Security Target Template for Consumer eUICC
Version 1.0
05 July 2023

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Scope

1.2 Definitions

Term	Description

1.3 Abbreviations

Term	Description
CC	Common Criteria
O.ENV	Objective for the environment
O.TOE	Objective for the TOE

1.4 References

Ref	DocNumber	Title	Version
[1]	[**CC-1**]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model	Version 3.1 Revision 5
[2]	[**CC-2**]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components	Version 3.1 Revision 5
[3]	[**CC-3**]	Common Criteria for Information Technology Security Evaluation Part Part 3: Security assurance components	Version 3.1 Revision 5
[4]	[**PP-eUICC**]	Embedded UICC for Consumer Devices Protection Profile	Version 1.0
[5]	[**PP-JCS**]	Java Card System – Open Configuration Protection Profile	Version 3.1
[6]	[**PP-GP**]	Global Platform – Secure Element Protection Profile	Version 1.0
[7]	[**JCRE3**]	Java Card Platform version 2.2.2, Runtime Environment Specification	March 2006
[8]	[**JCVM3**]	Java Card Platform - Classic Edition, Virtual Machine (Java Card VM) Specification.	Version 3.0 to 3.0.5
[9]	[**JCAPI3**]	Java Card Platform - Classic Edition, Application Programming Interface.	Versions 3.0 up to 3.0.5,
[10]	[**JCRE3**]	Java Card Platform - Classic Edition, Runtime Environment (Java Card RE) Specification.	Versions 3.0 up to 3.0.5,
[11]	[**JCRE**]	Java Card Platform- Runtime Environment Specification	Versions 2.2 through 3.1
[12]	[**JCAPI**]	Java Card Platform- Application Programming Interface	Versions 2.2 through 3.1
[13]	[**JCVM**]	Java Card Platform- Virtual Machine Specification	Versions 2.2 through 3.1

Ref	DocNumber	Title	Version
[14]	[**PP-84**]	Security IC Platform Protection Profile with Augmentation Packages	Version 1.0
[15]	[**PP-117**]	Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile	Version 1.5
[16]	[**GPCS**]	GlobalPlatform Technology Card Specification March 2018	Version 2.3.1
[17]	[**CC-1**]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model	Version 3.1 Revision 5

2 Security Target Introduction

[

Guideline to be deleted by ST writer

This paragraph provides guidelines on how to complete the different parts of the ST Template.

Each part where the Developer SHALL provide details is delimited by the following:

[To be defined by the ST writer]

Before completing the text, the Developer SHALL delete the text between square brackets (i.e. [this text to be deleted]) including the square brackets.

In this document, the “ST writer” is used to refer to the “Developer”.

]

[

Guideline to be deleted by ST writer

In this section, the ST writer will complete the table.

The ST writer is allowed to add additional information (ie. author, date, developer name, product name if different of the TOE, …) for the ST reader.

]

2.1 Security Target reference

Name	[ST name]
Version	[ST version]
Reference	[ST reference]

2.2 TOE reference

Name	[TOE name]
Version	[TOE version]
Reference	[TOE reference]

2.3 References

[

Guideline to be deleted by ST writer

In this section, the ST writer will complete/update references dedicated to the eUICC developed.

]

3 TOE overview

[

Guideline to be deleted by ST writer

In this section, the ST writer will complete the subsections dedicated to the eUICC developed from [PP-eUICC].

]

3.1 TOE description

3.2 TOE type and usage

3.3 TOE life cycle

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

Non-TOE is same than the ones mentioned in the [PP-EUICC].

NOTE: that RMI functions are supposed not to be implemented by the TOE. Additionally this ST template proposal only takes into account an eUICC architecture with LPAd.

3.4 TOE scope

3.4.1 Physical scope

[

Guideline to be deleted by ST writer

Here an example of the table completion for a discrete eUICC.

Category	Component	Version	Delivery form
HW	Chip name	AA	Diced wafer
FW	Crypto lib name	1.0	Binary in memory
SW	OS name	1.0	Binary in memory
DOC	Operative guidance	1.0	Pdf file
DOC	Preparative guidance	1.0	Pdf file
DOC	Security guidance	1.0	Pdf file

The ST writer is allowed to add additional information to support the understanding for the ST reader.

]

Category	Component	Version	Delivery form
HW	[name]	[version]	[form]
FW	[name]	[version]	[form]
SW	[name]	[version]	[form]
DOC	Operative guidance	[version]	[form]
DOC	Preparative guidance	[version]	[form]
DOC	Security guidance	[version]	[form]

3.4.2 Logical scope

[

Guideline to be deleted by ST writer

In this section, the ST writer will complete the logical scope of the TOE from the [PP-eUICC].

The ST writer is allowed to add additional information to support the understanding for the ST reader.

]

4 Conformance Claim

[

Guideline to be deleted by ST writer

In this section, no action of the ST writer is required cause it is already prefilled.

]

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

This Security Target conforms to CC version 3.1 release 5 [CC-1], [CC-2] and [CC-3].

This Security Target is CC Part 2 [CC-2] extended and CC Part 3 [CC-3] conformant of Common Criteria version 3.1, revision 5.

4.2 Assurance package

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

4.3 Protection Profile (PP) conformance claim

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

4.4 Conformance claim rationale

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

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

4.4.1 Conformity of the TOE Type

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

[

Guideline to be deleted by ST writer

The ST writer has to keep (between scenario 1 and 3) the scenario adapted to the developed eUICC and remove the non selected one.

]

[Case: Scenario 1] The TOE follows the first scenario from the definition in [PP-eUICC], with the IC, OS and JCS already certified, and the embedded eUICC certified on top of them. The ST refers to the IC, OS and JCS Security Target(s) to fulfil the corresponding security objectives.

[Case: Scenario 3] The TOE follows the third scenario from the definition in [PP-eUICC] when the embedded eUICC is embedded in a certified IC, but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs 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.

4.4.2 SPD Consistency

[

Guideline to be deleted by ST writer

In this section, no action of the ST writer is required cause the list is already prefilled. It is expected that additional assets, users, subjects, SFR, threats, OSPs, or assumptions will also be added by the ST writer.

]

4.4.2.1 Assets consistency

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

Assets	PP-eUICC	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_POLICY_RULES	X	(E)
D.PROFILE_USER_CODES	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)

D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(E)
D.APP_CODE		(A): Added from [PP-JCS].
D.APP_C_DATA		(A): Added from [PP-JCS].
D.APP_I_DATA		(A): Added from [PP-JCS].
D.APP_KEYs		(A): Added from [PP-JCS].
D.PIN		(A): Added from [PP-JCS].
D.API_DATA		(A): Added from [PP-JCS].
D.CRYPTO		(A): Added from [PP-JCS].
D.JCS_CODE		(A): Added from [PP-JCS].
D.JCS_DATA		(A): Added from [PP-JCS].
D.SEC_DATA		(A): Added from [PP-JCS].

Table 1 Assets Consistency table

4.4.2.2 Users and Subjects consistency

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

User	PP-eUICC	Security Target
U.SM-DPplus	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)

Table 2 User consistency table

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

Subjects	PP-eUICC	Security Target
S.ISD-R	X	(E)
S.ISD-P	X	(E)
S.ECASD	X	(E)
S.PPI	X	(E)
S.PPE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A): Added from [PP-JCS].
S.APPLET		(A): Added from [PP-JCS].
S.BCV		(A): Added from [PP-JCS].

S.CAD		(A): Added from [PP-JCS].
S.INSTALLER		(A): Added from [PP-JCS].
S.JCRE		(A): Added from [PP-JCS].
S.JCVM		(A): Added from [PP-JCS].
S.LOCAL		(A): Added from [PP-JCS].
S.MEMBER		(A): Added from [PP-JCS].
S.CAP_FILE		(A): Added from [PP-JCS].

Table 3 Subjects Consistency table

4.4.2.3 Threats consistency

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

Threats	PP-eUICC	Security Target
T.UNAUTHORIZED-PROFILE-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-PLATFORM-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-ELIGIBILITY	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-IDENTITY-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.IDENTITY-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-eUICC	X	(E)
T.LPAd-INTERFACE-EXPLOIT	X	(E)
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)
T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)

Table 4 Threats Consistency table

4.4.2.4 Organizational Security Policies consistency

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

OSPs	PP-eUICC	Security Target
OSP.LIFE-CYCLE	X	(E)

Table 5 Organizational Security Policies Consistency table

4.4.2.5 Assumptions consistency

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

Assumptions	PP-eUICC	Security Target
A.TRUSTED-PATHS-LPAd	X	(E)
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)

Table 6 Assumptions Consistency table

4.4.3 Security Objectives Consistency

[

Guideline to be deleted by ST writer

In this section, no action of the ST writer is required cause the list is already prefilled. It is expected that additional objectives will also be added by the ST writer.

The ST writer has to keep (between scenario 1 and 3) the scenario adapted to the eUICC developed and remove the non selected one.

]

4.4.3.1 Objective for the TOE consistency

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

[

Guideline to be deleted by ST writer

The ST writer has to keep (between scenario 1 and 3) the scenario adapted to the developed eUICC and remove the non selected one.

The current SFRs proposal include optional SFRs from [PP-GP] for assistance; but the ST writer can decide to use another selection of SFRs to cover the Security objectives of the TOE.

]

[Case: Scenario 1] Note that OE.RE* and OE.IC* from [PP-eUICC] become security objectives from the TOE in the present security target. However, a product certified against the [PP-JCS] already meets the security objectives OE.RE*.

[Case: Scenario 3] Note that OE.RE* and OE.IC* from [PP-eUICC] become security objectives from the TOE in the present security target. The [PP-eUICC] already provides the conversion of OE.RE* to objectives from the [PP-JCS] protection profile.

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

Table 7 Security objectives for the TOE consistency table

4.4.3.2 Objective for Environment consistency

O.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-DPplus	X	(E)
OE.MNO	X	(E)
OE.TRUSTED-PATHS-LPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.CODE-EVIDENCE		(A): Added from [PP-JCS].
OE.MNO-SD	X	(E)
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PPE-PPI	X	Removed and replaced by O.RE.PPE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.

OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE

Table 8 Security objectives for the Operational Environment consistency table

4.4.4 Conformity of the Requirement (SFR/SAR)

4.4.4.1 SFR consistency

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

FCS_RNG.1	X	(E)
FPT_EMS.1	X	(E)
FDP_SDI.1	X	(E)
FDP_RIP.1	X	(E)
FPT_FLS.1	X	(E)
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/PPR	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1	X	(E)
FMT_SMR.1	X	(E)
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.4/Mobile_network	X	(E)
FDP_ACC.2/FIREWALL		(A): Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A): Added from [PP-JCS].
FDP_IFC.1/JCVM		(A): Added from [PP-JCS].
FDP_IFF.1/JCVM		(A): Added from [PP-JCS].
FDP_RIP.1/OBJECTS		(A): Added from [PP-JCS].
FMT_MSA.1/JCRE		(A): Added from [PP-JCS].
FMT_MSA.1/JCVM		(A): Added from [PP-JCS].
FMT_MSA.2/FIREWALL_JCVM		(A): Added from [PP-JCS].
FMT_MSA.3/FIREWALL		(A): Added from [PP-JCS].
FMT_MSA.3/JCVM		(A): Added from [PP-JCS].
FMT_SMF.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FMT_SMR.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1		(A): Added from [PP-JCS].
FCS_CKM.4		(A): Added from [PP-JCS].
FCS_COP.1		(A): Added from [PP-JCS].
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		(A): Added from [PP-JCS].
FPT_TDC.1		(A): Added from [PP-JCS].
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ITC.2/Installer		(A): Added from [PP-JCS].
FMT_SMR.1/Installer		(A): Added from [PP-JCS].
FPT_FLS.1/Installer		(A): Added from [PP-JCS].
FPT_RCV.3/Installer		(A): Added from [PP-JCS].
FDP_ACC.2/ADEL		(A): Added from [PP-JCS].
FDP_ACF.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].
FMT_SMF.1/ADEL		(A): Added from [PP-JCS].
FMT_SMR.1/ADEL		(A): Added from [PP-JCS].
FPT_FLS.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/ODEL		(A): Added from [PP-JCS].
FCO_NRO.2/CM		(A): Added from [PP-JCS].
FDP_IFC.2/CM		(A): Added from [PP-JCS].
FDP_IFF.1/CM		(A): Added from [PP-JCS].
FDP_UIT.1/CM		(A): Added from [PP-JCS].
FIA_UID.1/CM		(A): Added from [PP-JCS].
FMT_MSA.1/CM		(A): Added from [PP-JCS].
FMT_MSA.3/CM		(A): Added from [PP-JCS].
FMT_SMF.1/CM		(A): Added from [PP-JCS].
FTP_ITC.1/CM		(A): Added from [PP-JCS].
FIA_AFL.1/GP		(A): Added from [PP-GP].

FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
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 9 Security Functional Requirement consistency table

4.4.4.2 SAR consistency

This ST claims the same evaluation assurance level as [PP-eUICC], i.e., EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

5 Security Problem definition

[

Guideline to be deleted by ST writer

In this section, no action of the ST writer is required. It is expected that additional assets, users, subjects, SFR, threats, OSPs, or assumptions will also be added by the ST writer.

]

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.

5.1 Assets

The definition of the assets from [PP-eUICC] and [PP-JCS] is not repeated here. See section 4.4.2.1 for complete list is assets.

5.2 Users and Subjects

The definition of users and subjects from [PP-eUICC] and [PP-JCS] is not repeated here. See section 4.4.2.2 for complete list is users and subjects.

5.3 Threats

The definition of threats from [PP-eUICC] where no refinements are made is not repeated here. See section 4.4.2.3 for complete list is threats.

Refined threats description are detailed below:

T.UNAUTHORIZED-PROFILE-MNG

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

Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.APP_C_DATA, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_CODE.

T.UNAUTHORIZED-PLATFORM-MNG

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

Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behaviour of ISD-R or PPE, the attacker indirectly threatens the provisioning

status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.

T.PROFILE-MNG-INTERCEPTION

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

Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*., D.APP_C_DATA, D.PIN and D.APP_KEYs.

T.PROFILE-MNG-ELIGIBILITY

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

Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, D.APP_C_DATA, D.PIN, D.APP_KEYs, D.APP_CODE and D.APP_I_DATA.

T.UNAUTHORIZED-IDENTITY-MNG

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

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

T.IDENTITY-INTERCEPTION

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

Directly threatens the assets: D.SECRETS, D.EID, D.APP_C_DATA, D.PIN and D.APP_KEYs.

T.LOGICAL-ATTACK

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

Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_POLICY_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, D.JCS_CODE, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_C_DATA.

5.4 Organizational Security Policies

The definition of organizational security policies from [PP-eUICC] and [PP-JCS] is not repeated here. See section 4.4.2.4 for complete list is organizational security policies.

6 Security Objectives

[

Guideline to be deleted by ST writer

In this section, no action of the ST writer is required. It is expected that additional objectives will also be added by the ST writer.

]

This section introduces the security objectives for the TOE.

6.1 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 4.4.3 for complete list is Security Objectives for the TOE.

Some objectives from the environment have been converted to objectives of the TOE, specifically the ones from [PP-eUICC] related to OE.RE* and OE.IC*. The replaced objectives from 4.4.3.2 and their description are listed next:

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

O.RE.PPE-PPI	The Runtime Environment shall provide secure means for card management activities, including: o load of a package file, o installation of a package file, o extradition of a package file or an application, o personalization of an application or a Security Domain, o deletion of a package file or an application, o privileges update of an application or a Security Domain, o o access to an application outside of its expected availability.
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.
O.RE.API	The Runtime Environment shall ensure that native code can be invoked only via an API.
O.RE.DATA-CONFIDENTIALITY	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
O.RE.IDENTITY	The Runtime Environment shall ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.

6.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 4.4.3.2 for complete list is Security Objectives for the Operational Environment.

6.3 Security Objectives Rationale

6.3.1 Threats

6.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

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

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

- OE.SM-DPplus and OE.MNO protect the corresponding credentials when used offcard. The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY). The authentication is supported by corresponding secure channels:
- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication with SM-DP+ and a secure channel for communication with MNO OTA Platform. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

Since the MNO-SD Security Domain is not part of the TOE, the operational environment has to guarantee that it will use securely the SCP80/81 secure channel provided by the TOE (OE.MNO-SD). In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required:

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

T.UNAUTHORIZED-PLATFORM-MNG

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

- O.PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.

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

In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required: o compliance to security guidelines for applications (OE.APPLICATIONS and OE.CODE-EVIDENCE).

T.PROFILE-MNG-INTERCEPTION

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

Consequently, the TSF ensures:

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

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

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

6.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

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

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

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

T.IDENTITY-INTERCEPTION

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

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

6.3.1.3 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).

6.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

OE.TRUSTED-PATHS-LPAd ensures that the interfaces ES10a, ES10b and ES10c are trusted paths to the LPAd.

6.3.1.5 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.

6.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

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

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

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

This threat is covered by prevention of unauthorized code execution by applications (O.RE.CODE-EXE),

The following objectives for the operational environment are also required:

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

T.PHYSICAL-ATTACK

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

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

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

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

6.3.2 Organizational Security Policies

The OSP defined is OSP.LIFE-CYCLE as in [PP-eUICC] section 4.3.2.

6.3.3 Assumptions

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

6.3.4 Rationale Tables

6.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZEDPROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DPplus, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Section 6.3.1.1
T.UNAUTHORIZEDPLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI,	Section 6.3.1.1

	OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	
T.PROFILE-MNG-INTERCEPTION	OE.SM-DPplus, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD	Section 6.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DPplus, OE.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 6.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 6.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 6.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 6.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	Section 6.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 6.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 6.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 6.3.1.6

Table 10 Threats and Security Objectives- Coverage

Security Objectives	Threats
O.PPE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY

O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DPplus	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
O.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.IC.RECOVERY	T.PHYSICAL-ATTACK
O.RE.PPE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK

OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION

Table 11 Security Objectives and threats

6.3.4.2 Organizational Security Policies Rationale

Organizational Security Policies	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PPE-PPI, OE.RE.PPE-PPI, O.OPERATE	Section 6.3.2

Table 12 Organizational Security Policies and Security Objectives- Coverage

Security Objectives	Organizational Security Policies
O.PPE-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-DPplus	
OE.MNO	
O.IC.PROOF_OF_IDENTITY	
O.IC.SUPPORT	
O.IC.RECOVERY	
O.RE.PPE-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	

OE.TRUSTED-PATHS-LPAd	
OE.APPLICATIONS	
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	
OE.SM-DS	

Table 13 Security Objectives and Organizational Security Policies

6.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd	OE.TRUSTED-PATHS-LPAd	Section 6.3.3
A.ACTORS	OE.CI, OE.SM-DPplus, OE.MNO	Section 6.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	Section 6.3.3

Table 14 Assumptions and Security Objectives for the Operational Environment-Coverage

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-DPplus	A.ACTORS
OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.MNO-SD	

Table 15 Assumptions and Security Objectives for the Operational Environment

7 Extended Components Definition

[

Guideline to be deleted by ST writer

In this section, no action of the ST writer is required. It is expected that additional extended components definition will also be added by the ST writer.

]

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

- Extended Family FIA_API - Authentication Proof of Identity
- Extended Family FPT_EMS - TOE Emanation
- Extended Family FCS_RNG – Random number generation
- Extended Family FAU_SAS – Audit Data Storage

The extended components definition (FIA_API, FPT_EMS, FCS_RNG) from [PP-eUICC] is not repeated here. The same for FAU_SAS.1 which definition from [PP-84] or [PP-117], section 5.3 have been taken with no modification.

8 Security Functional requirements

[

Guideline to be deleted by ST writer

The following subsections contains the list of applicable functional security requirements following [PP-eUICC].

Some requirements require the ST writer to complete the definition of the requirement by filling in the pending operations.

The requirements with pending operations are identified by:

- assignment: the ST writer should choose a specific operation which can be "*none*"
- selection: the ST writer must choose the applicable option from the ones listed and remove the others.

From Common Criteria, two additional operations can be defined:

- iterations: the ST writer must iterate a specific requirement when two different SFR implementations apply (e.g. FCS_COP.1/TDES and FCS_COP.1/AES).
- refinement: the ST writer can change the definition of a SFR to be more precise if it does not reduce the level of security required. In these cases, refinements must be marked with *italic font*.

For each requirement where an action is required, there is a specific Application Note that can be checked in [PP-eUICC] to support the understanding of the requirements. An example is provided for the first requirement.

The ST writer is allowed to additional Application Note after each SFR to support the understand of the SFR for the ST reader.

Application Notes should be identified as:

Application Note <number>: [text]

Details of the requirement are described in Application Note 24 from [PP-eUICC]. An example of how to fill the operation is shown below and marked with *italic font*:

FIA_UID.1.1/EXT The TSF shall allow

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

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

Application Note 1: The TOE does not allow additional operations than the ones defined by [PP-eUICC].

or

FIA_UID.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **[assignment: *requesting data that identifies the card or the Card Issuer*].**

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

]

8.1 eUICC Security Functional Requirements

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

8.1.1 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: list of additional TSF mediated actions].**

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

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

FIA_UAU.1/EXT Timing of authentication

FIA_UAU.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **user identification**
- **[assignment: list of additional TSF mediated actions]**

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

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

FIA_USB.1/EXT User-subject binding

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

FIA_UAU.4/EXT Single-use authentication mechanisms

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

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow

[assignment: list of TSF-mediated actions] on behalf of the user to be performed before the user is identified.

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

FIA_USB.1/MNO-SD User-subject binding

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

FIA_ATD.1 User attribute definition

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

FIA_API.1 Authentication Proof of Identity

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

8.1.2 Communication

FDP_IFC.1/SCP Subset information flow control

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

FDP_IFF.1/SCP Simple security attributes

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

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

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

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

FDP_IFF.1.3/SCP The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.4/SCP The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

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

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

FTP_ITC.1/SCP Inter-TSF trusted channel

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

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

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

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: additional importation control rules].

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

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

FDP_UCT.1/SCP Basic data exchange confidentiality

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

FDP_UIT.1/SCP Data exchange integrity

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

FCS_CKM.1/SCP-SM Cryptographic key generation

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

FCS_CKM.2/SCP-MNO Cryptographic key distribution

FCS_CKM.2.1/SCP-MNO The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: cryptographic key distribution method] that meets the following: [assignment: list of standards].

FCS_CKM.4/SCP-SM Cryptographic key destruction

FCS_CKM.4.1/SCP-SM The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

FCS_CKM.4/SCP-MNO Cryptographic key destruction

FCS_CKM.4.1/SCP-MNO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

8.1.3 Security Domains

FDP_ACC.1/ISDR Subset access control

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

FDP_ACF.1/ISDR Security attribute based access control

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

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

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

- **Enabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "DISABLED" and**
  - **the currently enabled S.ISD-P's PPR data allows its disabling.**
- **Disabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "ENABLED" and**
  - **the corresponding S.ISD-P's PPR data allows its disabling.**
- **Deleting a S.ISD-P is authorized only if**

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

FDP_ACF.1.3/ISDR The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects].

FDP_ACF.1.4/ISDR The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects].

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,**
1. **objects: S.ECASD,**
2. **operations:**
    - **execution of a ECASD function**
    - **access to output data of these functions,**
- **[assignment: additional list of subjects, objects, and operations between subjects and objects covered by the SFP].**

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"**
3. **objects: 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 CI public key (PK.CI.ECDSA)**
        - **Creation of an eUICC signature on material provided by an ISD-R.**
    - **access to output data of these functions**.
- **[assignment: additional list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].**

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

- **Authorized users: only S.ISD-R, identified by its AID, shall be authorized to execute the following S.ECASD functions:**

- **Verification of a certificate CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DP.TLS, CERT.DSauth.ECDSA, or CERT.DS.TLS, provided by an ISD-R, with the CI public key (PK.CI.ECDSA)**
- **Creation of an eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R**.

○ **[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects].**

FDP_ACF.1.3/ECASD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4/ECASD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

8.1.4 Platform Services

FDP_IFC.1/Platform_services Subset information flow control

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

FDP_IFF.1/Platform_services Simple security attributes

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

users/subjects:

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

information:

○ **D.PROFILE_NAA_PARAMS**

○ **D.PROFILE_POLICY_RULES**

○ **D.PLATFORM_RAT**

operations:

○ **installation of a profile**

○ **PPR and RAT enforcement**

○ **network authentication.**

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

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

FDP_IFF.1.3/Platform_services The TSF shall enforce the [assignment: additional information flow control SFP rules].

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows].

FDP_IFF.1.5/Platform_services The TSF shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows].

FPT_FLS.1/Platform_services Failure with preservation of secure state

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

- **failure that lead to a potential security violation during the processing of a S.PPE, S.PPI or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **PPR and RAT enforcement**
  - **Network authentication**
- **[assignment: other type of failure]**.

8.1.5 Security management

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a [selection: deterministic, hybrid deterministic, physical, hybrid physical] random number generator [selection: DRG.2, DRG.3, DRG.4, PTG.2, PTG.3] that implements: [assignment: list of security capabilities of the selected RNG class].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric of the selected RNG class].

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to

- **D.SECRETS;**
- **D.SK.EUICC.ECDSA**

and **the secret keys which are part of the following keysets:**

- **D.MNO_KEYS,**
- **D.PROFILE_NAA_PARAMS.**

FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to

- **D.SECRETS;**
- **D.SK.EUICC.ECDSA**

and **the secret keys which are part of the following keysets:**

- **D.MNO_KEYS,**
- **D.PROFILE_NAA_PARAMS.**

FDP_SDI.1 Stored data integrity monitoring

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

FDP_RIP.1 Subset residual information protection

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

FPT_FLS.1 Failure with preservation of secure state

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

FMT_MSA.1/PLATFORM_DATA Management of security attributes

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

FMT_MSA.1/PPR Management of security attributes

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

FMT_MSA.1/CERT_KEYS Management of security attributes

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

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: list of management functions to be provided by the TSF].

FMT_SMR.1 Security roles

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

FMT_MSA.1/RAT Management of security attributes

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

FMT_MSA.3 Static attribute initialisation

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

8.1.6 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, Tuak, [selection: other algorithm, no other algorithm]** 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.**

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: cryptographic key distribution method] that meets the following: [assignment: list of standards].

FCS_CKM.4/Mobile_network Cryptographic key destruction

FCS_CKM.4.1/Mobile_network The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: cryptographic key destruction method] that meets the following: [assignment: list of standards].

8.2 Runtime Environment Security Requirements

The Subjects (prefixed with an "S"), the Objects (prefixed with an "O"), Information (prefixed with an "I") are defined and described in [PP-JCS] section 7.1. Security attributes linked to these subjects, objects and information are also defined in [PP-JCS] section 7.1. Finally, Operations (prefixed with "OP") definition and description are present in [PP-JCS] section 7.1.

8.2.1 CoreLG Security Functional requirements

8.2.1.1 Firewall Policy

FDP_ACC.2/FIREWALL Complete access control

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

FDP_ACF.1/FIREWALL Security attribute based access control

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

FDP_IFC.1/JCVM Subset information flow control

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

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes
S.JCVM	Currently Active Context

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

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

FDP_IFF.1.3/JCVM The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/JCVM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly deny information flows]**.

FDP_RIP.1/OBJECTS Subset residual information protection

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

FMT_MSA.1/JCRE Management of security attributes

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

FMT_MSA.1/JCVM Management of security attributes

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

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

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

FMT_MSA.3/FIREWALL Static attribute initialisation

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

FMT_MSA.3/JCVM Static attribute initialisation

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

FMT_SMF.1/JC Specification of Management Functions

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

FMT_SMR.1/JC Security roles

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

8.2.1.2 Application Programming Interface

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

FCS_COP.1 Cryptographic operation

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

FDP_RIP.1/ABORT Subset residual information protection

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

FDP_RIP.1/APDU Subset residual information protection

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

FDP_RIP.1/bArray Subset residual information protection

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

FDP_RIP.1/GlobalArray Subset residual information protection

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

FDP_RIP.1/KEYS Subset residual information protection

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

FDP_RIP.1/TRANSIENT Subset residual information protection

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

FDP_ROL.1/FIREWALL Basic rollback

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

8.2.1.3 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: list of other actions]** 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: list of other runtime errors].**

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 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: user data attributes]**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **[assignment: action to be taken]**.

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **[assignment: list of users and/or subjects]** are unable to observe the operation **[assignment: list of operations]** on **[assignment: list of objects]** by **[assignment: list of protected users and/or subjects]**.

FPT_FLS.1 Failure with preservation of secure state

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

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use

- **the rules defined in [JCVM3] specification,**
- **the API tokens defined in the export files of reference implementation,**
- **[assignment: list of interpretation rules to be applied by the TSF]** when interpreting the TSF data from another trusted IT product.

8.2.1.4 AID Management

FIA_ATD.1/AID User attribute definition

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

FIA_UID.2/AID User identification before any action

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

FIA_USB.1/AID User-subject binding

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

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: rules for the initial association of attributes]**.

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: rules for the changing of attributes]**.

FMT_MTD.1/JCRE Management of TSF data

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

FMT_MTD.3/JCRE Secure TSF data

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

8.2.2 INSTG Security Functional requirements

This group consists of the SFRs related to the installation of the applets, which addresses security aspects outside the runtime. The installation of applets is a critical phase, which lies partially out of the boundaries of the firewall, and therefore requires specific treatment. In this PP, loading a package or installing an applet modeled as importation of user data (that is, user application's data) with its security attributes (such as the parameters of the applet used in the firewall rules).

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

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

FMT_SMR.1/Installer Security roles

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

FPT_FLS.1/Installer Failure with preservation of secure state

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

FPT_RCV.3/Installer Automated recovery without undue loss

FPT_RCV.3.1/Installer When automated recovery from **[assignment: list of failures/service discontinuities]** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/Installer For **[assignment: list of failures/service discontinuities]**, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

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

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

8.2.3 ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

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

FDP_ACF.1/ADEL Security attribute based access control

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

FDP_RIP.1/ADEL Subset residual information protection

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

FMT_MSA.1/ADEL Management of security attributes

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

FMT_MSA.3/ADEL Static attribute initialisation

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

FMT_SMF.1/ADEL Specification of Management Functions

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

FMT_SMR.1/ADEL Security roles

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

FPT_FLS.1/ADEL Failure with preservation of secure state

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

8.2.4 RMIG Security Functional Requirements

It is assumed the product does not support RMI features. If the product was supporting RMI functionality, the ST writer should include the SFRs from [PP-JCS].

8.2.5 ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

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

FPT_FLS.1/ODEL Failure with preservation of secure state

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

8.2.6 CARG Security Functional Requirements

FCO_NRO.2/CM Enforced proof of origin

FCO_NRO.2.1/CM The TSF shall enforce the generation of evidence of origin for transmitted **application packages** at all times.

FCO_NRO.2.2/CM [Editorially Refined] The TSF shall be able to relate the **identity** of the originator of the information, and the **application package contained in** the information to which the evidence applies.

FCO_NRO.2.3/CM The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given **[assignment: limitations on the evidence of origin]**.

FDP_IFC.2/CM Complete information flow control

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

FDP_IFF.1/CM Simple security attributes

FDP_IFF.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** based on the following types of subject and information security attributes: **[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]**.

FDP_IFF.1.2/CM The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment: the rules describing the communication protocol used by the CAD and the card for transmitting a new package]**.

FDP_IFF.1.3/CM The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/CM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

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

FDP_UIT.1/CM Data exchange integrity

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

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

FIA_UID.1/CM Timing of identification

FIA_UID.1.1/CM The TSF shall allow **[assignment: list of TSF-mediated actions]** on behalf of the user to be performed before the user is identified.

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

FMT_MSA.1/CM Management of security attributes

FMT_MSA.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to restrict the ability to **[selection: change_default, query, modify, delete, [assignment: other operations]]** the security attributes **[assignment: list of security attributes]** to **[assignment: the authorised identified roles]**.

FMT_MSA.3/CM Static attribute initialisation

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

FMT_SMF.1/CM Specification of Management Functions

FMT_SMF.1.1/CM The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF]**.

FMT_SMR.1/CM Security roles

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

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

FTP_ITC.1/CM Inter-TSF trusted channel

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

8.2.7 Card Content Management Security Functional requirements

[

Guideline to be deleted by ST writer

The ST writer can decide to use another selection of these SFRs to cover the Security objectives of the TOE.

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]** unsuccessful authentication attempts occur related to **the authentication of the origin of a card management operation command**.

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

FIA_UAU.1/GP Timing of authentication

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

FDP_UIT.1/GP Basic data exchange integrity

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

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

FDP_UCT.1/GP Basic data exchange confidentiality

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

8.2.8 Underlying platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide the test process before TOE Delivery with the capability to store **[selection: the Initialisation Data, Pre-personalisation Data, [assignment: other data]]** in the **[assignment: type of persistent memory]**.

FPT_RCV.3/OS Automated recovery without undue loss

FPT_RCV.3.1/OS When automated recovery from **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 **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

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

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

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

Application Note: there is no maintenance mode implemented within the TOE. Recovery is always enforced automatically as stated in FPT_RCV.3.2/OS.

FPT_RCV.4/OS Function recovery

FPT_RCV.4.1/OS The TSF shall ensure that **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.

8.3 Security Functional Requirements Rationale

8.3.1 SFRs for eUICC rationale

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

8.3.2 SFRs for Runtime Environment rationale

[

Guideline to be deleted by ST writer

The security functional requirements rationale for objectives O.RE* can be extracted from [PP-JCS] 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 should be extracted from [PP-GP].

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

	O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT
O.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE

Table 16 Runtime environment objectives conversion for SFR rationale.

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

8.3.3 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.

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

9 TOE Summary Specification

[

Guideline to be deleted by ST writer

In this section, the ST writer will map SFR defined in previous section into TOE features and provide rationale of how SFR are covered in the TOE. The TOE features are the high-level architecture definition of the eUICC product as described in TOE overview (TOE description and/or TOE logical scope).

This template has prefilled the list of SFR into tables however, it is expected that additional SFR added by the ST writer will also be added into this section (i.e., SFR that has been iterated for example FCS_COP.1 or FCS_CKM.1)

]

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

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

9.1 eUICC security functions

9.2 Runtime Environment security functions

9.3 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.

9.3.1 eUICC SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	
FIA_UAU.1/EXT	
FIA_USB.1/EXT	
FIA_UAU.4/EXT	
FIA_UID.1/MNO-SD	
FIA_USB.1/MNO-SD	
FIA_ATD.1	
FIA_API.1.1	
FDP_IFC.1/SCP	
FDP_IFF.1/SCP	
FTP_ITC.1/SCP	

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ITC.2/SCP	
FPT_TDC.1/SCP	
FDP_UCT.1/SCP	
FDP_UIT.1/SCP	
FCS_CKM.1/SCP-SM	
FCS_CKM.2/SCP-MNO	
FCS_CKM.4/SCP-SM	
FCS_CKM.4/SCP-MNO	
FDP_ACC.1/ISDR	
FDP_ACF.1/ISDR	
FDP_ACC.1/ECASD	
FDP_ACF.1/ECASD	
FDP_IFC.1/Platform_services	
FDP_IFF.1/Platform_services	
FPT_FLS.1/Platform_services	
FCS_RNG.1	
FPT_EMS.1	
FDP_SDI.1	
FDP_RIP.1	
FPT_FLS.1	
FMT_MSA.1/PLATFORM_DATA	
FMT_MSA.1/PPR	
FMT_MSA.1/CERT_KEYS	
FMT_SMF.1	
FMT_SMR.1	
FMT_MSA.1/RAT	
FMT_MSA.3	
FCS_COP.1/Mobile_network	
FCS_CKM.2/Mobile_network	
FCS_CKM.4/Mobile_network	

9.3.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	
FDP_ACF.1/FIREWALL	

FDP_IFC.1/JCVM	
FDP_IFF.1/JCVM	
FDP_RIP.1/OBJECTS	
FMT_MSA.1/JCRE	
FMT_MSA.1/JCVM	
FMT_MSA.2/FIREWALL_JCVM	
FMT_MSA.3/FIREWALL	
FMT_MSA.3/JCVM	
FMT_SMF.1/JC	
FMT_SMR.1/JC	
FCS_CKM.1	
FCS_CKM.4	
FCS_COP.1	
FDP_RIP.1/ABORT	
FDP_RIP.1/APDU	
FDP_RIP.1/bArray	
FDP_RIP.1/GlobalArray	
FDP_RIP.1/KEYS	
FDP_RIP.1/TRANSIENT	
FDP_ROL.1/FIREWALL	
FAU_ARP.1	
FDP_SDI.2/DATA	
FPR_UNO.1	
FPT_FLS.1	
FPT_TDC.1	
FIA_ATD.1/AID	
FIA_UID.2/AID	
FIA_USB.1/AID	
FMT_MTD.1/JCRE	
FMT_MTD.3/JCRE	
FDP_ITC.2/Installer	
FMT_SMR.1/Installer	
FPT_FLS.1/Installer	
FPT_RCV.3.1/Installer	
FDP_ACC.2/ADEL	
FDP_ACF.1/ADEL	

FDP_RIP.1/ADEL	
FMT_MSA.1/ADEL	
FMT_MSA.3/ADEL	
FMT_SMF.1/ADEL	
FMT_SMR.1/ADEL	
FPT_FLS.1/ADEL	
FDP_RIP.1/ODEL	
FPT_FLS.1/ODEL	
FCO_NRO.2/CM	
FDP_IFC.2/CM	
FDP_IFF.1/CM	
FDP_UIT.1/CM	
FIA_UID.1/CM	
FMT_MSA.1/CM	
FMT_MSA.3/CM	
FMT_SMF.1/CM	
FTP_ITC.1/CM	
FIA_AFL.1/GP	
FIA_UAU.1/GP	
FIA_UAU.4/GP	
FDP_UIT.1/GP	
FDP_UCT.1/GP	
FAU_SAS.1	
FPT_RCV.3/OS	
FPT_RCV.4/OS	

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
SGP.17-1 V1.0	05 July 2023	CR0001R02 - GSMA eSA ST template for Consumer eUICC CR0002R00 - GSMA eSA ST template for Consumer eUICC CR0004R00 - ST template contains a few minor errors	ISAG	Gloria Trujillo, GSMA

B.2 Other Information

Type	Description
Document Owner	eSIMG
Editor / Company	Gloria Trujillo, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsm.org

Your comments or suggestions & questions are always welcome.