



eSA Security Target of  
MSM IOT 9.3.1 v1.0

D1645750, Version 1.0p, October 1<sup>st</sup> ,2025

Security Target

**REVISION HISTORY**

Ver	Date	Author	Description of the modifications
1.0p	01/10/2025	S.COURTEAUD	Initial release

## 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
2.1.1	TOE type and usage.....	9
2.1.2	TOE life-cycle.....	11
2.1.3	Non-TOE HW/SW/FW available to the TOE .....	13
2.2	TOE scope.....	14
2.2.1	Physical scope .....	14
2.2.2	Logical scope .....	15
3	Conformance claim .....	17
3.1	Common Criteria Conformance Claims.....	17
3.2	Protection Profile (PP) conformance claim.....	18
3.3	Conformance claim rationale.....	18
3.3.1	Conformity of the TOE Type.....	18
3.3.2	SPD Consistency .....	19
3.3.3	Security Objectives Consistency.....	22
3.3.4	Conformity of the Requirement (SFR/SAR).....	24
4	Security Problem definition .....	28
4.1	Assets .....	28
4.2	Users and Subjects .....	29
4.3	Threats .....	30
4.4	Organizational Security Policies.....	32
4.5	Assumptions.....	32
5	Security Objectives.....	33
5.1	Security Objectives for the TOE .....	33
5.2	Security Objectives for the Operational Environment.....	34
5.3	Security Objectives Rationale .....	35
5.3.1	Threats .....	35
5.3.2	Organizational Security Policies.....	39
5.3.3	Assumptions.....	40
5.3.4	Rationale Tables.....	41
6	Extended Components Definition.....	47
7	Security Functional requirements.....	48
7.1	eUICC Security Functional Requirements .....	48
7.1.1	Identification and authentication .....	48
7.1.2	Communication.....	52
7.1.3	Security Domains .....	57
7.1.4	Platform Services .....	59
7.1.5	Security management .....	61
7.1.6	Mobile Network authentication.....	66
7.2	Runtime Environment Security Requirements .....	68

7.2.1	CoreLG Security Functional requirements .....	68
7.2.2	INSTG Security Functional requirements .....	78
7.2.3	ADELG Security Functional Requirements .....	79
7.2.4	RMIG Security Functional Requirements .....	82
7.2.5	ODELG Security Functional Requirements .....	82
7.2.6	Global Platform Security Functional requirements .....	83
7.2.7	Underlying platform IC Security Functional Requirements .....	98
7.3	Security Functional Requirements Rationale .....	100
7.3.1	SFRs for eUICC rationale .....	100
7.3.2	SFRs for Runtime Environment rationale .....	100
7.3.3	SFRs for Underlying platform IC rationale .....	101
7.3.4	SFRs dependency rationale .....	101
7.3.5	SAR refinement .....	106
8	TOE Summary Specification .....	107
8.1	eUICC security functions .....	107
8.1.1	GSMA.ProfileManagement .....	107
8.1.2	GSMA.ECASD .....	107
8.1.3	GSMA.ISDR .....	107
8.1.4	GSMA.ISDP .....	107
8.1.5	GSMA.PPR .....	108
8.2	Runtime Environment security functions .....	108
8.2.1	GP.CardContentManagement .....	108
8.2.2	GP.KeyLoading .....	108
8.2.3	GP.SecurityDomain .....	108
8.2.4	GP.SecureChannel .....	109
8.2.5	GP.GPRegistry .....	109
8.2.6	GP.OS-UPDATE .....	111
8.2.7	JCS.APDUBuffer .....	111
8.2.8	JCS.ByteCodeExecution .....	112
8.2.9	JCS.Firewall .....	112
8.2.10	JCS.Package .....	112
8.2.11	JCS.CryptoAPI .....	112
8.2.12	JCS.KeyManagement .....	113
8.2.13	JCS.EraseResidualData .....	113
8.2.14	JCS.OutOfLifeDataUndisclosure .....	113
8.2.15	JCS.RunTimeExecution .....	113
8.2.16	JCS.Exception .....	114
8.2.17	OS.Atomicity .....	114
8.2.18	OS.MemoryManagement .....	114
8.3	TSS Rationale .....	114
8.3.1	eUICC SFRs coverage .....	114
8.3.2	Runtime Environment SFRs coverage .....	115
9	Composition with IC .....	120
9.1	Statement of compatibility – Threats part .....	120
9.2	Statement of compatibility – OSPs part .....	120
9.3	Statement of compatibility – Assumptions part .....	120
9.4	Statement of compatibility – Security objectives for the environment part .....	120

9.5	Statement of compatibility – Security objectives part.....	121
9.6	Statement of compatibility – SFRs part .....	121
10	References, Glossary and Abbreviations .....	123
10.1	External references .....	123
10.2	Internal references.....	124
10.3	Glossary .....	124
10.4	Abbreviations .....	125

## TABLE OF FIGURES

Figure 1 - Example of Product environment .....	9
Figure 2 - MSM IOT 9.3.1 v1.0 Platform architecture .....	10
Figure 3 - TOE life-cycle and actors.....	11
Figure 4 - Product environment - TOE physical boundaries .....	14
Figure 5 – TOE logical boundaries.....	16

## TABLE OF TABLES

Table 1 - TOE life-cycle (manufacturing flow).....	12
Table 2 - TOE life-cycle (OS update flow).....	13
Table 3 – TOE components .....	15
Table 4 - Assets Consistency table .....	19
Table 5 - Security aspect Consistency table.....	20
Table 6 - User consistency table .....	20
Table 7 - Subjects Consistency table.....	21
Table 8 - Threats consistency table.....	21
Table 9 - Organizational Security Policies Consistency table.....	22
Table 10 -Assumptions Consistency table .....	22
Table 11 -Security objectives for the TOE consistency table .....	23
Table 12 - Security objectives for the Operational Environment consistency table .....	24
Table 13 -Security Functional Requirement consistency table.....	27
Table 14 - Assets .....	28
Table 15 - Users.....	29
Table 16 - Subjects .....	29
Table 17 - Threats .....	31
Table 18 – Security aspects.....	31
Table 19 - OSP .....	32
Table 20 - Assumptions.....	32
Table 21 - Security Objectives for the TOE .....	34
Table 22 - Security Objectives for the Environment.....	35
Table 23 -Threats and Security Objectives- Coverage .....	42
Table 24 - Security Objectives and threats .....	44
Table 25 -Organizational Security Policies and Security Objectives- Coverage.....	44
Table 26 - Security Objectives and Organizational Security Policies .....	45
Table 27 - Assumptions and Security Objectives for the Operational Environment- Coverage.....	46

Table 28 - Assumptions and Security Objectives for the Operational Environment ..... 46  
Table 29 – SFRs dependency table..... 105

*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 MSM IOT 9.3.1 v1.0
<b>Version</b>	1.0
<b>Author</b>	Thales
<b>Reference</b>	D1645750
<b>Publication date</b>	01/10/2025

The ST lite identification is the following:

<b>Name</b>	eSA Security Target of MSM IOT 9.3.1 v1.0
<b>Version</b>	1.0p
<b>Author</b>	Thales
<b>Reference</b>	D1645750
<b>Publication date</b>	01/10/2025

## 1.2 TOE reference

<b>Product name</b>	MSM IOT 9.3.1
<b>Developer</b>	Thales
<b>TOE name</b>	MSM IOT 9.3.1 v1.0
<b>TOE software version</b>	931100 (eUICInfo2) and D0023316080107 <b>or</b> D0023315F10107
<b>TOE documentation</b>	Guidance <b>[GUIDES]</b>
<b>TOE hardware part</b>	Orion_v4

## 2 TOE OVERVIEW

---

### 2.1 TOE description

The product MSM IOT 9.3.1 v1.0 on Orion is an eUICC (embedded UICC) for IoT Devices.

It is composed of:

- A hardware named Orion\_v4 from Thales DIS France SAS
- The embedded eUICC OS named eSIM software

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

As such, it is a multi-profile product, supporting remote profile management over SMS and over HTTP soldered in an IOT 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 opened [Javacard] / [GP] 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 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.

### 2.1.1 TOE type and usage

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

The eUICC is an UICC embedded in an IoT device (as example a smart meter). 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 IoT Device when accessing the network.

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

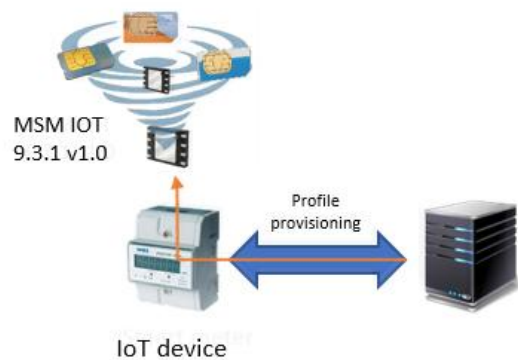


Figure 1 - Example of Product environment

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

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

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

MultiSIM IoT 9.3.1 Orion

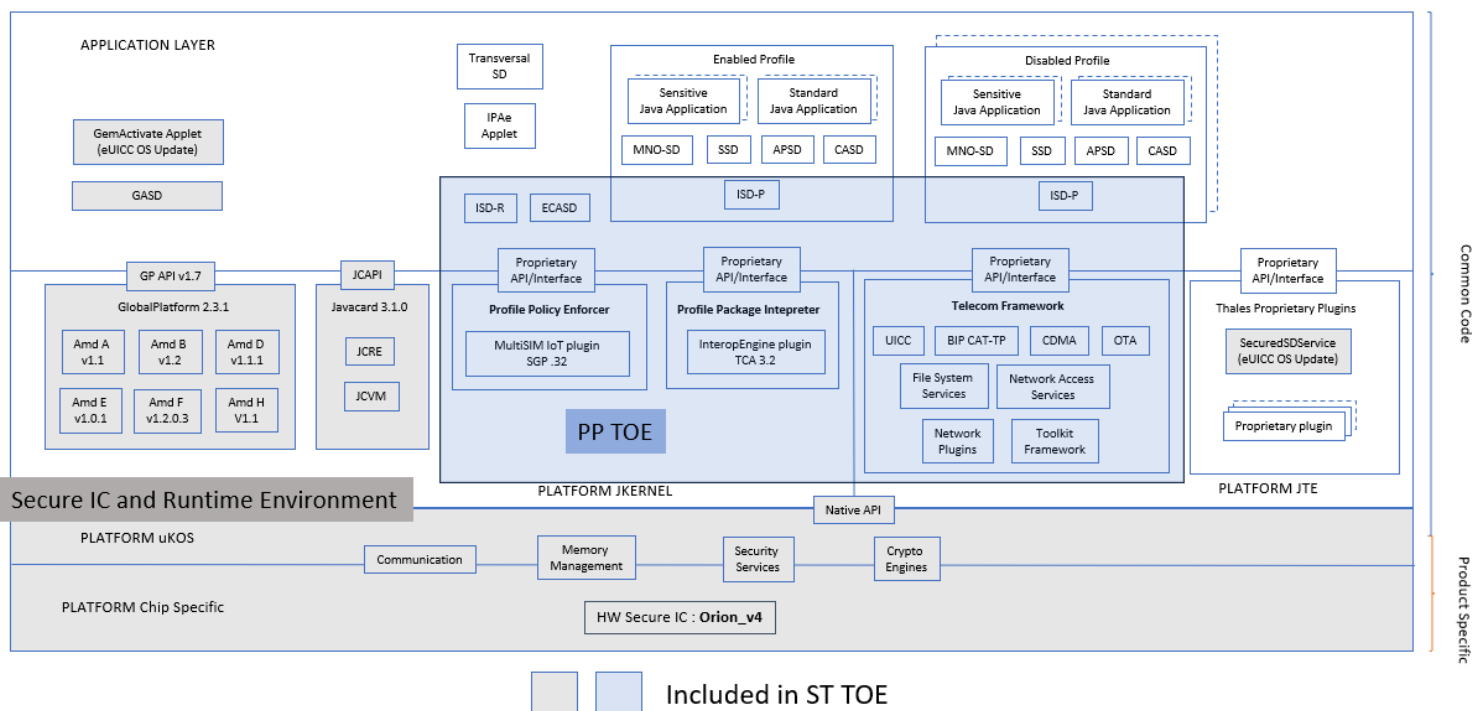


Figure 2 - MSM IOT 9.3.1 v1.0 Platform architecture

The TOE includes 3 layers:

- The hardware layer: ORION\_V4 providing support to the platform layer
- The platform layer: **MultiSim IoT 9.3.1 v1.0** OS including the 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).

### 2.1.2 TOE life-cycle

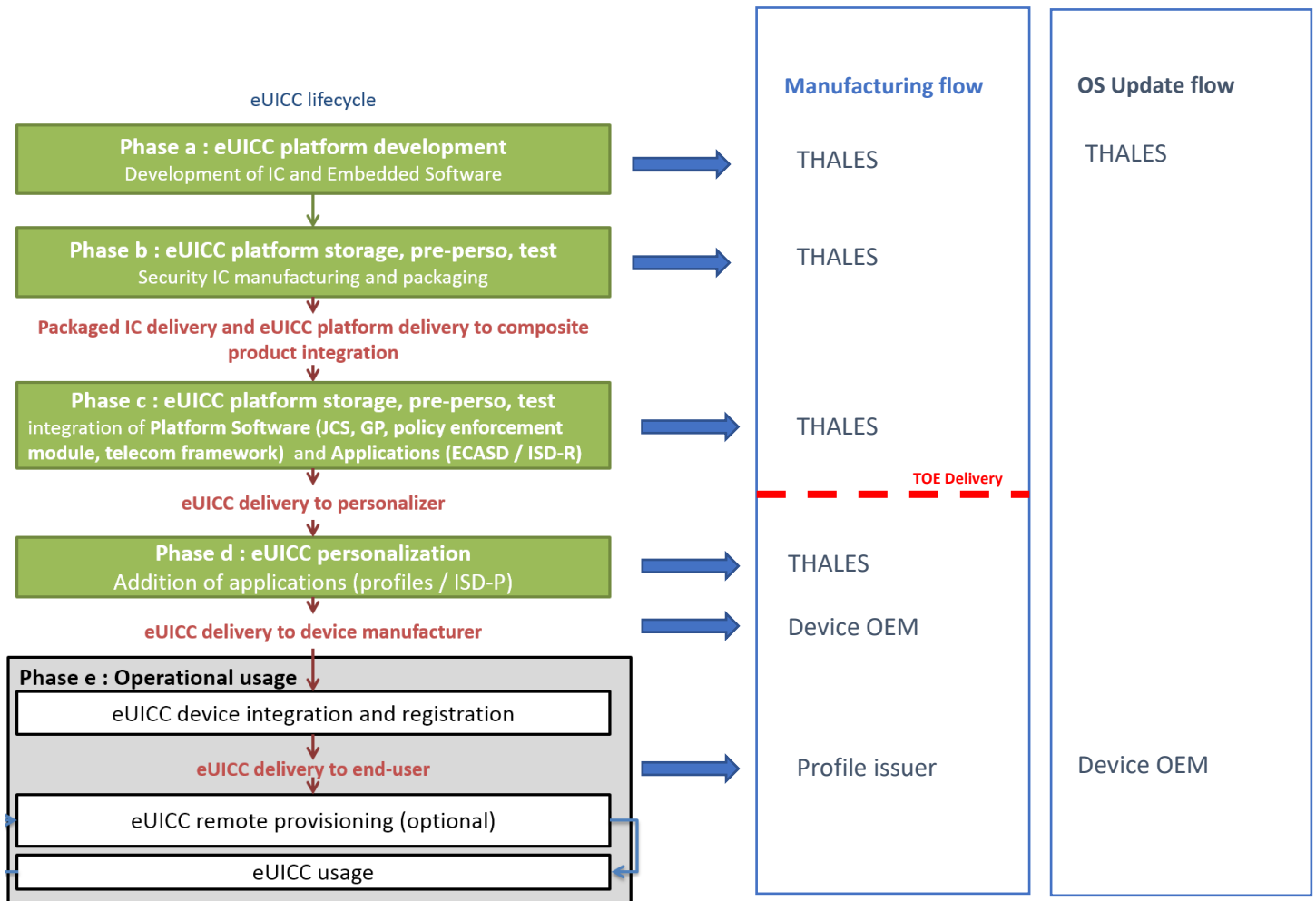


Figure 3 - TOE life-cycle and actors

The actors:

- The **eUICC Manufacturer (EUM)** is the developer of the eUICC secure application (Thales).
- The **IC manufacturer** is the developer and manufacturer of the IC (Thales). Thales is in charge of the **MultiSim IoT 9.3.1 v1.0** embedded software loading/initialization/pre-personalization in its own premises and proceeds to the delivery of the product directly to customers.
- The **Device OEM** manufacturer is the Original Equipment Manufacturer

- The **Profile issuer** is MNO that has privilege through its OTA Server to perform Remote Card Content Management (CCM) operations within its own profile (ISD-P). In addition, through its RSP servers, it also can provide Profiles to the end user, but has no privileges to manage profiles remotely without end user consent.
- The **End User** is the user of the device and the eUICC secure application.

The manufacturing flow is described in the following table:

Phase	Description	Actor	Location
a	MultiSim IoT SW (OS and Crypto)	Thales	Thales DIS Singapore site SAS-UP site audit
	Orion_v4 IC development	Thales	Development site(s) stated in the Orion certificate
b	Orion_v4 IC's manufacturing and packaging	Thales	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 Gemenos (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 PAU Datagen Team	THALES DIS Pont-Audemer (France)
	eUICC OS static image and Dynamic data loading in IC	Thales	Thales Site(s) stated in the Orion certificate
*** TOE delivery ***			
d	Personalization of data during wafer test flow	Thales	Thales DIS SAS-UP site audit
Device is delivered to point of sales and is reaching end user			
e	RSP process (Profile loading and activation)	Profile issuer (SM-DP+ server)	In the field Remote access by end user to server associated to MNO / Carrier

Table 1 - TOE life-cycle (manufacturing flow)

The OS update flow is described in the following table.

Phase	Description	Actor	Location
a	MultiSim IoT SW (OS and Crypto)	Thales	Thales DIS Singapore site
<i>Updated OS will be sent over the air to already deploy devices by the OEM</i>			
e	Operational usage Profile loading and activation	Profile issuer (SM-DP+ server)	In the field Remote access by end user to server associated to MNO

Table 2 - TOE life-cycle (OS update flow)

The conditions to trigger OS update are weakness on eUICC Secure Application (**MultiSim IoT 9.3.1 v1.0 OS**) at security, or functional, or both –OR– deployment of additional feature.

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

Non-TOE is same than the ones mentioned in the [PP-eUICC] except for Embedded Software, IC and RTE that are part of the TOE.

The product implements IP Ae services, but it is not part of the TOE. It is not required by the TOE as the TOE is dedicated to work with IP Ad.

The TOE does not implement the RMI functions from JCS. It is not required by the TOE.

Additionally, the following non-TOE components, which are external to the eUICC, are necessary for TOE operation:

- The TOE is intended to be plugged in a IoT device 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+, which provides Profile management commands and Profile,
  - MNO OTA Platforms.

The TOE requires the use of secure channels for these interactions.

- Application to be included in profile shall be verified prior loading using appropriate tool (Byte code verifier BCV) located in IoT device environment.

## 2.2 TOE scope

### 2.2.1 Physical scope

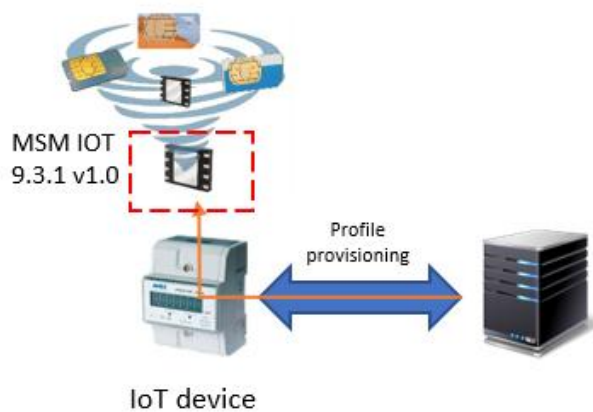


Figure 4 - Product environment - TOE physical boundaries

The physical boundaries encompass the **MultiSim IoT 9.3.1 v1.0** software executed inside the IC hardware. The other items are outside the scope of the evaluation as illustrated in Figure 4 - Product environment - TOE physical boundaries.

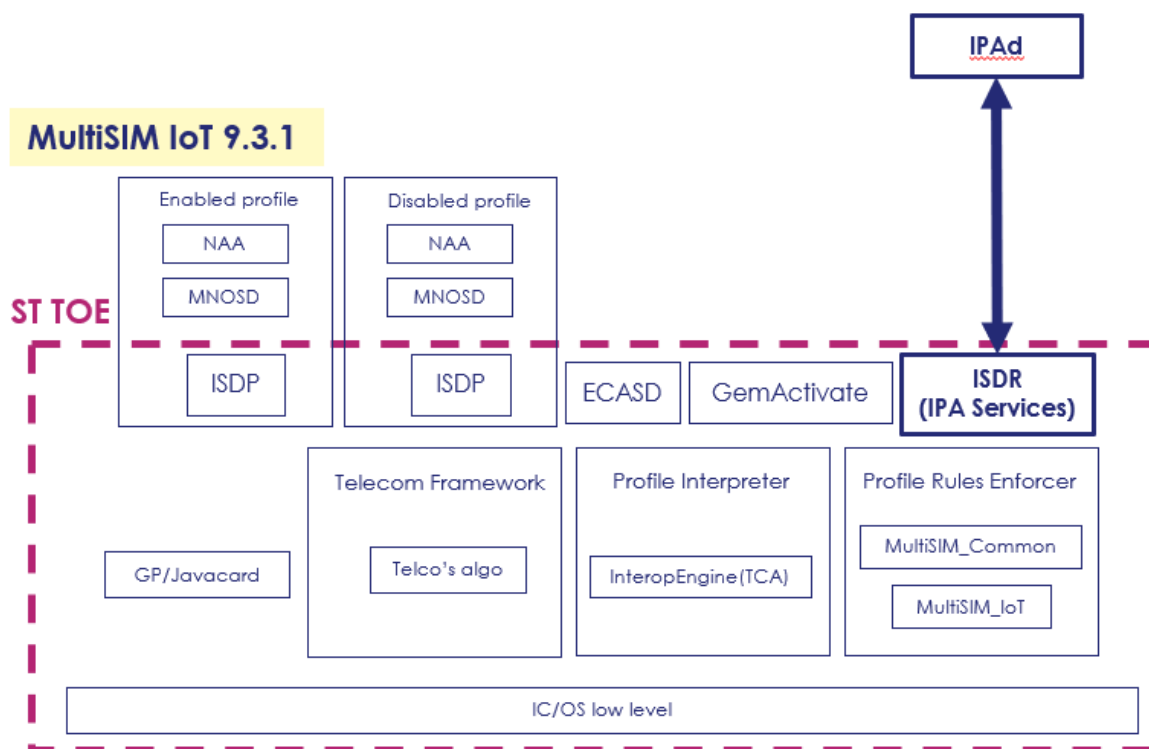
The TOE physical boundaries consist of the following components:

TOE component	Developer	Item	Identifier	Form of delivery
IC	Thales	Orion hardware	Orion_TOE_v4: ORION_CB_03 ORION_DB_03	Diced wafer – MFF2 (Embedding eUICC OS)
eUICC OS	Thales	MultiSim IoT 9.3.1	931100  D0023316080107  D0023315F10107	Software (Delivered embedded within the IC)  PDM Counter (D002331608) for GTO04M OS Release 1.7 (0107)  PDM Counter (D0023315F1) for GTO004 OS Release 1.7 (0107)
eUICC guidances	Thales	MultiSim IoT 9.3.1	[GUIDES]	Document (Electronic document (PDF) delivered via secure email)

Table 3 – TOE components

### 2.2.2 Logical scope

The logical boundaries are delimited (dash line in purple) in Figure 5.



*Figure 5 – TOE logical boundaries*

The eUICC OS implements the following services:

- Remote Sim Provisioning (RSP) and Local Profile Management (Enable, Disable, Delete MNO Profiles)
- Management and control of the communication between OS and external entities
- OS Security services as:
  - providing secure cryptographic primitives, algorithms, and services
  - ensure the security of assets.
  - generating random numbers
- Enforcement of the Javacard Runtime and Firewall mechanism
- Standard APIs such as Telecom APIs, JC APIs and GP APIs
- Secure loading of software patches (GemActivate)  
Oracle's Java Card 3.1.0 [JC], which consist of the Java Card 3.1.0 Virtual machine, Java Card Run Time Environment 3.1.0 and the Java Card 3.1.0 Application Programming Interface.
- Global Platform 2.3.1 [11], SE Configuration.

### 3 CONFORMANCE CLAIM

---

Evaluation type:

- This is a composite evaluation, which relies on the Orion\_v4 IC certificate and evaluation results.
  - Certification done under the ANSSI scheme.
  - CC certificate: ANSSI-CC-2017/41-R02
  - Security Target **[ST/IC]** strictly conformance to **[PP-84]**
  - CC version: 3.1, revision 4
  - Assurance level: EAL5+ (ALC\_DVS.2 / AVA\_VAN.5)

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

#### 3.1 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-1],
- CC Part 2 [CC-2] (extended)
- CC Part 3 [CC-3] (conformant),
- CC Part 5 [CC-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]

### 3.2 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, the PP Module 'OS Update' defined in Annex A of [PP-eUICC] is taken into account for the present evaluation.

### 3.3 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 is deleted from [PP-eUICC]
- X: The element is present in [PP-eUICC].

#### 3.3.1 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.

### 3.3.2 SPD Consistency

#### 3.3.2.1 Assets consistency

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

Assets	PP-eUICC	Data type	Security Target
D.MNO_KEYS	X	User Data	(E)
D.PROFILE_NAA_PARAMS	X	User Data	(E)
D.PROFILE_IDENTITY	X	User Data	(E)
D.PROFILE_RULES	X	User Data	(E)
D.PROFILE_USER_CODES (SGP.22)	X	User Data	(D) Deleted as it does not concern IoT architecture
D.PROFILE_CODE	X	User Data	(E)
D.TSF_CODE	X	TSF Data	(E)
D.PLATFORM_DATA	X	TSF Data	(E)
D.DEVICE_INFO	X	TSF Data	(E)
D.PLATFORM_RAT	X	TSF Data	(E)
D.SK.EUICC.ECDSA	X	TSF Data	(E)
D.CERT.EUICC.ECDSA	X	TSF Data	(E)
D.PK.CI.ECDSA	X	TSF Data	(E)
D.PK.EIM.ECDSA (SGP.32)	X	TSF Data	(E)
D.EID	X	TSF Data	(E)
D.SECRETS	X	TSF Data	(E)
D.CERT.EUM.ECDSA	X	TSF Data	(E)
D.CRLs	X	TSF Data	(E)
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.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].
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

Table 4 - Assets Consistency table

### 3.3.2.2 Security aspects

All Security aspects defined in [PP-eUICC] are relevant for the TOE of this Security Target. The table below indicates the Security aspect' 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 5 - Security aspect Consistency table

### 3.3.2.3 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-DP+	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.EIM (SGP.32)	X	(E)
U.End-User (SGP.22)	X	(D) Deleted as it does not concern IoT architecture

Table 6 - 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.PPI	X	(E)
S.PRE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A): Added from [PP-JCS].
S.OPEN		(A): Added from [PP-GP].
S.SD		(A): Added from [PP-GP].
S.APPLET		(A): Added from [PP-JCS].
S.BCV		(A): Added from [PP-JCS].
S.CAD		(A): Added from [PP-JCS].
S.INSTALLER		(A): Added from [PP-JCS].
S.JCRE		(A): Added from [PP-JCS].

<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.OSU</b>	X	(E) from [PP-eUICC] Annex A
<b>S.UpdateImageCreator</b>	X	(E) from [PP-eUICC] Annex A

Table 7 - Subjects Consistency table

### 3.3.2.4 Threats consistency

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

Some threats are described in terms of LPAd or IPAd in [PP-eUICC]. Only the definitions in terms of IPAd and SGP.32 are taken here (i.e., other terms classified as LPAd or SGP.22 are discarded), but they are still classified with (E) if they are not further refined.

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.PROFILE-MNG-ELIGIBILITY</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.LPAd-INTERFACE-EXPLOIT</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	(E)
<b>T.CONFID-UPDATE-IMAGE.LOAD</b>	X	(E) from [PP-eUICC] Annex A
<b>T.INTEG-UPDATE-IMAGE.LOAD</b>	X	(E) from [PP-eUICC] Annex A
<b>T.UNAUTH-UPDATE-IMAGE.LOAD</b>	X	(E) from [PP-eUICC] Annex A
<b>T.INTERRUPT_OSU</b>	X	(E) from [PP-eUICC] Annex A

Table 8 - Threats consistency table

Note that T.LPAd-INTERFACE-EXPLOIT is named after LPAd, but it still considers IPAd.

### 3.3.2.5 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].

Table 9 - Organizational Security Policies Consistency table

### 3.3.2.6 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.TRUSTED-PATHS-LPAd-IPAd	X	(E)
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.CAP_FILE		(A): Added from [PP-JCS].
A.VERIFICATION		(A): Added from [PP-JCS].

Table 10 - Assumptions Consistency table

## 3.3.3 Security Objectives Consistency

### 3.3.3.1 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. The [PP-eUICC] already provides the conversion of OE.RE\* to objectives from the [PP-JCS] protection profile.

O.TOE	PP-eUICC	Security Target
O.PRE-PPI	X	(E)
O.eUICC-DOMAIN-RIGHTS	X	(E)
O.SECURE-CHANNELS	X	(E)
O.INTERNAL-SECURE-CHANNELS	X	(E)
O.PROOF_OF_IDENTITY	X	(E)
O.OPERATE	X	(E)
O.API	X	(E)
O.DATA-CONFIDENTIALITY	X	(E)
O.DATA-INTEGRITY	X	(E)
O.ALGORITHMS	X	(E)

<b>O.IC.PROOF_OF IDENTITY</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.IC.SUPPORT</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.IC.RECOVERY</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.PRE-PPI</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.SECURE-COMM</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.API</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.DATA-CONFIDENTIALITY</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.DATA-INTEGRITY</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.IDENTITY</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.RE.CODE-EXE</b>		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
<b>O.SECURE_LOAD_ACODE</b>	X	(E) from [PP-eUICC] Annex A
<b>O.SECURE_AC_ACTIVATION</b>	X	(E) from [PP-eUICC] Annex A
<b>O.TOE_IDENTIFICATION</b>	X	(E) from [PP-eUICC] Annex A
<b>O.CONFID-UPDATE-IMAGE.LOAD</b>	X	(E) from [PP-eUICC] Annex A
<b>O.AUTH-LOAD-UPDATE-IMAGE</b>	X	(E) from [PP-eUICC] Annex A
<b>O.LOAD</b>		(A): Added from [PP-JCS].

Table 11 -Security objectives for the TOE consistency table

### 3.3.3.2 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. The [PP-eUICC] already provides the conversion of OE.RE\* to objectives from the [PP-JCS] protection profile.

OE.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.MNO	X	(E)
OE.EIM (SGP.32)	X	(E)
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF_IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PRE-PPI	X	Removed and replaced by O.RE.PRE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE
OE.TRUSTED-PATHS-LPAd-IPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.MNO-SD	X	(E)
OE.CAP_FILE		(A): added from [PP-JCS]
OE.VERIFICATION		(A): added from [PP-JCS]
OE.CODE-EVIDENCE		(A): added from [PP-JCS]
OE.CONFID_UPDATE_IMAGE.CREATE	X	(E) from [PP-eUICC] Annex A

Table 12 - Security objectives for the Operational Environment consistency table

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

#### 3.3.4.1 SFR consistency

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

FPT_TDC.1/SCP	X	(E)
FDP_UCT.1/SCP	X	(E)
FDP_UIT.1/SCP	X	(E)
FCS_CKM.1/SCP-SM	X	(E)
FCS_CKM.2/SCP-MNO	X	(E)
FCS_CKM.6/SCP-SM	X	(E)
FCS_CKM.6/SCP-MNO	X	(E)
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	(E)
FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
FCS_RNG.1	X	(E)
FPT_EMS.1/Base	X	(E)
FDP_SDI.1/Base	X	(E)
FDP_RIP.1/Base	X	(E)
FPT_FLS.1/Base	X	(E)
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/RULES	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1/Base	X	(E)
FMT_SMR.1/Base	X	(E)
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.6/Mobile_network	X	(E)
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-GP].
FCS_COP.1/GP-SCP		(A): Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A): Added from [PP-JCS].
FDP_RIP.1/APDU		(A): Added from [PP-JCS].
FDP_RIP.1/bArray		(A): Added from [PP-JCS].

FDP_RIP.1/GlobalArray		(A): Added from [PP-JCS].
FDP_RIP.1/KEYS		(A): Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A): Added from [PP-JCS].
FAU_ARP.1		(A): Added from [PP-JCS].
FDP_SDI.2/DATA		(A): Added from [PP-JCS].
FPR_UNO.1		(A): Added from [PP-JCS].
FPT_FLS.1/JC		(A): Added from [PP-JCS].
FPT_TDC.1		(A): Added from [PP-JCS].
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ACC.2/ADEL		(A): Added from [PP-JCS].
FDP_ACF.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].
FMT_SMF.1/ADEL		(A): Added from [PP-JCS].
FMT_SMR.1/ADEL		(A): Added from [PP-JCS].
FPT_FLS.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/GP		(A): Added from [PP-GP].
FDP_ROL.1/GP		(A): Added from [PP-GP].
FCO_NRO.2/GP		(A): Added from [PP-GP].
FMT_SMR.1/GP		(A): Added from [PP-GP].
FMT_SMF.1/GP		(A): Added from [PP-GP].
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP].
FDP_ITC.2/GP-KL		(A): Added from [PP-GP].
FPT_RCV.3/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP].
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP].
FIA_UID.1/GP		(A): Added from [PP-GP].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FTP_ITC.1/GP		(A): Added from [PP-GP].
FPR_UNO.1/GP		(A): Added from [PP-GP].
FPT_TDC.1/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-KL		(A): Added from [PP-GP].
FDP_IFF.1/GP-KL		(A): Added from [PP-GP].
FMT_MSA.1/GP		(A): Added from [PP-GP].
FMT_MSA.3/GP		(A): Added from [PP-GP].
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].
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 13 -Security Functional Requirement consistency table*

#### 3.3.4.2 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, 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 3.3.2.1 for complete list of assets.

Assets
D.MNO_KEYS
D.PROFILE_NAA_PARAMS
D.PROFILE_IDENTITY
D.PROFILE_RULES
D.PROFILE_CODE
D.TSF_CODE
D.PLATFORM_DATA
D.DEVICE_INFO
D.PLATFORM_RAT
D.SK.EUICC.ECDSA
D.CERT.EUICC.ECDSA
D.PK.CI.ECDSA
D.PK.EIM.ECDSA (SGP.32)
D.EID
D.SECRETS
D.CERT.EUM.ECDSA
D.CRLs
D.APP_CODE
D.APP_C_DATA
D.APP_I_DATA
D.APP_KEYS
D.API_DATA
D.CRYPTO
D.JCS_CODE
D.JCS_DATA
D.SEC_DATA
D.UPDATE_IMAGE
D.TOE_IDENTIFIER
D.OS-UPDATE_KEY(S)

Table 14 - 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 3.3.2.3 for complete list of users and subjects.

User
U.SM-DP+
U.SM-DS
U.MNO-OTA
U.MNO-SD
U.EIM (SGP.32)

Table 15 - Users

Subject
S.ISD-R
S.ISD-P
S.ECASD
S.PPI
S.PRE
S.TELECOM
S.ADEL
S.OPEN
S.SD
S.APPLET
S.BCV
S.CAD
S.INSTALLER
S.JCRE
S.JCVM
S.LOCAL
S.MEMBER
S.CAP_FILE
S.CAP_FILE
S.OSU
S.UpdateImageCreator

Table 16 - 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 3.3.2.4 for complete list of threats.

Refined threats description is detailed below:

Threats	Refined threats description
<b>T.UNAUTHORIZED-PROFILE-MNG</b>	Directly threatens the assets: 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>	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behavior of ISD-R or PRE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.
<b>T.PROFILE-MNG-INTERCEPTION</b>	Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, <b>D.APP_C_DATA and D.APP_KEYS.</b>
<b>T.PROFILE-MNG-ELIGIBILITY</b>	Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, <b>D.APP_C_DATA, D.APP_KEYS, D.APP_CODE and D.APP_I_DATA.</b>
<b>T.UNAUTHORIZED-IDENTITY-MNG</b>	Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, <b>D.APP_CODE, D.APP_I_DATA, D.APP_KEYS, D.APP_C_DATA and D.SEC_DATA, D.PK.EIM.ECDSA (SGP.32)</b>
<b>T.IDENTITY-INTERCEPTION</b>	Directly threatens the assets: D.SECRETS, D.EID, <b>D.APP_C_DATA and D.APP_KEYS.</b>
<b>T.UNAUTHORIZED-eUICC</b>	
<b>T.LPAd-INTERFACE-EXPLOIT</b>	
<b>T.UNAUTHORIZED-MOBILE-ACCESS</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, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.APP_KEYS and D.APP_C_DATA.</b>
<b>T.PHYSICAL-ATTACK</b>	All assets
<b>T.CONFID-UPDATE-IMAGE.LOAD</b>	Confidentiality of Update Image – Load  The attacker discloses (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the eUICC for installation. See SA.CONFID-UPDATE-IMAGE for details.

	Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, D.JCS_DATA
<b>T.INTEG-UPDATE-IMAGE.LOAD</b>	<p>Integrity of update Image -Load</p> <p>The attacker modifies (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the card for installation. See SA.INTEG-UPDATE-IMAGE for details.</p> <p>Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, D.JCS_DATA</p>
<b>T.UNAUTH-UPDATE-IMAGE.LOAD</b>	<p>Load an unauthorized update</p> <p>The attacker tries to upload an unauthorized update image. See SA.INTEG-UPDATEIMAGE for details.</p> <p>Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, D.JCS_DATA</p>
<b>T.INTERRUPT_OSU</b>	<p>OS Update procedure interrupted</p> <p>The attacker tries to interrupt the OS update procedure (Load Phase through activation of Additional Code) leaving the TOE in a partially functional state. Directly threatened asset(s): D.TOE_IDENTIFIER, D.UPDATE_IMAGE, D.JCS_CODE, D.JCS_DATA</p>

Table 17 - Threats

## Security Aspects (added to cover OS update)

<b>SA.CONFID-UPDATE-IMAGE</b>	<p>Confidentiality of Update Image</p> <p>The update image must be kept confidential. This concerns the non disclosure of the update image in the transit to the eUICC.</p>
<b>SA.INTEG-UPDATE-IMAGE</b>	<p>Integrity of Update Image</p> <p>The update image must be protected against unauthorized modification. This concerns the modification of the image in transit to the eUICC.</p>

Table 18 – Security aspects

## 4.4 Organizational Security Policies

The definition of organizational security policies from [PP-eUICC] where no refinements are made is not repeated here. See section 3.3.2.5 for complete list of organizational security policies.

OSPs
OSP.LIFE-CYCLE
OSP.VERIFICATION

Table 19 - OSP

## 4.5 Assumptions

The definition of assumptions from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here. See section 3.3.2.6 for complete list of assumptions.

Assumptions
A.TRUSTED-PATHS-LPAd-IPAd
A.ACTORS
A.APPLICATIONS
A.CAP_FILE
A.VERIFICATION

Table 20 - 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 3.3.3 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 3.3.3.2 and their description are listed next:

O.TOE	Replaced/Added objectives description
O.PRE-PPI	
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF IDENTITY	
O.OPERATE	
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
O.IC.PROOF_OF IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	<p>The IC embedded software shall support the following functionalities:</p> <ol style="list-style-type: none"> <li>(1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification).</li> <li>(2) It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PRE, S.PPI, and S.TELECOM).</li> <li>(3) It allows the S.PRE, S.PPI, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection).</li> <li>(4) It provides a means to perform memory operations atomically for S.PRE, S.PPI, and S.TELECOM.</li> </ol>
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.
<b>O.RE.PRE-PPI</b>	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>
<b>O.RE.SECURE-COMM</b>	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.
<b>O.RE.API</b>	The Runtime Environment shall ensure that native code can be invoked only via an API.
<b>O.RE.DATA-CONFIDENTIALITY</b>	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
<b>O.RE.DATA-INTEGRITY</b>	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
<b>O.RE.IDENTITY</b>	The Runtime Environment shall ensure the secure identification of the applications it executes.
<b>O.RE.CODE-EXE</b>	The Runtime Environment shall prevent unauthorized code execution by applications.
<b>O.SECURE_LOAD_ACODE</b>	
<b>O.SECURE_AC_ACTIVATION</b>	
<b>O.TOE_IDENTIFICATION</b>	
<b>O.CONFID-UPDATE-IMAGE.LOAD</b>	
<b>O.AUTH-LOAD-UPDATE-IMAGE</b>	
<b>O.LOAD</b>	

Table 21 - 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 3.3.3.2 for complete list of Security Objectives for the Operational Environment.

<b>OE.ENV</b>
<b>OE.CI</b>
<b>OE.SM-DP+</b>
<b>OE.SM-DS</b>

OE.MNO
OE.EIM (SGP.32)
OE.TRUSTED-PATHS-LPAd-IPAd
OE.APPLICATIONS
OE.MNO-SD
OE.CAP_FILE
OE.VERIFICATION
OE.CODE-EVIDENCE
OE.CONFID_UPDATE_IMAGE.CREATE

Table 22 - Security Objectives for the Environment

## 5.3 Security Objectives Rationale

### 5.3.1 Threats

#### 5.3.1.1 Unauthorized profile and platform management

#### T.UNAUTHORIZED-PROFILE-MNG

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

- O.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP+ and MNO OTA Platform) will access the Security Domains functions and content;
- OE.SM-DP+ and OE.MNO protect the corresponding credentials when used off- card.

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

The authentication is supported by corresponding secure channels:

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

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

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

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

#### T.UNAUTHORIZED-PLATFORM-MNG

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

- O.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.
- OE.SM-DP+ and OE.EIM (SGP.32) protect the corresponding credentials when used off- card.

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

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

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

#### **T.PROFILE-MNG-INTERCEPTION**

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

Consequently, the TSF ensures:

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

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

OE.SM-DP+, OE.MNO and OE.EIM (SGP.32) ensure that the credentials related to the secure channels will not be disclosed when used by off-card actors.

#### **T.PROFILE-MNG-ELIGIBILITY**

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

Consequently, the TSF ensures:

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

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

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

#### **5.3.1.2**     *Identity Tampering*

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

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

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

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

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

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

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

#### **5.3.1.3**     *eUICC cloning*

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

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

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

#### **5.3.1.4**     *LPAd impersonation*

##### **T.LPAd-INTERFACE-EXPLOIT**

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

#### **5.3.1.5**     *Unauthorized access to the mobile network*

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

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

### 5.3.1.6 *Second Level Threats*

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

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

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

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

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

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).

#### **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).

### 5.3.1.7 OS update

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

O.CONFID-UPDATEIMAGE.LOAD Counters the threat by ensuring the confidentiality of D.UPDATE\_IMAGE during installing it on the TOE.

OE.CONFID-UPDATEIMAGE.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.PRE-PPI ensures that there is a single ISD-P enabled at a time.

The profile deletion capability relies on the secure application deletion mechanisms provided by O.RE.PRE-PPI.

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

**OSP.VERIFICATION** 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.LOAD which shall ensure that the loading of a CAP file into the card is safe.

### 5.3.3 Assumptions

#### A.TRUSTED-PATHS-LPAd-IPAd

It is assumed that the interfaces ES10a, ES10b are trusted paths between the eUICC and IPAd, when IPAd is present and active. It is also assumed that the IPAd is a trusted component.

It is assumed that IPAd is protected against misuse (SGP.32).

It is assumed that the Device manufacturer is securing the following operations (SGP.32):

- Add of an initial eIM Configuration Data by the IPA.
- Complete removal of eIM Configuration Data by the IPA.

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

#### A.ACTORS

Actors of the infrastructure (eSIM CA, EUM, SM-DP+, SM-DS, eIM (SGP.32), and MNO) securely manage their own credentials and otherwise sensitive data. In particular for the overall mobile authentication mechanism defined in 3GPP TS 33.102 [22] to be secure, certain properties need to hold that are outside the scope of the eUICC. In particular, subscriber keys need to be strongly generated and securely managed. The following assumptions are therefore stated:

- o the key K is randomly generated during profile preparation and is securely transported to the Authentication Centre belonging to the MNO.

- o the random challenge RAND is generated with sufficient entropy in the Authentication Centre belonging to the MNO.

- o The Authentication Centre belonging to the MNO generates unique sequence numbers SQN, so that each quintuplet can only be used once.

- o Triplets / quintuplets are communicated securely between MNOs for roaming.

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

#### A.APPLICATIONS

The applications shall comply with the security guidelines document for the used platform (operating system). These guidelines must substantially describe the application writing style and the platform security mechanisms (e.g., security domains, application firewall) that shall be used to ensure that the applications do not harm the TOE.

The assumptions A.TRUSTED-PATHS-LPAd-IPAd, A.ACTORS and A.APPLICATIONS are defined as in [PP-eUICC]. A.CAP\_FILE is defined as in [PP-JCS] section 5.4.

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.

### 5.3.4 Rationale Tables

#### 5.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PRE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, OE.VERIFICATION and OE.CODE-EVIDENCE, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Section 5.3.1.1
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, OE.APPLICATIONS, OE.VERIFICATION and OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.EIM (SGP.32)	Section 5.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+, OE.MNO, O.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, OE.MNO-SD, OE.EIM (SGP.32)	Section 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY, O.RE.SECURE-COMM	Section 5.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 5.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 5.3.1.5

T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, OE.VERIFICATION and OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 5.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 5.3.1.6
T.CONFID-UPDATE IMAGE.LOAD	O.CONFID-UPDATEIMAGE.LOAD OE.CONFID-UPDATEIMAGE.CREATE	Section 5.3.1.7
T.INTEG-UPDATE- IMAGE.LOAD	O.SECURE_LOAD_ACODE	Section 5.3.1.7
T.UNAUTH-UPDATE- IMAGE.LOAD	O.SECURE_LOAD_ACODE O.AUTH-LOAD-UPDATE-IMAGE	Section 5.3.1.7
T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE O.TOE_IDENTIFICATION O.SECURE_AC_ACTIVATION	Section 5.3.1.7

Table 23 -Threats and Security Objectives- Coverage

Security Objectives	Threats
O.PRE-PPI	T.UNAUTHORIZED-PROFILE-MNG T.UNAUTHORIZED-PLATFORM-MNG T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY,

	T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
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.PRE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
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.LOAD	
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DP+	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY

OE.SM-DS	
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.EIM (SGP.32)	T.UNAUTHORIZED- PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION
OE.TRUSTED-PATHS-LPAd-IPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.CAP_FILE	
OE.VERIFICATION	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.CONFID_UPDATE_IMAGE.CREATE	T.CONFID-UPDATE-IMAGE.LOAD

Table 24 - Security Objectives and threats

#### 5.3.4.2 Organizational Security Policies Rationale

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

Table 25 -Organizational Security Policies and Security Objectives- Coverage

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

O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-DP+	
OE.SM-DS	
OE.MNO	
OE.EIM (SGP.32)	
O.IC.PROOF_OF_IDENTITY	
O.IC.SUPPORT	
O.IC.RECOVERY	
O.RE.PRE-PPI	OSP.LIFE-CYCLE
O.RE.SECURE-COMM	
O.RE.API	
O.RE.DATA-CONFIDENTIALITY	
O.RE.DATA-INTEGRITY	
O.RE.IDENTITY	
O.RE.CODE-EXE	
O.SECURE_AC_ACTIVATION	
O.SECURE_LOAD_ACODE	
O.TOE_IDENTIFICATION	
O.CONFID-UPDATE-IMAGE.LOAD	
O.AUTH-LOAD-UPDATE-IMAGE	
O.LOAD	OSP.VERIFICATION
OE.TRUSTED-PATHS-LPAd-IPAd	
OE.APPLICATIONS	
OE.MNO-SD	
OE.CAP_FILE	
OE.VERIFICATION	OSP.VERIFICATION
OE.CODE-EVIDENCE	OSP.VERIFICATION
OE.CONFID_UPDATE_IMAGE.CREATE	

Table 26 - Security Objectives and Organizational Security Policies

#### 5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.3
A.ACTORS	OE.CI, OE.SM-DP+, OE.MNO, OE.SM-DS, OE.EIM (SGP.32)	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 27 - Assumptions and Security Objectives for the Operational Environment- Coverage

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-DP+	A.ACTORS
OE.SM-DS	A.ACTORS
OE.MNO	A.ACTORS
OE.EIM (SGP.32)	A.ACTORS
OE.TRUSTED-PATHS-LPAd-IPAd	A.TRUSTED-PATHS-LPAd-IPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.MNO-SD	
OE.CAP_FILE	A.CAP_FILE
OE.VERIFICATION	A.VERIFICATION
OE.CODE-EVIDENCE	A.APPLICATIONS, A.VERIFICATION
OE.CONFID_UPDATE_IMAGE.CREATE	

Table 28 - 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 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**.
- This convention also applies for section 7.2 for SFRs in light blue (as example below) dedicated to RSP module.

- **example**

### 7.1 eUICC Security Functional Requirements

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

#### 7.1.1 Identification and authentication

##### FIA\_UID.1/EXT Timing of identification

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

- **application selection**
- **requesting data that identifies the eUICC**
- **[assignment: 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 following external (remote) users of the TOE:

- U.SM-DP+;
- U.MNO-OTA;
- U.EIM (SGP.32).

The identification of the only local user (U.MNO-SD) is addressed by the FIA\_UID.1/MNO-SD SFR. Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user.

#### FIA\_UAU.1/EXT Timing of authentication

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

- **application selection**
- **requesting data that identifies the eUICC**
- **user identification**
- **[assignment: 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 26:

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

- U.SM-DP+;
- U.MNO-OTA;
- U.EIM (SGP.32).

#### FIA\_USB.1/EXT User-subject binding

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

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

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

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

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

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

Application Note:

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

- U.SM-DP+ binds to a subject (S.ISD-R);
- U.MNO-OTA binds to an on-card user (U.MNO-SD);
- U.SM-DS binds to a subject (S.ISD-R)
- U.EIM binds to a subject (S.ISD-R).

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

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

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

Application Note 28:

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

- U.SM-DP+;
- U.MNO-OTA;
- U.EIM (SGP.32).

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

**FIA\_UID.1.1/MNO-SD** The TSF shall allow [assignment: [application selection](#)] on behalf of the user to be performed before the user is identified.

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

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

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

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

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

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

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

- **CERT.DPauth.ecdsa, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-DP+;**
- **MNO OID belonging to U.MNO-OTA;**
- **AID belonging to U.MNO-SD.**
- **CERT.DSauth.ECDSA and SM-DS OID belonging to U.SM-DS;**
- [selection: [CERT.EIM.ECDSA and eIM ID belonging to U.EIM](#)].

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

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

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

## 7.1.2 Communication

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

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

- between U.SM-DP+ and S.ISD-R;
- 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.SECRETS (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/objects:**
  - **U.SM-DP+ and S.ISD-R, SO.ISD-P**
  - **U.MNO-OTA and U.MNO-SD**
- **information: transmission of commands.**

### FDP\_IFF.1/SCP Simple security attributes

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

- **users/subjects/objects:**
  - **U.SM-DP+, SO.ISD-P and S.ISD-R, with security attribute D.SECRETS**
  - **U.MNO-OTA and U.MNO-SD, with security attribute D.MNO\_KEYS**
- **information: transmission of commands.**

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

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

**FDP\_IFF.1.3/SCP** 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: [none](#)].

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

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

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

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

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

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

[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-DP+ to open a SCP-SGP22 secure channel to transmit the following operations:](#)

- [ES8+.InitialiseSecureChannel](#)
- [ES8+.ConfigureISDP](#)
- [ES8+.StoreMetadata](#)
- [ES8+.ReplaceSessionKeys](#)
- [ES8+.LoadProfileElements](#).

[The TSF shall permit the IPAd to transmit the following operations:](#)

- ES10a.SetDefaultDpAddress
- ES10b.PrepareDownload
- ES10b.LoadBoundProfilePackage
- ES10b.GetEUICCChallenge
- ES10b.GetEUICCInfo
- ES10b.ListNotification
- ES10b.RetrieveNotificationsList
- ES10b.RemoveNotificationFromList
- ES10b.AuthenticateServer
- ES10b.CancelSession
- ES10b.LoadEuiccPackage (SGP.32)
- ES10b.AddInitialEim (SGP.32)
- ES10b.GetCerts (SGP.32)
- ES10b.EnableUsingDD (SGP.32)
- ES10b.ProfileRollback (SGP.32)
- ES10b.ConfigureAutomaticProfileEnabling (SGP.32)
- ES10b.GetEimConfigurationData (SGP.32)
- ES10b.GetProfilesInfo (SGP.32)
- ES10b.GetEID (SGP.32)

The TSF may permit the Ipad to transmit the following operations:

- ES10b.LoadCRL (SGP.22 V2.x)
- ES10b.eUICCMemoryReset (SGP.32).

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

- ES6.UpdateMetadata

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

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

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

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

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

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

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

**FPT\_TDC.1.1/SCP** The TSF shall provide the capability to consistently interpret

- **Commands from U.SM-DP+ and U.MNO-OTA**
- **Downloaded objects from U.SM-DP+ and U.MNO-OTA**

when shared between the TSF and another trusted IT product.

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

**FDP\_UCT.1/SCP Basic data exchange confidentiality**

**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+.

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform

Related keys are:

- either generated on-card (D.SECRETS): 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.

**FDP\_UIT.1/SCP Data exchange integrity**

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

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

Application Note:

This SFR is related to the protection of:

- Profiles downloaded from SM-DP+;
- Commands received from SM-DP+ and MNO OTA Platform;
- PPR and Enterprise Rules (optional) received from the MNO OTA Platform.

Related keys are:

- either generated on-card (D.SECRETS): 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.

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

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

- [NISTP-256 \(FIPS PUB 186-3 Digital Signature Standard\)](#)
- [brainpoolP 256r1 \(BSITR-03111, Version1.11, RFC5639\)](#)
- [FRP256V1 \(ANSSI ECC FRP256V1\).](#)

Note: in this TOE, the **FRP256V1 (ANSSI ECC FRP256V1)** is not required by the product

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

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

#### FCS\_CKM.6/SCP-SM Cryptographic key destruction

**FCS\_CKM.6.1/SCP-SM** The TSF shall destroy [assignment: **D.SECRETS, CERT.Dpauth.ECDSA, CERT.DPpb.ECDSA, CERT.Dsauth.ECDSA, D.CERT.EUICC.ECDSA, D.SK.EUICC.ECDSA and D.PK.CI.ECDSA**] when [selection: [no longer needed](#)].

**FCS\_CKM.6.2/SCP-SM** The TSF shall destroy cryptographic keys and keying material specified by FCS\_CKM.6.1/SCP-SM in accordance with a specified cryptographic key destruction method [assignment: [wipe the buffer with random bytes](#)] that meets the following: [assignment: [none](#)].

#### FCS\_CKM.6/SCP-MNO Cryptographic key destruction

**FCS\_CKM.6.1/SCP-MNO** The TSF shall destroy [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/SCP-MNO in accordance with a specified cryptographic key destruction method [assignment: [deletion of the key and removing it from the memory by garbage collection](#)] that meets the following: [assignment: [none](#)].

### 7.1.3 Security Domains

#### FDP\_ACC.1/ISDR Subset access control

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

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

#### FDP\_ACF.1/ISDR Security attribute based access control

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

- **subjects: S.ISD-R**
- **objects:**
  - **S.ISD-P with security attributes “state” and “PPR” and [Selection: *none*]**
- **operations:**
  - **Create and configure profile**
  - **Store profile metadata**
  - **Enable profile**
  - **Disable profile**
  - **Delete profile**
  - **Perform a Memory reset.**

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

- **Enabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state “DISABLED” and**
  - **in case a currently enabled S.ISD-P has to be disabled, the PPR data of this S.ISD-P allows its disabling, and**
  - **[Selection: *no additional conditions*].**

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

**FDP\_ACF.1.3/ISDR** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: [none](#)].

**FDP\_ACF.1.4/ISDR** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: [none](#)].

#### FDP\_ACC.1/ECASD Subset access control

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

- **subjects: S.ISD-R, S.ECASD**
- 1. **objects: data and attributes of ECASD,**
- 2. **operations:**
  - **execution of a ECASD function**
  - **access to output data of these functions,**
- **[assignment: [none](#)].**

#### FDP\_ACF.1/ECASD Security attribute based access control

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

- **subjects: S.ISD-R, with security attribute “AID” , S.ECASD**
- 3. **objects: data and attributes of S.ECASD**
- 4. **operations:**
  - **execution of a ECASD function**
    - **Verification of the off-card entities Certificates (SM-DP+, SM-DS), provided by an ISD-R, with the eSIM CA public key (PK.Cl.ECDSA)**
    - **Creation of an eUICC signature on material provided by an ISD-R.**
  - **access to output data of these functions.**
- **[assignment: [none](#)].**

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

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

**FDP\_ACF.1.3/ECASD** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *none*].

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

#### 7.1.4 Platform Services

#### FDP\_IFC.1/Platform\_services Subset information flow control

**FDP\_IFC.1.1/Platform\_services** The TSF shall enforce the **Platform services information flow control SFP** on

**users/subjects:**

- **S.ISD-R, S.ISD-P, U.MNO-SD**
- **Platform code (S.PRE, S.PPI, S.TELECOM)**

**information:**

- **D.PROFILE\_NAA\_PARAMS**
- **D.PROFILE\_RULES**
- **D.PLATFORM\_RAT**

**operations:**

- **installation of a profile**
- **PPR and RAT enforcement**
- **network authentication.**
  - **[selection: *none*]**

**FDP\_IFF.1/Platform\_services Simple security attributes**

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

**users/subjects:**

- **S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute “application identifier (AID)”**

**information:**

- **D.PROFILE\_NAA\_PARAMS**
- **D.PROFILE\_RULES**
- **D.PLATFORM\_RAT**

**operations:**

- **installation of a profile**
- **PPR and RAT enforcement**
- **network authentication.**
- [selection: *none*]

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

- **D.PROFILE\_NAA\_PARAMS shall be transmitted only:**
  - **by U.MNO-SD to S.TELECOM in order to execute the network authentication function**
  - **by S.ISD-R to S.PPI using the profile installation function**
- **D.PROFILE\_RULES shall be transmitted only**
  - **by S.ISD-R to S.PRE in order to execute the PPR enforcement function**
  - [selection: *none*]
- **D.PLATFORM\_RAT shall be transmitted only**
  - **by S.ISD-R to S.PRE in order to execute the RAT enforcement function.**

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

**FDP\_IFF.1.4/Platform\_services** The TSF shall explicitly authorize an information flow based on the following rules: [assignment: [none](#)].

**FDP\_IFF.1.5/Platform\_services** The TSF shall explicitly deny an information flow based on the following rules: [assignment: [none](#)].

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

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

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

## **7.1.5 Security management**

This package includes several supporting security functions:

- Random number generation (FCS\_RNG.1)
- User data and TSF self-protection measures:
  - TOE emanation (FPT\_EMS.1/Base)
  - protection from integrity errors (FDP\_SDI.1/Base)
  - residual data protection (FDP\_RIP.1/Base)
  - preservation of a secure state (FPT\_FLS.1/Base)
- Security management measures:
  - Management of security attributes such as Platform data (FMT\_MSA.1/PLATFORM\_DATA), PPR and Enterprise Rules (FMT\_MSA.1/RULES), (FMT\_MSA.1/RAT) and keys (FMT\_MSA.1/CERT\_KEYS) with restrictive default values (FMT\_MSA.3);
  - Management of roles and security functions (FMT\_SMR.1/Base and FMT\_SMF.1/Base).

### **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: [Hybrid design, Forward secrecy, enhanced backward secrecy, Enhanced forward secrecy, Entropy input quality](#)].

## Application Note:

- Hybrid design: (DRG.4.1) “The internal state of the RNG shall use PTRNG of class PTG.2 as random source”.
- Forward secrecy: (DRG.4.2) “The RNG provides forward secrecy”.
- Enhanced backward secrecy: (DRG.4.3) “The RNG provides backward secrecy even if the current internal state is known”.
- Enhanced forward secrecy: (DRG.4.4) “The RNG provides enhanced forward secrecy after calling the JAVA API “ALG\_KEYGENERATION” or “ALG\_TRNG” **algorithms from [JCAPI310] RandomData class are used.**
- Entropy input quality: (DRG.4.5) “The internal state of the RNG is seeded by an PTRNG of class PTG.2”.

**FCS\_RNG.1.2** The TSF shall provide [selection: **bits, octets of bits, numbers** [assignment: **format of numbers that meet the requirements of class DRG.4**]] that meet [assignment: **a defined quality metric of the selected RNG class**].

## Application Note:

- Output and mutual difference: (DRG.4.6) “The RNG generates output for which 235 strings of bit length 128 are mutually different with probability greater than or equal to  $1 - \frac{1}{2^{58}}$ ”.
- Statistical tests: (DRG.4.7) “Statistical tests suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [AIS31]”.

<b>FPT_EMS.1/Base TOE Emanation of TSF and User data</b>
--

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

ID	Emission	Attack surface	TSF data	User data
1	[assignment: <i>power consumption and electromagnetic fluctuations</i> ]	Any	-	<ul style="list-style-type: none"> <li>o D.SECRETS;</li> <li>o D.SK.EUICC.ECDSA</li> </ul> <p>and the secret keys which are part of the following keysets:</p> <ul style="list-style-type: none"> <li>o D.MNO_KEYS,</li> <li>o D.PROFILE_NAA_PARAMS.</li> </ul>

<b>FDP_SDI.1/Base Stored data integrity monitoring</b>
--

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

**Refinement:**

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

- D.MNO\_KEYS
- Profile data
  - D.PROFILE\_NAA\_PARAMS
  - D.PROFILE\_IDENTITY
  - D.PROFILE\_RULES
  - D.PROFILE\_USER\_CODES
- Management data
  - D.PLATFORM\_DATA
  - D.DEVICE\_INFO
  - D.PLATFORM\_RAT
- Identity management data
  - D.SK.EUICC.ECDSA
  - D.CERT.EUICC.ECDSA
  - D.PK.CI.ECDSA
  - D.PK.EIM.ECDSA (SGP.32)
  - D.EID
  - D.SECRETS
  - D.CERT.EUM.ECDSA
  - D.CRLs if existing

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

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

- **D.SECRETS;**
- **D.SK.EUICC.ECDSA;**
- **The secret keys which are part of the following keysets:**
  - **D.MNO\_KEYS,**
  - **D.PROFILE\_NAA\_PARAMS.**

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

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

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

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

**FMT\_MSA.1.1/PLATFORM\_DATA** The TSF shall enforce the **ISD-R access control policy** to restrict the ability to **modify** the security attributes **the following parts of D.PLATFORM\_DATA:**

- ISD-P state

to

- S.ISD-R to modify ISD-P state
  - from “INSTALLED” to “SELECTABLE” (during ISD-P creation)
  - from “ENABLED” to “DISABLED” (during profile disabling)
- S.ISD-R to modify ISD-P state
  - from “DISABLED” to “ENABLED” (during profile enabling).

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

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

- D.PROFILE\_RULES

to

- S.ISD-R to change\_default, via function “ES8+.ConfigureISDP”
- S.ISD-R to query
- S.ISD-P to modify, via function “ES6.UpdateMetadata”
- [selection: S.ISD-R to delete, via function “ESep.Delete” (SGP.32)]

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

**FMT\_MSA.1.1/CERT\_KEYS** The TSF shall enforce the **ECASD access control SFP** to restrict the ability to **query and delete** the security attributes

- D.CERT.EUICC.ECDSA
- D.PK.CI.ECDSA
- D.CERT.EUM.ECDSA
- D.MNO\_KEYS

to

- **S.ISD-R for:**
  - query D.PK.CI.ECDSA
  - delete D.MNO\_KEYS via function [selection: [ESep.delete \(SGP.32\)](#)]
- **no actor for other operations.**

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

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

[List of management functions:](#)

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

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

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

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

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

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

**FMT\_MSA.1.1/RAT** The TSF shall enforce the **Platform services information flow SFP** to restrict the ability to **query** the security attributes

- **D.PLATFORM\_RAT**
- **D.PROFILE\_NAA\_PARAMS**
- **D.PROFILE\_RULES**

to

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

### FMT\_MSA.3 Static attribute authorized

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

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

## 7.1.6 Mobile Network authentication

This package defines the requirements related to the authentication of the eUICC on MNO networks.

The TSF must implement cryptographic mechanisms for the authentication on the MNO network (FCS\_COP.1/Mobile\_network) and manage the keys securely (FCS\_CKM.2/Mobile\_network and FCS\_CKM.6/Mobile\_network).

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

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

- **MILENAGE according to standard [20] with the following restrictions:**
  - **Only use 128-bit AES as the kernel function? do not support other choices**
  - **Allow any value for the constant OP**
  - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [20]**

- **Tuak according to [21] with the following restrictions:**
  - Allow any value of TOP
  - Allow multiple iterations of Keccak
  - Support 256-bit K as well as 128-bit
  - To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.
- **CAVE according to standard TIA TR-45.AHAG Common Cryptographic Algorithms**

#### FCS\_CKM.2/Mobile\_network Cryptographic key distribution

**FCS\_CKM.2.1/Mobile\_network** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: [following key distribution methods](#)] that meets the following: [assignment: [following standards](#)].

Item	Method	Standard
Milenage	distribution method from SCP-SGP22 (SCP03t)	[SGP.22]
Tuak	distribution method from SCP-SGP22 (SCP03t)	[SGP.22]
CAVE	distribution method from SCP-SGP22 (SCP03t)	[SGP.22]

#### FCS\_CKM.6/Mobile\_network Cryptographic key destruction

**FCS\_CKM.6.1/ Mobile\_network** The TSF shall destroy [assignment: [list of cryptographic keys \(including keying material\)](#)] 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/Mobile\_network in accordance with a specified cryptographic key destruction method [assignment: [deletion of the key and removing it from the memory by garbage collection](#)] that meets the following: [assignment: [none](#)].

## 7.2 Runtime Environment Security Requirements

The Subjects (prefixed with an “S”), the Objects (prefixed with an “O”), Information (prefixed with an “I”) are defined and described in [PP-JCS] section 7.2. 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

#### FDP\_ACC.2/FIREWALL Complete access control

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

#### Refinement:

The operations involved in the policy are:

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

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

#### FDP\_ACF.1/FIREWALL Security attribute based access control

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

Subject/Object	Security attributes
----------------	---------------------

S.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.7 ([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\_ACCESS or OP.ARRAY\_LENGTH upon any O.JAVAOBJECT whose Sharing attribute has value “global array”.

**FDP\_ACF.1.3/FIREWALL** The TSF shall explicitly 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

#### FCS\_COP.1/GP-SCP Cryptographic operation

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

SCP protocol	Cryptographic operation	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
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, P-384, P-521 brainpoolP256r1, P384r1, P512r1	SCP11 [Amd F]: FIPS PUB 186-3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639 ○
SCP80	Secure communication	AES	AES: 128, 192, or 256 bits	[TS 102.225] [TS 102.226]

	channel with OTA Server			
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 [JCRE3], §7.7, within the bounds of the Commit Capacity ([JCRE3], §7.8), and those described in [JCAPI3]**.

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

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

- **throw an exception,**
  - **lock the card session,**
  - **reinitialize the Java Card System and its data,**
  - **[assignment: none]**
- upon detection of a potential security violation.

#### Refinement:

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

- CAP file inconsistency,
- typing error in the operands of a bytecode,
- applet life cycle inconsistency,
- card tearing (unexpected removal of the Card out of the CAD) and power failure, abort of a transaction in an unexpected context, (see abortTransaction(), [JCAPI3] and ([JCRE3], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow
- [assignment: **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 [JVM3] 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 AID are defined with associated value during loading and with context identifier]**.

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

**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 related to the installation of the applets, meaning FDP\_ITC.2/Installer, FMT\_SMR.1/Installer, FPT\_FLS.1/Installer, FPT\_RCV.3/Installer have been removed from the ST, as covered by their GP equivalent.

- For FDP\_ITC.2/Installer, please refer to FDP\_ITC.2/GP-ELF
- For FMT\_SMR.1/Installer, please refer to FMT\_SMR.1/GP
- For FPT\_FLS.1/Installer, please refer to FPT\_FLS.1/GP
- For FPT\_RCV.3/Installer, please refer to FPT\_RCV.3/GP

### 7.2.3 ADELG Security Functional Requirements

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

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

**FDP\_ACC.2.1/ADEL** The TSF shall enforce the **ADEL access control SFP** on **S.ADEL, S.JCRE, S.JCVM, O.JAVAOBJECT, O.APPLET and O.CODE\_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 ([JCRE3], §11.3.4.1, Applet Instance Deletion): S.ADEL may perform OP.DELETE\_APPLET upon an O.APPLET only if,**
  - 1) **S.ADEL is currently selected,**
  - 2) **there is no instance in the context of O.APPLET that is active in any logical channel and**
  - 3) **there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance distinct from O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.**
- **R.JAVA.15 ([JCRE3], §11.3.4.2.1, Multiple Applet Instance Deletion): S.ADEL may perform OP.DELETE\_APPLET upon several O.APPLET only if,**
  - 1) **S.ADEL is currently selected,**
  - 2) **there is no instance of any of the O.APPLET being deleted that is active in any logical channel and**
  - 3) **there is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.**
- **R.JAVA.16 ([JCRE3], §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 ([JCRE3], §11.3.4.4, Applet Package and Contained Instances Deletion):  
S.ADEL may perform OP.DELETE\_PCKG\_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 'nitial values to override the default values when an object or information is created.

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

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

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

**FMT\_SMR.1.1/ADEL** The TSF shall maintain the roles: **applet deletion manager.**

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

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

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

Application Note:

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

## 7.2.4 RMIG Security Functional Requirements

The product does not support RMI features.

## 7.2.5 ODELG Security Functional Requirements

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

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

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

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

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

Application Note:

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

## 7.2.6 Global Platform Security Functional requirements

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

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

- **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].**

### FDP\_ROL.1/GP Basic rollback

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

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

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

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

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

Refinement:

The TSF shall be able to generate 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**].

#### 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].**

#### **FDP\_ITC.2/GP-ELF Import of user data with security attributes**

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

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

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

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

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

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

#### **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]].

#### **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: 0% 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

#### **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's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively

**FDP\_IFF.1/GP-ELF Complete information flow control**

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

**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 ELFs**
- **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.

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

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

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

Application Note:

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

#### FIA\_AFL.1/GP Authentication failure handling

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

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

#### FIA\_UAU.1/GP Timing of authentication

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

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

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

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

#### **FDP\_UIT.1/GP Basic data exchange integrity**

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

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

#### **FDP\_UCT.1/GP Basic data exchange confidentiality**

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

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

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

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

**FTP\_ITC.1.3/GP** The TSF shall initiate communication via the trusted channel for:

- **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].**

#### **FPR\_UNO.1/GP Unobservability**

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

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

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

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

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

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

- **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**

**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].

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].

#### 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</del> , or <del>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	
<del>INTERNAL AUTHENTICATE</del>		<del>None</del>	
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
<b>Remote File Management Commands</b> 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]
<b>Remote Applet Management Commands</b> 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
STORE DATA	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, <del>CARD_LOCKED</del> , 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.

#### **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”**

#### **FDP\_ACF.1/OS-UPDATE Security attribute based access control**

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

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

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

- **The verification of the additional code cryptographic signature (using D.OS-UPDATE\_SGNVER-KEY) by S.OS-DEVELOPER is successful.**

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

**FDP\_ACF.1.3/OS-UPDATE** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: none].

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

Application Note:

- Identification data verification is necessary to ensure that the received additional code is 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.

<b>FCS_COP.1/OS-UPDATE-DEC</b>	<b>Cryptographic operation</b>
--------------------------------	--------------------------------

**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**].

<b>FCS_COP.1/OS-UPDATE-VER</b>	<b>Cryptographic operation</b>
--------------------------------	--------------------------------

**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**].

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

**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:
  - o step 1: loading
  - o step 2: activation
  - o 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:
  - o 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

<b>FAU_SAS.1 Audit Storage</b>
--------------------------------

**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:

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

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

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

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

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

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

## 7.3 Security Functional Requirements Rationale

### 7.3.1 SFRs for eUICC rationale

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

### 7.3.2 SFRs for Runtime Environment rationale

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

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

RE objectives	Translation from JavaCard PP
O.RE.PRE-PPI	O.INSTALL, O.DELETION, O.LOAD, O.CARD-MANAGEMENT
O.RE.SECURE-COMM	O.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.KEY-MNGT, O.REALLOCATION, OE.VERIFICATION, O.ARRAYS_VIEWS_CONFID, O.ARRAY_VIEWS_INTEG, OE.CODE_EVIDENCE
O.RE.API	O.CARD-MANAGEMENT, O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM, OE.VERIFICATION, OE.CODE_EVIDENCE
O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.KEY-MNGT, O.REALLOCATION, ADV_ARC “non-bypassability” refinement, O.ARRAYS_VIEWS_CONFID, OE.VERIFICATION
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE, O.ARRAY_VIEWS_INTEG, OE.CODE_EVIDENCE, OE.VERIFICATION
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT
O.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE, OE.VERIFICATION, OE.CAP_FILE

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

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

### 7.3.3 SFRs for Underlying platform IC rationale

**O.IC.PROOF\_OF\_IDENTITY** coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for identification data storage as dealt with FAU\_SAS.1.

**O.IC.RECOVERY** coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for recovery operations as dealt with in FPT\_RCV.3/OS and FPT\_RCV.4/OS, for secure state preservation against security violations as in FPT\_FLS.1/Platform\_services.

**O.IC.SUPPORT** coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially , for secure low-level cryptographic processing as in FCS\_CKM.1and FCS\_COP.1.

### 7.3.4 SFRs dependency rationale

SFR	CC dependencies	Satisfied dependencies
FIA_UID.1/EXT	No Dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_UAU.4/EXT	No Dependencies	
FIA_UID.1/MNO-SD	No Dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1/Base

FIA_ATD.1/Base	No Dependencies	
FIA_API.1	No Dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	No Dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, 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 (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1/GP-SCP, FCS_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, <b>See rationale</b>
FCS_CKM.6/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) or (FCS_CKM.5)	FDP_ITC.2/SCP, <b>See rationale</b>
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	
FCS_RNG.1	No Dependencies	
FPT_EMS.1/Base	No Dependencies	
FDP_SDI.1/Base	No Dependencies	
FDP_RIP.1/Base	No Dependencies	
FPT_FLS.1/Base	No Dependencies	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base

FMT_MSA.1/RULES	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_SMF.1/Base	No Dependencies	
FMT_SMR.1/Base	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS, FMT_SMR.1/Base, FMT_MSA.1/RAT
FCS_COP.1/Mobile_network	(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 <b>See rationale</b>
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 <b>See rationale</b> 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 FCS_RNG.1

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
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)	<b>See rationale</b>
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPR_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
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)	<b>See rationale</b>
FPT_FLS.1/ADEL	No Dependencies	
FDP_RIP.1/ODEL	No Dependencies	
FPT_FLS.1/ODEL	No Dependencies	
FPT_FLS.1/GP	No Dependencies	
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMR.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/GP	No Dependencies	
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1/GP FTP_ITC.1/GP
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL FPT_TDC.1/GP FTP_ITC.1/GP
FPT_RCV.3/GP	(AGD_OPE.1)	AGD_OPE.1
FDP_IFC.2/GP-ELF	(FDP_IFF.1)	FDP_IFF.1/GP-ELF

FDP_IFF.1/GP-ELF	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FIA_UID.1/GP	No Dependencies	
FIA_AFL.1/GP	(FIA_UAU.1)	FIA_UAU.1/GP
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No Dependencies	
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FTP_ITC.1/GP	No Dependencies	
FPR_UNO.1/GP	No Dependencies	
FPT_TDC.1/GP	No Dependencies	
FDP_IFC.2/GP-KL	(FDP_IFF.1)	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-KL FMT_MSA.3/GP
FMT_MSA.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
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 <b>See rationale</b>
FMT_SMR.1/OS-UPDATE	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.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 or FCS_CKM.5) and (FCS_CKM.6)	FDP_ITC.2/GP-ELF <b>See rationale</b>
FCS_COP.1/OS-UPDATE-VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FDP_ITC.2/GP-ELF <b>See rationale</b>
FIA_ATD.1/OS-UPDATE	No Dependencies	
FPT_FLS.1/OS-UPDATE	No dependencies	
FAU_SAS.1	No Dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No Dependencies	

Table 29 – SFRs dependency table

**Rationale for the exclusion of dependencies:**

- The dependency FCS\_CKM.5 of FCS\_CKM.6/SCP-SM, CKM.6/SCP-MNO, and CKM.6/Mobile\_network is unsupported.

The dependency between is not satisfied because no Key Access Interface exists.

- **The dependency FMT\_SMF.1 of FMT\_MSA.1/JCRE is unsupported.**

The dependency between FMT\_MSA.1/JCRE and FMT\_SMF.1 is not satisfied because no management functions are required for the Java Card RE.

- **The dependency 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.

### 7.3.5 SAR refinement

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

## 8 TOE SUMMARY SPECIFICATION

---

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

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

### 8.1 eUICC security functions

#### 8.1.1 GSMA.ProfileManagement

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

- Profile downloading
- Profile elements installation
- Profile deletion
- Profile enabling and disabling.

It also supports everything related to profile data isolation.

#### 8.1.2 GSMA.ECASD

This security function handles the Embedded UICC Controlling Authority Security Domain (ECASD) management as defined by **[SGP.32]**. The ECASD is responsible for secure storage of credentials required to support the required Security Domains on the eUICC.

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

#### 8.1.3 GSMA.ISDR

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

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

#### 8.1.4 GSMA.ISDP

This security function handles the ISD-P management as defined by **[SGP.32]**. The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile. The ISD-P is used for the Profile download and installation in collaboration with the Profile Package Interpreter for the decoding/interpretation of the received Profile Package.

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

### **8.1.5 GSMA.PPR**

This security function implements Profile Policy Rules management as defined by [SGP.32]. The PPRs are defined by the Profile Owners and set by the SM-DP+ in the Profile Metadata. Upon downloading a profile with defined PPR, eUICC is required to follow these defined rules.

Secure management and processing of the PPRs are covered.

## **8.2 Runtime Environment security functions**

### **8.2.1 GP.CardContentManagement**

This security function provides the capability and a dedicated flow control for the loading, installation, extradition, registry update, selection and removal of card content and especially executable files and application instances. Such features are offered to the Card Issuer and its business partners, allowing the Card Issuer to delegate card content management to an Application Provider according to privileges assigned to the various security domains on the card. It supports Delegated management (DM), Authorized management (AM) and it can use DAP or Mandated DAP verification and generation of Reception token. It also checks that only the card management commands specified and allowed at each state of the smart card's life cycle are accepted, and ill-formed ones are rejected with an appropriate error response.

### **8.2.2 GP.KeyLoading**

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

### **8.2.3 GP.SecurityDomain**

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

### 8.2.4 GP.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 eSIM OS to be updated post-issuance. OS updates are performed through the loading, installation and activation of related ELF, fulfilling the same rules as for any other ELF. DAP verification (AES128 CMAC) is mandatory for ELFs containing OS updates, ensuring the authenticity and integrity protection of the code update, and the content of the ELF is directly encrypted (AES128 in CBC mode) with a dedicated encryption key, ensuring the confidentiality protection. Note that both the DAP signature verification key and the encryption key are proprietary KEYS, meaning that OS updates can only be issued and decrypted by Thales. Verification of TOE identification data is also enforced before allowing any OS update. 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 [JCAPI3]. The APDU class API is designed to be transport protocol independent T=0, T=1, T=CL (as defined in ISO 7816-3).

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

### 8.2.8 JCS.ByteCodeExecution

This security function handles applet bytecode execution according to the rules defined in [JVM3]. The JVM execution may be summarized in JVM interpreter start-up, bytecode execution and JVM 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 JavaCard API:

- Encryption and decryption using AES (128, 192 or 256 bits key) algorithm as defined in [JCAPI3] Cipher class.
- Data hash computation as defined in [JCAPI3] MessageDigest class.
- HMAC computation as defined in [JCAPI3] Signature class.
- Generation and verification of ECDSA signatures as defined in [JCAPI3] Signature class. Elliptic curve cryptography over GF(p) is considered here, with P ranging from 160 to 521 bits.
- Secret key agreement according to the ECDH algorithm, as defined in [JCAPI3] KeyAgreement class.
- Secret key agreement according to the DH algorithm (ALG\_DH\_PLAIN), as defined in [JCAPI3] KeyAgreement class.

### 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 is done using method protecting confidentiality and integrity of key.
- Key masking protects the confidentiality of cryptographic keys from being read out from the memory. It ensures the service of accessing and modifying them.
- Key destruction (implemented through the method clearKey() of the Key class) disables the use of a key both logically and physically. Reuse is only possible after erase.

### 8.2.13 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 [JCRE3], 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 [JCRE3].

### 8.2.15 JCS.RunTimeExecution

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

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

### 8.2.16 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 check 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.ISDR
FIA_UAU.1/EXT	This SFR is covered by GSMA.ECASD and GP.SecureChannel
FIA_USB.1/EXT	This SFR is covered by GSMA.ECASD and GP.SecurityDomain
FIA_UAU.4/EXT	This SFR is covered by GSMA.ECASD and GP.SecureChannel
FIA_UID.1/MNO-SD	This SFR is covered by GP.SecurityDomain
FIA_USB.1/MNO-SD	This SFR is covered by GP.SecurityDomain, GSMA.ISDP, GSMA.ECASD
FIA_ATD.1/Base	This SFR is covered by GP.SecurityDomain and GSMA.ECASD
FIA_API.1	This SFR is covered by GP.SecurityDomain and GSMA.ECASD
FDP_IFC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_IFF.1/SCP	This SFR is covered by GSMA.ProfileManagement
FTP_ITC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_ITC.2/SCP	This SFR is covered by GSMA.ProfileManagement
FPT_TDC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_UCT.1/SCP	This SFR is covered by GSMA.ProfileManagement

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_UIT.1/SCP	This SFR is covered by GSMA.ProfileManagement
FCS_CKM.1/SCP-SM	This SFR is covered by GSMA.ProfileManagement and JCS.CryptoAPI for ECKA-EG
FCS_CKM.2/SCP-MNO	This SFR is covered by JCS.CryptoAPI
FCS_CKM.6/SCP-SM	This SFR is covered by JCS.KeyManagement
FCS_CKM.6/SCP-MNO	This SFR is covered by JCS.KeyManagement
FDP_ACC.1/ISDR	This SFR is covered by GSMA.ISDR
FDP_ACF.1/ISDR	This SFR is covered by GSMA.ISDR
FDP_ACC.1/ECASD	This SFR is covered by GSMA.ECASD
FDP_ACF.1/ECASD	This SFR is covered by GSMA.ECASD
FDP_IFC.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FDP_IFF.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FPT_FLS.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FCS_RNG.1	This SFR is covered by JCS.CryptoAPI providing AIS31 DRG.4 random number generation to applets.
FPT_EMS.1/Base	This SFR is covered by JCS.CryptoAPI and JCS.KeyManagement
FDP_SDI.1/Base	This SFR is covered by GSMA.ProfileManagement
FDP_RIP.1/Base	This SFR is covered by GSMA.ProfileManagement
FPT_FLS.1/Base	This SFR is covered by GSMA.ProfileManagement
FMT_MSA.1/PLATFORM_DATA	This SFR is covered by GSMA.ISDR
FMT_MSA.1/RULES	This SFR is covered by GSMA.PPR
FMT_MSA.1/CERT_KEYS	This SFR is covered by GSMA.ProfileManagement
FMT_SMF.1/Base	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR
FMT_SMR.1/Base	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR
FMT_MSA.1/RAT	This SFR is covered by GSMA.ISDR
FMT_MSA.3	This SFR is covered by GSMA.ISDR, GSMA.ISDP, GSMA.ECASD
FCS_COP.1/Mobile_network	This SFR is covered by JCS.CryptoAPI
FCS_CKM.2/Mobile_network	This SFR is covered by JCS.CryptoAPI
FCS_CKM.6/Mobile_network	This SFR is covered by JCS.KeyManagement

### 8.3.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	This SFR is covered by JCS.Firewall.
FDP_ACF.1/FIREWALL	This SFR is covered by JCS.Firewall.
FDP_IFC.1/JCVM	This SFR is covered by JCS.Firewall and JCS.APDUBuffer controlling unauthorized access or invalid storage of reference.
FDP_IFF.1/JCVM	This SFR is covered by JCS.Firewall.
FDP_RIP.1/OBJECTS	This SFR is covered by JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data).

<b>FMT_MSA.1/JCRE</b>	This SFR is covered by JCS.RunTimeExecution covering context switch and application selection.
<b>FMT_MSA.1/JCVM</b>	This SFR is covered by JCS.ByteCodeExecution requiring context switch for specific code execution and JCS.RunTimeExecution covering context switch and modification of the Currently Active Context according to given rules.
<b>FMT_MSA.2/FIREWALL_JCVM</b>	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
<b>FMT_MSA.3/FIREWALL</b>	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
<b>FMT_MSA.3/JCVM</b>	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
<b>FMT_SMF.1/JC</b>	This SFR is addressed by JCS.RunTimeExecution covering context management and instance registration.
<b>FMT_SMR.1/JC</b>	This SFR is addressed by JCS.RunTimeExecution covering JCVM and JCRE roles.
<b>FCS_CKM.1/GP-SCP</b>	This SFR is covered by GP.SecureChannel.
<b>FCS_COP.1/GP-SCP</b>	This SFR is covered by GP.SecureChannel.
<b>FDP_RIP.1/ABORT</b>	This SFR is addressed by JCS.EraseResidualData covering data erasure.
<b>FDP_RIP.1/APDU</b>	This SFR is addressed by JCS.EraseResidualData covering data erasure.
<b>FDP_RIP.1/bArray</b>	This SFR is addressed by JCS.OutOfLifeDataUndisclosure and JCS.EraseResidualData covering data erasure.
<b>FDP_RIP.1/GlobalArray</b>	This SFR is addressed by JCS.EraseResidualData covering data erasure.
<b>FDP_RIP.1/KEYS</b>	This SFR is addressed by JCS.EraseResidualData covering data erasure.
<b>FDP_RIP.1/TRANSIENT</b>	This SFR is covered by JCS.OutOfLifeDataUndisclosure managing the access control to transient object to be erased prior the erasure of the content in memory.
<b>FDP_ROL.1/FIREWALL</b>	This SFR is addressed by JCS.RunTimeExecution covering transaction rollback during specific operations.
<b>FAU_ARP.1</b>	This SFR is addressed by JCS.RunTimeExecution, JCS.Exception, JCS.Firewall, and OS.MemoryManagement covering exception handling with different specific operations.
<b>FDP_SDI.2/DATA</b>	This SFR is addressed by JCS.KeyManagement, OS.Atomicity and OS.MemoryManagement covering integrity handling with specific operations.
<b>FPR_UNO.1</b>	This SFR is addressed by JCS.KeyManagement, JCS.CryptoAPI and OS.MemoryManagement covering data handling with specific operations avoiding observation.
<b>FPT_FLS.1/JC</b>	This SFR is addressed by JCS.Exception, JCS.ByteCodeExecution, JCS.RunTimeExecution, and OS.Atomicity preserving a secure state when unexpected events occur during specific operations.
<b>FPT_TDC.1</b>	This SFR is covered by JCS.Package enforcing export check, CAP file translation and link specific operations.
<b>FIA_ATD.1/AID</b>	This SFR is covered by JCS.RunTimeExecution and GP.GPRegistry controlling applet registration and uninstallation.

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

<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>FDP_ROL.1/GP</b>	This SFR is addressed by GP.CardContentManagement, GP.KeyLoading and OS.Atomicity.
<b>FCO_NRO.2/GP</b>	This SFR is covered by GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading: * mutual authentication between the external entity (Issuer or Application provider) and the selected security Domain, including creation of a session key, * by the verification of a (chained) MAC that the Issuer or Application provider attaches to each file or data block sent, * by the erase of the session key at the end of the session.
<b>FMT_SMR.1/GP</b>	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain managing the roles: S.OPEN, issuer, application provider, verification authority and controlling authority.
<b>FMT_SMF.1/GP</b>	This SFR is covered by GP.SecurityDomain and GP.SecureChannel.
<b>FDP_ITC.2/GP-ELF</b>	This SFR is covered by JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations.
<b>FDP_ITC.2/GP-KL</b>	This SFR is covered by GP.KeyLoading.
<b>FPT_RCV.3/GP</b>	This SFR is addressed by JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails.
<b>FDP_IFC.2/GP-ELF</b>	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
<b>FDP_IFF.1/GP-ELF</b>	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
<b>FIA_UID.1/GP</b>	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
<b>FIA_AFL.1/GP</b>	This SFR is covered by GP.SecureChannel.
<b>FIA_UAU.1/GP</b>	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain (as for FIA_UID.1/GP).
<b>FIA_UAU.4/GP</b>	This SFR is covered by GP.SecureChannel.
<b>FDP_UIT.1/GP</b>	This SFR is covered by GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
<b>FDP_UCT.1/GP</b>	This SFR is covered by GP.SecureChannel which provides confidentiality protection for sensitive data (such as secret keys).
<b>FTP_ITC.1/GP</b>	This SFR is addressed by GP.SecureChannel.
<b>FPR_UNO.1/GP</b>	This SFR is covered by JCS.RunTimeExecution and JCS.CryptoAPI.
<b>FPT_TDC.1/GP</b>	This SFR is addressed by GP.CardContentManagement, GP.SecureChannel and GP.KeyLoading.
<b>FDP_IFC.2/GP-KL</b>	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
<b>FDP_IFF.1/GP-KL</b>	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.

<b>FMT_MSA.1/GP</b>	This SFR is covered by GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.
<b>FMT_MSA.3/GP</b>	This SFR is covered by GP.SecureChannel providing setting of the default value.
<b>FDP_ACC.1/OS-UPDATE</b>	This SFR is covered by GP.OS-UPDATE.
<b>FDP_ACF.1/OS-UPDATE</b>	This SFR is covered by GP.OS-UPDATE.
<b>FMT_MSA.3/OS-UPDATE</b>	This SFR is covered by GP.OS-UPDATE.
<b>FMT_SMR.1/OS-UPDATE</b>	This SFR is covered by GP.OS-UPDATE.
<b>FMT_SMF.1/OS-UPDATE</b>	This SFR is covered by GP.OS-UPDATE.
<b>FTP_TRP.1/OS-UPDATE</b>	This SFR is covered by GP.OS-UPDATE.
<b>FCS_COP.1/OS-UPDATE-DEC</b>	This SFR is covered by GP.OS-UPDATE.
<b>FCS_COP.1/OS-UPDATE-VER</b>	This SFR is covered by GP.OS-UPDATE.
<b>FIA_ATD.1/OS-UPDATE</b>	This SFR is covered by GP.SecurityDomain
<b>FPT_FLS.1/OS-UPDATE</b>	This SFR is covered by GP.SecurityDomain
<b>FAU_SAS.1</b>	This SFR is covered by OS.MemoryManagement
<b>FPT_RCV.3/OS</b>	This SFR is covered by OS.Atomicity.
<b>FPT_RCV.4/OS</b>	This SFR is covered by 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. CfPOE
OE.Process-Sec-IC	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. <ul style="list-style-type: none"> <li>• During phases b, c: CfPOE</li> <li>• During phase d, e: SgOE</li> </ul>
OE.Lim_Block_Loader	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. <ul style="list-style-type: none"> <li>• During phases b, c: CfPOE</li> </ul>
OE.Loader_Usage	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. <ul style="list-style-type: none"> <li>• During phases b, c: CfPOE</li> </ul>
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: CfPOE

## 9.5 Statement of compatibility – Security objectives part

IC Security objectives	Rationale
O.Leak_inherent	This objective is covered by TOE evaluation.
O.Phys-Probing	This objective is covered by TOE evaluation.
O.Malfunction	This objective is covered by TOE evaluation.
O.Phys-Manipulation	This objective is covered by the IC evaluation.
O.Leak-Forced	This objective is covered by the IC evaluation.
O.Abuse-Func	This objective is covered by the TOE evaluation.
O.Identification	This objective is covered by the IC evaluation.
O.RND	This objective is covered by the IC evaluation.
O.Cap_Avail_Loader	This objective is covered by the TOE evaluation.
O.Authentication	This objective is covered by the TOE evaluation.
O.Ctrl_Auth_Loader	This objective is covered by the TOE evaluation.
O.Prot_TSF_Confidentiality	This objective is covered by the IC evaluation.
O.Mem-Access	This objective is covered by the IC evaluation.

## 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	Rationale
<b>Part of [ST/IC]</b>	
From "Malfunction"	
FRU_FLT.2	RP_SFR-MECH
FPT_FLS.1	RP_SFR-MECH
From "Abuse of Functionality"	
FMT_LIM.1	RP_SFR-MECH
FMT_LIM.2	RP_SFR-MECH
FAU_SAS.1	RP_SFR_SERV
From "Physical Manipulation and Probing"	
FDP_SDC.1	RP_SFR-MECH

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
FPT_ITT.1	RP_SFR-MECH
FDP_IFC.1	RP_SFR_SERV
From "Random Numbers"	
FCS_RNG.1/PTG.2	RP_SFR_SERV
From "Loader – Package 1"	
FMT_LIM.1/Loader	RP_SFR-MECH
FMT_LIM.2/Loader	RP_SFR-MECH
From "Authentication Proof of Identity"	
FIA_API.1	RP_SFR_SERV
From "Loader Package 2 Lite"	
FDP_UIT.1	RP_SFR_SERV
FDP_ACC.1/ Loader	RP_SFR_SERV
FDP_ACF.1/ Loader	RP_SFR_SERV
From "Trusted path"	
FTP_TRP.1	RP_SFR_SERV
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-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022 Revision 1
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional components, CCMB-2022-11-002, CC:2022 Revision 1
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance components, CCMB-2022-11-003, CC:2022 Revision 1
[CC-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-5]	Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, version CC:2022 Revision 1
[CC-Errata]	Common Criteria for Information Technology Security Evaluation Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)
[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
[11]	[GPCS] Global Platform Card Specification v2.3.1 (GPC_SPE_034), March 2018 – ref [11] in [PP/0100] 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) – ref [13] in [PP/0100]</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]
[JC]	Java Card Specification v3.1, April 2020
[JCAPI3]	Java Card 3 Platform - Java Card API, Classic Edition, Version 3.1, February 2021
[JCEM3]	Java Card 3 Platform - Virtual Machine Specification, Classic Edition, Version 3.1, February 2021
[JCRE3]	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]	Embedded UICC for Consumer and IoT Devices Protection Profile version 2.1, February 2025, (SGP.25 v2.1 by GSMA)
[PP-JCS]	Java Card System – Open Configuration Protection Profile version 3.1, April 2020, BSI-CC-PP-0099-V2-2020 – ref [01] in [PP/0100]
[PP-GP]	Secure Element Protection Profile version 1.0, February 2021, GPC_SPE_174
[SGP.02]	Remote Provisioning Architecture for Embedded UICC Technical Specification version 4.3, January 2023 – ref [03] in [PP/0100]
[SGP.06]	eUICC Security Assurance Principles, version 2.3, May 2025
[SGP.07]	eUICC Security Assurance Methodology, version 2.3, May 2025
[SGP.22]	RSP Technical Specification Version 2.6, 20 September 2024
[SGP.31]	eSIM IoT Architecture and Requirement Specification, version 1.2, April 2024
[SGP.32]	eSIM IoT Technical Specification, version 1.2, June 2024
[SGP.33]	eSIM IoT Test Specification, version 1.2, January 2025
[SGP.24]	SGP.24 Compliance Process, Version 2.6, January 2025
[ST/IC]	Security Target Lite for ORION (ORION_ST_Security_Target_Lite_v1.53 – April 19,2024)

Reference	Title
[GUIDES/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_v029</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>
[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
[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
[GUIDES]	<p>List of documents applicable to the certified product:</p> <ul style="list-style-type: none"> <li>• Guidance for Secure application development on Thales MultiSIM IoT Products (D1624503 v1.2)</li> <li>• Operational guidance of MSM IOT 9.3.1 V1.0 (D1645760 v1.2)</li> <li>• Preparative guidance of MSM IOT 9.3.1 V1.0 (D1645757 v1.2)</li> <li>• Platform Identification and Configuration for MSM IOT 9.3.1 V1.0 (D1626926 v1.10)</li> <li>• Patch Loading Management for Certified Secure Elements (D1344508 A04)</li> <li>• MSM IOT 9.3.1 V1.0 User's Guide (D1626925 v1.1)</li> <li>• IoT 9.3.1 APDU guide (D1649179A v1.0)</li> <li>• GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications (GPC_GUI_050, v2.0)</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 (Keysformatted 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.

Term	Definition
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**