.
FDP_RIP.1/KEYS	This SFR is addressed by JCS.EraseResidualData and GSMA.Security covering data erasure.
FDP_RIP.1/TRANSIENT	This SFR is covered by JCS.OutOfLifeDataUndisclosure and GSMA.Security managing the access control to transient object to be erased prior the erasure of the content in memory.
FDP_ROL.1/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering transaction rollback during specific operations and JCS.Firewall.

FAU_ARP.1	This SFR is addressed by JCS.RunTimeExecution, JCS.Exception, JCS.Firewall, GSMA.Security and OS.MemoryManagement covering exception handling with different specific operations.
FDP_SDI.2/DATA	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, OS.Atomicity, GSMA.Integrity and OS.MemoryManagement covering integrity handling with specific operations.
FPR_UNO.1	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, JCS.CryptoAPI, GSMA.Security and OS.MemoryManagement covering data handling with specific operations avoiding observation.
FPT_FLS.1/JC	This SFR is addressed by JCS.Exception, JCS.ByteCodeExecution, JCS.RunTimeExecution, OS.MemoryManagement and OS.Atomicity preserving a secure state when unexpected events occur during specific operations.
FPT_TDC.1	This SFR is covered by JCS.Package enforcing export check, CAP file translation and link specific operations.
FIA_ATD.1/AID	This SFR is covered by JCS.RunTimeExecution and GP.GPRegistry controlling applet registration and uninstallation.
FIA_UID.2/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing user identity (package AID) during applet selection and identify associated context provided.
FIA_USB.1/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing registration of each applet and associated package during its installation with its AID.
FMT_MTD.1/JCRE	This SFR is covered by JCS.RunTimeExecution offering services for applet registration and uninstallation managing associated access rights.
FMT_MTD.3/JCRE	This SFR is fully covered by JCS.RunTimeExecution managing presence and legacy of AID with ISO rules.
FDP_ITC.2/Installer	This SFR is covered by JCS.Package and GSMA.AccessControl.
FMT_SMR.1/Installer	This SFR is covered by JCS.Package.
FPT_FLS.1/Installer	This SFR is covered by JCS.Package and GSMA.Security.
FPT_RCV.3/Installer	This SFR is covered by JCS.Package and JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails.

FDP_ACC.2/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_ACF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_RIP.1/ADEL	This SFR is covered by GP.CardContentManagement and JCS.OutOfLifeDataUndisclosure by checking operations to avoid access to freed resources prior to its reuse.
FMT_MSA.1/ADEL	This SFR is covered by GP.GPRegistry, GP.CardContentManagement and JCS.RunTimeExecution responsible of checking rules concerning applet attributes, implicit and explicit selection rules prior to authorize deletion operation.
FMT_MSA.3/ADEL	This SFR is covered by JCS.RunTimeExecution and GP.CardContentManagement dealing with Security Attributes initialization, providing secure, restrictive default values for the security attributes of subject and objects involved in applet deletion.
FMT_SMF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.SecurityDomain and JCS.RunTimeExecution.
FMT_SMR.1/ADEL	This SFR is covered by GP.SecurityDomain maintaining the ISD and SDD roles responsible of applet deletion. This SFR is also covered by JCS.RunTimeExecution maintaining the JCRE role for applet uninstallation.
FPT_FLS.1/ADEL	This SFR is covered by GP.GPRegistry, JCS.RunTimeExecution and OS.Atomicity preserving a secure state when unexpected events occur during package or instance deletion, managing the transaction part of the deletion operation by either rolling back, or completing it.
FDP_RIP.1/ODEL	This SFR is covered by JCS.EraseResidualData and OS.MemoryManagement ensuring that the content of deleted objects is erased upon the deletion and by JCS.OutOfLifeDataUndisclosure making unavailable for disclosure upon further reallocation of the freed space.

FPT_FLS.1/ODEL	This SFR is covered by JCS.RunTimeExecution and OS.MemoryManagement performing memory management to release no more used memory on unreferenced objects and preserves a secure state when unexpected events occur during object deletion.
FCO_NRO.2/CM	This SFR is addressed by GP.SecureChannel.
FDP_IFC.2/CM	This SFR is addressed by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_IFF.1/CM	This SFR is addressed by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_UIT.1/CM	This SFR is addressed by JCS.Package.
FIA_UID.1/CM	This SFR is covered by JCS.RunTimeExecution, GP.SecureChannel and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
FMT_MSA.1/CM	This SFR is addressed by JCS.Package and GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.
FMT_MSA.3/CM	This SFR is addressed by JCS.Package.
FMT_SMF.1/CM	This SFR is addressed by JCS.Package, JCS.RunTimeExecution, GP.SecurityDomain, GP.SecureChannel and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FMT_SMR.1/CM	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain managing the roles: S.OPEN, issuer, application provider, verification authority and controlling authority.
FTP_ITC.1/CM	This SFR is addressed by GP.SecureChannel.
FPT_FLS.1/GP	This SFR is addressed by JCS.Package, JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FDP_ROL.1/GP	This SFR is addressed by GP.CardContentManagement, GP.KeyLoading and OS.Atomicity.
FCO_NRO.2/GP	This SFR is covered by GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading:

	- Mutual authentication between the external entity (Issuer or Application provider) and the selected Security Domain, including creation of a session key. - Verification of a MAC that the Issuer or Application provider attaches to each file or data block sent. Erasing the session key at the end of the session.
FMT_SMF.1/GP	- This SFR is covered by GP.SecurityDomain and GP.SecureChannel.
FDP_ITC.2/GP-ELF	This SFR is covered by JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations.
FDP_ITC.2/GP-KL	This SFR is covered by GP.KeyLoading.
FIA_AFL.1/GP	This SFR is covered by GP.SecureChannel.
FIA_UAU.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain (as for FIA_UID.1/CM).
FIA_UAU.4/GP	This SFR is covered by GP.SecureChannel.
FDP_UIT.1/GP	This SFR is covered by GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
FDP_UCT.1/GP	This SFR is covered by GP.SecureChannel which provides confidentiality protection for sensitive data (such as secret keys).
FTP_ITC.1/GP	This SFR is addressed by GP.SecureChannel.
FPR_UNO.1/GP	This SFR is covered by JCS.RunTimeExecution and JCS.CryptoAPI.
FPT_TDC.1/GP	This SFR is addressed by GP.CardContentManagement, GP.SecureChannel and GP.KeyLoading.
FDP_IFC.2/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FDP_IFF.1/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FMT_MSA.3/GP	This SFR is covered by GP.SecureChannel providing setting of the default value.
FDP_ACC.1/OS-UPDATE	This SFR is covered by GP.OSU.
FDP_ACF.1/OS-UPDATE	This SFR is covered by GP.OSU.
FMT_MSA.3/OS-UPDATE	This SFR is covered by GP.OSU.
FMT_SMR.1/OS-UPDATE	This SFR is covered by GP.OSU.

FMT_SMF.1/OS-UPDATE	This SFR is covered by GP.OSU.
FIA_ATD.1/OS-UPDATE	This SFR is covered by GP.OSU.
FTP_TRP.1/OS-UPDATE	This SFR is covered by GP.OSU.
FCS_COP.1/OS-UPDATE-DEC	This SFR is covered by GP.OSU.
FCS_COP.1/OS-UPDATE-VER	This SFR is covered by GP.OSU.
FPT_FLS.1/OS-UPDATE	This SFR is covered by GP.OSU.
FAU_SAS.1	This SFR is covered by OS.MemoryManagement.
FPT_RCV.3/OS	This SFR is covered by OS.Atomicity.
FPT_RCV.4	This SFR is covered by OS.MemoryManagement.

Table 43 - Runtime Environment SFRs coverage

9. Composition with IC

9.1 Statement of compatibility

This section provides a statement of compatibility between this Composite Security Target (Composite-ST) and the Platform Security Target (Platform-ST) of the underlying Infineon Security IC.

This statement is compliant with the requirements of [SUPP] (Supporting Document, Mandatory Technical Document, Composite Product Evaluation for Smart Card and similar Devices, May 2018, version 1.5.1).

The Platform-ST considered for the underlying IC is: IFX_CCI_00007Ah/8Fh A11/R11/M11 – Security Target Lite (Release 62 Rev 1.0, 2025-10-31).

The Platform-ST claims strict conformance to [PP-0084] and is evaluated according to [CC-1]–[CC-3] (CC:2022, Release 1) at assurance level EAL6 augmented with ALC_FLR.1 and ATE_SDP.1.

The evaluated configuration of the underlying IC for this composite TOE uses Flash Loader functionality only in controlled manufacturing/personalization phases and blocks (or permanently deactivates) Flash Loader for operational use (Phase 7). Mutual authentication of the Flash Loader is not required for operational use in the evaluated configuration.

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

- Certified microcontroller Infineon IFX_CCI_00007Ah A11/R11/M11 (SLx22 family) as defined in the Platform-ST.
- True Random Number Generation provided by the IC (FCS_RNG.1/TRNG) and, if applicable, Crypto Suite RNG services, in accordance with [AIS31].
- Cryptographic services implemented in hardware, at least AES (FCS_COP.1/AES, FCS_CKM.6/AES) and Triple DES (FCS_COP.1/TDES, FCS_CKM.6/CS/TDES), as used by the composite TOE.
- Additional cryptographic services required by the composite TOE (e.g. ECC, HMAC, Hash) as provided by the IC Crypto Suite option, where applicable.
- Platform protection mechanisms against physical attacks and malfunction (sensors, fault detection and secure state behavior) as covered by the Platform-ST.
- Memory protection and access control mechanisms (e.g. Application Firewall) used by the embedded software to isolate applications and TSF data.

9.1.1 Threats

IC Threats	Rationale
Part of [PP-0084]	
T.Phys-Manipulation	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.Phys-Probing	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.Malfunction	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.Leak-Inherent	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.Leak-Forced	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.Abuse-Func	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.RND	This threat is addressed by the Platform-ST and is covered by the IC evaluation.
T.Masquerade_TOE	This threat is addressed by the Platform-ST (authentication to external entities and, where applicable, secure Loader authentication). Applicability depends on the selected Flash Loader configuration.
Threats defined in the Platform-ST	
T.Open_Samples_Diffusion	This threat is addressed by the Platform-ST (e.g. O.Prot_TSF_Confidentiality) and by composite TOE life-cycle controls (secure handling of open samples and delivery procedures).
T.Load_Non_Authentic	This threat is addressed by the Platform-ST secure loading mechanisms (authenticity/integrity checks).
T.Corrupt_Image_Load	This threat is addressed by the Platform-ST secure update/atomicity mechanisms.

Table 44 - State of compatibility threats

9.1.2 OSPs

IC OSPs	Rationale
Part of [PP-0084]	
P.Process-TOE	This policy is related to protection during IC Development and Production. It is covered by the IC evaluation.
P.Crypto-Service	This policy is related to cryptographic services of the IC. It is covered by the IC evaluation.
P.Lim_Block_Loader	This policy is related to limiting and blocking the Loader functionality. It is covered by the IC evaluation. The composite TOE life-cycle ensures that Loader availability is restricted as defined for the evaluated configuration.
P.Ctrl_Loader	This policy is related to controlled usage of the Loader functionality. It is covered by the IC evaluation. The composite TOE life-cycle defines secure Loader usage (roles, procedures and key management) for the phases where Loader use is permitted.
OSPs defined in the Platform-ST	
P.Firewall	This policy is related to memory access control (MPU/SAU) provided by the IC. It is covered by the IC evaluation and is used by the composite TOE embedded software.

Table 45 - State of compatibility OSPs

9.1.3 Assumptions

IC Assumptions	Rationale
Part of [PP-0084]	

A.Process-Sec-IC	This assumption ensures the security of the delivery, storage and handling of the IC during packaging, finishing and personalization. It is covered by the ALC_DVS.2 activity of the TOE evaluation.
A.Resp-Appl	This assumption ensures that security relevant data of the current TOE are properly treated according to the IC security needs. It is covered by the ADV_IMP.1 activity of the TOE evaluation.

Table 46 - State of compatibility assumptions

9.1.4 Security Objectives for the environment

IC Oes are separated in the following groups as defined in appendix 1.1 of [CC-COMP] or [CEM-2022]:

- **CfPOE**: IC OE being fulfilled by the current TOE automatically.
- **SgOE**: The remaining IC OE which shall be addressed by the current TOE.

IC OEs	Rationale
Part of [PP-0084]	
OE.Resp-Appl	This objective deals with the treatment of TOE user data by the TOE itself. It is covered by the ADV_IMP.1 activity of the TOE evaluation. CfPOE
OE.Process-Sec-IC	This objective deals with protection during composite product manufacturing. It is covered by the TOE evaluation. CfPOE
OE.Lim_Block_Loader	This objective deals with limitation of capability and blocking the Loader. It is addressed by the composite TOE life-cycle definition and by delivery/operational procedures (Flash Loader blocked or permanently deactivated for operational use in the evaluated configuration). CfPOE

OE.Loader_Usage	This objective deals with secure communication and secure usage of the Loader. It is addressed by the composite TOE life-cycle procedures (secure key material handling and authorized usage in the permitted phases). CfPOE
OE.TOE_Auth	This objective is only applicable if the Flash Loader mutual authentication package is enabled. For the evaluated configuration, Flash Loader mutual authentication is not required for operational use. CfPOE
OEs defined in the Platform-ST	
OE.Secure_UC_Load	This objective is only applicable if the Flash Loader is active. For the phases where secure image loading is used, the composite TOE provides and manages the relevant key material for the image. SgOE
OE.Secure_Delivery	When the IC is ordered with a disabled Flash Loader or with an enabled Flash Loader but mutual authentication disabled, the IC does not provide transport protection. The composite TOE therefore defines technical and/or organizational security procedures to secure the personalized TOE during delivery. SgOE

Table 47 - State of compatibility security objectives for the environment

9.1.5 Security Objectives

IC Security Objectives	Rationale
Part of [PP-0084]	

O.Phys-Manipulation	This objective is covered by the IC evaluation.
O.Phys-Probing	This objective is covered by the IC evaluation.
O.Malfunction	This objective is covered by the IC evaluation.
O.Leak-Inherent	This objective is covered by the IC evaluation.
O.Leak-Forced	This objective is covered by the IC evaluation.
O.Abuse-Func	This objective is covered by the IC evaluation.
O.Identification	This objective is covered by the IC evaluation.
O.RND	This objective is covered by the IC evaluation.
O.Cap_Avail_Loader	This objective is covered by the IC evaluation. It is applicable only during the permitted life-cycle phases where the Flash Loader is enabled for loading the Static Data. At TOE delivery, after completion of Phase C, the TOE is self-protected and the Flash Loader is deactivated. Therefore, this objective is not applicable to operational use of the delivered TOE.
O.Ctrl_Auth_Loader	This objective is covered by the IC evaluation. It is applicable only during the permitted life-cycle phases where the Flash Loader is enabled for loading the Static Data. At TOE delivery, after completion of Phase C, the TOE is self-protected and the Flash Loader is deactivated. Therefore, this objective is not applicable to operational use of the delivered TOE.
O.Authentication	This objective is covered by the IC evaluation. It is applicable only during the permitted life-cycle phases where the Flash Loader is enabled for loading the Static Data. At TOE delivery, after completion of Phase C, the TOE is self-protected and the Flash Loader is deactivated. Therefore, this objective is not applicable to operational use of the delivered TOE.
O.AES	This objective is covered by the IC evaluation.
O.TDES	This objective is covered by the IC evaluation.

Part of [PDCL]	
O.Secure_UC_Load	This objective is covered by the IC evaluation. It is applicable only during the permitted life-cycle phases where the Flash Loader is active. At TOE delivery, after completion of Phase C, the TOE is self-protected and the Flash Loader is deactivated. Therefore, this objective is not applicable to operational use of the delivered TOE.
O.Secure_UC_Activation	This objective is covered by the IC evaluation. It is applicable only during the permitted life-cycle phases where the Flash Loader is active. At TOE delivery, after completion of Phase C, the TOE is self-protected and the Flash Loader is deactivated. Therefore, this objective is not applicable to operational use of the delivered TOE.
Objectives defined in the Platform-ST	
O.Firewall	This objective is covered by the IC evaluation and supports the composite TOE embedded software in managing and enforcing memory access control.
O.Prot_TSF_Confidentiality	This objective is covered by the IC evaluation and addresses protection against disclosure of confidential TSF operations through the use of dedicated code loaded on open samples.
Crypto Suite objectives	
O.FFC	This objective is covered by the IC evaluation. The composite TOE does not rely on this IC Crypto Suite service.
O.RSA	This objective is covered by the IC evaluation.
O.ECC	This objective is covered by the IC evaluation.
O.ML	This objective is covered by the IC evaluation. The composite TOE does not rely on this IC Crypto Suite service.
O.HMAC	This objective is covered by the IC evaluation. The composite TOE does not rely on the IC Crypto Suite HMAC service; HMAC operations used by the TOE are covered by the Runtime Environment through JCS.CryptoAPI.

O.Hash	This objective is covered by the IC evaluation.

Table 48 - State of compatibility security objectives rationale

9.1.6 SFRs

IC SFRs are separated into the following groups as defined in appendix 1.1 of [CC-COMP] or [CEM-2022]:

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

The Composite-ST requires EAL4 according to Common Criteria 2022 release 1 augmented by ALC_DVS.2 and AVA_VAN.5.

The Platform-ST has been evaluated to EAL6 according to Common Criteria 2022 release 1 augmented with ALC_FLR.1 and ATE_SDP.1.

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

IC SFRs	**Relevance** **(IP_SFR / RP_SFR_SERV / RP_SFR_MECH)**
Part of [PP-0084]	
From "Hardware random number generators"	
FCS_RNG.1/TRNG	RP_SFR_SERV
From "Cryptographic services implemented in hardware"	
FCS_COP.1/AES	RP_SFR_SERV
FCS_CKM.6/AES	RP_SFR_SERV

FCS_COP.1/TDES	RP_SFR_SERV
FCS_CKM.6/TDES	RP_SFR_SERV
From "Malfunctions"	
FRU_FLT.2	RP_SFR_MECH
FPT_FLS.1	RP_SFR_MECH
From "Abuse of Functionality"	
FMT_LIM.1	RP_SFR_MECH
FMT_LIM.2	RP_SFR_MECH
FAU_SAS.1	RP_SFR_SERV
From "Physical Manipulation and Probing"	
FPT_PHP.3	RP_SFR_MECH
FDP_SDC.1	RP_SFR_MECH
FDP_SDI.2	RP_SFR_MECH
From "Leakage"	
FDP_ITT.1	RP_SFR_MECH
FPT_ITT.1	RP_SFR_MECH
FDP_IFC.1	RP_SFR_MECH
From "Self-secured digital protection (SDP)"	
FPT_SDP.1	RP_SFR_MECH
FDP_ITT.1/SDP	RP_SFR_MECH
FPT_ITT.1/SDP	RP_SFR_MECH
FDP_IFC.1/SDP	RP_SFR_MECH
From "TSF testing"	
FPT_TST.1	RP_SFR_MECH

From "Application Firewall"	
FDP_ACC.2/AF	RP_SFR_MECH
FDP_ACF.1/AF	RP_SFR_MECH
FMT_MSA.3/AF	RP_SFR_MECH
FMT_MSA.1/AF/S	RP_SFR_MECH
FMT_MSA.1/AF/NS	RP_SFR_MECH
FMT_SMF.1/AF	RP_SFR_MECH
FMT_SMR.1/AF	RP_SFR_MECH
From "Authentication of the Security IC"	
FIA_API.1	RP_SFR_SERV
From "Flash Loader"	
FMT_LIM.1/Loader	RP_SFR_MECH
FMT_LIM.2/Loader	RP_SFR_MECH
FTP_ITC.1	RP_SFR_MECH
FDP_UCT.1	RP_SFR_MECH
FDP_UIT.1	RP_SFR_MECH
FDP_ACC.1/Loader	RP_SFR_MECH
FDP_ACF.1/Loader	RP_SFR_MECH
FMT_MTD.1/Loader	RP_SFR_MECH
FMT_SMR.1/Loader	RP_SFR_MECH
FMT_SMF.1/Loader	RP_SFR_MECH
FIA_UID.2/Loader	RP_SFR_MECH
FPT_FLS.1/Loader	RP_SFR_MECH
Crypto Suite SFRs	

FCS_COP.1/CS/AES/ENC	RP_SFR_SERV
FCS_COP.1/CS/AES/CMAC	RP_SFR_SERV
FCS_COP.1/CS/AES/CBC_MAC	RP_SFR_SERV
FCS_COP.1/CS/AES/CCM	IP_SFR
FCS_COP.1/CS/AES/GCM	RP_SFR_SERV
FCS_CKM.6/CS/AES	RP_SFR_SERV
FCS_COP.1/CS/TDES/ENC	RP_SFR_SERV
FCS_COP.1/CS/TDES/RMAC	IP_SFR
FCS_COP.1/CS/TDES/CBC_MAC	RP_SFR_SERV
FCS_CKM.6/CS/TDES	RP_SFR_SERV
FCS_COP.1/CS/ECC/ECDSA_SIG	RP_SFR_SERV
FCS_COP.1/CS/ECC/ECDSA_VER	RP_SFR_SERV
FCS_COP.1/CS/ECC/ECDH	RP_SFR_SERV
FCS_COP.1/CS/ECC/PACE_IM	IP_SFR
FCS_COP.1/CS/ECC/X25519	RP_SFR_SERV
FCS_COP.1/CS/ECC/X448	IP_SFR
FCS_COP.1/CS/ECC/ECSDSA_SIG	IP_SFR
FCS_COP.1/CS/ECC/ECSDSA_VER	IP_SFR
FCS_COP.1/CS/ECC/EdDSA_SIG	IP_SFR
FCS_COP.1/CS/ECC/EdDSA_VER	IP_SFR
FCS_COP.1/CS/ECC/HashEdDSA_SIG	IP_SFR
FCS_COP.1/CS/ECC/HashEdDSA_VER	IP_SFR
FCS_CKM.1/CS/ECC/ECDSA	RP_SFR_SERV
FCS_CKM.1/CS/ECC/EdDSA	IP_SFR

FCS_CKM.1/CS/ECC/ECSDSA	IP_SFR
FCS_COP.1/CS/HMAC/SHA	IP_SFR
FCS_COP.1/CS/Hash/SHA1	IP_SFR
FCS_COP.1/CS/Hash/SHA2	RP_SFR_SERV
FCS_COP.1/CS/Hash/SHA3	IP_SFR
FCS_COP.1/CS/Hash/XOF	IP_SFR
FCS_RNG.1/CS/PTG2	IP_SFR
FCS_RNG.1/CS/PTG3	IP_SFR
FCS_RNG.1/CS/DRG3	IP_SFR
FCS_RNG.1/CS/DRG4	IP_SFR
FCS_COP.1/CS/FFC/<iter>	IP_SFR
FCS_CKM.1/CS/FFC	IP_SFR
FCS_COP.1/CS/RSA/<iter>	IP_SFR
FCS_CKM.1/CS/RSA/<iter>	IP_SFR
FCS_COP.1/CS/ML/<iter>	IP_SFR
FCS_CKM.1/CS/ML/<iter>	IP_SFR

Table 49 - State of compatibility SFRs

Rationale for Flash Loader SFRs: FTP_ITC.1, FDP_UCT.1, FDP_UIT.1, FDP_ACC.1/Loader, FDP_ACF.1/Loader, FMT_MTD.1/Loader, FMT_SMR.1/Loader, FMT_SMF.1/Loader, FIA_UID.2/Loader and FIA_API.1 are Platform-ST SFRs related to Flash Loader functionality. In the evaluated composite TOE configuration, the Flash Loader is used only during the permitted manufacturing phase for loading the Static Data, before TOE delivery, and is no longer available for operational use after TOE delivery. Therefore, these SFRs are not exposed as operational TOE functionality after delivery, their applicability is limited to the controlled pre-delivery life-cycle phases where Flash Loader use is permitted.

10. References, Glossary, Tables and abbreviations

10.1 References

Reference	Title
[AIS31]	Anwendungshinweise und Interpretationen zum Schema (AIS), AIS 31, Funktionalitätsklassen und Evaluierungsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013.
[ANSI X9.62]	ANSI X9.62:2005, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA).
[ANSI X9.63]	ANSI X9.63-2011, Public Key Cryptography For The Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography.
[BSI TR 03111]	Technical Guideline BSI TR-03111: Elliptic Curve Cryptography Version 2.10, 01.06.2018, Bundesamt für Sicherheit in der Infor-mationstechnik (BSI).
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model. CC:2022, Revision 1, November 2022. CCMB-2022-11-001.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements. CC:2022, Revision 1, November 2022. CCMB-2022-11-002.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components. CC:2022, Revision 1, November 2022. CCMB-2022-11-003.
[CC-5]	Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements. CC:2022, Revision 1, November 2022. CCMB-2022-11-005.

[CC-ERRATA]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.2.
[CC-COMP]	Common Criteria Supporting Document, Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018.
[CEM-2022]	Common Methodology for Information Technology Security Evaluation, November 2022 Revision 1. CCMB-2022-11-06.
[CIC]	Common Implementation Configuration v2.1, July 2018 Ref: GPC_GUI_080.
[EUPP]	TCA eUICC Profile Package Interoperable Format Test Specification v3.2, May 2022.
[FIPS46-3]	Federal Information Processing Standards PUB 46-3, Data Encryption Standard, reaffirmed 1999 October 25.
[FIPS180-4]	Federal Information Processing Standards Publication 180-4, Secure Hash Standard, March 2012.
[FIPS197]	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001.
[GPCS]	Global Platform Card Specification v2.3.1 (GPC_SPE_034), March 2018 and amendments: • Amendment A – Confidential Card–Content Management, v1.2, July 2019. • Amendment B – Remote Application Management over HTTP, v1.2, March 2022. • Amendment D – Secure Channel Protocol 03, v1.2, April 2020.
[ISO 9796-2]	ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorization-based mechanisms, 2002
[ISO 9797-1]	ISO/IEC 9797-1:2011: Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanism using a block cipher.

[ISO 18031]	ISO/IEC 18031:2011: Information technology — Security techniques - Random bit generation.
[ISO 15946]	ISO/IEC 15946-5:2009, Cryptographic techniques based on elliptic curves.
[JCRE3]	Java Card Platform, version 3.0.5, Classic Edition, Runtime Environment (Java Card RE) Specification.
[JCVM3]	Java Card 3 Platform, version 3.0.5 - Virtual Machine Specification, Classic Edition.
[KS2011]	W. Killmann, W. Schindler, A proposal for: Functionality classes for random number generators, version 2.0, September 2011.
[MILENAGE]	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 11): "3rd Generation Partner-ship Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General. Document 2: Algorithm Specification. Document 3: Implementers Test Data Document 4: Design Conformance Test Data Document 5: Summary and results of design and evaluation.
[PKCS1]	PKCS #1: RSA Encryption Standard – An RSA Laboratories Technical Note, Version 2.1, February 2003.
[PKCS3]	PKCS#3: Diffie-Hellman Key Agreement Standard, An RSA Laboratories Technical Note, Version 1.4, Revised November 1, 1993.
[PP-0084]	Security IC Platform Protection Profile with Augmentation Packages version 1.0, February 2014, BSI-CC-PP-0084-2014.
[PP-eUICC]	eUICC for Consumer and IoT Devices Protection Profile Version 2.1, February 2025 (SGP.25 v2.1 by GSMA).
[PP-GP]	GlobalPlatform Technology – Secure Element Protection Profile, Version 1.0, February 2021, Document Reference: GPC_SPE_174.

[PP-JCS]	Java Card Protection Profile - Open Configuration Protection Profile Version 3.1. April 2020.
[GP SG]	GlobalPlatfrom Card Composition Model Security Guidelines for Basic Applications, Version 2.0, December 2014.
[RFC2104]	Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: KeyedFDP_.1-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997 <https://www.rfc-editor.org/info/rfc2104>.
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S.Bradner <http://www.ietf.org/rfc/rfc2119.txt>
[RFC3447]	Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, DOI 10.17487/RFC3447, February 2003, <https://www.rfc-editor.org/info/rfc3447>.
[RFC5639]	Lochter, M. and J. Merkle, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation", RFC 5639, DOI 10.17487/RFC5639, March 2010. <https://www.rfc-edi-tor.org/info/rfc5639>.
[RFC7748]	Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016 <https://www.rfc-editor.org/info/rfc7748>.
[RFC8032]	Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (ECDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017 <https://www.rfc-editor.org/info/rfc8032>.
[SGP.02]	Remote Provisioning Architecture for Embedded UICC Technical Specification.
[SGP.06]	eUICC Security Assurance Principles, version 1.1, July 2023.
[SGP.07]	eUICC Security Assurance Methodology, version 1.1, July 2023.
[SGP.08]	Security Evaluation of Integrated eUICC, version 1.2, October 2022.
[SGP.17]	Security Target Template for Consumer eUICC, version 1.0, July 2023.

[SGP.21]	RSP Architecture Specification, version 2.5, November 2022.
[SGP.22]	RSP Technical Specification, version 2.5, May 2023.
[SGP.23]	RSP Test Specification, version 1.14, July 2023.
[SGP.24]	SGP.24 Compliance Process, Version 2.5, March 2023.
[SGP.25]	eUICC for Consumer and IoT Devices Protection Profile V2.1
[SGP.31]	eSIM IoT Architecture and Requirement Specification, version 1.2, April 2024
[SGP.32]	eSIM IoT Technical Specification, version 1.2, June 2024
[SGP.33]	eSIM IoT Test Specification, version 1.2, January 2025
[SIMalliance]	SIMalliance eUICC Profile Package: Interoperable Format Technical Specification, version 2.1.
[SP800-38a]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001.
[SP800-38b]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005.
[SP800-67]	National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, version 1.2, July 2011.
[SP800-90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, January 2012.
[ST/IC]	IFX_CCI_00007Ah/8Fh A11/R11/M11 with optional Crypto Suite Security Target Lite, Rev 1.0
[SUPP]	Supporting Document, Mandatory Technical Document, Composite product evaluation for Smart Cards and similar devices, May 2018, Version 1.5.1.
[TS 102.223]	ETSI TS 102 223 V15.1.0 (2019-02), Smart Cards; Card Application Toolkit (CAT) (Release 15).

[TS 102.225]	ETSI TS 102 225 V16.0.0 (2020-06), Smart Cards; Secured packet structure for UICC based applications (Release 16).
[TS 102.226]	ETSI TS 102 226 V16.0.0 (2020-07), Smart Cards; Remote APDU structure for UICC based applications (Release 16).
[TUAK]	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0, release 12, December 2014. Document 1: Algorithm specification. Document 2: Implementers' test data. Document 3: Design conformance test data.
[GUIDES]	- [EN] AGD_OPE - Valid eUICC IoT v1.0 - Operational User Guidance - v1.2 - [EN] AGD_OPE - Valid eUICC IoT v1.0 - Operational User Guidance - Basic Applet Guidelines - v1.1 - [EN] AGD_OPE - Valid eUICC IoT v1.0 - Operational User Guidance - Sensitive Applet Guidelines - v1.0 - [EN] AGD_PRE - Valid eUICC IoT V1.0 - Preparative Procedures - v1.2

10.2 Glossary

Term	Definition
Application	Instance of an Executable Module after it has been installed and made selectable.
Controlling Authority	A Controlling Authority is entity independent from the OEM represented on the eSIM and responsible for securing the keys creation and personalization of the Supplementary Security Domains.
Certificate or Public Key Certificate	A certificate as defined in RFC.5280 and GlobalPlatform specifications GPC_SPE_034.
DAP Block	Part of the Load File used for ensuring Load File Data Block verification.
DAP Verification	A mechanism used by a Security Domain to verify that a Load File Data Block is authentic.
Developer	Person/Company acting on behalf of the EUM.

Device	User equipment used in conjunction with an eUICC to connect to a mobile network (e.g. Tablet, wearable, smartphone or handset).
Device Manufacturer	An entity responsible for manufacturing Devices. The Device manufacturer may be responsible for the selection and insertion of eUICCs in Devices.
Disabled Profile	The state of a Profile where all files and applications present in the Profile are not selectable over the eUICC Terminal interface.
Enabled Profile	The state of a Profile when its files and/or applications are selectable over the eUICC Terminal Interface.
eUICC	Embedded UICC - A removable or non-removable UICC which enables the remote and/or local management of Profiles in a secure way.
eUICC Manufacturer (EUM)	The eUICC Manufacturer provides eUICC products.
eUICC Memory Reset	An action that returns the eUICC to a state equivalent to a factory state.
Issuer Security Domain	The primary on-card entity providing support for the control, security, and communication requirements of the card administrator-
Local Profile Assistant (LPA)	A functional element in the Device or in the eUICC that provides the LPD, LDS and LUI interfaces.
OTA Platform	A platform used by an Operator for the Remote File/Application management of enabled Profiles on eUICCs.
Profile	Security Domains, UICC file system and secure objects (Keys, PIN codes…) formatted as defined by [EUPP]. A Profile can be downloaded from RSP Servers onto a eUICC by end user consent as defined by [SGP.21] and [SGP.22].
Remote SIM Provisioning	The downloading, installing, enabling, disabling and deletion of a Profile on an eUICC.
RSP Servers	GSMA-defined SM-DP+ and SM-DS servers. Used to distribute a Profile to the end user.
Replay attack	An attack based on previously used or outdated data.
Roles	Roles are representing a logical grouping of functions.
Security Domain	On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the Profile Issuer, an Application Provider or a Controlling Authority).

Supplementary Security Domain	A Security Domain other than the Issuer Security Domain dedicated to Application provider.
Verification Authority	The Verification Authority (VA), is a trusted third party represented on the (U)SIM card, acting on behalf of the OEM and responsible for the verification of application signatures (mandated DAP) during the loading process.

10.3 Tables

10.4 Abbreviations

Term	Definition
AID	Application Identifier
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
CERT.DPauth.ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for SM-DP+ authentication
CERT.DPpb.ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for Profile Package Binding
CERT.DSauth.ECDSA	Certificate of the SM-DS for its Public ECDSA key used for SM-DS authentication

CERT.EUICC.ECDSA	Certificate of the eUICC for its Public ECDSA key
CERT.EUM.ECDSA	Certificate of the EUM for its Public ECDSA key
CERT.DP.TLS	Certificate of the SM-DP+ for securing TLS connections (version >= 1.2)
CERT.DS.TLS	Certificate of the SM-DS for securing TLS connections (version >= 1.2)
CMAC	Cipher-based MAC
CRL	Certificate Revocation List
DH	Diffie-Hellman
ECASD	eUICC Certificate Authority Security Domain
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve cryptography Digital Signature Algorithm
ECKA	Elliptic Curve cryptography Key Agreement algorithm
EID	eUICC-ID
ETSI	European Telecommunications Standards Institute
EUM	eUICC Manufacturer
GP	GlobalPlatform
GSMA	GSM Association
HTTP	Hypertext Transfer Protocol
HW	Hardware
IC	Integrated Circuit
IPA	IoT Profile Assistant (see [SGP.32])
IPAd	IoT Profile Assistant in the IoT Device (see [SGP.32])
IPAe	IoT Profile Assistant in the eUICC (see [SGP.32])
iSIM	Integrated SIM
I-TRE	Integrated Tamper Resistant Element (e.g. TRE embedded within a SoC)
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile (see [SGP.22])
ISD-R	Issuer Security Domain Root (see [SGP.22])
ISIM	IP Multimedia Services Identity Module
ISO	International Standards Organization
LPA	Local Profile Assistant
LPAd	Local Profile Assistant on Device (see [SGP.22])
LPAe	Local Profile Assistant on eUICC (see [SGP.22])
LPD	Local Profile Download
LUI	Local User Interface
MAC	Message Authentication Code

MNO	Mobile Network Operator
MNO-SD	Mobile network Operator – Security Domain
NAA	Network Access Application
OCE	Off Card Entity
OEM	Original Equipment Manufacturer
OPL	Offline Profile Loading
OS	Operating System
OSP	Organizational Security Policies
OTA	Over-The-Air
PP	Protection Profile
PPE	Profile Package Enabler
PPI	Profile Package Interpreter
PPR	Profile Policy Rule
RAT	Rules Authorization Table
REE	Rich Execution Environment (e.g. Android, iOS, Linux, Windows, etc.)
RMA	Return Merchandise Authorization (i.e. return a product under warranty for a replacement, refund, repair)
RMI	Remote Method Invocation
RSP	Remote SIM Provisioning
RTE	Run Time Environment
SAS	Security Accreditation Scheme
SCP	Secure Channel Protocol
SD	Security Domain
SFR	Security Functional Requirements
SIM	Subscriber Identity Module
SM-DP+	Subscription Manager – Data Preparation +
SM-DS	Subscription Manager – Discovery Server
SPD	Security Profile Document
SSD	Supplementary Security Domain
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
VA	Verification Authority

USIM	Universal Subscriber Identity Module