



eSA public Security Target of  
MultiSIM M2M 4.3.1 v1.0

D1643035, Version 1.1p, February 12<sup>th</sup>, 2026

Security Target

**REVISION HISTORY**

<b>Ver</b>	<b>Date</b>	<b>Author</b>	<b>Description of the modifications</b>
1.0p	26/01/2026	I. TOBOR	Initial release. Based on "eSA Security Target of MultiSIM M2M 4.3.1 v1.0" v1.0
1.1p	12/02/2026	I. TOBOR	Completing the Guidances versions

## TABLE OF CONTENTS

## Contents

1	ST Introduction.....	7
1.1	ST reference.....	7
1.2	TOE reference.....	7
2	TOE Overview.....	8
2.1	TOE description .....	8
2.2	TOE configuration.....	8
2.2.1	TOE type and usage.....	8
2.2.2	TOE life-cycle.....	11
2.2.3	Non-TOE HW/SW/FW available to the TOE .....	17
2.3	TOE Physical scope .....	17
2.4	TOE Logical scope .....	18
2.4.1	Application layer .....	19
2.4.2	Platform layer.....	23
3	Conformance claim .....	25
3.1	Note about CC version 3.1 and CC version 2022.....	25
3.2	Composition .....	25
3.3	Common Criteria Conformance Claims .....	25
3.4	Protection Profile (PP) conformance claim .....	26
3.5	Conformance claim rationale .....	26
3.5.1	Conformity of the TOE Type.....	26
3.5.2	SPD Consistency .....	26
3.5.3	Security Objectives Consistency.....	30
3.5.4	Conformity of the Requirement (SFR/SAR).....	33
4	Security Problem definition .....	39
4.1	Assets.....	39
4.2	Users and Subjects .....	39
4.3	Threats.....	39
4.4	Security Aspects (added to cover OS update).....	40
4.5	Organizational Security Policies .....	40
4.6	Assumptions .....	40
5	Security Objectives.....	41
5.1	Security Objectives for the TOE.....	41
5.2	Security Objectives for the Operational Environment .....	42
5.3	Security Objectives Rationale.....	42
5.3.1	Threats .....	42
5.3.2	Organizational Security Policies .....	47
5.3.3	Assumptions.....	47
5.3.4	Rationale Tables.....	48
6	Extended Components Definition.....	53
7	Security Functional and Assurance requirements .....	54
7.1	eUICC Security Functional Requirements.....	54
7.1.1	Introduction .....	54
7.1.2	Identification and Authentication .....	54
7.1.3	Communication .....	58
7.1.4	Security Domains .....	64
7.1.5	Platform Services .....	69
7.1.6	Security Management.....	71

7.1.7	Mobile Network Authentication .....	76
7.2	Runtime Environment Security Functional Requirements .....	77
7.2.1	CoreLG Security Functional requirements .....	77
7.2.2	InstG Security Functional requirements .....	87
7.2.3	ADELG Security Functional Requirements .....	87
7.2.4	ODELG Security Functional Requirements .....	90
7.2.5	CarG Security Functional Requirements .....	90
7.2.6	Global Platform Security Functional requirements .....	90
7.2.7	Underlying platform IC Security Functional Requirements .....	104
7.3	Security Assurance Requirements .....	105
7.4	Rationale .....	105
7.4.1	SFRs for eUICC rationale .....	105
7.4.2	SFRs for Runtime Environment rationale .....	106
7.4.3	SFR dependency rationale .....	107
7.4.4	SAR Evaluation Assurance Level rationale .....	112
7.4.5	SAR dependency rationale .....	112
8	TOE Summary Specification .....	114
8.1	eUICC security functions .....	114
8.1.1	GSMA.Ident-Auth .....	114
8.1.2	GSMA.SecureChannels .....	114
8.1.3	GSMA.SecurityDomains .....	115
8.1.4	GSMA.PlatformServices .....	115
8.1.5	GSMA.SecurityMngt .....	115
8.1.6	GSMA.NetworkAuthent .....	116
8.2	Runtime Environment security functions .....	116
8.2.1	GP.CardContentManagement .....	116
8.2.2	GP.KeyLoading .....	116
8.2.3	GP.SecurityDomain .....	116
8.2.4	GP.SecureChannel .....	116
8.2.5	GP.GPRegistry .....	117
8.2.6	GP.OS-UPDATE .....	118
8.2.7	JCS.APDUBuffer .....	118
8.2.8	JCS.ByteCodeExecution .....	118
8.2.9	JCS.Firewall .....	119
8.2.10	JCS.Package .....	119
8.2.11	JCS.CryptoAPI .....	119
8.2.12	JCS.KeyManagement .....	120
8.2.13	JCS.EraseResidualData .....	120
8.2.14	JCS.OutOfLifeDataUndisclosure .....	120
8.2.15	JCS.RunTimeExecution .....	120
8.2.16	JCS.Exception .....	121
8.2.17	OS.Atomicity .....	121
8.2.18	OS.MemoryManagement .....	121
8.3	TSS Rationale .....	121
8.3.1	eUICC SFRs coverage .....	121
8.3.2	Runtime Environment SFRs coverage .....	122
9	Composition with IC .....	127
9.1	Statement of compatibility – Threats part .....	127
9.2	Statement of compatibility – OSPs part .....	127

9.3	Statement of compatibility – Assumptions part .....	128
9.4	Statement of compatibility – Security objectives for the environment part .....	128
9.5	Statement of compatibility – Security objectives part .....	128
9.6	Statement of compatibility – SFRs part .....	129
10	References, Glossary and Abbreviations .....	131
10.1	External references .....	131
10.2	Internal references .....	132
10.3	Glossary .....	132
10.4	Abbreviations .....	133

## TABLE OF FIGURES

Figure 1 – TOE Architecture .....	10
Figure 2 – "Thales" life-cycle .....	13
Figure 3 – "Alternative" life-cycle .....	15
Figure 4 – TOE logical boundaries .....	19

## TABLE OF TABLES

Table 1 – "Thales" life cycle .....	14
Table 2 – "Alternative" life cycle .....	17
Table 3 – Assets Consistency table .....	27
Table 4 – Security aspect Consistency table .....	28
Table 5 – User consistency table .....	28
Table 6 – Subjects Consistency table .....	29
Table 7 – Threats consistency table .....	30
Table 8 – Organizational Security Policies Consistency table .....	30
Table 9 – Assumptions Consistency table .....	30
Table 10 – Security objectives for the TOE consistency table .....	32
Table 11 – Security objectives for the Operational Environment consistency table .....	33
Table 12 – Security Functional Requirement consistency table .....	37
Table 13 – Threats .....	40
Table 14 – Security Objectives for the TOE .....	42
Table 15 – Threats and Security Objectives- Coverage .....	49
Table 16 – Security Objectives and threats .....	51
Table 17 – Organizational Security Policies and Security Objectives- Coverage .....	51
Table 18 – Security Objectives and Organizational Security Policies .....	52
Table 19 – Assumptions and Security Objectives for the Operational Environment- Coverage .....	52
Table 20 – Assumptions and Security Objectives for the Operational Environment .....	52

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

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

*Product is certified including preparation, user and administration guidance.*

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

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

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

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

# 1 ST INTRODUCTION

---

## 1.1 ST reference

The ST identification is the following:

<b>Name</b>	eSA Security Target of MultiSIM M2M 4.3.1 v1.0
<b>Version</b>	1.1
<b>Author</b>	Thales
<b>Reference</b>	D1643035
<b>Publication date</b>	February 12, 2026

The ST lite identification is the following:

<b>Name</b>	eSA public Security Target of MultiSIM M2M 4.3.1 v1.0
<b>Version</b>	1.1p
<b>Author</b>	Thales
<b>Reference</b>	D1643035
<b>Publication date</b>	February 12, 2026

## 1.2 TOE reference

<b>Product name</b>	MultiSIM M2M 4.3.1
<b>Developer</b>	Thales
<b>TOE name</b>	MultiSIM M2M 4.3.1
<b>TOE software version</b>	83030 (EID)
<b>TOE documentation</b>	See [GUIDANCE]
<b>TOE hardware part</b>	ORION_TOE_v5, see [CERT-IC], [ST-IC] and [GUIDANCE-IC]

TOE unique reference is composed from four above elements: TOE name, TOE software version, TOE documentation and TOE hardware. In the rest of this ST these elements will be grouped as an alias MultiSIM M2M 4.3.1 v1.0.

## 2 TOE OVERVIEW

---

### 2.1 TOE description

MultiSIM M2M 4.3.1 v1.0 on ORION is an eUICC (embedded UICC) component in a machine-to-machine device.

It is composed of:

- A hardware named ORION, see [ST-IC] from Thales DIS France SAS
- The embedded eUICC OS named eSIM software

MultiSIM M2M 4.3.1 v1.0 product is a discrete eUICC with M2M configuration, compliant with the GSMA [SGP.01] and [SGP.02] specifications that implements the GSMA Remote SIM Provisioning (RSP). As such, it is a multi-profile product, supporting remote profile management over SMS and over HTTP. Soldered in an M2M device, it provides connectivity to the MNO network corresponding to the currently enabled profile and ability to switch to another MNO network.

The product is built upon an open Java Card [JC31] and GlobalPlatform [GPCS] technologies, meaning that additional applications - which may not be known at the time of the present evaluation - can be remotely loaded and installed on the eUICC “post-issuance”, i.e., after the IOT device has been delivered to the end-user. Applications can also be installed “pre-issuance” during the pre-personalization or personalization phases. Whatever the scenario (pre-issuance or post-issuance), applications’ loading, and installation are secured by the GP security mechanisms and verification processes.

### 2.2 TOE configuration

Two TOE configurations are used:

- TOE based on ORION\_CB\_03 configuration of ORION
- TOE based on ORION\_DB\_03 configuration of ORION

(See [ST-IC] for details).

#### 2.2.1 TOE type and usage

The TOE type is software on secure hardware IC applying composite evaluation principle.

The eUICC is an UICC embedded in an M2M device. The eUICC will contain several MNO Profiles (with only one activated at a given time). The Profile is the MNO’s property, and stores MNO specific information as a given International Mobile Subscriber Identity (IMSI) and relevant keys. The primary function of the Profile is to authenticate the M2M Device when accessing the network. The Profile can also contain executable application.

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

The eUICC is connected to a given mobile network, by means of its currently enabled MNO Profile.

MultiSIM M2M 4.3.1 v1.0 product is built upon an open Java Card and GlobalPlatform specification (called later “platform”), meaning that additional applications - which may not be known at the time of the present evaluation - can be remotely loaded and installed on the eUICC “post-issuance”, i.e. after the M2M device has been delivered to the end-user. Applications loading and installation are secured by the GP security mechanisms and verification processes.

The platform has two main roles:

- Allow to load and execute the application contained in Profiles
- Provide the services (such as input/output communication or cryptographic support for communication protocols) and support the execution of items and applications implemented in higher layers.

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

The TOE includes 3 layers:

- The hardware layer: ORION (GTO04M and GTO004 are the internal names of ORION IC<sup>1</sup>) providing support to the platform layer.
- The platform layer: OS including
  - $\mu$ KOS: low level OS services tightly related to the hardware,
  - JKernel: Java Card Runtime Environment necessary to execute Java Card application and GlobalPlatform component managing them,
  - JTE: eUICC GSMA Remote Provisioning composed of set of functions providing support to the application layer.
- The application layer: composed of privileged applications providing the remote provisioning and administration functionality, encompassing standard and sensitive applications, as well as the security domains (ISD-R, ECASD, ISD-P) and the OS Update security domain (GASD).

Figure 1 – TOE Architecture presents the overall MultiSIM M2M 4.3.1 v1.0 architecture. Note that this figure is broader than the TOE scope: this figure includes Profiles. For the exact TOE limits and logical scope see Figure 5 – TOE logical boundaries later in section 2.4 TOE Logical scope.

---

<sup>1</sup> GTP004 is ORION\_CB\_03 configuration and GTO04M is ORION\_DB\_03

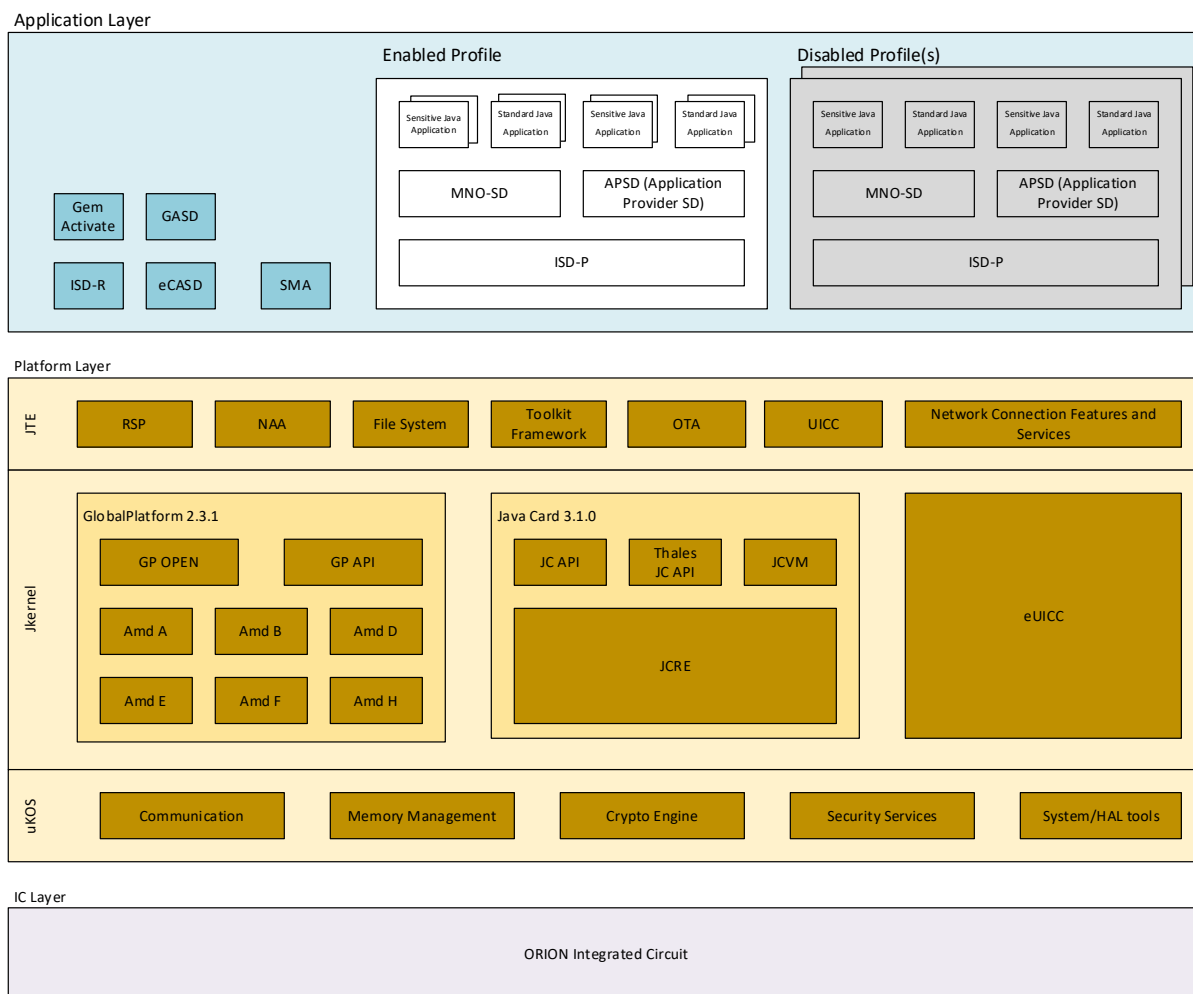


Figure 1 – TOE Architecture

The major security features are (see also section 2.4 TOE Logical scope for the detailed list):

- IC layer: Provides a secure hardware as a platform for the Embedded Software execution:
  - Implements the low-level hardware security protections against physical attacks (observation, disturbance)
  - Provides secured interfaces for low level hardware services (cryptographic acceleration, input/output communication, resource management)
- Platform layer: Provides a software platform for management and execution of Java Card application. These applications can be part of the TOE or the Profile
  - Hardware abstraction layer between IC and OS
  - Low level libraries for memory management, communication, atomic NVM update
  - Low level Crypto Library between HW crypto accelerators and Java Card cryptographic API
  - Secure environment for Java Card applet execution, firewall, standard Java Card library
  - Abnormal conditions (attacks) detection and processing and maintaining the secure state
  - Secure environment for applet management: user authentication, security domains management, key import, applet loading/installing/deleting,

- Secure OS-update (patching): user authentication, patch deciphering, atomic update
- Application layer: Remote SIM Provisioning related services as specified in [SGP.01] and [SGP.02]:
  - User (MNO, SM-SR, SM-DP, ...) identification authentication
  - Enforcing of ISD-R, ISD-P, eCASD, MNO-SD access policy
  - Enforcing of all necessary Secure Channel between appropriate ES interfaces from [SGP.02]
  - Managing the profiles.

## 2.2.2 TOE life-cycle

In accordance with [PP-eUICC], the product and TOE life cycle is composed of 5 phases which are described in the following subsections. Two possible life cycle options are considered in the present ST:

- In the “Thales life-cycle”, the integration of MultiSIM M2M 4.3.1 v1.0 Embedded Software into the IC is done by Thales. The TOE delivery point is put at the end of phase c, as illustrated in Figure 3 – "Thales" life-cycle.
- In the “alternative life-cycle”, the integration of the MultiSIM M2M 4.3.1 v1.0 Embedded Software into the IC is done by an accredited manufacturing actor. The intermediate HW/SW delivery point is put during the phase c, as illustrated in Figure 4 – "Alternative" life-cycle.

### 2.2.2.1 Actors

- Thales is the eUICC Manufacturer (EUM) in charge of
  - development of the eUICC platform
  - development of the production scripts used during the production phase
  - embedded software loading in its own premises and proceeds to the delivery of the product directly to customers (“Thales life-cycle”).
- INVIA<sup>2</sup> is the IC manufacturer in charge of the development and manufacturing of the ORION IC.
- Others accredited manufacturing actors can also load the embedded software on the IC in its own premises and proceeds to the delivery of the product directly to customers (“alternative life-cycle”)
- The Device Manufacturer is the Original Equipment Manufacturer
- The Profile Issuer is MNO that has privilege through its OTA Server to perform Remote Card Content Management (CCM) operations within its own profile (ISD-P). In addition, through its RSP servers, it also can provide Profiles to the end user

Figure 2 – Actors and life cycle phases below show the correspondence between the phases from [PP-eUICC] protection profile and the above actors.

---

<sup>2</sup> INVIA is the commercial brand for Thales DIS Design Services SAS legal entity

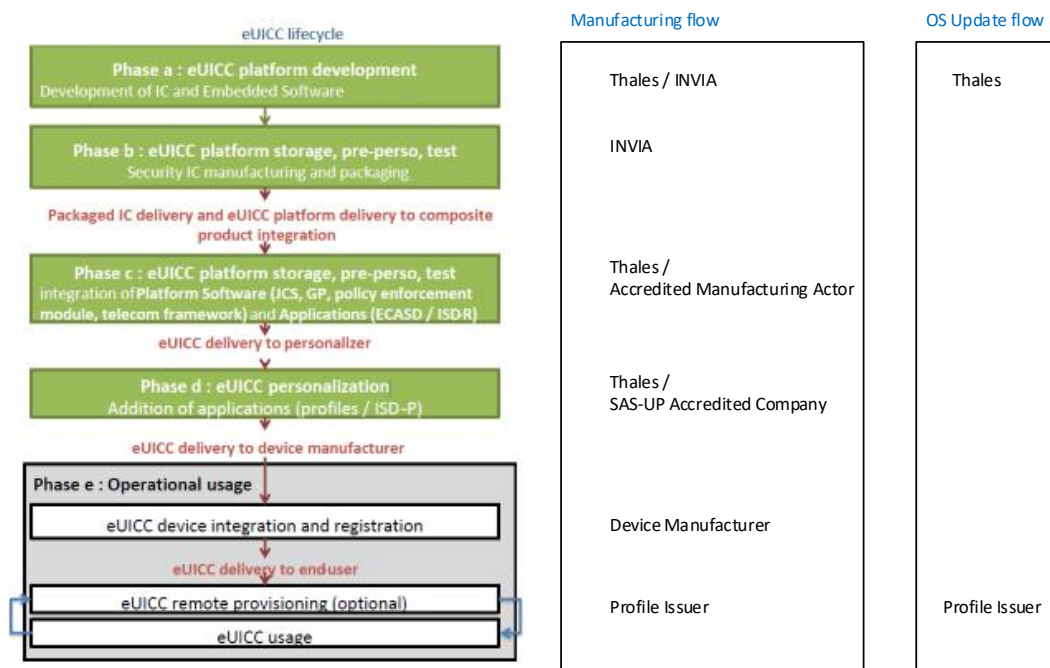


Figure 2 – Actors and life cycle phases

### 2.2.2.2 “Thales” life cycle

In the Thales life-cycle, the integration of MultiSIM M2M 4.3.1 v1.0 Embedded Software into the IC is done by Thales. The life cycle is composed of 5 phases which are described in Table 1 – “Thales” life cycle.

The loading of the MultiSIM M2M 4.3.1 v1.0 Embedded Software occurs during phase c, after which the IC loading service is locked and no more available. The TOE delivery point is put at the end of phase c, as illustrated in figure Figure 3 – “Thales” life-cycle. At this stage, the TOE is entirely built and protects itself through the security mechanisms implemented in the operating system and the underlying IC.

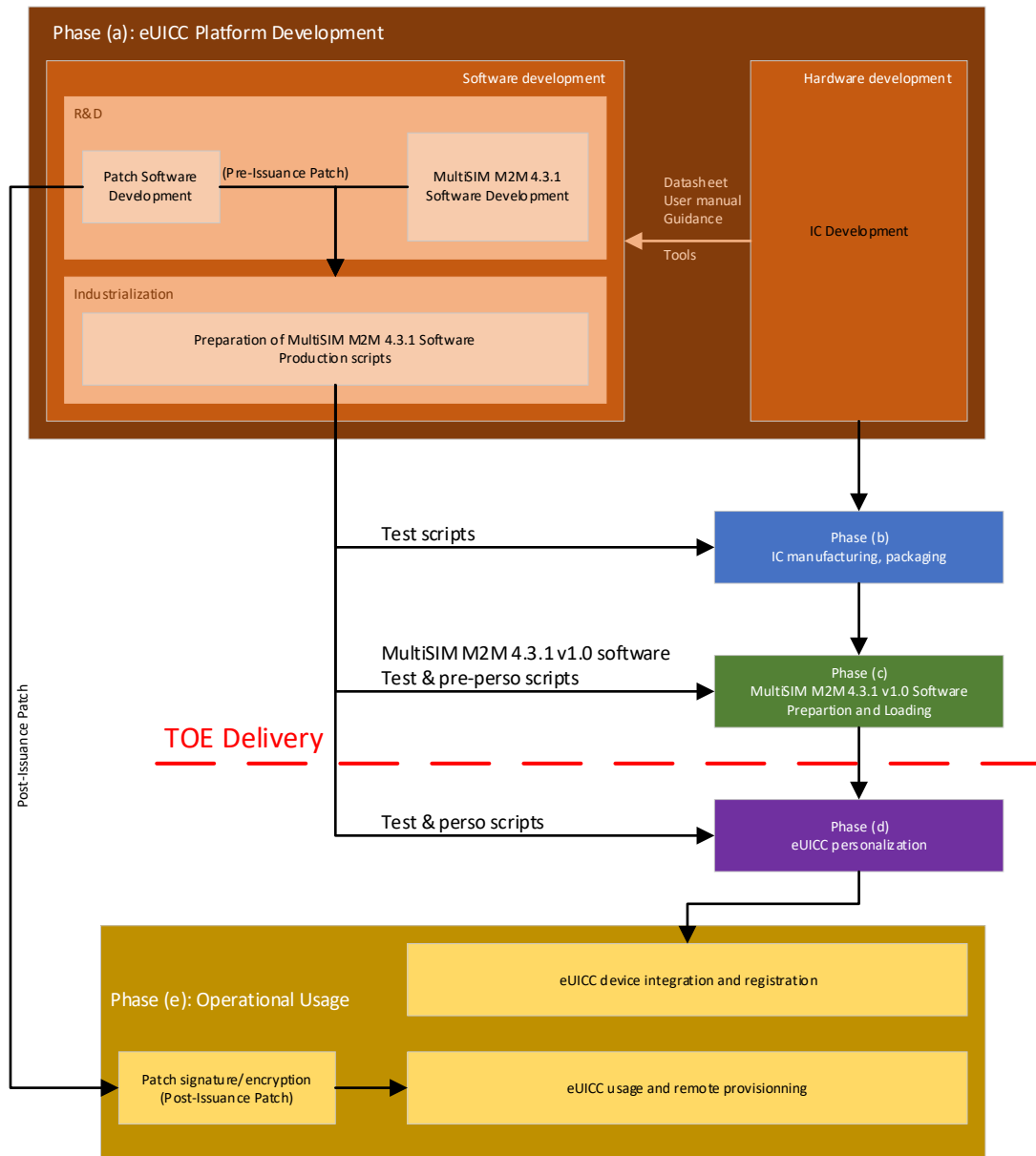


Figure 3 – "Thales" life-cycle

**Note: the TOE has an OS Update capability. If a patch is needed once the TOE is on the field, its development and validation will be done by Thales during phase a, and patch deployment will be performed by the OEM during phase e. The corresponding steps are highlighted in grey color in Table 1 – "Thales" life cycle below:**

Phase	Description	Actor	Location
a	MultiSIM M2M 4.3.1 v1.0 SW development (OS and Crypto)	Thales	Thales DIS: Singapore, La Ciotat (France)

	Optional OS UPDATE case: Patch development and validation	Thales	Thales DIS: Singapore, La Ciotat (France)
	MultiSIM M2M 4.3.1 v1.0 SW industrialization preparation:  Product Engineering, Process definition and tools, OS static image preparation (for usage in phase c)	Thales	Thales DIS: Géménos(France), Singapore, Tczew(Poland)
	ORION IC development	INVIA	Development sites stated in the Orion certificate
b	ORION IC manufacturing and packaging	INVIA	Manufacturing sites stated in the Orion certificate
c	eUICC OS secure static image build and secure dynamic data generation		
	Product Engineering: Process definition and tools	Thales	Thales DIS: Géménos (France)
	CPC Team: eUICC OS static image preparation	Thales CPC Team	Thales DIS: Tczew (Poland)
	Data Generation: Dynamic data generation upon input file reception	Thales Datagen Team	Thales DIS: Pont-Audemer (France)
	eUICC OS static image and Dynamic data loading in IC	Thales	Thales DIS: Pont-Audemer (France), Cuernavaca(Mexico), Shanghai(China), Curitiba(Brazil)
<b>TOE delivery</b>			
d	Personalization of data. Final tests	Thales or any other SAS-UP accredited company	eUICC Personalizer SAS-UP accredited site
Device is delivered to point of sales and is reaching end user			
e	eUICC device integration and registration	Device Manufacturer	Sites manufacturing the targeted M2M device
	eUICC remote provisioning	Profile Issuer	Field
	Optional OS UPDATE case: Remote loading of patch on deployed eUICC	Profile Issuer	Field

Table 1 – "Thales" life cycle

### 2.2.2.3 "Alternative" life cycle

In the alternative life-cycle, the integration of the MultiSIM M2M 4.3.1 v1.0 Embedded Software into the IC is done by an accredited manufacturing actor. The life cycle is composed of 5 phases which are

described in Table 2 – "Alternative" life cycle. The table also mentions the actor(s) involved in each phase, as well as the associated location(s).

The loading of the MultiSIM M2M 4.3.1 v1.0 Embedded Software occurs during phase c, after which the IC loading service is locked and no more available. In this life cycle, the TOE delivery point is put at the end of phase c, as illustrated in Figure 4 – "Alternative" life-cycle below.

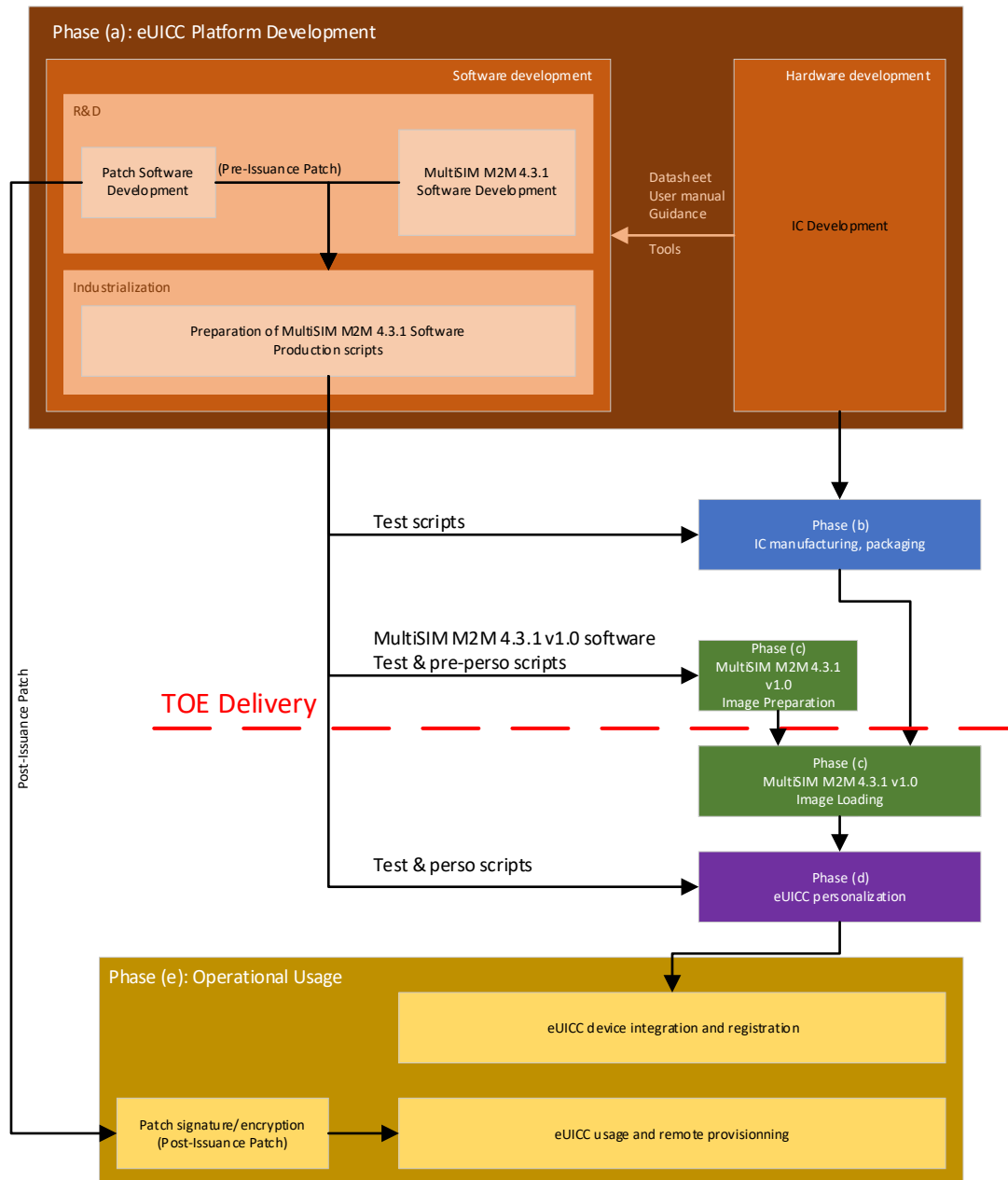


Figure 4 – "Alternative" life-cycle

At the TOE delivery point, the accredited manufacturing actor receives the TOE in two separate parts:

- IC, already initialized with a dedicated IC loading key (in phase (b)).

- Software MultiSIM M2M 4.3.1 v1.0 TOE representation, containing static image and dynamic data (post-loading scripts) , prepared by Thales and encrypted with an appropriated encryption key (phase (c)).

This script (static image and dynamic data) is sent to accredited manufacturing actor with integrity and confidentiality protections using Thales proprietary Secure File Transfer system and appropriate additional transport keys.

The static image loading and integration is performed by the SAS-UP accredited manufacturing actor through a black box process using Thales in-house protocol at the end of phase (c). The accredited manufacturing actors have no plaintext access to static image nor dynamic data.

The dynamic data is sent to the IC which decrypts it on-the-fly, after which the IC loading service is locked and no more available.

The same note as above about OS Update capability applies. If a patch is needed once the TOE is on the field, its development and validation will be done by Thales during phase (a), and patch deployment will be performed by the OEM during phase (e). The corresponding steps are highlighted in grey color in Table 2 – "Alternative" life cycle below.

Phase	Description	Actor	Location
a	MultiSIM M2M 4.3.1 v1.0 SW development (OS and Crypto)	Thales	Thales DIS: Singapore, La Ciotat (France)
	Optional OS UPDATE case: Patch development and validation	Thales	Thales DIS: Singapore, La Ciotat (France)
	MultiSIM M2M 4.3.1 v1.0 SW industrialization preparation: Product Engineering, Process definition and tools, OS static image preparation (for usage in phase c)	Thales	Thales DIS: Géménos(France), Singapore, Tczew
	ORION IC development	INVIA	Development site(s) stated in the Orion certificate
b	ORION IC manufacturing and packaging	INVIA	Manufacturing site(s) stated in the Orion certificate
c	eUICC OS secure static image build and secure dynamic data generation		
	Product Engineering: Process definition and tools	Thales	Thales DIS: Géménos (France)
	eUICC OS static image preparation	Thales CPC Team	Thales DIS: Tczew (Poland)

	Data Generation: Dynamic data generation upon input file reception	Thales Datagen Team	Thales DIS: Pont-Audemer (France)
	<b>TOE delivery:</b>		
	<ul style="list-style-type: none"> <li>• <b>HW part: IC is delivered from phase (b)</b></li> <li>• <b>SW part: Static image and dynamic data are securely delivered for integration on IC</b></li> </ul>		
	eUICC OS static image and dynamic data loading in IC	SAS-UP Accredited manufacturing actor	Accredited manufacturing actor site
d	Personalization of data. Final tests	eUICC Personalizer: any other SAS-UP accredited company	eUICC Personalizer SAS-UP accredited site
Device is delivered to point of sales and is reaching end user			
e	eUICC device integration and registration	Device Manufacturer	Sites manufacturing the targeted M2M device
	eUICC remote provisioning	Profile Issuer	Field
	Optional OS UPDATE case: Remote loading of patch on deployed eUICC	Profile Issuer	Field

Table 2 – "Alternative" life cycle

### 2.2.3 Non-TOE HW/SW/FW available to the TOE

Non-TOE is same than the ones mentioned in section 1.2.4 of [PP-eUICC]. Only a summary of these components is provided below:

- The TOE is intended to be plugged in a M2M device that is not part of the TOE, but it provides power and communication means to external world.
- The provisioning system and relevant network infrastructure are not part of TOE, but they interact with it to manage profile provisioning and administration. It includes at least remote servers of:
  - SM-DP and SM-SR, which provides Profile management commands and Profile,
  - MNO OTA Platforms.
  - MNO-SD is a Security Domain owned and managed by MNO via OTA. It is responsible for securely storing and managing the MNO's credentials and applications on the eUICC (MNO-SD is representative of MNO on the profile)
- Application to be included in profile shall be verified prior loading using appropriate tool (Byte code verifier BCV) located in IoT device environment.

## 2.3 TOE Physical scope

The physical boundaries encompass the MultiSIM M2M 4.3.1 v1.0 software executed inside the IC hardware. The TOE physical boundaries consist of the following components:

TOE component	Developer	Item	Identifier	Form of delivery
IC	Thales	Orion hardware	ORION_TOE_v5: ORION_CB_03 ORION_DB_03	Diced wafer – MFF2 (Embedding eUICC OS)
eUICC OS	Thales	MultiSIM M2M 4.3.1 v1.0	EID: 83030	Software (Delivered embedded within the IC)
eUICC guidances	Thales	MultiSIM M2M 4.3.1 v1.0	[GUIDANCE]	Document (Electronic document (PDF) delivered via secure email)

## 2.4 TOE Logical scope

The present Security Target claims conformance to the [PP-eUICC] protection profile; the TOE logical boundaries are delimited (dash line in red) on Figure 5 – TOE logical boundaries below

Note that the widely use “platform” term encompasses the following TOE parts:

- $\mu$ KOS: low level OS services tightly related to the hardware,
- JKernel: Java Card Runtime Environment and GlobalPlatform components,
- JTE: eUICC GSMA Remote Provisioning and Telecom related features.

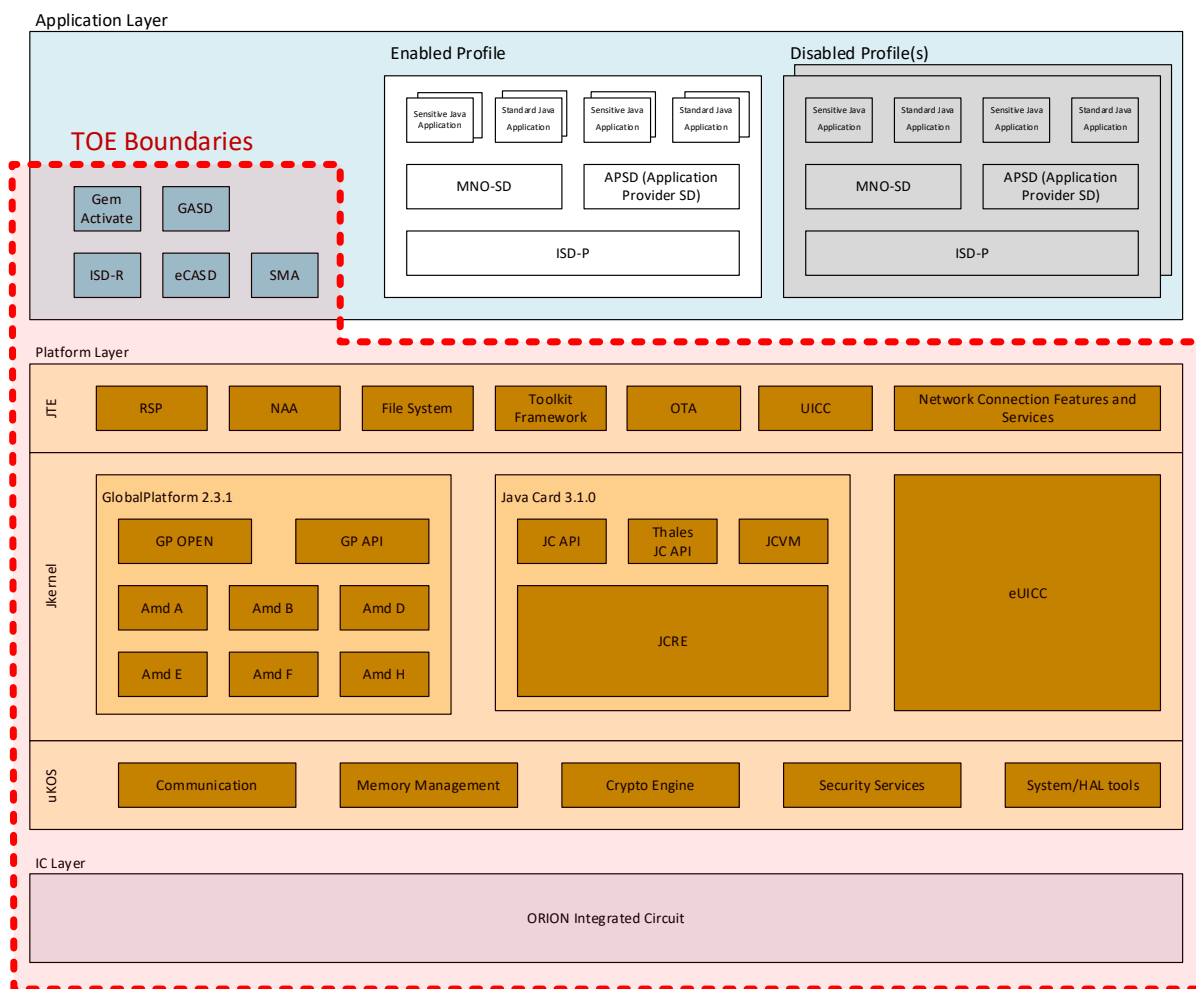


Figure 5 – TOE logical boundaries

## 2.4.1 Application layer

### 2.4.1.1 Profiles

The goal of the application layer is to implement the eUICC functionalities described in [SGP.02], which rely on the notion of Profile. A Profile is the combination of a file structure, data and applications to be provisioned onto, or present on, a eUICC. Each Profile, combined with the functionality of the eUICC, behaves basically as a SIM card. A eUICC may contain more than one Profile, but one and only one is activated at a time. Each Profile is controlled by a unique ISD-P; consequently, there is one and only one enabled ISD-P at a time on the eUICC.

A Profile can have several forms:

- A Provisioning Profile: A Profile containing Network Authentication Parameters. When installed on a eUICC, it enables access to communication network(s), only to provide transport capability for eUICC management and Profile management between the eUICC and an SM-SR.

- An Operational Profile: A Profile containing Network Authentication Parameters as well as MNO's applications and 3rd party applications.
- A Test Profile: A Profile that is used to provide connectivity to test equipment and cannot be used to connect to any MNO.
- Additionally, an operational profile can be set with the Emergency Profile attribute which can be only used to make/receive Emergency calls.

The present document will use the term "Profile" to describe either Provisioning Profiles, operational Profiles or Test Profiles.

All Profiles include Network Access Applications and associated Parameters, but these applications rely on the algorithms stored in the Platform layer of the eUICC. In the same manner, the Profile includes policy rules (POL1 data) but rely on the Platform layer to have them enforced on the eUICC.

The Profile structure, composed of a set of Profile Components, is specified by, and under the full control of, the MNO. The full Profile structure shall be contained in a unique ISD-P. The Profile structure shall contain a Profile Component, called MNO-SD, which performs an identical Role as the ISD for a UICC. The Profile structure shall include:

- The MNO-SD
- At least one NAA
- POL1, even if not used
- The file system
- Connectivity parameters of the Profile

More details on the Profile can be found in [SGP.02].

#### 2.4.1.2 ISD-P

The ISD-P is the on-card representative of the MNO, or SM-DP if delegated by the MNO.

An ISD-P controls the content of a single MNO Profile. The ISD-P may be created during the operational life of the eUICC. In order to create a new Profile, a SM-DP will use the secure routing functionalities of the SM-SR to:

- Require the creation of a new ISD-P
- Perform a confidential key establishment with the ISD-P
- Download and install the Profile.

The Profile is then managed by SM-SR Platform management commands. It should be noted that the SM-SR shall not have access to the content of a Profile, including the ISD-P.

As defined in [SGP.01], the ISD-P shall:

- Be a separate and independent entity on the eUICC
- Contain a Profile including file system, NAAs and Policy Rules
- Contain a state machine related to creating, enabling and disabling the Profile
- Contain keys for Profile management for the loading and installation phase

- Implement a key establishment protocol to generate a keyset for personalization of the ISD-P
- Be able to receive and decrypt, load and install the Profile created by the SM-DP
- Be able to set its own state to disabled once the Profile is installed
- Provide SCP03(t) capabilities to secure its communication with the SM-DP
- Be able to contain a CASD. This CASD is optional within the Profile and provides services only to security domains of the Profile and only when the Profile is in Enabled state.

### 2.4.1.3 ISD-R

The ISD-R is the on-card representative of the SM-SR that executes the Platform Management commands. An ISD-R shall be created within a eUICC at the time of manufacture.

During operational life of the eUICC, the ISD-R is associated with a single SM-SR, which routes securely the Profiles transmitted by a SM-DP and triggers the Platform management operations (enabling/disabling a Profile, and so on).

As defined in [SGP.01], the ISD-R shall:

- Be created within an eUICC at time of manufacture
- Be associated to an SM-SR
- Not be deleted or disabled
- Provide a secure OTA channel using Platform Management Credentials (SCP80 or SCP81) to the SM-SR
- Implement a key establishment protocol for the support of the change of SM-SR
- Offer wrapping and unwrapping service of the transport part during Profile download
- Be able to create new ISD-Ps with the Cumulative Granted Non Volatile Memory
- Not be able to create any SD except an ISD-P
- Execute Platform Management functions in accordance to the Policy Rules
- Not be able to perform any operation inside an ISD-P.

The ISD-R may change its associated SM-SR during the life of the eUICC.

The Subscription Manager Applet (SMA) complies with the GSMA Remote Provisioning Architecture and is located under the ISD-R. It is used to notify the SM-SR platform whenever there is a change of subscription, to manage the swap to the emergency profile or the fallback procedure. It cannot be installed post-issuance.

### 2.4.1.4 MNO-SD

The MNO-SD is the on-card representative of the MNO Platform. It is, according to [SGP.02], the Security domain part of the Profile, owned by the MNO, providing the Secured Channel to the MNO's OTA Platform. It is used to manage the content of a Profile once the Profile is enabled. The MNO-SD is used to perform two operations on the eUICC:

- Modifying the POL1 policy data, which defines how, and if, the Profile can be disabled or deleted

- Modifying the connectivity parameters of the MNO OTA Platform. The connectivity parameters are a set of data (for example SMSC address) required by the eUICC to open a communication channel (for example SMS, HTTPS).

As defined in [SGP.01], the MNO-SD shall:

- Be associated to itself
- Contain the MNO OTA Keys
- Provide a secure OTA channel (SCP80 or SCP81)
- Have the capability to host Supplementary Security Domains.

#### 2.4.1.5 ECASD

The ECASD is the representative of the off-card entity CI root. It contains the data used to enforce trust in the identities of Actors (eUICC, remote Actors such as SM-SR or SM-DP).

The ECASD provides services to the ISD-P and ISD-R, in order to perform confidential key establishments.

As defined in [SGP.01], the ECASD:

- Is created within an eUICC at time of manufacture
- Cannot be deleted or disabled after delivery
- Is based on the concept of CASD from Global Platform
- Is configured by the eUICC Manufacturer at pre-issuance
- Contains a non-modifiable eUICC private key, the associated Certificate, the CI's root public keys and the EUM keyset for key/certificate renewal
- Is associated to the ISD-R, which provides the underlying secure OTA channel
- Is required for (and is not limited to) establishment of the new keysets in the ISD-P(s) and ISD-R
- Does not support the Mandated DAP verification feature

#### 2.4.1.6 GASD, GemActivate and SMA

The GASD (GemActivate Security Domain) is the Security Domain representing a Thales administrator on the card. This entity can authorize the activation of optional services and the loading of additional code (i.e. patch) post issuance.

The GemActivate application, located under the GASD, is the Thales application supporting this OS Update capability.

SMA (Subscription Management Application) is a Thales proprietary application allowing the local profile swap used also in fallback functionality defined in [SGP.02]. If a local profile management is necessary, SMA communicates with SM-SR (the only entity being allowed to manage the profiles) to remote request the appropriate operation. This component does not claim any security functionality. Conforming to Application Notes 13 and 53 from [PP-eUICC], the fallback functionality is not addressed in this Security Target.

## 2.4.2 Platform layer

MultiSIM M2M 4.3.1 v1.0 implements two major industry standards:

- Oracle's Java Card 3.1.0 [JC31], which consists of the Java Card 3.1.0 Virtual Machine, Java Card 3.1.0 Runtime Environment and the Java Card 3.1.0 Application Programming Interface.
- GlobalPlatform 2.3.1 [GPCS], UICC Configuration.

The platform implements the following services:

- Management and control of the communication between the eUICC and external entities
- Basic security services as follows:
  - Checking environmental operating conditions using information provided by the IC
  - Checking life cycle consistency
  - Providing secure cryptography primitives and algorithms
  - Ensuring the security of the PIN and cryptographic key objects
  - Generating random numbers
  - Handling secure data object and backup mechanisms
  - Managing memory content
- Enforcement of the Java Card firewall mechanism
- Standard Application Programming Interfaces (APIs) such as the Java Card API (JCAPI) and the Global Platform API (GPAPI)
- Proprietary Thales API: Secure API which provides security services to applications
- Creation and management of Security Domains (SSD)
- Management of lifecycle information (for the eUICC, Security Domains and Applications)
- SCP02, SCP03(t), SCP11, SCP80 and SCP81 support
- Secure loading, installation and deletion of applications within each SD
- Secure loading of software patches (OS Update feature implemented by GemActivate mechanism).

Note that the following optional features are not supported by the platform:

- Java Card Remote Method Invocation (JCRMI)
- Contactless features of GP [Amd C] (only the non-contactless features of [Amd C] are supported).

MultiSIM M2M 4.3.1 v1.0 platform also implements a Java Telecom Environment (JTE) compliant with the [GSMA], [ETSI] and [3GPP] specifications. The JTE implements the GSMA Remote SIM Provisioning (RSP) Architecture and supports network authentication and Telecom communication protocols. The following capabilities are supported, according to [SGP.01] and [SGP.02]:

- Extended GlobalPlatform OPEN functions. The extension of the GP capabilities is typically needed to enforce additional states of the SDs (ENABLED and DISABLED) or the restrictions of privileges granted to SDs.
- Policy Enforcement functions, which are in charge of the verification and application of POL1 rules during eUICC Management activities.

- Telecom Framework, which includes algorithms used by Network Access Applications (NAA) to access mobile networks. The NAAs are part of the Profiles, but the algorithms, as part of the Telecom Framework, are provisioned onto the eUICC during manufacturing.

## 3 CONFORMANCE CLAIM

---

### 3.1 Note about CC version 3.1 and CC version 2022

According to [CC:2022-Transition] the new Security Target must be conformed to CC version 2022 even if the used Protection Profiles can still be conformant to CC version 3.1. Some adaptation concerning the SFRs are therefore performed in this Security Target:

- FCS\_RNG, FPT\_EMS, FIA\_API are now defined in [CC:2022-2] and they are no more necessary to be defined as extended components.
- FCS\_CKM.4 is replaced by FSC\_CKM.6.

The corrections and complements from [CC:2022-Errata] are also taken in account.

### 3.2 Composition

This is a composite evaluation, which relies on the ORION IC certificate and evaluation results.

- Certification done under the ANSSI scheme.
- CC certificate: ANSSI-CC-2017/41-R03 [CERT-IC]
- Security Target [ST-IC] strictly conformant to [PP-84]
- CC version: 2022, revision 1
- Assurance level: EAL5+ (ALC\_DVS.2 / AVA\_VAN.5)

The composite evaluation includes the additional composition tasks defined in the [CEM:2022].

### 3.3 Common Criteria Conformance Claims

The Security Target is conformant to Common Criteria 2022 release 1.

This Security Target is conformant to:

- CC Part 1 [CC:2022-1],
- CC Part 2 [CC:2022-2] (extended),
- CC Part 3 [CC:2022-3] (conformant),
- CC Part 5 [CC:2022-5].

The assurance requirement of this Security Target is EAL4 augmented. Augmentation results from the selection of:

- ALC\_DVS.2 Sufficiency of security measures,
- AVA\_VAN.5 Advanced methodical vulnerability analysis,

ADV\_ARC.1.2C is refined as described in [PP-eUICC].

For the composition task, the additional claimed package is COMP from chapter “6 Composite product package” of [CC:2022-5].

### 3.4 Protection Profile (PP) conformance claim

This Security Target claims demonstrable conformance to the [PP-eUICC] protection profile. As the TOE has an OS Update capability, this Security Target claims also the PP Module “OS Update” defined in Annex A of [PP-eUICC].

Additional Protection Profiles are used but this ST does not claim the full conformance for them (only the elements necessary for [PP-eUICC]):

- [PP-JCS] for the Runtime Environment features, as required in section 2.3 of [PP-eUICC],
- [PP-GP] for:
  - “Core” SFRs: complements and refinements comparing to [PP-JCS] concerning Card Content Management features implemented as specified in [GPCS],
  - “OS Update” related SFRs: as required in Annex A.4 of [PP-eUICC].

### 3.5 Conformance claim rationale

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

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

#### 3.5.1 Conformity of the TOE Type

The TOE type for this ST is software on IC.

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

#### 3.5.2 SPD Consistency

##### 3.5.2.1 Assets consistency

All assets<sup>3</sup> 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].

---

<sup>3</sup> Except D.PIN: see rationale in the table.

Assets	PP-eUICC	Data type	Security Target
D.MNO_KEYS	X	User Data	(E)
D.ISDR_KEYS	X	User Data	(E)
D.ISDP_KEYS	X	User Data	(E)
D.PROFILE_NAA_PARAMS	X	User Data	(E)
D.PROFILE_IDENTITY	X	User Data	(E)
D.PROFILE_POL1	X	User Data	(E)
D.PROFILE_CODE	X	TSF Data	(E)
D.TSF_CODE	X	TSF Data	(E)
D.PSF_DATA	X	TSF Data	(E)
D.eUICC_PRIVKEY	X	TSF Data	(E)
D.eUICC_CERT	X	TSF Data	(E)
D.CI_ROOT_PUBKEY	X	TSF Data	(E)
D.EID	X	TSF Data	(E)
D.SECRETS	X	TSF Data	(E)
D.UPDATE_IMAGE	X	TSF Data	(E): From [PP-eUICC] Annex A
D.TOE_IDENTIFIER	X	TSF Data	(E): From [PP-eUICC] Annex A
D.OS-UPDATE_KEY(S)	X	TSF Data	(E): From [PP-eUICC] Annex A
D.APP_CODE		TSF Data	(A): Added from [PP-JCS].
D.APP_C_DATA		TSF Data	(A): Added from [PP-JCS].
D.APP_I_DATA		TSF Data	(A): Added from [PP-JCS].
D.APP_KEYS		TSF Data	(A): Added from [PP-JCS].
D.PIN		TSF Data	(D): Deleted: No PIN features nor semantic is used in M2M specification.
D.API_DATA		TSF Data	(A): Added from [PP-JCS].
D.CRYPTO		TSF Data	(A): Added from [PP-JCS].
D.JCS_CODE		TSF Data	(A): Added from [PP-JCS].
D.JCS_DATA		TSF Data	(A): Added from [PP-JCS].
D.SEC_DATA		TSF Data	(A): Added from [PP-JCS].

Table 3 – Assets Consistency table

### 3.5.2.2 Security aspects

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

Security aspects	PP-eUICC	Security Target
SA.CONFID-UPDATE-IMAGE	X	(E): From [PP-eUICC] Annex A
SA.INTEG -UPDATE-IMAGE	X	(E): From [PP-eUICC] Annex A

Table 4 – Security aspect Consistency table

### 3.5.2.3 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-SR	X	(E)
U.SM-DP	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.DEVICE	X	(E)

Table 5 – User consistency table

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

Subjects	PP-eUICC	Security Target
S.ISD-R	X	(E)
S.ISD-P	X	(E)
S.ECASD	X	(E)
S.PSF	X	(E)
S.TELECOM	X	(E)
S.OSU	X	(E): From [PP-eUICC] Annex A
S.UpdateImageCreator	X	(E): From [PP-eUICC] Annex A
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].

<b>S.JCRE</b>		(A): Added from [PP-JCS].
<b>S.JCVM</b>		(A): Added from [PP-JCS].
<b>S.LOCAL</b>		(A): Added from [PP-JCS].
<b>S.MEMBER</b>		(A): Added from [PP-JCS].
<b>S.CAP_FILE</b>		(A): Added from [PP-JCS].
<b>S.OPEN</b>		(A): Added from [PP-GP].
<b>S.SD</b>		(A): Added from [PP-GP].

Table 6 – Subjects Consistency table

### 3.5.2.4 Threats consistency

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

Threats	PP-eUICC	Security Target
<b>T.UNAUTHORIZED-PROFILE-MNG</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.UNAUTHORIZED-PLATFORM-MNG</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.PROFILE-MNG-INTERCEPTION</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.PLATFORM-MNG-INTERCEPTION</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.UNAUTHORIZED-IDENTITY-MNG</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.IDENTITY-INTERCEPTION</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.UNAUTHORIZED-eUICC</b>	X	(E)
<b>T.UNAUTHORIZED-MOBILE-ACCESS</b>	X	(E)
<b>T.LOGICAL-ATTACK</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.PHYSICAL-ATTACK</b>	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.CONFID-UPDATE-IMAGE.LOAD</b>	X	(E): From [PP-eUICC] Annex A (R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.INTEG-UPDATE-IMAGE.LOAD</b>	X	(E): From [PP-eUICC] Annex A

		(R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.UNAUTH-UPDATE-IMAGE.LOAD</b>	X	(E): From [PP-eUICC] Annex A (R): Assets added from [PP-JCS] are mapped as threatened assets.
<b>T.INTERRUPT_OSU</b>	X	(E): From [PP-eUICC] Annex A (R): Assets added from [PP-JCS] are mapped as threatened assets.

Table 7 – Threats consistency table

### 3.5.2.5 Organizational Security Policies consistency

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

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

Table 8 – Organizational Security Policies Consistency table

### 3.5.2.6 Assumptions consistency

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

Assumptions	PP-eUICC	Security Target
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.CAP_FILE		(A): Added from [PP-JCS].
A.VERIFICATION		(A): Added from [PP-JCS].

Table 9 – Assumptions Consistency table

## 3.5.3 Security Objectives Consistency

### 3.5.3.1 Objective for the TOE consistency

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

Note that OE.RE\* and OE.IC\* from [PP-eUICC] become security objectives from the TOE in the present security target.

O.TOE	PP-eUICC	Security Target
O.PSF	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): From [PP-eUICC] Annex A
O.SECURE_AC_ACTIVATION	X	(E): From [PP-eUICC] Annex A
O.TOE_IDENTIFICATION	X	(E): From [PP-eUICC] Annex A
O.CONFID-UPDATE-IMAGE.LOAD	X	(E): From [PP-eUICC] Annex A
O.AUTH-LOAD-UPDATE-IMAGE	X	(E): From [PP-eUICC] Annex A
O.IC.PROOF_OF IDENTITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.IC.SUPPORT		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.IC.RECOVERY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.PSF		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.SECURE-COMM		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.API		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.DATA-CONFIDENTIALITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.DATA-INTEGRITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.

O.RE.IDENTITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.CODE-EXE		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.

Table 10 – Security objectives for the TOE consistency table

### 3.5.3.2 Objective for Environment consistency

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

Note that OE.RE\* and OE.IC\* from [PP-eUICC] become security objectives from the TOE in the present security target.

OE.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-SR	X	(E)
OE.SM-DP	X	(E)
OE.MNO	X	(E)
OE.IC.PROOF_OF_IDENTITY	X	(D): Removed and replaced by O.IC.PROOF_OF IDENTITY.
OE.IC.SUPPORT	X	(D): Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	(D): Removed and replaced by O.IC.RECOVERY.
OE.RE.PSF	X	(D): Removed and replaced by O.RE.PSF
OE.RE.SECURE-COMM	X	(D): Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	(D): Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	(D): Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	(D): Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	(D): Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	(D): Removed and replaced by O.RE.CODE-EXE
OE.APPLICATIONS	X	(E)
OE.MNO-SD	X	(E)
OE.CONFID_UPDATE_IMAGE.CREATE	X	(E): From [PP-eUICC] Annex A
OE.CAP_FILE		(A): Added from [PP-JCS]

OE.VERIFICATION		(A): Added from [PP-JCS]
OE.CODE-EVIDENCE		(A): Added from [PP-JCS]

Table 11 – Security objectives for the Operational Environment consistency table

### 3.5.4 Conformity of the Requirement (SFR/SAR)

#### 3.5.4.1 SFR consistency

SFR	PP-eUICC	Security Target
Identification & Authentication group from [PP-eUICC]		
FIA_UID.1/EXT	X	(E)
FIA_UAU.1/EXT	X	(E)
FIA_USB.1/EXT	X	(E)
FIA_UAU.4/EXT	X	(E)
FIA_UID.1/MNO-SD	X	(E)
FIA_USB.1/MNO-SD	X	(E)
FIA_ATD.1	X	(E)
FIA_API.1	X	(E)
Communication group from [PP-eUICC]		
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)
Security Domains group from [PP-eUICC]		
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	(E)
FDP_ACC.1/ISDP	X	(E)

FDP_ACF.1/ISDP	X	(E)
FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
Platform Services group from [PP-eUICC]		
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
Security Management group from [PP-eUICC]		
FCS_RNG.1	X	(E)
FPT_EMS.1	X	(E)
FDP_SDI.1	X	(E)
FDP_RIP.1	X	(E)
FPT_FLS.1	X	(E)
FMT_MSA.1/PSF_DATA	X	(E)
FMT_MSA.1/POL1	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_MSA.3	X	(E)
FMT_SMF.1	X	(E)
FMT_SMR.1	X	(E)
Mobile Network Authentication group from [PP-eUICC]		
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.6/Mobile_network	X	(E)
CoreG group from [PP-JCS]		
FDP_ACC.2/FIREWALL		(A): Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A): Added from [PP-JCS].
FDP_IFC.1/JCVM		(A): Added from [PP-JCS].
FDP_IFF.1/JCVM		(A): Added from [PP-JCS].
FDP_RIP.1/OBJECTS		(A): Added from [PP-JCS].
FMT_MSA.1/JCRE		(A): Added from [PP-JCS].
FMT_MSA.1/JCVM		(A): Added from [PP-JCS].
FMT_MSA.2/FIREWALL_JCVM		(A): Added from [PP-JCS].
FMT_MSA.3/FIREWALL		(A): Added from [PP-JCS].

FMT_MSA.3/JCVM		(A): Added from [PP-JCS].
FMT_SMF.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FMT_SMR.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/GP-SCP		(A): Added from [PP-JCS]. Refined as in [PP-GP].
FCS_COP.1/GP-SCP		(A): Added from [PP-JCS]. Refined as in [PP-GP].
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].
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].
InstG group from [PP-JCS]		
FDP_ITC.2/Installer		(R): Removed and added refined from [PP-GP]
FMT_SMR.1/Installer		(R): Removed and added refined from [PP-GP]
FPT_FLS.1/Installer		(R): Removed and added refined from [PP-GP]
FPT_RCV.3/Installer		(R): Removed and added refined from [PP-GP]
ADELG group 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].
ODELG group from [PP-JCS]		
FDP_RIP.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/ODEL		(A): Added from [PP-JCS].
CarG group from [PP-JCS]		
FCO_NRO.2/CM		(R): Removed and added refined from [PP-GP].
FDP_IFC.2/CM		(R): Removed and added refined from [PP-GP].
FDP_IFF.1/CM		(R): Removed and added refined from [PP-GP].
FDP_UIT.1/CM		(R): Removed and added refined from [PP-GP].
FIA_UID.1/CM		(R): Removed and added refined from [PP-GP].
FMT_MSA.1/CM		(R): Removed and added refined from [PP-GP].
FMT_MSA.3/CM		(R): Removed and added refined from [PP-GP].
FMT_SMF.1/CM		(R): Removed and added refined from [PP-GP].
FMT_SMR.1/CM		(R): Removed and added refined from [PP-GP].
FTP_ITC.1/CM		(R): Removed and added refined from [PP-GP].
Refinements of InstG and CarG by the SFRs from [PP-GP]		
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP]. Refinement of FDP_IFC.2/CM.
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP]. Refinement of FDP_IFF.1/CM.
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP]. Refinement of FDP_ITC.2/Installer.
FDP_IFC.2/GP-KL		(A): Added from [PP-GP]. Dependency of FDP_UIT.1/GP.
FDP_IFF.1/GP-KL		(A): Added from [PP-GP]. Dependency of FDP_IFC.2/GP-KL.
FDP_ITC.2/GP-KL		(A): Added from [PP-GP]. Dependency of FCS_COP.1/GP-SCP.
FMT_MSA.1/GP		(A): Added from [PP-GP]. Refinement of FMT_MSA.1/CM from [PP-JCS].
FMT_MSA.3/GP		(A): Added from [PP-GP]. Refinement of FMT_MSA.3/CM from [PP-JCS].

FMT_SMR.1/GP		(A): Added from [PP-GP]. Refinement of FMT_SMR.1/Installer and FMT_SMR.1/CM from [PP-JCS].
FMT_SMF.1/GP		(A): Added from [PP-GP]. Refinement of FMT_SMF.1/CM from [PP-JCS].
FPT_RCV.3/GP		(A): Added from [PP-GP]. Refinement of FPT_RCV.3/Installer from [PP-JCS].
FPT_FLS.1/GP		(A): Added from [PP-GP]. Refinement of FPT_FLS.1/Installer from [PP-JCS].
FPT_TDC.1/GP		(A): Added from [PP-GP]. Dependency of FDP_ITC.2/GP-ELF.
FTP_ITC.1/GP		(A): Added from [PP-GP]. Refinement of FTP_ITC.1/CM from [PP-JCS].
FCO_NRO.2/GP		(A): Added from [PP-GP]. Refinement of FCO_NRO.2/CM from [PP-JCS].
FIA_UID.1/GP		(A): Added from [PP-GP]. Refinement of FIA_UID.1/CM from [PP-JCS].
FDP_UIT.1/GP		(A): Added from [PP-GP]. Refinement of FDP_UIT.1/CM from [PP-JCS].
OS Update related SFR taken from [PP-GP]		
FDP_ACC.1/OS-UPDATE		(A): Added from [PP-GP].
FDP_ACF.1/OS-UPDATE		(A): Added from [PP-GP].
FMT_MSA.3/OS-UPDATE		(A): Added from [PP-GP].
FMT_SMR.1/OS-UPDATE		(A): Added from [PP-GP].
FMT_SMF.1/OS-UPDATE		(A): Added from [PP-GP].
FIA_ATD.1/OS-UPDATE		(A): Added from [PP-GP].
FTP_TRP.1/OS-UPDATE		(A): Added from [PP-GP].
FCS_COP.1/OS-UPDATE-DEC		(A): Added from [PP-GP].
FCS_COP.1/OS-UPDATE-VER		(A): Added from [PP-GP].
FPT_FLS.1/OS-UPDATE		(A): Added from [PP-GP].
IC		
FAU_SAS.1		(A): Added to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added to cover O.IC.RECOVERY.
FPT_RCV.4/OS		(A): Added to cover O.IC.SUPPORT.

Table 12 – Security Functional Requirement consistency table

#### **3.5.4.2 SAR consistency**

This ST claims the same evaluation assurance level as [PP-eUICC], i.e., EAL4 augmented with ALC\_DVS.2 and AVA\_VAN.5.

For the composition needs it is completed with ASE\_COMP.1, ADV\_COMP.1, ATE\_COMP.1, ALC\_COMP.1, and AVA\_COMP.1

## 4 SECURITY PROBLEM DEFINITION

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

### 4.1 Assets

The definition of the assets from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.5.2.1 for complete list of assets.

### 4.2 Users and Subjects

The definition of users and subjects from [PP-eUICC], [PP-JCS] and [PP-GP] where no refinements are made is not repeated here. See section 3.5.2.3 for complete list of users and subjects.

### 4.3 Threats

The definition of threats from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here. See section 3.5.2.4 for complete list of threats.

Refined threats description is detailed below:

Threats	Refined threats description and threatened assets
<b>T.UNAUTHORIZED-PROFILE-MNG</b>	Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, <b>D.APP_C_DATA, D.APP_I_DATA, D.APP_KEYS and D.APP_CODE.</b>
<b>T.UNAUTHORIZED-PLATFORM-MNG</b>	Directly threatened assets are D.ISDR_KEYS, D.TSF_CODE (ISD-R). By altering the behavior of ISD-R, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens D.PSF_DATA and the same assets as T.UNAUTHORIZED-PROFILE-MNG.
<b>T.PROFILE-MNG-INTERCEPTION</b>	Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, <b>D.APP_C_DATA and D.APP_KEYS.</b>
<b>T.PLATFORM-MNG-INTERCEPTION</b>	Directly threatens the assets: D.ISDR_KEYS, D.TSF_CODE (ISD-R) By altering the behavior of ISD-R, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens D.PSF_DATA and the same assets as T.UNAUTHORIZED-PROFILE-MNG.
<b>T.UNAUTHORIZED-IDENTITY-MNG</b>	Directly threatens the assets: D.TSF_CODE (ECASD), D.eUICC_PRIVKEY, D.eUICC_CERT, D.CI_ROOT_PUBKEY, D.EID, D.SECRETS, <b>D.APP_CODE, D.APP_I_DATA, D.APP_KEYS, D.APP_C_DATA and D.SEC_DATA</b>

<b>T.IDENTITY-INTERCEPTION</b>	Directly threatens the assets: D.SECRETS, <b>D.APP_C_DATA</b> and <b>D.APP_KEYS</b>
<b>T.LOGICAL-ATTACK</b>	Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, <b>D.JCS_CODE</b> , <b>D.API_DATA</b> , <b>D.SEC_DATA</b> , <b>D.JCS_DATA</b> , <b>D.CRYPTO</b> , <b>D.APP_CODE</b> , <b>D.APP_I_DATA</b> , <b>D.APP_KEYS</b> and <b>D.APP_C_DATA</b> .
<b>T.PHYSICAL-ATTACK</b>	<b>All assets</b>
<b>T.CONFID-UPDATE-IMAGE.LOAD</b>	Directly threatens the assets: D.UPDATE_IMAGE, <b>D.JCS_CODE</b> , <b>D.JCS_DATA</b>
<b>T.INTEG-UPDATE-IMAGE.LOAD</b>	Directly threatens the assets: D.UPDATE_IMAGE, <b>D.JCS_CODE</b> , <b>D.JCS_DATA</b>
<b>T.UNAUTH-UPDATE-IMAGE.LOAD</b>	Directly threatens the assets: D.UPDATE_IMAGE, <b>D.JCS_CODE</b> , <b>D.JCS_DATA</b>
<b>T.INTERRUPT_OSU</b>	Directly threatens the assets: D.TOE_IDENTIFIER, D.UPDATE_IMAGE, <b>D.JCS_CODE</b> , <b>D.JCS_DATA</b>

Table 13 – Threats

#### 4.4 Security Aspects (added to cover OS update)

The definition of organizational security policies from [PP-eUICC] where no refinements are made is not repeated here. See section 3.5.2.2 for complete list of Security Aspects.

#### 4.5 Organizational Security Policies

The definition of organizational security policies from [PP-eUICC] where no refinements are made is not repeated here. See section 3.5.2.5 for complete list of organizational security policies.

#### 4.6 Assumptions

The definition of assumptions from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here. See section 3.5.2.6 for complete list of assumptions.

## 5 SECURITY OBJECTIVES

This section introduces the security objectives for the TOE.

### 5.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 3.5.3 for complete list of Security Objectives for the TOE.

Some objectives from the environment have been converted to objectives of the TOE, specifically the ones from [PP-eUICC] related to OE.RE\* and OE.IC\*. The replaced objectives from 3.5.3.2 and their description are listed next:

O.TOE	Replaced/Added objectives description
O.IC.PROOF_OF IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	<p>The IC embedded software shall support the following functionalities:</p> <ul style="list-style-type: none"> <li>• It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification).</li> <li>• It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PSF and S.TELECOM).</li> <li>• It allows the S.PSF, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection).</li> <li>• It provides a means to perform memory operations atomically for S.PSF, and S.TELECOM.</li> </ul>
O.IC.RECOVERY	If there is a loss of power while an operation is in progress, the underlying IC must allow the TOE to eventually complete the interrupted operation successfully or recover to a consistent and secure state.
O.RE.PSF	The Runtime Environment shall provide secure means for card management activities, including:

	<ul style="list-style-type: none"> <li>• load of a package file</li> <li>• installation of a package file</li> <li>• extradition of a package file or an application</li> <li>• personalization of an application or a Security Domain</li> <li>• deletion of a package file or an application</li> <li>• privileges update of an application or a Security Domain</li> <li>• access to an application outside of its expected availability</li> </ul>
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.
O.RE.API	The Runtime Environment shall ensure that native code can be invoked only via an API.
O.RE.DATA-CONFIDENTIALITY	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
O.RE.IDENTITY	The Runtime Environment shall ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.

Table 14 – Security Objectives for the TOE

## 5.2 Security Objectives for the Operational Environment

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 here. See section 3.5.3.2 for complete list of Security Objectives for the Operational Environment.

## 5.3 Security Objectives Rationale

### 5.3.1 Threats

#### T.UNAUTHORIZED-PROFILE-MNG

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

- O.PSF and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP and MNO OTA Platform) will access the Security Domains functions and content.

- OE.SM-DP and OE.MNO protect the corresponding credentials when used off-card.

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

The authentication is supported by corresponding secure channels:

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

Since the MNO-SD Security Domain is not part of the TOE, the operational environment has to guarantee that it will use securely the SCP80/81 secure channel provided by the TOE (OE.MNOSD).

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.UNAUTHORIZED-PLATFORM-MNG**

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

- O.PSF and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-SR) will access the Security Domains functions and content.
- OE.SM-SR 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 a corresponding secure channel:

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

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-INTERCEPTION**

Commands and profiles are transmitted by the SM-DP to its on-card representative (ISD-P), while POL1 is transmitted by the MNO OTA Platform to its on-card representative (MNO-SD). Consequently, the TSF ensures:

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

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).

Since the MNO-SD Security Domain is not part of the TOE, the operational environment has to guarantee that it will securely use the SCP80/81 secure channel provided by the TOE (OE.MNOSD).

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

#### **T.PLATFORM-MNG-INTERCEPTION**

Commands and profiles are transmitted by the SM-SR to its on-card representative (ISD-R). Consequently, the TSF ensures:

- Security of the transmission to the ISD-R (O.SECURE-CHANNELS and O.INTERNALSECURE-CHANNELS) by requiring authentication from SM-SR, 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).

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).

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

#### **T.UNAUTHORIZED-IDENTITY-MNG**

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

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

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

#### **T.IDENTITY-INTERCEPTION**

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

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

#### **T.UNAUTHORIZED-eUICC**

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

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

#### **T.UNAUTHORIZED-MOBILE-ACCESS**

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

#### **T.LOGICAL-ATTACK**

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

- by the APIs provided by the Runtime Environment (O.RE.API)
- by the APIs of the TSF (O.API). The APIs of Telecom Framework and Platform Support Functions shall ensure atomic transactions.

Whenever sensitive data of the TOE are processed by applications, confidentiality and integrity must be protected at all times by the Runtime Environment (O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY).

However, these sensitive data are also be processed by the Platform Support Functions and the Telecom Framework, which are not protected by these mechanisms. Consequently:

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

The following objectives for the operational environment are also required:

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

The IC embedded software supports these objectives via the objective O.IC.SUPPORT. In particular, the IC embedded software:

- provides secure low-level cryptographic processing to Platform Support Functions and Telecom Framework (S.PSF and S.TELECOM).
- allows the S.PSF and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection)

## **T.PHYSICAL-ATTACK**

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

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

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

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

## **T.CONFID-UPDATE-IMAGE.LOAD**

- O.CONFID-UPDATE-IMAGE.LOAD Counters the threat by ensuring the confidentiality of D.UPDATE\_IMAGE during installing it on the TOE.
- OE.CONFID-UPDATE-IMAGE.CREATE Counters the threat by ensuring that the D.UPDATE\_IMAGE is not transferred in plain and that the keys are kept secret.

## **T.INTEG-UPDATE-IMAGE.LOAD**

- O.SECURE\_LOAD\_ACODE Counters the threat directly by ensuring the authenticity and integrity of D.UPDATE\_IMAGE

## **T.UNAUTH-UPDATE-IMAGE.LOAD**

- O.SECURE\_LOAD\_ACODE Counters the threat directly by ensuring that only authorized (allowed version) images can be installed.
- O.AUTH-LOAD-UPDATE-IMAGE Counters the threat directly by ensuring that only authorized (allowed version) images can be loaded.

## **T.INTERRUPT\_OSU**

- O.SECURE\_LOAD\_ACODE Counters the threat directly by ensuring that the TOE remains in a secure state after interruption of the OS Update procedure (Load Phase).

- O.TOE\_IDENTIFICATION Counters the threat directly by ensuring that D.TOE\_IDENTIFICATION is only updated after successful OS Update procedure.
- O.SECURE\_AC\_ACTIVATION Counters the threat directly by ensuring that the update OS is only activated after successful (atomic) OS Update procedure.

### 5.3.2 Organizational Security Policies

#### OSP.LIFE-CYCLE

- O.PSF ensures that a blocking orphaned profile can be deleted by the SM-SR, and only by the SM-SR. This deletion capability relies on the secure application deletion mechanisms provided by O.RE.PSF.
- O.PSF ensures that there is a single ISD-P enabled at every moment.
- O.OPERATE contributes to this OSP by ensuring that the PSF security functions are always enforced.

**OSP.VERIFICATION** is upheld by the security objective of the 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 bytecode is valid at execution time. This policy is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that evidence exist that the application code has been verified and not changed after verification, and by the security objective for the TOE O.RE.PSF<sup>4</sup> which shall ensure that the loading of a CAP file into the card is safe.

### 5.3.3 Assumptions

**A.ACTORS.** This assumption is upheld by objectives OE.CI, OE.SM-SR, OE.SM-DP and OE.MNO, which ensure that credentials and otherwise sensitive data will be managed correctly by each actor of the infrastructure.

**A.APPLICATIONS** is directly upheld by OE.APPLICATIONS (which implies verifying all the bytecodes at least once) and by OE.CODE-EVIDENCE (which ensures that the sequence of bytecodes has not changed after their verification).

**A.CAP\_FILE** is upheld by the security objective for the operational environment OE.CAP\_FILE which ensures that no CAP file loaded post-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 bytecode is valid at execution time. This assumption is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that evidence exist that the application code has been verified and not changed after verification.

---

<sup>4</sup> O.LOAD from the OSP.VERIFICATION definition from [PP-JCS] is refined here using O.RE.PSF being the equivalent objective for the runtime environment from [PP-eUICC].

### 5.3.4 Rationale Tables

#### 5.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP, OE.MNO, O.PSF, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNOSD	See 5.3.1
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PSF, O.SECURE-CHANNELS, OE.SM-SR, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	See 5.3.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP, OE.MNO, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, OE.MNOSD	See 5.3.1
T.PLATFORM-MNG-INTERCEPTION	O.SECURE-CHANNELS, OE.SM-SR, OE.APPLICATIONS, O.INTERNAL-SECURECHANNELS, OE.RE.SECURE-COMM	See 5.3.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PSF, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	See 5.3.1
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	See 5.3.1
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	See 5.3.1
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	See 5.3.1

T.LOGICAL-ATTACK	O.IC.SUPPORT, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA- INTEGRITY	See 5.3.1
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.OPERATE, O.DATA-CONFIDENTIALITY, O.RE.DATA- CONFIDENTIALITY	See 5.3.1
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATE-IMAGE.LOAD OE.CONFID-UPDATE-IMAGE.CREATE	See 5.3.1
T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE	See 5.3.1
T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE O.AUTH-LOAD-UPDATE-IMAGE	See 5.3.1
T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE O.TOE_IDENTIFICATION O.SECURE_AC_ACTIVATION	See 5.3.1

Table 15 – Threats and Security Objectives- Coverage

Security Objectives	Threats
O.PSF	T.UNAUTHORIZED-PROFILE-MNG T.UNAUTHORIZED-PLATFORM-MNG T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG T.UNAUTHORIZED-PLATFORM-MNG T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG T.UNAUTHORIZED-PLATFORM-MNG T.PROFILE-MNG-INTERCEPTION T.PLATFORM-MNG-INTERCEPTION
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG T.UNAUTHORIZED-PLATFORM-MNG T.PROFILE-MNG-INTERCEPTION T.PLATFORM-MNG-INTERCEPTION T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK T.PHYSICAL-ATTACK

O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
O.SECURE_LOAD_ACODE	T.INTEG-UPDATE-IMAGE.LOAD T.UNAUTH-UPDATE-IMAGE.LOAD T.INTERRUPT_OSU
O.SECURE_AC_ACTIVATION	T.INTERRUPT_OSU
O.TOE_IDENTIFICATION	T.INTERRUPT_OSU
O.CONFID-UPDATE-IMAGE.LOAD	T.CONFID-UPDATE-IMAGE.LOAD
O.AUTH-LOAD-UPDATE-IMAGE	T.UNAUTH-UPDATE-IMAGE.LOAD
O.IC.PROOF_OF IDENTITY	T.UNAUTHORIZED-eUICC
O.IC.SUPPORT	T.LOGICAL-ATTACK T.PHYSICAL-ATTACK
O.IC.RECOVERY	T.PHYSICAL-ATTACK
O.RE.PSF	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-SR	T.UNAUTHORIZED-PLATFORM-MNG T.PLATFORM-MNG-INTERCEPTION
OE.SM-DP	T.UNAUTHORIZED-PROFILE-MNG T.PROFILE-MNG-INTERCEPTION
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG T.PROFILE-MNG-INTERCEPTION
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG,

	T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG T.PROFILE-MNG-INTERCEPTION
OE.CONFID_UPDATE_IMAGE.CREATE	T.CONFID-UPDATE-IMAGE.LOAD
OE.CAP_FILE	
OE.VERIFICATION	
OE.CODE-EVIDENCE	

Table 16 – Security Objectives and threats

### 5.3.4.2 Organizational Security Policies Rationale

Security Objectives	Threats	Rationale
OSP.LIFE-CYCLE	O.PSF, O.RE.PSF, O.OPERATE	Section 5.3.2
OSP.VERIFICATION	OE.VERIFICATION, O.RE.PSF, OE.CODE-EVIDENCE	Section 5.3.2

Table 17 – Organizational Security Policies and Security Objectives- Coverage

Security Objectives	Organizational Security Policies
O.PSF	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	-
O.SECURE-CHANNELS	-
O.INTERNAL-SECURE-CHANNELS	-
O.PROOF_OF_IDENTITY	-
O.OPERATE	OSP.LIFE-CYCLE
O.API	-
O.DATA-CONFIDENTIALITY	-
O.DATA-INTEGRITY	-
O.ALGORITHMS	-
O.IC.PROOF_OF_IDENTITY	-
O.IC.SUPPORT	-
O.IC.RECOVERY	-
O.RE.PSF	OSP.LIFE-CYCLE, OSP.VERIFICATION
O.RE.SECURE-COMM	-
O.RE.API	-
O.RE.DATA-CONFIDENTIALITY	-
O.RE.DATA-INTEGRITY	-
O.RE.IDENTITY	-
O.RE.CODE-EXE	-
O.SECURE_AC_ACTIVATION	-

O.SECURE_LOAD_ACODE	-
O.TOE_IDENTIFICATION	-
O.CONFID-UPDATE-IMAGE.LOAD	-
O.AUTH-LOAD-UPDATE-IMAGE	-
OE.CI	-
OE.SM-SR	-
OE.SM-DP	-
OE.MNO	-
OE.APPLICATIONS	-
OE.MNO-SD	-
OE.CONFID_UPDATE_IMAGE.CREATE	-
OE.CAP_FILE	-
OE.VERIFICATION	OSP.VERIFICATION
OE.CODE-EVIDENCE	OSP.VERIFICATION

Table 18 – Security Objectives and Organizational Security Policies

### 5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.ACTORS	OE.CI OE.SM-SR OE.SM-DP OE.MNO	Section 5.3.3
A.APPLICATIONS	OE.APPLICATIONS OE.CODE-EVIDENCE	Section 5.3.3
A.CAP_FILE	OE.CAP_FILE	Section 5.3.3
A.VERIFICATION	OE.VERIFICATION OE.CODE-EVIDENCE	Section 5.3.3

Table 19 – Assumptions and Security Objectives for the Operational Environment- Coverage

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-SR	A.ACTORS
OE.SM-DP	A.ACTORS
OE.MNO	A.ACTORS
OE.APPLICATIONS	A.APPLICATIONS
OE.MNO-SD	-
OE.CONFID_UPDATE_IMAGE.CREATE	-
OE.CAP_FILE	A.CAP_FILE
OE.VERIFICATION	A.VERIFICATION
OE.CODE-EVIDENCE	A.APPLICATIONS A.VERIFICATION

Table 20 – Assumptions and Security Objectives for the Operational Environment

## 6 EXTENDED COMPONENTS DEFINITION

---

The same extended component definition than [PP-eUICC] and [PP-84] are defined in the current Security target:

- Extended Family FAU\_SAS – Audit Data Storage

For FAU\_SAS.1, definitions from [PP-84], section 5.3 have been taken with no modification.

## 7 SECURITY FUNCTIONAL AND ASSURANCE REQUIREMENTS

---

### 7.1 eUICC Security Functional Requirements

For section 7.1, the following conventions are used in the definitions of the SFRs:

- Selections and assignments that have already been made in the [PP-eUICC] are in bold, and the original text on which the selection or assignment has been made is not reminded.
- Selections and assignments made in this ST are in blue or bold blue depending if the operation has already been applied in [PP-eUICC].
- Refinements are introduced by using the “Refinements” or “Application Note” words.
- Iteration are introduced by using “/iteration-name” notation after the SFR component name.

#### 7.1.1 Introduction

#### 7.1.2 Identification and Authentication

This package describes the identification and authentication measures of the TOE.

The TOE must:

- identify the remote user U.SM-SR by its smsr-id
- identify the remote user U.SM-DP by its smdp-id
- identify the remote user U.MNO-OTA by its mno-id
- identify the on-card user U.MNO-SD by its AID

The TOE must:

- authenticate U.SM-SR:
  - using CERT.SR.ECDSA (for U.SM-SR first connection, in order to create a shared SCP80/81 keyset)
  - via SCP80/81 once the keyset is initialized
- authenticate U.SM-DP:
  - using CERT.DP.ECDSA (for U.SM-DP first connection, in order to create a shared SCP03(t) keyset)
  - via SCP03(t) once the keyset is initialized
- authenticate U.MNO-OTA via SCP80/81 using the keyset loaded in the MNO profile.

U.MNO-SD is not authenticated by the TOE. It is created on the eUICC during the profile download and installation by the U.SM-DP. For this reason, the U.MNO-SD is bound to the internal subject S.ISD-P and this binding requires the U.SM-DP authentication. During the operational life of the TOE, U.MNO-SD acts on behalf of U.MNO-OTA, thus requiring U.MNO-OTA authentication.

The TOE shall bind the off-card and on-card users to internal subjects:

- U.SM-SR is bound to S.ISD-R
- U.SM-DP is bound to S.ISD-P
- U.MNO-OTA is bound to U.MNO-SD, and U.MNO-SD is bound to the S.ISD-P managing the corresponding MNO profile.

Finally, the TOE shall provide a means to prove its identity to off-card users.

<b>FIA_UID.1/EXT</b>	<b>Timing of identification</b>
----------------------	---------------------------------

**FIA\_UID.1.1/EXT** The TSF shall allow:

- **application selection**
- **requesting data that identifies the eUICC**
- [assignment: requesting non-sensitive configuration data (e.g. available memory size) through GET DATA command].

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 external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA

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.

<b>FIA_UAU.1/EXT</b>	<b>Timing of authentication</b>
----------------------	---------------------------------

**FIA\_UAU.1.1/EXT** The TSF shall allow:

- **application selection**
- **requesting data that identifies the eUICC**
- **user identification**
- [assignment: requesting non-sensitive configuration data (e.g. available memory size) through GET DATA command].

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 external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA

#### **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:

- **smsr-id is associated to S.ISD-R, acting on behalf of U.SM-SR**
- **smdp-id is associated to S.ISD-P, acting on behalf of U.SM-DP**
- **mno-id is associated to U.MNO-SD, acting on behalf of U.MNO-OTA.**

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

- **Initial association of smsr-id requires U.SM-SR to be authenticated via "CERT.SR.ECDSA"**
- **Initial association of smdp-id and mno-id requires U.SM-DP to be authenticated via "CERT.DP.ECDSA".**

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

- **change of smsr-id requires U.SM-SR to be authenticated via "CERT.SR.ECDSA"**
- **change of smdp-id and mno-id is not allowed.**

Application Note:

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

- U.SM-SR binds to a subject (S.ISD-R)
- U.SM-DP binds to a subject (S.ISD-P)
- U.MNO-OTA binds to an on-card user (U.MNO-SD)

This SFR is related to the following commands:

- Initial association and change of the D.ISDP\_KEYS keyset is performed by the ES8.EstablishISDPKeySet command
- Initial association and change of the D.ISDR\_KEYS keyset is performed by the ES5.EstablishISDRKeySet command
- Initial association of the D.MNO\_KEYS keyset is performed by the ES8.DownloadAndInstallation command

#### **FIA\_UAU.4/EXT Single-use authentication mechanisms**

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

- **U.SM-SR**

- **U.SM-DP**
- **U.MNO-OTA.**

Application Note: this SFR is related to the authentication of external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA

#### **FIA\_UID.1/MNO-SD    Timing of identification**

**FIA\_UID.1.1/MNO-SD** The TSF shall allow **application selection** 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.MNOSD is installed on the TOE by the U.SM-DP via the subject S.ISD-P (see "Download and install" in FDP\_ACF.1/ISDP), and the binding between U.SM-DP and S.ISD-P requires authentication of U.SM-DP, as described in FIA\_USB.1/EXT.
- Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user.

#### **FIA\_USB.1/MNO-SD    User-subject binding**

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

**FIA\_USB.1.2/MNO-SD** The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **Initial association of AID requires U.SM-DP to be authenticated via CERT.DP.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-P which is responsible for its installation during the "Profile download and install". This profile

installation is controlled by the FDP\_ACC.1/ISDP SFP. Being performed by the S.ISD-P, it requires authentication of the U.SM-DP.

- In order to perform operations such as POL1 update and connectivity parameters update, U.MNO-OTA authenticates, then sends a command to U.MNO-SD, which transmits it to S.ISDP; the operation is eventually executed by the S.ISD-P according to the FDP\_ACC.1/ISDP SFP.
- The identification does not depend on direct authentication of the MNO OTA Platform, but on the authentication of the S.ISD-P: The S.ISD-P installs a profile which includes a U.MNO-SD and associated keyset.

#### **FIA\_ATD.1 User attribute definition**

**FIA\_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users:

- **CERT.SR.ECDSA and smsr-id belonging to U.SM-SR**
- **CERT.DP.ECDSA and smdp-id belonging to U.SM-DP**
- **mno-id belonging to U.MNO-OTA**
- **AID belonging to U.MNO-SD.**

#### **FIA\_API.1 Authentication Proof of Identity**

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

Application Note: this proof is obtained by including the EID value in the eUICC certificate, which is signed by the eUICC Manufacturer.

### **7.1.3 Communication**

This package describes how the TSF shall protect communications with external users.

The TSF shall enforce secure channels (FTP\_ITC.1/SCP and FTP\_ITC.2/SCP):

- between U.SM-SR and S.ISD-R
- between U.SM-DP and S.ISD-P
- between U.MNO-OTA and U.MNO-SD

These secure channels are used to import commands and objects, thus requiring that these commands and objects are consistently interpreted by the TSF (FPT\_TDC.1/SCP).

These secure channels are established according to a security policy (Secure Channel Protocol Information flow control SFP described in FDP\_IFC.1/SCP and FDP\_IFF.1/SCP). This policy specifically requires protection of the confidentiality (FDP\_UCT.1/SCP) and integrity (FDP\_UIT.1/SCP) of transmitted information.

The TSF must use cryptographic means to enforce this protection, and securely manage the associated keysets:

- generation and deletion of D.ISDP\_KEYS and D.ISDR\_KEYS (FCS\_CKM.1/SCP-SM and FCS\_CKM.6/SCP-SM)
- distribution and deletion of D.MNO\_KEYS (FCS\_CKM.2/SCP-MNO and FCS\_CKM.6/SCP-MNO)

#### 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:**
  - U.SM-SR and S.ISD-R
  - U.SM-DP and S.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 the **Secure Channel Protocol Information flow control SFP** based on the following types of subject and information security attributes:

- **users/subjects:**
  - U.SM-SR and S.ISD-R, with security attribute D.ISDR\_KEYS
  - U.SM-DP and S.ISD-P, with security attribute D.ISDP\_KEYS
  - U.MNO\_OTA and U.MNO-SD, with security attribute D.MNO\_KEYS
- **information: transmission of commands.**

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

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

**FDP\_IFF.1.3/SCP** The TSF shall enforce the [assignment: [No additional information flow control SFP rules](#)].

**FDP\_IFF.1.4/SCP** The TSF shall explicitly authorize an information flow based on the following rules: [assignment: [No additional rules](#)].

**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-SR and S.ISD-R if it is not performed in a SCP80 or SCP81 secure channel through SMS, CAT\_TP or HTTPS**
- **The TOE shall reject communication between U.SM-DP and S.ISD-P if it is not performed in a SCP03(t) secure channel, through the tunnel previously created between U.SM-SR and S.ISD-R.**

Application Note: More details on the secure channels can be found in [SGP.02]

- For SM-SR: section 2.2.5.1 and section 2.4
- For SM-DP: section 2.2.5.2 and section 2.5
- For MNO-SD: section 2.2.5.3 and section 2.7

#### FTP\_ITC.1/SCP Inter-TSF trusted channel

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

**FTP\_ITC.1.2/SCP** The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

**FTP\_ITC.1.3/SCP** The TSF shall initiate communication via the trusted channel for **[assignment: List of functions for which a trusted channel is required]**.

#### List of functions for which a trusted channel is required

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 SM-SR to open a SCP80 or SCP81 secure channel to perform Profile Download and Installation, divided in the following steps:
  - The TSF shall permit the SM-SR to transmit a ES5.CreateISDP command
  - The TSF shall then permit the SM-DP to open a SCP03(t) secure channel to transmit
    - a ES8.EstablishISDPKeySet command, followed by
    - a ES8.DownloadAndInstallation command
  - The TSF shall permit the SM-SR to transmit a ES5.EnableProfile command (optional)
- The TSF shall permit the SM-SR to open a SCP80 or SCP81 secure channel to transmit the following Platform Management commands:
  - ES5.EnableProfile
  - ES5.DisableProfile
  - ES5.DeleteProfile
  - ES5.eUICCCapabilityAudit
  - ES5.MasterDelete
  - ES5.SetFallbackAttribute
  - ES5.HandleNotificationConfirmation
  - The TSF shall permit the SM-SR to open a SCP80 or SCP81 secure channel to transmit the following eUICC management commands:
    - ES5.EstablishISDRKeySet
    - ES5.FinaliseISDRhandover
    - ES5.UpdateSMSRAddressingParameters
- The TSF shall permit the SM-SR to open a SCP80 or SCP81 secure channel to modify the connectivity parameters of the SM-DP:
  - The TSF shall then permit the SM-DP to open a SCP03(t) secure channel to transmit a ES8.UpdateConnectivityParameters SCP03 command
- The TSF shall permit the remote OTA Platform to open a SCP80 secure channel to transmit the following Profile management operations:
  - ES6.UpdatePOL1byMNO

- ES6.UpdateConnectivityParametersByMNO
- In terms of commands, the TSF shall initiate communication via the trusted channel for:
  - ES5.HandleDefaultNotification

Application Note: Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP\_KEYS, D.ISDR\_KEYS); see FCS\_CKM.1/SCP-SM for further details
- or distributed along with the profile (D.MNO\_KEYS); see FCS\_CKM.2/SCP-MNO for further details

The cryptographic operations taking place to enforce the SCP03(t), SCP80 and SCP81 secure channel are addressed through FCS\_COP.1/GP-SCP.

### FDP\_ITC.2/SCP Import of user data with security attributes

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

**FDP\_ITC.2.2/SCP** The TSF shall use the security attributes associated with the imported user data.

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

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

**FDP\_ITC.2.5/SCP** The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: [No additional rules](#)].

### 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-SR, U.SM-DP and U.MNO-OTA**
- **Downloaded objects from U.SM-SR, 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: [the interpretation rules specified in \[SGP.02\] chapter 4](#)] 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-SR commands:
  - ES5.CreateISDP,
  - ES5.EnableProfile,

- ES5.DisableProfile,
- ES5.DeleteProfile,
- ES5.eUICCCapabilityAudit,
- ES5.MasterDelete,
- ES5.SetFallbackAttribute,
- ES5.EstablishISDRKeySet,
- ES5.FinaliseISDRhandover,
- ES5.UpdateSMSRAddressingParameters,
- ES5.SetEmergencyProfileAttribute
- Downloaded objects from SM-SR:
  - Platform management keysets
- SM-DP commands:
  - ES8.EstablishISDPKeySet,
  - ES8.DownloadAndInstallation,
  - ES8.UpdateConnectivityParameters SCP03
- Downloaded objects from SM-DP:
  - Profile management keysets,
  - MNO profiles
- MNO commands:
  - ES6.UpdatePOL1byMNO,
  - ES6.UpdateConnectivityParametersByMNO
- Downloaded objects from MNO OTA Platform:
  - POL1 data,
  - Connectivity parameters

<b>FDP_UCT.1/SCP</b>	<b>Basic data exchange confidentiality</b>
----------------------	--

**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
- SM-SR credentials received from SM-SR during handover

Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP\_KEYS, D.ISDR\_KEYS); see FCS\_CKM.1/SCP-SM for further details
- or distributed along with the Profile (D.MNO\_KEYS); see FCS\_CKM.2/SCP-MNO for further details

The cryptographic operations taking place to enforce confidentiality within the SCP03(t), SCP80 and SCP81 secure channel are addressed through FCS\_COP.1/GP-SCP.

### 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
- SM-SR credentials received from SM-SR during handover
- Commands received from the SM-SR, SM-DP, and MNO OTA Platform
- POL1 received from the MNO OTA Platform.

Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP\_KEYS, D.ISDR\_KEYS); see FCS\_CKM.1/SCP-SM for further details
- or distributed along with the Profile (D.MNO\_KEYS); see FCS\_CKM.2/SCP-MNO for further details.

The cryptographic operations taking place to enforce integrity within the SCP03(t), SCP80 and SCP81 secure channel are addressed through FCS\_COP.1/GP-SCP.

### FCS\_CKM.1/SCP-SM Cryptographic key generation

**FCS\_CKM.1.1/SCP-SM** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ElGamal Elliptic Curves key agreement** and specified cryptographic key sizes **256** that meet the following: **ECKA-EG using one of the following standards:**

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard)**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639)**
- **FRP256V1 (ANSSI ECC FRP256V1)<sup>5</sup>.**

Application Note: This key generation mechanism is used to generate:

- D.ISDP\_KEYS keyset via the ES8.EstablishISDPKeySet command, using the U.SM-DP public key included in CERT.DP.ECDSA
- D.ISDR\_KEYS keyset via the ES5.EstablishISDRKeySet command, using the U.SM-SR public key included in CERT.SR.ECDSA

<sup>5</sup> In this TOE, the FRP256V1 (ANSSI ECC FRP256V1) is not supported

**FCS\_CKM.2/SCP-MNO Cryptographic key distribution**

**FCS\_CKM.2.1/SCP-MNO** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: **distribution method from SCP03t [SGP.02]**] that meets the following: [assignment: **[SGP.02]**].

Application Note: This SFR is related to the distribution of

- D.MNO\_KEYS during profile download
- Public keys distributed in the user certificates (CERT.SR.ECDSA and CERT.DP.ECDSA) or loaded pre-issuance of the TOE (D.eUICC\_CERT, D.CI\_ROOT\_PUBKEY)

This SFR does not apply to the private keys loaded pre-issuance of the TOE (D.eUICC\_PRIVKEY)

**FCS\_CKM.6/SCP-SM Timing and event of cryptographic key destruction**

**FCS\_CKM.6.1/SCP-SM** The TSF shall destroy [assignment: **D.ISDP\_KEYS, D.ISDR\_KEYS, CERT.SR.ECDSA, CERT.DP.ECDSA, D.eUICC\_CERT, D.eUICC\_PRIVKEY, D.CI\_ROOT\_PUBKEY**] 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 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 Timing and event of cryptographic key destruction**

**FCS\_CKM.6.1/SCP-MNO** The TSF shall destroy [assignment: **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 in accordance with a specified cryptographic key destruction method [assignment: **wipe the buffer with random bytes**] that meets the following: [assignment: **None**].

#### 7.1.4 Security Domains

This package describes the specific requirements applicable to the Security Domains belonging to the TOE. In particular it defines:

- The rules under which the S.ISD-R can perform its functions (ISD-R access control SFP in FDP\_ACC.1/ISDR and FDP\_ACF.1/ISDR)
- The rules under which the S.ISD-P can perform its functions (ISD-P access control SFP in FDP\_ACC.1/ISDP and FDP\_ACF.1/ISDP)
- The rules under which the S.ISD-R and S.ISD-P can perform ECASD functions and obtain output data from these functions (ECASD content access control SFP in FDP\_ACC.1/ECASD and FDP\_ACF.1/ECASD)

<b>FDP_ACC.1/ISDR</b>	<b>Subset access control</b>
-----------------------	------------------------------

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

- **subjects: S.ISD-R**
- **objects: S.ISD-R and S.ISD-P**
- **operations:**
  - **Create (S.ISD-P)**
  - **Enable (S.ISD-P)**
  - **Disable (S.ISD-P)**
  - **Delete (S.ISD-P)**
  - **Set the fallback attribute (S.ISD-P)**
  - **Set the Emergency profile attribute (S.ISD-P)**
  - **Perform a capability audit (S.ISD-P)**
  - **Perform a Master Delete (S.ISD-P)**
  - **Updating the SM-SR addressing parameters (S.ISD-R)**
  - **Finalizing the SM-SR handover (S.ISD-R).**

Application Note: This policy describes the rules to be applied to access Platform Management operations. It covers the access to all operations by ISD-R required by sections 3.x of [SGP.02].

It should be noted that ISD-R is subject and object of this SFP, since the SFP controls the modification of S.ISD-P and S.ISD-R by S.ISD-R.

<b>FDP_ACF.1/ISDR</b>	<b>Security attribute based access control</b>
-----------------------	--

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

- **subjects:**
  - **S.ISD-R**
- **objects:**
  - **S.ISD-R with security attribute "state"**
  - **S.ISD-P with security attributes "state", "fallback" and "POL1"**
- **operations:**
  - **Create (S.ISD-P)**
  - **Enable (S.ISD-P)**
  - **Disable (S.ISD-P)**
  - **Delete (S.ISD-P)**
  - **Set the fallback attribute (S.ISD-P)**
  - **Set the Emergency profile attribute (S.ISD-P)**
  - **Perform a capability audit (S.ISD-P)**
  - **Perform a Master Delete (S.ISD-P)**
  - **Updating the SM-SR addressing parameters (S.ISD-R)**
  - **Finalizing the SM-SR handover (S.ISD-R).**

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

**Authorized states:**

- **Enabling a S.ISD-P is authorized only if**
  - the corresponding S.ISD-P is in the state "DISABLED" and
  - the previously enabled S.ISD-P is in the state "DISABLED"
- **Enabling a Test/Emergency Profile triggered by U.DEVICE is authorized only if**
  - The corresponding S.ISD-P is a Test Profile and is in state "DISABLED" and Emergency profile is not already enabled or
  - The corresponding S.ISD-P is an Emergency Profile and is in state "DISABLED".
- **Disabling a S.ISD-P is authorized only if**
  - the corresponding S.ISD-P is in the state "ENABLED" or "PERSONALIZED" and
  - the corresponding S.ISD-P's POL1 data allows its disabling and
  - the corresponding S.ISD-P's fallback attribute is not set.
- **Disabling a Test/Emergency Profile triggered by U.DEVICE is authorized only if**
  - The corresponding S.ISD-P is a Test or Emergency Profile and is in state "ENABLED"
- **Deleting a S.ISD-P is authorized only if**
  - the corresponding S.ISD-P is not in the state "ENABLED" and
  - the corresponding S.ISD-P's POL1 data allows its deletion and
  - the corresponding S.ISD-P's fallback attribute is not set or
  - the corresponding S.ISD-P is not a Test Profile
- **Performing a S.ISD-P Master Delete is authorized only if**
  - the corresponding S.ISD-P is in the state "DISABLED" and
  - the corresponding S.ISD-P's fallback attribute is not set and
  - the corresponding S.ISD-P has successfully verified the U.SM-DP token transmitted with the command.

**FDP\_ACF.1.3/ISDR** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **No additional rules.**

**FDP\_ACF.1.4/ISDR** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any of the following operations is rejected if S.ISD-R is not in the state "PERSONALIZED":**

- **Creating an ISD-P**
- **Performing a capability audit on a S.ISD-P**
- **Setting the fallback attribute of a S.ISD-P**
- **Updating the SM-SR addressing parameters on the S.ISD-R**
- **Finalizing the SM-SR handover on the S.ISD-R** o **Any operation on S.ISD-R is forbidden to other subjects than S.ISD-R.**

Application Note: This policy describes the rules to be applied to access Platform Management or eUICC Management operations. It covers the access to all operations by ISD-R required by sections 3.x of [SGP.02], that is:

- CreateISDP (Creating an ISD-P)
- EnableProfile (Enabling a profile)
- DisableProfile (Disabling a profile)
- DeleteProfile (Deleting a profile)

- eUICCCapabilityAudit (Performing a capability audit)
- MasterDelete (Performing a Master Delete)
- SetFallbackAttribute (Setting the fallback attribute)
- UpdateSMSRAddressingParameters (Updating the SM-SR addressing parameters)
- FinaliseISDRhandover (Finalizing the SM-SR handover)

Identification and authentication SFRs (FIA\_\*/EXT) require that these operations are only available for the legitimate user U.SM-SR after being authenticated.

<b>FDP_ACC.1/ISDP</b>	<b>Subset access control</b>
-----------------------	------------------------------

**FDP\_ACC.1.1/ISDP** The TSF shall enforce the **ISD-P access control SFP** on:

- **subjects:**
  - S.ISD-P
- **objects:**
  - Profile (received from U.SM-DP)
  - S.ISD-P
- **operations:**
  - Download and install (Profile)
  - Establish keyset (S.ISD-P)
  - Update the POL1 data (S.ISD-P)
  - Update the ISD-P connectivity parameters using a secure channel SCP03(t) as defined in FDP\_IFF.1.1/SCP (S.ISD-P)
  - Update the ISD-P connectivity parameters by MNO (S.ISD-P).

Application Note: this policy describes the rules to be applied during Platform Management operations. It covers all operations by ISD-P required by sections 3.x of [SGP.02]. NB: this includes Profile installation.

<b>FDP_ACF.1/ISDP</b>	<b>Security attribute based access control</b>
-----------------------	--

**FDP\_ACF.1.1/ISDP** The TSF shall enforce the **ISD-P access control SFP** to objects based on the following:

- **subjects:**
  - S.ISD-P
- **objects:**
  - Profile data (received from U.SM-DP)
  - S.ISD-P with security attribute "state"
- **operations:**
  - Download and install (Profile data)
  - Establish keyset (S.ISD-P)
  - Update the POL1 data (S.ISD-P)
  - Update the ISD-P connectivity parameters using SCP03(t) (S.ISD-P)
  - Update the ISD-P connectivity parameters by MNO (S.ISD-P).

**FDP\_ACF.1.2/ISDP** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **Downloading and installing profile data is authorized only if S.ISD-P's attribute "state" is "PERSONALIZED"**
- **Establishing a D.ISDP\_KEYS keyset is authorized if S.ISD-P's attribute "state" is at least "SELECTABLE"**
- **Updating POL1 is authorized only if S.ISD-P's attribute "state" is "ENABLED"**
- **Updating the ISD-P connectivity parameters by SCP03(t) is authorized only if S.ISD-P's attribute "state" is "DISABLED", "ENABLED"**
- **Updating the ISD-P connectivity parameters by MNO is authorized only if S.ISD-P's attribute "state" is "PERSONALIZED".**

**FDP\_ACF.1.3/ISDP** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[assignment: No additional rules]**.

**FDP\_ACF.1.4/ISDP** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any operation on Profile data or S.ISD-P is forbidden to other subjects than S.ISD-P.**

Application Note: This policy describes the rules to be applied during profile management operations. It covers SM-DP operations described in [SGP.02]:

- DownloadAndInstallation (Downloading and installing a profile)
- EstablishISDPKeySet (Establishing a D.ISDP\_KEYS keyset)
- UpdateConnectivityParameters SCP03 (Updating the ISD-P connectivity parameters using SCP03(t))

Identification and authentication SFRs (FIA\_\*/EXT) require that these operations are only available for the legitimate user U.SM-DP after being authenticated.

It also covers the MNO operations described in [SGP.02]:

- POL1 update (updating the POL1 data)
- UpdateConnectivityParametersByMNO (Connectivity Parameters Update by MNO)

Identification and authentication SFRs (FIA\_\*/EXT and FIA\_\*/MNO-SD) require that these operations are only available for the legitimate user U.MNO-OTA, via the local user U.MNOSD, after being authenticated.

<b>FDP_ACC.1/ECASD</b> <b>Subset access control</b>
---

**FDP\_ACC.1.1/ECASD** The TSF shall enforce the **ECASD content access control SFP** on:

- **subjects:**
  - **S.ISD-R and S.ISD-P**
- **objects:**
  - **S.ECASD**
- **operations:**

- execution of a ECASD function
- access to output data of these functions.

<b>FDP_ACF.1/ECASD</b>	<b>Security attribute based access control</b>
------------------------	--

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

- **subjects:**
  - S.ISD-R and S.ISD-P, with security attribute "AID"
- **objects:**
  - S.ECASD
- **operations:**
  - **execution of a ECASD function:**
    - Verification of a certificate
    - Generation of a random challenge (and access to the generated random challenge)
    - Verification of a signed random challenge using a public key
    - Generation of a shared secret (and access to the generated shared secret)
  - access to output data of these functions.

Application Note: The length of the random challenge is 16 or 32 bytes.

**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-P (resp. S.ISD-R), identified by its AID, shall be authorized to execute the following S.ECASD functions:**

- **Verification of a certificate CERT.DP.ECDSA (resp. CERT.SR.ECDSA)**
- **Generation of a random challenge (and access to the generated random challenge)**
- **Verification of a signed random challenge using PK.DP.ECDSA (resp. PK.SR.ECDSA)**
- **Generation of shared secret (and access to the generated shared secret).**

**FDP\_ACF.1.3/ECASD** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **The value of EID, PK.CI.ECDSA and CERT.ECASD.ECKA may be retrieved by any on-card subject without authentication.**

**FDP\_ACF.1.4/ECASD** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Other data controlled by S.ECASD cannot be accessed by any other subject than S.ECASD.**

### 7.1.5 Platform Services

This package describes the specific requirements applicable to the Platform Support Functions and the Telecom Framework. In particular it defines:

- FDP\_IFC.1/Platform\_services and FDP\_IFF.1/Platform\_services: the measures taken to control the flow of information between the Security Domains and Platform Support Functions (or Telecom Framework)
- FPT\_FLS.1/Platform\_Services: the measures to enforce a secure state in case of failures of Platform Support Functions (or Telecom Framework).

<b>FDP_IFC.1/Platform_services</b>	<b>Subset information flow control</b>
------------------------------------	--

**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.PSF, S.TELECOM)
- **information:**
  - D.PROFILE-NAA-PARAMS
  - D.PROFILE-POL1
- **operations:**
  - installation of a profile
  - POL1 enforcement
  - network authentication.

<b>FDP_IFF.1/Platform_services</b>	<b>Simple security attributes</b>
------------------------------------	-----------------------------------

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

- **users/subjects:**
  - S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"
- **information:**
  - D.PROFILE-NAA-PARAMS
  - D.PROFILE-POL1
- **operations:**
  - installation of a profile
  - POL1 enforcement
  - network authentication.

**FDP\_IFF.1.2/Platform\_services** The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **D.PROFILE-NAA-PARAMS shall be transmitted only:**
  - by U.MNO-SD to S.TELECOM in order to execute the "Network authentication" API function
  - by S.ISD-P to S.PSF using the "Installation" API function
- **D.PROFILE-POL1 shall be transmitted only**
  - by S.ISD-P to S.PSF in order to execute the "POL1 enforcement" function.

**FDP\_IFF.1.3/Platform\_services** The TSF shall enforce [assignment: **no additional information flow control SFP rules**].

**FDP\_IFF.1.4/Platform\_services** The TSF shall explicitly authorize an information flow based on the following rules: [assignment: **No additional rules**].

**FDP\_IFF.1.5/Platform\_services** The TSF shall explicitly deny an information flow based on the following rules: [assignment: **No additional rules**].

Application Note: This SFR aims to control which subject is able to transmit POL1 or network authentication keys to the PSF 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.PSF or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **POL1 enforcement**
  - **Network authentication**
- [assignment: **None**].

### **7.1.6 Security Management**

This package includes several supporting security functions:

- Random number generation that will be used by the ECASD (FCS\_RNG.1)
- User data and TSF self-protection measures:
  - TOE emanation (FPT\_EMS.1)
  - protection from integrity errors (FDP\_SDI.1)
  - residual data protection (FDP\_RIP.1)
  - preservation of a secure state (FPT\_FLS.1)
- Security management measures:
  - Management of security attributes such as PSF data (FMT\_MSA.1/PSF\_DATA), POL1 and connectivity parameters (FMT\_MSA.1/POL1) and keys (FMT\_MSA.1/CERT\_KEYS) with restrictive default values (FMT\_MSA.3)
  - Management of roles and security functions (FMT\_SMR.1 and FMT\_SMF.1)

#### **FCS\_RNG.1 Random number generation**

**FCS\_RNG.1.1** The TSF shall provide a [selection: **hybrid deterministic**] random number generator [selection: **DRG.4**] that implements:

[assignment:

- (DRG.4.1) The internal state of the RNG shall use PTRNG of class PTG.2 as random source.
- (DRG.4.2) The RNG provides forward secrecy.
- (DRG.4.3) The RNG provides backward secrecy even if the current internal state is known.
- (DRG.4.4) The RNG provides enhanced forward secrecy on condition the ALG\_KEYGENERATION or ALG\_TRNG algorithms from [JCAPI310] RandomData class are used.
- (DRG.4.5) The internal state of the RNG is seeded by a PTRNG of class PTG.2.]

**FCS\_RNG.1.2** The TSF shall provide random numbers that meet:

[assignment:

- (DRG.4.6) The RNG generates output for which  $2^{35}$  strings of bit length 128 are mutually different with probability greater than or equal to  $1-1/(2^{58})$ .
- (DRG.4.7) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.]

#### FPT\_EMS.1 TOE Emanation

**FPT\_EMS.1.1** The TOE shall not emit [assignment: Side-channel information (through power consumption, electromagnetic emanations and processing timings)] in excess of [assignment: IC limits] enabling access to:

- D.SECRETS
- D.eUICC\_PRIVKEY
- the secret keys which are part of the following keysets:
  - D.MNO\_KEYS
  - D.ISDR\_KEYS
  - D.ISDP\_KEYS
  - D.PROFILE\_NAA\_PARAMS.

**FPT\_EMS.1.2** The TSF shall ensure [assignment: users] are unable to use the following interface [assignment: ISO7816 Power and IO lines, IC surface] to gain access to:

- D.SECRETS
- D.eUICC\_PRIVKEY
- the secret keys which are part of the following keysets:
  - D.MNO\_KEYS
  - D.ISDR\_KEYS
  - D.ISDP\_KEYS
  - D.PROFILE\_NAA\_PARAMS.

#### FDP\_SDI.1 Stored data integrity monitoring

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

**Refinement:** The notion of integrity-sensitive data covers the assets of the TOE that require to be protected against unauthorized modification, including:

- D.MNO\_KEYS
- D.ISDR\_KEYS
- D.ISDP\_KEYS
- Profile data
  - D.PROFILE\_NAA\_PARAMS
  - D.PROFILE\_IDENTITY
  - D.PROFILE\_POL1
- Identity management data:
  - D.eUICC\_PRIVKEY
  - D.eUICC\_CERT
  - D.CI\_ROOT\_PUBKEY
  - D.EID
  - D.SECRETS

#### FDP\_RIP.1 Subset residual information protection

**FDP\_RIP.1.1** The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from and allocation of the resource to** the following objects:

- D.SECRETS
- D.eUICC\_PRIVKEY
- The secret keys which are part of the following keysets:
  - D.MNO\_KEYS
  - D.ISDR\_KEYS
  - D.ISDP\_KEYS
  - D.PROFILE\_NAA\_PARAMS.

#### FPT\_FLS.1 Failure with preservation of secure state

**FPT\_FLS.1.1** The TSF shall preserve a secure state when the following types of failures occur:

- failure of creation of a new ISD-P by ISD-R
- failure of creation of a profile by ISD-P
- failure of installation due to the presence of an orphaned profile.

#### FMT\_MSA.1/PSF\_DATA Management of security attributes

**FMT\_MSA.1.1/PSF\_DATA** The TSF shall enforce the ISD-R access control policy and ISD-P access control policy to restrict the ability to **modify** the security attributes mentioned in the table below to the subjects mentioned in the table below:

Security attribute	Subject
ISD-P state	S.ISD-R

Security attribute	Subject
from "INSTALLED" to "SELECTABLE" (during ISD-P creation) from "DISABLED" to "ENABLED" (during profile enabling) from "ENABLED" to "DISABLED" (during profile disabling)	
ISD-P state from "SELECTABLE" to "PERSONALIZED" (during profile personalization) from "PERSONALIZED" to "DISABLED" (during profile personalization)	S.ISD-P
ISD-P state from "ENABLED" to "DISABLED" (during fall-back)	S.PSF
Fallback attribute (when setting the fallback attribute)	S.ISD-R

**Refinement: the usage of a table to instantiate this SFR has been done to express the requirement in a more readable manner. The requirement itself is strictly equivalent to the [PP-SGP05] wording.**

Application Note: [SGP02] includes a fallback functionality ensuring that the eUICC is able to detect a loss of connectivity, then fallback to a secure provisioning profile and notify the SM-SR. This function is not addressed by [PP-SGP05] (and hence not addressed by the present ST). However, the fallback attribute is still included, since it has an impact on the lifecycle policy and capacity to disable/delete a given profile (see FDP\_ACF.1/ISDR).

#### FMT\_MSA.1/POL1 Management of security attributes

**FMT\_MSA.1.1/POL1** The TSF shall enforce the **Secure Channel Protocol information flow SFP, ISD-P access control SFP and ISD-R access control SFP** to restrict the ability to **perform the operations mentioned in the table below on the security attributes mentioned in the table below to the subjects mentioned in the table below:**

Security attribute	Operation	Subject
D.PROFILE_POL1	change_default	S.ISD-P, upon request of U.SM-DP via "ES8.DownloadAndInstallation"
D.PROFILE_POL1	query	S.ISD-R, S.ISD-P
D.PROFILE_POL1	modify	S.ISD-P, upon request of U.MNO-SD via "ES6.UpdatePOL1byMNO"
D.PROFILE_POL1	delete	S.ISD-R, upon request of U.SM-SR by "ES5.DeleteProfile"
Connectivity parameters	query	S.ISD-R, S.ISD-P

**Refinement: the usage of a table to instantiate this SFR has been done to express the requirement in a more readable manner. The requirement itself is strictly equivalent to the [PP-SGP05] wording.**

#### FMT\_MSA.1/CERT\_KEYS Management of security attributes

**FMT\_MSA.1.1/CERT\_KEYS** The TSF shall enforce the **Secure Channel Protocol information flow SFP, ISD-P access control SFP, ISD-R access control SFP and ECASD content access control SFP** to

restrict the ability to **perform the operations mentioned in the table below** on **the security attributes mentioned in the table below** to **the subjects mentioned in the table below**:

Security attribute	Operation	Subject
CERT.DP.ECDSA	query	S.ISD-P
D.ISDP_KEYS	change_default	S.ISD-P, upon request of U.SM-DP via "ES8.EstablishISDPKeySet"
D.MNO_KEYS	change_default	S.ISD-P, upon request of U.SM-DP via "ES8.DownloadAndInstallation"
D.ISDP_KEYS	query	S.ISD-P
CERT.SR.ECDSA	query	S.ISD-R
D.ISDR_KEYS	change_default	S.ISD-R, upon request of U.SM-SR via "ES5.EstablishISDRKeySet"
D.ISDR_KEYS	query	S.ISD-R
D.ISDR_KEYS	delete	S.ISD-R, upon request of U.SM-SR via "ES5.FinaliseISDRhandover"
D.ISDP_KEYS and D.MNO_KEYS	delete	S.ISD-R, upon request of U.SM-SR by "ES5.DeleteProfile"
CERT.DP.ECDSA, CERT.SR.ECDSA, D.ISDP_KEYS, D.ISDR_KEYS, D.MNO_KEYS	Any other operation	No actor

**Refinement: the usage of a table to instantiate this SFR has been done to express the requirement in a more readable manner. The requirement itself is strictly equivalent to the [PP-SGP05] wording.**

Application Note: the modification of D.ISDP\_KEYS and D.MNO\_KEYS keysets is forbidden. To modify the keysets, one must delete the profile and load another profile.

### FMT\_MSA.3 Static attribute initialization

**FMT\_MSA.3.1** The TSF shall enforce the **Secure Channel Protocol information flow SFP, ISD-P access control SFP, ISD-R access control SFP and ECASD access 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 **no actor** to specify alternative initial values to override the default values when an object or information is created.

### FMT\_SMF.1 Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions: [assignment: [following list of management functions](#)].

List of management functions:

- Secure Channel Protocol information flow control
- Platform services information flow control
- ISD-R access control
- ISD-P access control
- ECASD content access control.

#### FMT\_SMR.1 Security roles

**FMT\_SMR.1.1** The TSF shall maintain the roles:

- **External users:**
  - U.SM-DP
  - U.SM-SR
  - U.MNO-SD
  - U.MNO-OTA
- **Subjects:**
  - S.ISD-R
  - S.ISD-P
  - S.ECASD
  - S.PSF
  - S.TELECOM.

**FMT\_SMR.1.2** The TSF shall be able to associate users with roles.

Application Note: The roles defined here correspond to the users and subjects defined in section 4.2 Users and Subjects.

### 7.1.7 Mobile Network Authentication

#### FCS\_COP.1/Mobile\_network Cryptographic operation

**FCS\_COP.1.1/Mobile\_network** The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE**, [selection: **TUAK**, **CAVE**] and cryptographic key sizes **according to the corresponding standard** that meet the following:

- **MILENAGE according to standard [TS 35 206] with the following restrictions:**
  - Only use 128-bit AES as the kernel function – do not support other choices
  - Allow any value for the constant OP
  - Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [TS 35 206]
- **TUAK according to [TS 35 231] with the following restrictions:**
  - Allow any value of TOP
  - Allow multiple iterations of Keccak
  - Support 256-bit K as well as 128-bit
  - To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.
- **CAVE according to standard TIA TR-45.AHAG Common Cryptographic Algorithms**

Application Note: The keys used by these algorithms are distributed within the profiles during provisioning (FDP\_ITC.2/SCP) and must be securely deleted (FCS\_CKM.6/Mobile\_network).

<b>FCS_CKM.2/Mobile_network</b>	<b>Cryptographic key distribution</b>
---------------------------------	---------------------------------------

**FCS\_CKM.2.1/Mobile\_network** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: [SCP03t distribution method from SCP-SGP02](#)] that meets the following: [assignment: [SGP.02](#)].

Application Note: The keys in this SFR are the Mobile Network authentication keys included in the asset D.PROFILE\_NAA\_PARAMS. These keys are distributed as a part of the MNO profile during profile download.

<b>FCS_CKM.6/Mobile_network</b>	<b>Timing and event of cryptographic key destruction</b>
---------------------------------	--

**FCS\_CKM.6.1/Mobile\_network** The TSF shall destroy [assignment: [following List of Cryptographic Keys](#)] when [selection: [no longer needed](#)].

Item	List of Cryptographic keys
Milenage	K, RAND, SQN, AMF
Tuak	K, RAND, SQN, AMF
CAVE	SSDA, LFSR

**FCS\_CKM.6.2/Mobile\_network** 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: [wipe the buffer with random bytes](#)] that meets the following: [assignment: [None](#)].

## 7.2 Runtime Environment Security Functional Requirements

The Subjects (prefixed with an “S”), the Objects (prefixed with an “O”), Information (prefixed with an “I”) are defined and described in [PP-JCS] section 7.2. Security attributes linked to these subjects, objects and information are also defined in [PP-JCS] section 7.2. Finally, Operations (prefixed with “OP”) definition and description are present in [PP-JCS] section 7.2.

### 7.2.1 CoreLG Security Functional requirements

#### 7.2.1.1 Firewall Policy

<b>FDP_ACC.2/FIREWALL Complete access control</b>
---

**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 operations involved in the policy are:

- OP.CREATE,
- OP.INVK\_INTERFACE,
- OP.INVK\_VIRTUAL,
- OP.JAVA,
- OP.THROW,
- OP.TYPE\_ACCESS
- OP.ARRAY\_LENGTH,
- OP.ARRAY\_T\_ALOAD,
- OP.ARRAY\_T\_ASTORE,
- OP.ARRAY\_AASTORE.

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

<b>FDP_ACF.1/FIREWALL Security attribute based access control</b>
---

**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

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

- **R.JAVA.1 ([JCRE3], §6.2.8):** S.CAP\_FILE may freely perform OP.ARRAY\_ACCESS, OP.INSTANCE\_FIELD, OP.INVK\_VIRTUAL, OP.INVK\_INTERFACE, OP.THROW or OP.TYPE\_ACCESS upon any O.JAVAOBJECT whose sharing attribute has value “JCRE entry point” or “global array”.
- **R.JAVA.’ ([JCRE3], §6.2.8):** 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 ([JCRE3], §6.2.8.10):** S.CAP\_FILE may perform OP.TYPE\_ACCESS upon an O.JAVAOBJECT whose Sharing attribute has value “SIO” only if O.JAVAOBJECT is cast into (checkcast) or is being verified as being an instance of (instanceof) an interface that extends the Shareable interface.
- **R.JAVA.4 ([JCRE3], §6.2.8.6):** S.CAP\_FILE may perform OP.INVK\_INTERFACE upon an O.JAVAOBJECT 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:
  - a) The value of the attribute Selection Status of the package whose AID is “CAP File AID” is “Multiselectable”,

- b) The value of the attribute Selection Status of the package 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 only if the value of the Sharing parameter is “Standard”.
  - R.JAVA.6 ([JCRE3], §6.2.8): S.CAP\_FILE may freely perform OP.ARRAY\_ACC“SS or OP.ARRAY\_LENGTH upon any O.JAVAOBJECT whose Sharing attribute has value “global array”.

**FDP\_ACF.1.3/FIREWALL** 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\_ACF.1.4/FIREWALL, provided it is the Currently Active Context.
- 2) The only means that the subject S.JCVM shall provide for an application to execute native code is the invocation of a JavaCard API method (Through OP.INVK\_INTERFACE or OP.INVK\_VIRTUAL).

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

- 1) Any subject with OP.JAVA upon an O.JAVAOBJECT whose LifeTime attribute has value “CLEAR\_ON\_DESELECT” if O.JAVAOBJECT’s Context attribute is not the same as the Selected Applet Context.
- 2) Any subject attempting to create an object by the means of OP.CREATE and a “CLEAR\_ON\_DESELECT” LifeTime parameter if the active context is not the same as the Selected Applet Context.
- 3) S.CAP\_FILE performing OP.ARRAY\_AASTORE of the reference of an O.JAVAOBJECT whose sharing attribute has value “global array” or “Temporary”.
- 4) S.CAP\_FILE performing OP.PUTFIELD or OP.PUTSTATIC of the reference of an O.JAVAOBJECT whose sharing attribute has value “global array” or “Temporary”.
- 5) R.JAVA.7 ([JCRE3], §6.2.8.2): S.CAP\_FILE performing OP.ARRAY\_T\_ASTORE into an array view without ATTR\_WRITABLE\_VIEW access attribute.
- 6) R.JAVA.8 ([JCRE3], §6.2.8.2):S.CAP\_FILE performing OP.ARRAY\_T\_ALOAD into an array view without ATTR\_READABLE\_VIEW access attribute.

#### **FDP\_IFC.1/JCVM Subset information flow control**

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

**FDP\_IFF.1/JCVM Simple security attributes**

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

Subjects	Security attributes
S.JCVM	Currently Active Context

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

- 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].

**FDP\_RIP.1/OBJECTS Subset residual information protection**

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

**FMT\_MSA.1/JCRE Management of security attributes**

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

**FMT\_MSA.1/JCVM Management of security attributes**

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

**FMT\_MSA.2/FIREWALL\_JCVM Secure security attributes**

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

**FMT\_MSA.3/FIREWALL Static attribute authorized**

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

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

**FMT\_MSA.3/JCVM Static attribute authorized**

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

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

**FMT\_SMF.1/JC Specification of Management Functions**

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

**FMT\_SMR.1/JC Security roles**

**FMT\_SMR.1.1/JC** The TSF shall maintain the roles:

- **JavaCard RE(JCRE),**
- **Java Card VM (JCVM).**

**FMT\_SMR.1.2/JC** The TSF shall be able to associate users with roles.

**7.2.1.2 Application Programming Interface****FCS\_CKM.1/GP-SCP Cryptographic key generation**

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

SCP protocol	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP03	AES	128, 192, 256 bits	[Amd D] section 6.2.1
SCP11	AES	128, 192, 256 bits	[Amd F] section 2.1
SCP81	AES	128 bits	[Amd B] section 3.3.2

<b>FCS_COP.1/GP-SCP Cryptographic operation</b>
---

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

SCP protocol	Cryptographic operation	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP03, SCP11	Symmetric Encryption/Decryption	AES in CBC mode	128, 192, or 256 bits	FIPS 197 NIST 800 38A
SCP03 SCP11	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
SCP11	Hash Computing	SHA-256		FIPS 180 4
SCP11	Secure communication channel with the OCE for mutual authentication	ECKA-EG	NIST P-256, brainpoolP256r1	SCP11 [Amd F]: FIPS PUB 186-3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639
SCP80	Secure communication channel with OTA Server	AES	128, 192, or 256 bits	[TS 102.225] [TS 102.226]
SCP81	Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_AES_128_CBC_SHA256		[Amd B] section 3.3.2
SCP-SGP22	Secure communication channel with the SM-DP+ for mutual authentication	ECKA-EG	NIST P-256, brainpoolP256r1	SGP.22: FIPS PUB 186-3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639

SCP- SGP22 (SCP03t)	Secure communication channel with the SM-DP+ for profile download	AES	AES: 128	SGP.02
SCP- SGP22	Secure mutual authentication with the SM-DP+ for PrepareDownload	ECDSA signature generation ECDSA signature verification	NIST P-256, brainpoolP256r1	FIPS PUB 186-4 Digital signature standard, RFC 5639

#### FDP\_RIP.1/ABORT Subset residual information protection

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

#### FDP\_RIP.1/APDU Subset residual information protection

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

#### FDP\_RIP.1/bArray Subset residual information protection

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

#### FDP\_RIP.1/GlobalArray Subset residual information protection

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

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

#### FDP\_RIP.1/KEYS Subset residual information protection

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

**FDP\_RIP.1/TRANSIENT Subset residual information protection**

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

**FDP\_ROL.1/FIREWALL Basic rollback**

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

**FDP\_ROL.1.2/FIREWALL** The TSF shall permit operations to be rolled back within the **scope of a select(), deselect(), process(), install() or uninstall() call, notwithstanding the restrictions given in [JCRE31], §7.7, within the bounds of the Commit Capacity ([JCRE31], §7.8), and those described in [JCAPI31]**.

**7.2.1.3 Card Security Management****FAU\_ARP.1 Security alarms**

**FAU\_ARP.1.1** The TSF shall take **one of the following actions**:

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

upon detection of a potential security violation.

**Refinement:**

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

- CAP file inconsistency,
- typing error in the operands of a bytecode,
- applet life cycle inconsistency,
- card tearing (unexpected removal of the Card out of the CAD) and power failure, abort of a transaction in an unexpected context, (see abortTransaction(), [JCAPI31] and ([JCRE31], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow
- **[assignment: GlobalPlatform card state inconsistency].**

**FDP\_SDI.2/DATA Stored data integrity monitoring and action**

**FDP\_SDI.2.1/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 (i.e. objects instance of classes implemented the interface Key)
- CAP File
- GlobalPlatform card state (OP\_READY, SECURED, ~~CARD\_LOCKED~~, TERMINATE)

The card states CARD\_LOCKED and TERMINATE are not applicable to eUICC.

**FPR\_UNO.1 Unobservability**

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

**FPT\_FLS.1/JC Failure with preservation of secure state**

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

**FPT\_TDC.1 Inter-TSF basic TSF data consistency**

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

**FPT\_TDC.1.2** The TSF shall use

- **the rules defined in [JCVM31] specification,**
- **the API tokens defined in the export files of reference implementation,**
- [assignment: **none**]

when interpreting the TSF data from another trusted IT product.

#### 7.2.1.4 AID Management

##### FIA\_ATD.1/AID User attribute definition

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

**Application note: JC3.1 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.

##### 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 AIDs are defined with associated value during loading and with context identifier]**.

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

**Application note: JC3.1 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.

**FMT\_MTD.3/JCRE Secure TSF data**

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

**7.2.2 InstG Security Functional requirements**

This group consists of the SFRs have been removed from the ST, as covered by their GP equivalent. See [PP-GP] and section 3.5.4.1 of this Security Target.

**7.2.3 ADELG Security Functional Requirements**

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

**FDP\_ACC.2/ADEL Complete access control**

**FDP\_ACC.2.1/ADEL** The TSF shall enforce the **ADEL access control SFP** on **S.ADEL, S.JCRE, S.JCVM, O.JAVAOBJECT, O.APPLET and O.CODE\_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\_PCKG,
- OP.DELETE\_PCKG\_APPLET.

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

**FDP\_ACF.1/ADEL Security attribute based access control**

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

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

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

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

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

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

- **R.JAVA.14 ([JCRE31], §11.3.4.1, Applet Instance Deletion):** S.ADEL may perform OP.DELETE\_APPLET upon an O.APPLET only if,
  - 1) S.ADEL is currently selected,
  - 2) there is no instance in the context of O.APPLET that is active in any logical channel and
  - 3) there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance distinct from O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE31], §8.5) O.JAVAOBJECT is remote reachable.
- **R.JAVA.15 ([JCRE31], §11.3.4.2.1, Multiple Applet Instance Deletion):** S.ADEL may perform OP.DELETE\_APPLET upon several O.APPLET only if,
  - 1) S.ADEL is currently selected,
  - 2) there is no instance of any of the O.APPLET being deleted that is active in any logical channel and
  - 3) there is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.
- **R.JAVA.16 ([JCRE31], §11.3.4.4, Applet/Library Package Deletion):** S.ADEL may perform OP.DELETE\_PKG upon an O.CODE\_PKG only if,
  - 1) S.ADEL is currently selected,
  - 2) no reachable O.JAVAOBJECT, from a package distinct from O.CODE\_PKG that is an instance of a class that belongs to O.CODE\_CAP\_FILE, exists on the card and
  - 3) there is no resident package on the card that depends on O.CODE\_CAP\_FILE.
- **R.JAVA.17 ([JCRE31], §11.3.4.4, Applet Package and Contained Instances Deletion):** S.ADEL may perform OP.DELETE\_PKG\_APPLET upon an O.CODE\_CAP\_FILE only if,
  - 1) S.ADEL is currently selected,

- 2) no reachable O.JAVAOBJECT, from a package 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 package loaded on the card that depends on O.CODE\_CAP\_FILE, and
- 4) for every O.APPLET of those being deleted it holds that: (i) there is no instance in the context of O.APPLET that is active in any logical channel and (ii) there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance not being deleted, or O.JAVAOBJECT is reachable from a package not being deleted, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.

**FDP\_ACF.1.3/ADEL** The TSF shall explicitly 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 packages when one of the deletion operations in FDP\_ACC.2.1/ADEL is performed on them**.

#### **FMT\_MSA.1/ADEL Management of security attributes**

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

#### **FMT\_MSA.3/ADEL Static attribute authorized**

**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 [JCRE31], §11.3.4.**

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

### **7.2.4 ODELG Security Functional Requirements**

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

#### **FDP\_RIP.1/ODEL Subset residual information protection**

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

#### **FPT\_FLS.1/ODEL Failure with preservation of secure state**

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

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

### **7.2.5 CarG Security Functional Requirements**

This group consists of the SFRs have been removed from the ST, as covered by their GP equivalent. See [PP-GP] and section 3.5.4.1 of this Security Target.

### **7.2.6 Global Platform Security Functional requirements**

#### **FDP\_IFC.2/GP-ELF Complete information flow control**

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

- **Subjects: S.SD, S.CAD, S.OPEN**
- **Information: APDU commands INSTALL and LOAD, GlobalPlatform APIs for loading and installing ELF**

and all operations that cause that information to flow to and from subjects covered by the SFP.

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

Application Note:

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

#### **FDP\_IFF.1/GP-ELF Complete information flow control<sup>6</sup>**

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

[assignment:

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

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP03], each with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- ~~**On receipt of INSTALL or LOAD commands, S.OPEN checks that the card Life Cycle State is not CARD\_LOCKED or TERMINATED.**~~
- **S.OPEN accepts an 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].**

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

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

<sup>6</sup> This SFR name is misspelled in [PP-GP]. According to [CC:2022-2] it should be named *FDP\_IFF.1/GP\_ELF Simple security attributes*. Note that the content is correct. In this ST the text from [PP-GP] is kept.

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

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELF**s
- **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 ELF AID is already registered within the card].**

Application Note:

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

#### **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 [JCVM31] and [JCRE31]: 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].**

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

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

**FDP\_IFF.1/GP-KL Complete information flow control<sup>7</sup>**

**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, S.OPEN**
- **GlobalPlatform APDU commands STORE DATA and PUT KEY, 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: SCP03, SCP80, SCP81], each equipped with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **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 card Life Cycle State is not CARD\_LOCKED or TERMINATED.~~
- **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 prior 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].

<sup>7</sup> This SFR name is misspelled in [PP-GP]. According to [CC:2022-2] it should be named *FDP\_IFF.1/GP\_KL Simple security attributes*. Note that the content is correct. In this ST, the text from [PP-GP] is kept.

**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 and SD Life Cycle states.
- S.OPEN fails to verify the privileges belonging to an SD or an 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 that the targeted application implements a personalization interface].

#### 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]].

#### FMT\_MSA.1/GP Management of security attributes

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

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorized Identified Roles with Privileges
DELETE Executable Load File	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorized Identified Roles with Privileges
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	ISD, AM SD, DM SD,
SET STATUS	OP_READY, INITIALIZED, SECURED, <del>or</del> <del>CARD_LOCKED</del>	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, <del>CARD_LOCKED, or TERMINATED</del>	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, <del>or</del> <del>CARD_LOCKED</del>	ISD, AM SD, DM SD, SD

Operations: SCP03 Commands	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorized Identified Roles with Privileges
INITIALIZE UPDATE	OP_READY, INITIALIZED, SECURED, <del>or</del> <del>CARD_LOCKED</del>	None	ISD, AM SD, DM SD, SD
EXTERNAL AUTHENTICATE		C-MAC	

Operations: SCP11 Commands	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorized Identified Roles with Privileges
GET DATA (ECKA Certificate)	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	None	ISD, AM SD, DM SD, SD
GET DATA (CA-KLOC KID-KVN)		None	
PERFORM SECURITY OPERATION		None	
INTERNAL AUTHENTICATE		None	
MUTUAL AUTHENTICATE		None	
STORE DATA (ECKA Certificate)		AUTHENTICATED	
STORE DATA (CA-KLOC Identifier)		AUTHENTICATED	
STORE DATA (Whitelist)		AUTHENTICATED	

Operations: SCP80 Command	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, DEACTIVATE FILE, ACTIVATE FILE, READ BINARY, READ RECORD, CREATE FILE, DELETE FILE, RESIZE FILE, SET DATA, RETRIEVE DATA	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]
Remote Applet Management Commands DELETE, SET STATUS, INSTALL, LOAD, PUT KEY, GET STATUS, GET DATA, STORE DATA	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]	See [TS 102.225] and [TS 102.226]

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

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

Legend for tables above:

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

#### 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.

#### FMT\_SMR.1/GP Security roles

**FMT\_SMR.1.1/GP** The TSF shall maintain the roles:

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

**FMT\_SMR.1.2/GP** The TSF shall be able to associate users with roles.

Application Note: this SFR refines and replaces FMT\_SMR.1/Installer, applied to roles involved in card content management operations.

#### FMT\_SMF.1/GP Specification of Management Functions

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

- **Card and Application Security Management as defined in [GPCS]: Life Cycle, Privileges, Application/SD Locking and Unlocking, Card Locking and Unlocking, Card Termination,**

**Application Status interrogation, Card Status Interrogation, command dispatch, Operational Velocity Checking, and Tracing and Event Logging.**

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

#### **FPT\_RCV.3/GP Automated recovery without undue loss**

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

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

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

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

Application Note:

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

#### **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].**

**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.

**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]**.

**FCO\_NRO.2/GP Enforced proof of origin**

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

- Refinement: The TSF shall be able to generate an evidence of origin at all times for 'Executable Load Files, SD/Application data and keys' received from the off-card entity (originator of transmitted data) that communicates with the card.
- **FCO\_NRO.2.2/GP** The TSF shall be able to relate the [assignment: **identity**] of the originator of the information, and the [assignment: **Executable Load Files, SD/Application data and keys**] of the information to which the evidence applies.
- Refinement: The TSF shall be able to load 'Executable Load Files, SD/Application data and keys' to the card with associated security attributes (the identity of the originator, the destination) such that the evidence of origin can be verified.

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

**FIA\_UID.1/GP Timing of identification**

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

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

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

**FDP\_UIT.1/GP Basic data exchange integrity<sup>8</sup>**

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

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

**FDP\_ACC.1/OS-UPDATE Subset access control**

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

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

**Refinement: S.OSU corresponds to “S.OS-DEVELOPER”**

---

<sup>8</sup> This SFR name is misspelled in [PP-GP]. According to [CC:2022-2] it should be named *FDP\_UIT.1/GP Data exchange integrity*. Note that the SFR content is correct. In this ST the text from [PP-GP] is kept.

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

**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 actually targeting the TOE and that its version is compatible with the TOE version.
- Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading (See OE.OS-UPDATE-ENCRYPTION). Confidentiality protection is achieved through direct encryption of the additional code.

**Refinement:**

- **S.OSU corresponds to “S.OS-DEVELOPER”**
- **D.OS-UPDATE\_KEY(S) corresponds to “D.OS-UPDATE\_SGNVER-KEY” and “D.OS-UPDATE\_DEC-KEY”**
- **OE.CONFID\_UPDATE\_IMAGE.CREATE corresponds to “OE.OS-UPDATE-ENCRYPTION”**

<b>FMT_MSA.3/OS-UPDATE</b>	<b>Security attribute initialization</b>
----------------------------	--

**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.

<b>FMT_SMR.1/OS-UPDATE</b>	<b>Security roles</b>
----------------------------	-----------------------

**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.

<b>FMT_SMF.1/OS-UPDATE</b>	<b>Specification of Management Functions</b>
----------------------------	--

**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 need “to be activated” to become effective.

<b>FIA_ATD.1/OS-UPDATE</b>	<b>User attribute definition</b>
----------------------------	----------------------------------

**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.

<b>FTP_TRP.1/OS-UPDATE</b>	<b>Trusted Path</b>
----------------------------	---------------------

**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, hence the ‘none’ selection in FTP\_TRP.1.1/OS-UPDATE.

**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 with null IV**] and cryptographic key sizes [assignment: **128 bits**] that meet the following: [assignment: **FIPS 197**].

**FCS\_COP.1/OS-UPDATE-VER Cryptographic operation**

**FCS\_COP.1.1/OS-UPDATE-VER** The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm [assignment: **AES-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 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 / step 3 (activation / update of TOE identification data), 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 the TOE identification data is not updated (i.e. initial state)
    - Alternatively, the atomic sequence completes successfully, i.e. the OS update is activated and the TOE identification data is updated accordingly.

## 7.2.7 Underlying platform IC Security Functional Requirements

### FAU\_SAS.1 Audit Storage

**FAU\_SAS.1.1** The TSF shall provide [assignment: **the test process before TOE delivery**] with the capability to store [assignment: **the Initialisation Data, Pre-personalisation Data**] in the [assignment: **chip non-volatile memory**].

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

### FPT\_RCV.3/OS Automated recovery without undue loss

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

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

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

[assignment:

- **the contents of Java Card static fields, instance fields, and array positions that fall under the scope of an open transaction;**
- **the Java Card objects that were allocated into the scope of an open transaction;**
- **the contents of Java Card transient objects;**
- **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.

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

### FPT\_RCV.4/OS Function recovery

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

## 7.3 Security Assurance Requirements

This ST is based on the EAL4 assurance package augmented with the components AVA\_VAN.5 and ALC\_DVS.2. For the composition needs it is completed with ASE\_COMP.1, ADV\_COMP.1, ATE\_COMP.1, ALC\_COMP.1, and AVA\_COMP.1.

The SAR refinement in ADV-ARC.1.2C is the same as described in [PP-eUICC].

## 7.4 Rationale

### 7.4.1 SFRs for eUICC rationale

The security functional requirements rationale is the same than the ones present in section 6.3.2 from [PP-eUICC]:

Security Objective	SFR
O.PSF	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FMT_MSA.1/POL1, FMT_MSA.1/PSF_DATA, FPT_FLS.1, FCS_RNG.1
O.eUICC-DOMAIN-RIGHTS	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FTP_ITC.1/SCP, FMT_MSA.1/POL1, FMT_MSA.1/PSF_DATA, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FCS_RNG.1
O.SECURE-CHANNELS	FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FDP_IFC.1/SCP, FDP_IFT.1/SCP, FCS_CKM.1/SCP-SM, FCS_COP.1/ECKA-EG, FCS_CKM.2/SCP-MNO, FCS_CKM.6/SCP-SM, FCS_CKM.6/SCP-MNO, FIA_UID.1/EXT, FIA_UAU.1/EXT, FCS_COP.1/AUTH_SMSR, FCS_COP.1/AUTH_SMDP, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD, FIA_USB.1/MNO-SD, FIA_USB.1/EXT, FIA_ATD.1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
O.INTERNAL-SECURE-CHANNELS	FPT_EMS.1, FDP_SDI.1, FDP_RIP.1
O.PROOF_OF_IDENTITY	FIA_API.1
O.OPERATE	FPT_FLS.1/Platform_services
O.API	FDP_IFC.1/Platform_services, FDP_IFT.1/Platform_services, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1, FPT_FLS.1/Platform_services
O.DATA-CONFIDENTIALITY	FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FPT_EMS.1, FDP_RIP.1, FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network, FCS_CKM.6/Mobile_network
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FDP_SDI.1
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network, FCS_CKM.6/Mobile_network

The security functional requirements rationale for OS\_UPDATE features from Annex A from [PP-eUICC]:

Security Objective	SFR
O.SECURE_AC_ACTIVATION	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC, FCS_COP.1/OS-UPDATE-VER, FPT_FLS.1/OS-UPDATE
O.SECURE_LOAD_ACODE	FMT_SMF.1/OS-UPDATE, FPT_FLS.1/OS-UPDATE
O.TOE_IDENTIFICATION	FIA_ATD.1/OS-UPDATE
O.CONFID-UPDATE-IMAGE.LOAD	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC
O.AUTH-LOAD-UPDATE-IMAGE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-VER, FPT_FLS.1/OS-UPDATE

#### 7.4.2 SFRs for Runtime Environment rationale

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

Security Objective	SFR
O.RE.PSF	FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_ITC.2/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FDP_ITC.2/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP, FMT_SMR.1/GP, FMT_SMF.1/GP, FPT_RCV.3/GP, FPT_FLS.1/GP, FPT_TDC.1/GP, FTP_ITC.1/GP, FCO_NRO.2/GP, FIA_UID.1/GP, FDP_UIT.1/GP, FDP_ROL.1/GP, FDP_UCT.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FIA_AFL.1/GP, FPT_TDC.1, FMT_MTD.1/JCRE, FDP_ACC.2/ADEL, FDP_ACF.1/ADEL, FDP_RIP.1/ADEL, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL, FPT_FLS.1/ADEL
O.RE.SECURE-COMM	FCS_CKM.1/GP-SCP, FCS_COP.1/GP-SCP, FMT_MSA.1/GP, FMT_MSA.3/GP, FMT_SMR.1/GP, FMT_SMF.1/GP, FPT_TDC.1/GP, FTP_ITC.1/GP, FIA_UID.1/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FPR_UNO.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FIA_AFL.1/GP, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_RIP.1/APDU, FDP_RIP.1/KEYS, FAU_ARP.1, FDP_SDI.2/DATA, FPR_UNO.1, FPT_FLS.1/JCS
O.RE.API	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL
O.RE.DATA-CONFIDENTIALITY	FPR_UNO.1/GP, FIA_AFL.1/ETSI-PIN, FPR_UNO.1/ETSI-PIN, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FDP_RIP.1/OBJECTS, FMT_MSA.1/JCRE,

Security Objective	SFR
	FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_RIP.1/ABORT, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT, FDP_ROL.1/FIREWALL, FAU_ARP.1, FPR_UNO.1, FPT_FLS.1/JCS, FDP_RIP.1/ADEL, FDP_RIP.1/ODEL, FPT_FLS.1/ODEL
O.RE.DATA-INTEGRITY	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_ROL.1/FIREWALL, FAU_ARP.1, FDP_SDI.2/DATA, FPT_FLS.1/JCS
O.RE.IDENTITY	FIA_ATD.1/AID, FIA_UID.2/AID, FIA_USB.1/AID, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE
O.RE.CODE-EXE	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS
O.IC.PROOF_OF IDENTITY	Addressed by FAU_SAS.1 of [ST_IC]
O.IC.SUPPORT	FPT_RCV.4/OS
O.IC.RECOVERY	FPT_RCV.3/OS

### 7.4.3 SFR dependency rationale

SFR	CC dependencies	Satisfied dependencies
SFRs from [PP-eUICC]		
FIA_UID.1/EXT	No Dependencies	-
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1
FIA_UAU.4/EXT	No Dependencies	-
FIA_UID.1/MNO-SD	No Dependencies	-
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1	No Dependencies	-
FIA_API.1	No Dependencies	-
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP and 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 FPT_TDC.1/SCP FTP_ITC.1/SCP
FPT_TDC.1/SCP	No Dependencies	-
FDP_UCT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and	FDP_IFC.1/SCP FTP_ITC.1/SCP

SFR	CC dependencies	Satisfied dependencies
	(FTP_ITC.1 or FTP_TRP.1)	
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_RNG.1, FCS_CKM.6/SCP-SM
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	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 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/ISDP	(FDP_ACF.1)	FDP_ACF.1/ISDP
FDP_ACF.1/ISDP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDP FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	-
FCS_RNG.1	No Dependencies	-
FPT_EMS.1	No Dependencies	-
FDP_SDI.1	No Dependencies	-
FDP_RIP.1	No Dependencies	-
FPT_FLS.1	No Dependencies	-
FMT_MSA.1/PSF_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_ACC.1/ISDP FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/POL1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_ACC.1/ISDP FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP FMT_SMF.1, FMT_SMR.1

SFR	CC dependencies	Satisfied dependencies
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FMT_MSA.1/CERT_KEYS, FMT_SMR.1
FMT_SMF.1	No Dependencies	-
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT FIA_UID.1/MNO-SD
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 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 or FCS_CKM.5)	FDP_ITC.2/SCP
CoreLG from [PP-JCS]		
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 below the table 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_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/GP-SCP	(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_CKM.6/SCP-MNO FCS_RNG.1

SFR	CC dependencies	Satisfied dependencies
FCS_COP.1/GP-SCP	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FCS_CKM.1/GP-SCP FCS_CKM.6/SCP-SM FCS_CKM.6/SCP-MNO
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 below the table
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)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/JC FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
ADELG from [PP-JCS]		
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 below the table
FPT_FLS.1/ADEL	No Dependencies	-
ODELG from [PP-JCS]		
FDP_RIP.1/ODEL	No Dependencies	-
FPT_FLS.1/ODEL	No Dependencies	-
Core from [PP-GP]		
FDP_IFC.2/GP-ELF	(FDP_IFF.1)	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP

SFR	CC dependencies	Satisfied dependencies
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1/GP FTP_ITC.1/GP
FDP_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
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
FMT_MSA.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FMT_SMR.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/GP	No Dependencies	-
FPT_RCV.3/GP	(AGD_OPE.1)	AGD_OPE.1
FPT_FLS.1/GP	No Dependencies	-
FPT_TDC.1/GP	No Dependencies	-
FTP_ITC.1/GP	No Dependencies	-
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UID.1/GP	No Dependencies	-
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF, FDP_IFC.2/GP-KL FTP_ITC.1/GP
OS Update from [PP-GP]		
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 below the table
FMT_SMR.1/OS-UPDATE	(FIA_UID.1)	FIA_UID.1/GP
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 See rationale below the table
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 See rationale below the table
FPT_FLS.1/OS-UPDATE	No dependencies	-
Underlying platform IC		
FAU_SAS.1	No Dependencies	-
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No Dependencies	-

Rationale for exclusion of dependencies:

- **Dependency FMT\_SMF.1 of FMT\_MSA.1/JCRE is unsupported**
  - The dependency between FMT\_MSA.1/JCRE and FMT\_SMF.1 is not satisfied because no management functions are required for the Java Card RE.
- **The dependency FAU\_SAA.1 of FAU\_ARP.1 is unsupported**
  - The dependency of FAU\_ARP.1 on FAU\_SAA.1 assumes that a “potential security violation” generates an audit event. On the contrary, the events listed in FAU\_ARP.1 are self-contained (arithmetic exception, ill-formed bytecodes, access failure) and ask for a straightforward reaction of the TSFs on their occurrence at runtime. The JCVM or other components of the TOE detect these events during their usual working order. Thus, there is no mandatory audit recording in this ST
- **The dependency FIA\_UID.1 of FMT\_SMR.1/ADEL is unsupported**
  - This ST does not require the identification of the “deletion manager” since it can be considered as part of the TSF.
- **The dependency FMT\_MSA.1 of FMT\_MSA.3/OS-UPDATE is unsupported.**
  - No history information must be kept by the TOE.
- **The dependency FCS\_CKM.6 of FCS\_COP.1/OS-UPDATE-DEC and FCS\_COP.1/OS-UPDATE-VER is unsupported.**
  - No destruction of the proprietary KEYS used for OS update.

#### 7.4.4 SAR Evaluation Assurance Level rationale

The EAL4 package and addition of ALC\_DVS.2 and AVA\_VAN.5 are required by [PP-eUICC].

It is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks: the evaluators should have access to the low level design and source code. The lowest for which such access is required is EAL4.

#### 7.4.5 SAR dependency rationale

Security Assurance Requirement	CC dependencies	Satisfied dependencies
<b>ADV_ARC.1</b>	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4 ADV_TDS.3
<b>ADV_FSP.4</b>	(ADV_TDS.1)	ADV_TDS.3
<b>ADV_TDS.3</b>	(ADV_FSP.4)	ADV_FSP.4
<b>ADV_IMP.1</b>	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3 ALC_TAT.1
<b>AGD_OPE.1</b>	(ADV_FSP.1)	ADV_FSP.4
<b>AGD_PRE.1</b>	No dependencies	

Security Assurance Requirement	CC dependencies	Satisfied dependencies
<b>ALC_CMC.4</b>	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4 ALC_DVS.2 ALC_LCD.1
<b>ALC_CMS.4</b>	No dependencies	
<b>ALC_DEL.1</b>	No dependencies	
<b>ALC_DVS.2</b>	No dependencies	
<b>ALC_LCD.1</b>	No dependencies	
<b>ALC_TAT.1</b>	(ADV_IMP.1)	ADV_IMP.1
<b>ASE_CCL.1</b>	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1 ASE_INT.1 ASE_REQ.2
<b>ASE_ECD.1</b>	No dependencies	
<b>ASE_INT.1</b>	No dependencies	
<b>ASE_OBJ.2</b>	(ASE_SPD.1)	ASE_SPD.1
<b>ASE_REQ.2</b>	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1 ASE_OBJ.2
<b>ASE_SPD.1</b>	No dependencies	
<b>ASE_TSS.1</b>	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4 ASE_INT.1 ASE_REQ.2
<b>ATE_COV.2</b>	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4 ATE_FUN.1
<b>ATE_DPT.1</b>	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1 ADV_TDS.3 ATE_FUN.1
<b>ATE_FUN.1</b>	(ATE_COV.1)	ATE_COV.2
<b>ATE_IND.2</b>	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4 AGD_OPE.1 AGD_PRE.1 ATE_COV.2 ATE_FUN.1
<b>AVA_VAN.5</b>	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1 ADV_FSP.4 ADV_IMP.1 ADV_TDS.3 AGD_OPE.1 AGD_PRE.1 ATE_DPT.1

## 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 following Security Features to meet the security functional requirements.

### 8.1 eUICC security functions

#### 8.1.1 GSMA.Ident-Auth

This security function handles the identification and authentication of TOE external actors, according to the [GSMA] specifications:

- Identification and authentication of U.SM-SR
- Identification and authentication of U.SM-DP
- Identification and authentication of U.MNO-OTA
- Identification and authentication of U.MNO-SD

For each actor, all aspects of identification and authentication are implemented according to the [SGP.01] and [SGP.02] specifications, such as:

- Allowed operations before identification/authentication is performed
- Authentication processes (through certificate verification, SCP establishment...)
- Related cryptographic operations
- Definition of security attributes
- User/subject binding
- Prevention of the reuse of authentication data

This security function also provides a proof of the identity of the eUICC to external actors. This proof is obtained by including the EID value in the eUICC certificate, which is signed by the eUICC Manufacturer.

#### 8.1.2 GSMA.SecureChannels

This security function handles the secure channel requirements specified by [SGP.01] and [SGP.02]:

- Between U.SM-SR and S.ISD-R
- Between U.SM-DP and S.ISD-P
- Between U.MNO-OTA and U.MNO-SD
- The related SCPs are SCP03(t), SCP80 and SCP81
- The related SM-SR, SM-DP and MNO-OTA commands, as well as the required protection level (integrity and/or confidentiality), are those specified in [SGP.01] and [SGP.02].
- The generation of ISD-R and ISD-P keysets is also handled by this security function. This operation is also implemented according to [SGP.01] and [SGP.02] specifications.

### 8.1.3 GSMA.SecurityDomains

This security function implements the [SGP.01] and [SGP.02] requirements related to the ISD-R, ISD-P and e-CASD security domains:

- Enforcement of the ISD-R Access Control policy
- Enforcement of the ISD-P Access Control policy
- Enforcement of the e-CASD Access Control policy.

### 8.1.4 GSMA.PlatformServices

This security function monitors the information flow between S.ISD-R, S.ISD-P, U.MNO-SD and the underlying Telecom environment during profile installation, network authentication and profile policy enforcement. In particular, the security function ensures that:

- D.PROFILE-NAA-PARAMS can be transmitted only:
  - by U.MNO-SD to S.TELECOM in order to execute the "Network authentication" API function
  - by S.ISD-P to S.PSF using the "Installation" API function.
- D.PROFILE-POL1 can be transmitted only by S.ISD-P to S.PSF in order to execute the "POL1 enforcement" function.

This security function also ensures that the TOE remains in a secure state in case some failures occur during such information flow.

### 8.1.5 GSMA.SecurityMngt

This security function handles general security requirements related to the GSMA assets, such as:

- Integrity protection of the following GSMA assets: D.MNO\_KEYS, D.ISDR\_KEYS, D.ISDP\_KEYS, D.PROFILE\_NAA\_PARAMS, D.PROFILE\_IDENTITY, D.PROFILE\_POL1, D.eUICC\_PRIVKEY, D.eUICC\_CERT, D.CI\_ROOT\_PUBKEY, D.EID, D.SECRETS.
- Removal of the content of the following GSMA assets/objects upon deallocation/allocation: D.SECRETS, D.eUICC\_PRIVKEY, D.MNO\_KEYS, D.ISDR\_KEYS, D.ISDP\_KEYS, D.PROFILE\_NAA\_PARAMS.
- Ensuring that the TOE remains in a secure state in case of failure during creation of a new ISD-P by ISD-R, during creation of a profile by ISD-P or during installation due to the presence of an orphaned profile.
- Management of ISD-P state and related transitions, and of the fallback attribute, according to the [SGP.01] and [SGP.02] specifications.
- Management of the operations on D.PROFILE\_POL1 according to the [SGP.01] and [SGP.02] specifications.
- Management of the operations on CERT.DP.ECDSA, CERT.SR.ECDSA, D.ISDP\_KEYS, D.ISDR\_KEYS, D.MNO\_KEYS according to the [SGP.01] and [SGP.02] specifications.
- Management of roles according to [SGP.01] and [SGP.02] specifications.

### 8.1.6 GSMA.NetworkAuthent

This security function handles mobile network authentication using the MILENAGE, TUAK or CAVE algorithms. The related keys are distributed according to the [SGP.01] and [SGP.02] specifications.

## 8.2 Runtime Environment security functions

### 8.2.1 GP.CardContentManagement

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

It also checks that only the card management commands specified and allowed at each state of the smart card's life cycle are accepted, and ill-formed ones are rejected with an appropriate error response.

### 8.2.2 GP.KeyLoading

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

### 8.2.3 GP.SecurityDomain

This security function provides security domain management, as SD creation, SD selection, SD privileges setting and SD deletion in SD hierarchy. It provides means to associate or extradite an application to a security domain in order to provide services (as secure channel) to the dedicated application without sharing the related keys stored in SD. It also provides Keyset Management in SD, with Key Set creation, Key set deletion, key importation, replacement, or deletion in Key Set.

Security Domains are privileged Applications as defined in [GPCS], holding cryptographic keys to be used to support Secure Channel Protocol operations and/or to authorize card content management functions. There are different types of security domain with dedicated privileges and associated operations: ISD Security domain, Supplementary Security domains, and Controlling Authority Security domains.

### 8.2.4 GP.SecureChannel

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

A Secure Channel Session is divided into three sequential phases:

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

The following services are provided by the Secure Channel:

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

The following Secure Channel Protocols are supported by the TOE: SCP03, SCP11 (variants 'a' and 'c'), SCP80 and SCP81.

### 8.2.5 GP.GPRegistry

This security function provides management and access to the GlobalPlatform Registry used for:

- Store card management information.
- Store relevant application management information (e.g., AID, associated Security Domain and Privileges).
- Support card resource management data.
- Store Application Life Cycle information.
- Store card Life Cycle information.
- Track any counters associated with logs.

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

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

### 8.2.6 GP.OS-UPDATE

This security function implements an OS update capability by proprietary mechanism, allowing the OS to be updated post-issuance. OS updates are performed through the loading, installation and activation of related ELF's, fulfilling the same rules as for any other ELF.

The whole OS update operation is done through an atomic process, ensuring the permanent consistency between the eSIM 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 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 / step 3 (activation / update of TOE identification data), 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 the TOE identification data is not updated (i.e. initial state)
    - Alternatively, the atomic sequence completes successfully, i.e. the OS update is activated and the TOE identification data is updated accordingly.

### 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 according to [JCAPI31]. The APDU class API is designed to be transport protocol independent T=0, T=1, T=CL (as defined in ISO 7816-3).

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

### 8.2.8 JCS.ByteCodeExecution

This security function handles applet bytecode execution according to the rules defined in [JCAPI31]. The JCVM execution may be summarized in JCVM interpreter start-up, bytecode execution and JCVM interpreter loop. The applet bytecode consists in:

- fetching the next bytecode to execute the applet's code flow control,

- decoding the next bytecode,
- executing the fetched bytecode.

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

### 8.2.9 JCS.Firewall

This security function enforces a Firewall access control policy and a JVM information flow control policy at runtime. It defines how accessing the following items: Static Class Fields, Array Objects, Class Instance Object Fields, Class Instance Object Methods, Standard Interface Methods, Shareable Interface Methods, Classes, Standard Interfaces, Shareable Interfaces, Array Object Methods.

Based on security attributes (Sharing, Context, Lifetime), it performs access control to object fields between objects and throws security exception when access is denied. Thus, it enforces applet isolation located in different packages and controls the access to global data containers shared by all applet instances.

The JCRE shall allocate and manage a context for each Java API package containing applets. The JCRE maintains for its own context a special system privilege so that it can perform operations that are denied to contexts of applets.

### 8.2.10 JCS.Package

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

### 8.2.11 JCS.CryptoAPI

This security function offers the following cryptographic services to applets through the Java Card API:

- Encryption and decryption using AES (128, 192 or 256 bits key) algorithm as defined in [JCAPI31] Cipher class.
- Data hash computation as defined in [JCAPI31] MessageDigest class.
- HMAC computation as defined in [JCAPI31] Signature class.
- Generation and verification of ECDSA signatures as defined in [JCAPI31] Signature class. Elliptic curve cryptography over GF(p) is considered here, with P ranging from 160 to 521 bits.
- Secret key agreement according to the ECDH algorithm, as defined in [JCAPI31] KeyAgreement class.
- Secret key agreement according to the DH algorithm (ALG\_DH\_PLAIN), as defined in [JCAPI31] KeyAgreement class.
- Generation of random numbers as defined in [JCAPI31] RandomData class, to be used for key values or challenges during external exchanges. The Random Number Generator (RNG) is hybrid deterministic and conformant to [AIS31] DRG.4, providing enhanced

backward secrecy & enhanced forward secrecy. It passes [AIS31] test procedure A. The RNG provides enhanced forward secrecy after calling the JavaCard API with ALG\_KEYGENERATION or ALG\_TRNG algorithms.

### 8.2.12 JCS.KeyManagement

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

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

### 8.2.13 JCS.EraseResidualData

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

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

They are erased when space needs to be reused for allocation of new objects.

This security function also ensures that the sensitive temporary buffers (transient object, bArray object, Global Array object, APDU buffer, Cryptographic buffer) are securely cleared after their usage with respect to their life-cycle and interface as defined in [JCRE31], transient object at reset or allocation and persistent object are erased at allocation for new object.

### 8.2.14 JCS.OutOfLifeDataUndisclosure

This security function ensures that sensitive data are locked until postponed erasure on the following operations: Deletion of persistent and transient objects according to [JCRE31].

### 8.2.15 JCS.RunTimeExecution

This security function provides a secure run time environment conformant to [JCRE31] and deals with:

- Instance registration or deletion,
- Application selection,
- Applet opcode execution,
- JCAPI methods execution,

- Logical channel management,
- APDU flow control, dispatch and buffer management,
- JCRE memory and context management,
- JCRE reference deletion,
- JCRE access rights,
- JCRE throw exception,
- JCRE security reaction.

### 8.2.16 JCS.Exception

This security function manages throwing of an instance of Exception class in the following cases:

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

### 8.2.17 OS.Atomicity

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

### 8.2.18 OS.MemoryManagement

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

## 8.3 TSS Rationale

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

### 8.3.1 eUICC SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	This SFR is covered by GSMA.Ident-Auth
FIA_UAU.1/EXT	GSMA.Ident-Auth
FIA_USB.1/EXT	GSMA.Ident-Auth

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UAU.4/EXT	GSMA.Ident-Auth
FIA_UID.1/MNO-SD	GSMA.Ident-Auth
FIA_USB.1/MNO-SD	GSMA.Ident-Auth
FIA_ATD.1	GSMA.Ident-Auth
FIA_API.1	GSMA.Ident-Auth
FDP_IFC.1/SCP	GSMA.SecureChannels
FDP_IFF.1/SCP	GSMA.SecureChannels
FDP_ITC.1/SCP	GSMA.SecureChannels and GP.SecureChannel
FDP_ITC.2/SCP	GSMA.SecureChannels
FDP_TDC.1/SCP	GSMA.SecureChannels
FDP_UCT.1/SCP	GSMA.SecureChannels and GP.SecureChannel
FDP_UIT.1/SCP	GSMA.SecureChannels and GP.SecureChannel
FCS_CKM.1/SCP-SM	GSMA.SecureChannels
FCS_CKM.2/SCP-MNO	GSMA.SecureChannels
FCS_CKM.6/SCP-SM	JCS.KeyManagement
FCS_CKM.6/SCP-MNO	JCS.KeyManagement
FDP_ACC.1/ISDR	GSMA.SecurityDomains
FDP_ACF.1/ISDR	GSMA.SecurityDomains
FDP_ACC.1/ISDP	GSMA.SecurityDomains
FDP_ACF.1/ISDP	GSMA.SecurityDomains
FDP_ACC.1/ECASD	GSMA.SecurityDomains
FDP_ACF.1/ECASD	GSMA.SecurityDomains
FDP_IFC.1/Platform_services	GSMA.PlatformServices
FDP_IFF.1/Platform_services	GSMA.PlatformServices
FDP_FLS.1/Platform_services	GSMA.PlatformServices
FCS_RNG.1	JCS.CryptoAPI
FDP_EMS.1	JCS.KeyManagement and JCS.CryptoAPI
FDP_SDI.1	GSMA.SecurityMngt
FDP_RIP.1	GSMA.SecurityMngt
FDP_FLS.1	GSMA.SecurityMngt
FMT_MSA.1/PSF_DATA	GSMA.SecurityMngt
FMT_MSA.1/POL1	GSMA.SecurityMngt
FMT_MSA.1/CERT_KEYS	GSMA.SecurityMngt
FMT_MSA.3	GSMA.SecureChannels and GSMA.SecurityDomains
FMT_SMF.1	GSMA.SecureChannels and GSMA.SecurityDomains
FMT_SMR.1	GSMA.SecurityMngt
FCS_COP.1/Mobile_network	GSMA.NetworkAuthent
FCS_CKM.2/Mobile_network	GSMA.NetworkAuthent
FCS_CKM.6/Mobile_network	JCS.KeyManagement

### 8.3.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
From [PP-JCS]	
FDP_ACC.2/FIREWALL	JCS.Firewall

<b>FDP_ACF.1/FIREWALL</b>	JCS.Firewall
<b>FDP_IFC.1/JCVM</b>	JCS.Firewall and JCS.APDUBuffer controlling unauthorized access or invalid storage of reference
<b>FDP_IFF.1/JCVM</b>	JCS.Firewall
<b>FDP_RIP.1/OBJECTS</b>	JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data)
<b>FMT_MSA.1/JCRE</b>	JCS.RunTimeExecution covering context switch and application selection
<b>FMT_MSA.1/JCVM</b>	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
<b>FMT_MSA.2/FIREWALL_JCVM</b>	JCS.RunTimeExecution covering object sharing
<b>FMT_MSA.3/FIREWALL</b>	JCS.RunTimeExecution covering object sharing
<b>FMT_MSA.3/JCVM</b>	JCS.RunTimeExecution covering object sharing
<b>FMT_SMF.1/JC</b>	JCS.RunTimeExecution covering context management and instance registration
<b>FMT_SMR.1/JC</b>	JCS.RunTimeExecution covering JCVM and JCRE roles
<b>FCS_CKM.1/GP-SCP</b>	GP.SecureChannel, JCS.KeyManagement and JCS.CryptoAPI
<b>FCS_COP.1/GP-SCP</b>	GP.SecureChannel and JCS.CryptoAPI
<b>FDP_RIP.1/ABORT</b>	JCS.EraseResidualData covering data erasure
<b>FDP_RIP.1/APDU</b>	JCS.EraseResidualData covering data erasure
<b>FDP_RIP.1/bArray</b>	JCS.OutOfLifeDataUndisclosure and JCS.EraseResidualData covering data erasure
<b>FDP_RIP.1/GlobalArray</b>	JCS.EraseResidualData covering data erasure
<b>FDP_RIP.1/KEYS</b>	JCS.EraseResidualData covering data erasure
<b>FDP_RIP.1/TRANSIENT</b>	JCS.OutOfLifeDataUndisclosure managing the access control to transient object to be erased prior the erasure of the content in memory
<b>FDP_ROL.1/FIREWALL</b>	JCS.RunTimeExecution covering transaction rollback during specific operations
<b>FAU_ARP.1</b>	JCS.RunTimeExecution, JCS.Exception, JCS.Firewall, and OS.MemoryManagement covering exception handling with different specific operations
<b>FDP_SDI.2/DATA</b>	JCS.KeyManagement, OS.Atomicity and OS.MemoryManagement covering integrity handling with specific operations
<b>FPR_UNO.1</b>	JCS.KeyManagement, JCS.CryptoAPI and OS.MemoryManagement covering data handling with specific operations avoiding observation
<b>FPT_FLS.1/JC</b>	JCS.Exception, JCS.ByteCodeExecution, JCS.RunTimeExecution, and OS.Atomicity preserving a secure state when unexpected events occur during specific operations.
<b>FPT_TDC.1</b>	JCS.Package enforcing export check, CAP file translation and link specific operations.
<b>FIA_ATD.1/AID</b>	JCS.RunTimeExecution and GP.GPRegistry controlling applet registration and uninstallation.

<b>FIA_UID.2/AID</b>	GP.GPRegistry and JCS.RunTimeExecution managing user identity (package AID) during applet selection and identify associated context provided.
<b>FIA_USB.1/AID</b>	GP.GPRegistry and JCS.RunTimeExecution managing registration of each applet and associated package during its installation with its AID.
<b>FMT_MTD.1/JCRE</b>	JCS.RunTimeExecution offering services for applet registration and uninstallation managing associated access rights.
<b>FMT_MTD.3/JCRE</b>	JCS.RunTimeExecution managing presence and legacy of AID with ISO rules.
<b>FDP_ACC.2/ADEL</b>	GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
<b>FDP_ACF.1/ADEL</b>	GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
<b>FDP_RIP.1/ADEL</b>	GP.CardContentManagement and JCS.OutOfLifeDataUndisclosure by checking operations to avoid access to freed resources prior to its reuse.
<b>FMT_MSA.1/ADEL</b>	GP.GPRegistry, GP.CardContentManagement and JCS.RunTimeExecution responsible of checking rules concerning applet attributes, implicit and explicit selection rules prior to authorize deletion operation.
<b>FMT_MSA.3/ADEL</b>	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.
<b>FMT_SMF.1/ADEL</b>	GP.CardContentManagement, GP.SecurityDomain and JCS.RunTimeExecution.
<b>FMT_SMR.1/ADEL</b>	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
<b>FPT_FLS.1/ADEL</b>	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.
<b>FDP_RIP.1/ODEL</b>	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
<b>FPT_FLS.1/ODEL</b>	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

Core from [PP-GP]	
<b>FDP_IFC.2/GP-ELF</b>	GP.CardContentManagement managing flow control for loading and installing application instances
<b>FDP_IFF.1/GP-ELF</b>	GP.CardContentManagement managing flow control for loading and installing application instances
<b>FDP_ITC.2/GP-ELF</b>	JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations
<b>FDP_IFC.2/GP-KL</b>	GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel
<b>FDP_IFF.1/GP-KL</b>	GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel
<b>FDP_ITC.2/GP-KL</b>	GP.KeyLoading
<b>FMT_MSA.1/GP</b>	GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU
<b>FMT_MSA.3/GP</b>	GP.SecureChannel providing setting of the default value.
<b>FMT_SMR.1/GP</b>	JCS.RunTimeExecution and GP.SecurityDomain managing the roles: S.OPEN, issuer, application provider, verification authority and controlling authority
<b>FMT_SMF.1/GP</b>	GP.SecurityDomain and GP.SecureChannel
<b>FPT_RCV.3/GP</b>	JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails
<b>FPT_FLS.1/GP</b>	This SFR is addressed by JCS.Package, JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling
<b>FPT_TDC.1/GP</b>	GP.CardContentManagement, GP.SecureChannel and GP.KeyLoading
<b>FPT_ITC.1/GP</b>	GP.SecureChannel
<b>FCO_NRO.2/GP</b>	GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading: <ul style="list-style-type: none"> <li>- mutual authentication between the external entity (Issuer or Application provider) and the selected security Domain, including creation of a session key,</li> <li>- by the verification of a (chained) MAC that the Issuer or Application provider attaches to each file or data block sent,</li> <li>- by the erase of the session key at the end of the session.</li> </ul>
<b>FIA_UID.1/GP</b>	JCS.RunTimeExecution and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
<b>FDP_UIT.1/GP</b>	GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
OS Update from [PP-GP]	
<b>FDP_ACC.1/OS-UPDATE</b>	GP.OS-UPDATE
<b>FDP_ACF.1/OS-UPDATE</b>	GP.OS-UPDATE
<b>FMT_MSA.3/OS-UPDATE</b>	GP.OS-UPDATE
<b>FMT_SMR.1/OS-UPDATE</b>	GP.OS-UPDATE

<b>FMT_SMF.1/OS-UPDATE</b>	GP.OS-UPDATE
<b>FTP_TRP.1/OS-UPDATE</b>	GP.OS-UPDATE
<b>FCS_COP.1/OS-UPDATE-DEC</b>	GP.OS-UPDATE
<b>FCS_COP.1/OS-UPDATE-VER</b>	GP.OS-UPDATE
<b>FIA_ATD.1/OS-UPDATE</b>	GP.OS-UPDATE
<b>FPT_FLS.1/OS-UPDATE</b>	GP.OS-UPDATE
Underlying platform IC related	
<b>FAU_SAS.1</b>	OS.MemoryManagement
<b>FPT_RCV.3/OS</b>	OS.Atomicity
<b>FPT_RCV.4/OS</b>	OS.MemoryManagement

## 9 COMPOSITION WITH IC

### 9.1 Statement of compatibility – Threats part

IC Threats	Rationale
T.Leak-Inherent	This threat is related to the information which is leaked from the TOE during usage of the Security IC in order to disclose sensitive data of the TOE. It is considered in the TOE evaluation.
T.Phys-Probing	This threat is related to physical probing of the TOE to disclose relevant information. It is considered in the TOE evaluation.
T.Malfunction	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. It is considered in the TOE evaluation.
T.Phys-Manipulation	This threat is related to physical manipulation of the Security IC. It is covered by the IC evaluation.
T.Leak-Forced	This threat is related to information, which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the composite TOE. It is covered by the IC evaluation.
T.Abuse-Func	This threat is related to the usage of functions of the TOE that are not allowed once the TOE Delivery and can affect the security of the TOE. It is considered in the TOE evaluation.
T.RND	This threat is related to the deficiency of random numbers. It is covered by the IC evaluation.
T.Masquerade_TOE	This threat is related to the IC masquerade. It is covered by the IC evaluation.
T.Open_Samples_Diffusion	This threat is related to the diffusion of open samples. It is covered by the IC evaluation.
T.Mem-Access	This threat is related to the Memory access Violation It is covered by the IC evaluation.

### 9.2 Statement of compatibility – OSPs part

IC OSPs	Rationale
P.Process-TOE	This policy is related to the accurate unique identification during IC Development and Production. It is covered by the IC evaluation.
P.Lim_Block_Loader	Limiting and blocking the loader functionality for loading of TOE Software. It is covered by the ALC_DVS.2 activity of the TOE evaluation.
P.Ctrl_loader	Controlled usage to loader functionality.

	It is covered by the ALC_DVS.2 activity of the TOE evaluation.
--	--

### 9.3 Statement of compatibility – Assumptions part

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

### 9.4 Statement of compatibility – Security objectives for the environment part

IC OEs are separated in the following groups as defined in [CEM:2022]:

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

IC OEs	Rationale
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. <b>CfPOE</b>
OE.Process-Sec-IC	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. - During phases b, c: <b>CfPOE</b> - During phase d, e: <b>SgOE</b>
OE.Lim_Block_Loader	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. - During phases b, c: <b>CfPOE</b>
OE.Loader_Usage	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. - During phases b, c: <b>CfPOE</b>
OE.TOE_Auth	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. - During phases b, c: <b>CfPOE</b>

### 9.5 Statement of compatibility – Security objectives part

IC Security objectives	Rationale
O.Leak_inherent	Linked to O.IC.SUPPORT. No contradiction.
O.Phys-Probing	Linked to O.IC.SUPPORT. No contradiction.
O.Malfunction	Linked to O.IC.SUPPORT. No contradiction.
O.Phys-Manipulation	Linked to O.IC.SUPPORT. No contradiction.
O.Leak-Forced	Linked to O.IC.SUPPORT. No contradiction.

O.Abuse-Func	Linked to O.IC.SUPPORT. No contradiction.
O.Identification	Used by the composite TOE to fulfil O.IC.PROOF_OF_IDENTITY. No contradiction.
O.RND	Used by the composite TOE to implement the composite TOE security objectives. No contradiction.
O.Cap_Avail_Loader	Used by the composite TOE, although there is no direct link to the composite TOE security objectives. No contradiction.
O.Authentication	This IC security objective supports the loading of the MultiSIM M2M 4.3.1 v1.0 software during phase c. No contradiction
O.Ctrl_Auth_Loader	This IC security objective supports the loading of the MultiSIM M2M 4.3.1 v1.0 software during phase c. No contradiction.
O.Prot_TSF_Confidentiality	No direct link to the composite TOE security objectives, nevertheless it supports the IC global robustness and thus participates to the composite TOE resistance to attacks. No contradiction.
O.Mem-Access	Used by the composite TOE to fulfil O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.CODE-EXE. No contradiction.

## 9.6 Statement of compatibility – SFRs part

**IP\_SFR:** Irrelevant IC SFR not being used by the current TOE.

**RP\_SFR-SERV:** Relevant IC SFR being used by the current TOE to implement a security service with associated TSFI.

**RP\_SFR-MECH:** Relevant IC SFR being used by the current evaluation because of its security properties providing protection attacks to the TOE as a whole and are addressed in ADV\_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the IC.

IC SFRs	Classification	Rationale
From "Malfunction"		
FRU_FLT.2	RP_SFR-MECH	No direct link to composite TOE SFRs but provides global protection against attacks
FPT_FLS.1	RP_SFR-MECH	
From "Abuse of Functionality"		
FMT_LIM.1	RP_SFR-MECH	No direct link to composite TOE SFRs but provides global protection against attacks.
FMT_LIM.2	RP_SFR-MECH	
FAU_SAS.1	RP_SFR-SERV	Used for the composite-product identification
From "Physical Manipulation and Probing"		
FDP_SDC.1	RP_SFR-MECH	No direct link to composite TOE SFRs but provides global protection against attacks
FDP_SDI.2/RAM	RP_SFR-MECH	
FDP_SDI.2/NVM	RP_SFR-MECH	
FDP_SDI.2/Register&Bus	RP_SFR-MECH	
FPT_PHP.3	RP_SFR-MECH	
From "Leakage"		
FDP_ITT.1	RP_SFR-MECH	FPR_UNO.1

FPT_ITT.1	RP_SFR-MECH	
FDP_IFC.1	RP_SFR-MECH	
From "Random Numbers"		
FCS_RNG.1/PTG.2	RP_SFR-SERV	FCS_RNG.1
From "Loader – Package 1"		
FMT_LIM.1/Loader	IP_SFR	Not applicable to the composite TOE, as the IC Loader is no more available after phase c.
FMT_LIM.2/Loader	IP_SFR	
From "Authentication Proof of Identity"		
FIA_API.1	RP_SFR-SERV	The IC Loader is no more available after phase c. However, this IC SFR is essential to protect the composite TOE during phases b and c.
From "Loader Package 2 Lite"		
FDP_UIT.1	RP_SFR-SERV	The IC Loader is no more available after phase c. However, this IC SFR is essential to protect the composite TOE during phases b and c.
FDP_ACC.1/Loader	RP_SFR-SERV	
FDP_ACF.1/Loader	RP_SFR-SERV	
From "Trusted path"		
FTP_TRP.1	IP_SFR	All communication paths used in current TOE are implemented by the current TOE embedded software.
From "Memory Access Control"		
FDP_ACC.1	RP_SFR-SERV	
FDP_ACF.1	RP_SFR-SERV	
FMT_MSA.3	RP_SFR-MECH	
FMT_MSA.1	RP_SFR-MECH	
FMT_SMF.1	RP_SFR-SERV	

## 10 REFERENCES, GLOSSARY AND ABBREVIATIONS

### 10.1 External references

Reference	Title
[ISO7816]	Identification cards – Integrated circuit(s) cards with contacts - Books 1 to 9
[CC:2022-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022 Revision 1
[CC:2022-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional components, CCMB-2022-11-002, CC:2022 Revision 1
[CC:2022-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance components, CCMB-2022-11-003, CC:2022 Revision 1
[CC:2022-4]	Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022 Revision 1
[CC:2022-5]	Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, version CC:2022 Revision 1
[CC:2022-Errata]	Common Criteria for Information Technology Security Evaluation Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1
[CC:2022-Transition]	Common Criteria for Information Technology Security Evaluation Transition Policy to CC:2022 and CEM:2022, CCMC-2023-04-001
[CEM:2022]	Common Criteria for Information Technology Security Evaluation Evaluation methodology, CCMB-2022-11-006, CEM:2022 Revision 1 November 2022
[CIC]	Common Implementation Configuration v2.0 (GPC_GUI_080)
[EUPP]	TCA eUICC Profile Package Interoperable Format Test Specification v2.3.1, September 2020
[GPCS]	Global Platform Card Specification v2.3.1 (GPC_SPE_034), March 2018 and amendments <ul style="list-style-type: none"> <li>• [Amd A] Amendment A - Confidential Card Content Management, v1.1 (GPC_SPE_007)</li> <li>• [Amd B] Amendment B - Remote Application Management over HTTP, v1.2 (GPC_SPE_011)</li> <li>• [Amd D] Amendment D - Secure Channel Protocol 03, v1.1.1 (GPC_SPE_014)</li> <li>• [Amd E] Amendment E - Security Upgrade for Card Content Management for ECDSA/ECC, v1.0.1</li> <li>• [Amd F] Amendment F - Secure Channel Protocol '11' (SCP11c), v1.2.0.3</li> <li>• [Amd H] Amendment H – Executable Load File Upgrade v1.1</li> </ul>
[12]	SCP80 ETSI TS 102 225, ETSI TS 102 226 – ref [12] in [PP/0100]
[JC31]	Java Card Specification v3.1, April 2020
[JCAP131]	Java Card 3 Platform - Java Card API, Classic Edition, Version 3.1, February 2021
[JCV31]	Java Card 3 Platform - Virtual Machine Specification, Classic Edition, Version 3.1, February 2021
[JCRE31]	Java Card 3 Platform - Runtime Environment Specification, Classic Edition, Version 3.1, February 2021
[JCBV]	Java Card 3.1.0 Off-card Verifier and onwards
[PP-84]	Security IC Platform Protection Profile with Augmentation Packages version 1.0, February 2014, BSI-CC-PP-0084-2014
[PP-eUICC]	SGP.05 Embedded UICC Protection Profile, Version 4.1, 10 March 2023
[PP-JCS]	Java Card System – Open Configuration Protection Profile version 3.2, July 2024, BSI-CC-PP-0099-V2-2020
[PP-GP]	Secure Element Protection Profile version 1.0, February 2021, GPC_SPE_174
[SGP.01]	Embedded SIM Remote Provisioning Architecture, Version 4.3, 18 November 2022
[SGP.02]	Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 4.3, 25 January 2023
[SGP.06]	eUICC Security Assurance Principles, version 2.2, March 2025
[SGP.07]	eUICC Security Assurance Methodology, version 2.2, March 2025
[ST-IC]	Security Target Lite for ORION (ORION_ST_Security_Target_Lite_v1.61 – September 12,2025)
[GUIDANCE-IC]	<ul style="list-style-type: none"> <li>• AGD- Secure delivery-v1.0</li> <li>• Orion Assembly - rev 0.2</li> <li>• ORION_Security_Guidance – rev 0.30</li> <li>• Orion_User_Manual_Rev1.2</li> <li>• Secure 32 bits CPU Embedded Application Binary Interface (EABI), référence s8-abi, version 0.6, mars 2013</li> <li>• s8-isa-v1.1b</li> <li>• UserManual_CC_Loader_v1.7</li> </ul>
[CERT-IC]	CERTIFICAT ANSSI-CC-2017/41-R03, Microcontrôleur ORION_CB_03 et ORION_DB_03, Référence ORION_TOE_v5, 01/12/2025,
[VER]	Global Platform Card Composition Model, Security Guidelines for Basic Applications (GPC_GUI_050, v2.0)
[AIS31]	BSI AIS 20 and AIS 31 Evaluation of random number generators Version 0.10 Functionality classes for random number generators, Version 2.0, 18 September 2011

Reference	Title
[20]	Release 11 3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; <ul style="list-style-type: none"> <li>• Document 1: General;</li> <li>• Document 2: Algorithm Specification;</li> <li>• Document 3: Implementers Test Data;</li> <li>• Document 4: Design Conformance Test Data;</li> <li>• Document 5: Summary and results of design and evaluation.</li> </ul>
[21]	Release 12, December 2014 3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233 <ul style="list-style-type: none"> <li>• Document 1: Algorithm specification;</li> <li>• Document 2: Implementers' test data;</li> <li>• Document 3: Design conformance test data.</li> </ul>
[22]	3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture, version 12.2.0, release 12, December 2014. 3GPP TS 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, version 12.16.0, release 12, December 2015.

## 10.2 Internal references

Reference	Title
[GUIDANCE]	List of documents applicable to the certified product: <ul style="list-style-type: none"> <li>• Platform Identification and Configuration for MultiSIM M2M 4.3.1 v1.0 (D1644051 v1.0)</li> <li>• Operational guidance of MultiSIM M2M 4.3.1 v1.0 (D1644052 v1.1)</li> <li>• Preparative guidance of MultiSIM M2M 4.3.1 v1.0 (D1644053 v1.0)</li> <li>• MultiSIM M2M 4.3.1 User's Guide (D1642140A, version 27 May 2025)</li> <li>• MultiSIM M2M 4.3.1 APDU guide (D1642139A, version 27 May 2025)</li> <li>• Guidance for Secure application development on Thales MultiSIM M2M Products (D1608375 v1.0)</li> <li>• GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications (GPC_GUI_050, v2.0)</li> <li>• Application Note Preventing the misuse of an eUICC Profile and the installation of a malicious Java Card Application (AN-2025-07, v1.0, 25<sup>th</sup> June 2025)</li> </ul>

## 10.3 Glossary

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

## 10.4 Abbreviations

CC	Common Criteria
HW	Hardware
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile (see [SGP.32])
ISD-R	Issuer Security Domain Root (see [SGP.32])
IPA	IoT Profile Assistant (see [SGP.32])
IPAd	IoT Profile Assistant in the IoT Device (see [SGP.32])
OEM	Original Equipment Manufacturer
OTA	Over-The-Air
PP	Protection Profile
REE	Rich Execution Environment (e.g., Android, iOS, Linux, Windows, etc.)
RMA	Return Merchandise Authorization (i.e., return a product under warranty for a replacement, refund, repair)
ST	Security Target
SW	Software
TOE	Target of Evaluation
VA	Verification Authority
BCV	Byte code verifier
CC	Common Criteria

**END OF DOCUMENT**