

Security Target Template for Consumer eUICC

Version 1.0

05 July 2023

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2023 GSM Association

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

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 4](#_Toc133402596)

[1.1 Scope 4](#_Toc133402597)

[1.2 Definitions 4](#_Toc133402598)

[1.3 Abbreviations 4](#_Toc133402599)

[1.4 References 4](#_Toc133402600)

[2 Security Target Introduction 5](#_Toc133402601)

[2.1 Security Target reference 6](#_Toc133402602)

[2.2 TOE reference 6](#_Toc133402603)

[2.3 References 6](#_Toc133402604)

[3 TOE overview 6](#_Toc133402605)

[3.1 TOE description 6](#_Toc133402606)

[3.2 TOE type and usage 6](#_Toc133402607)

[3.3 TOE life cycle 6](#_Toc133402608)

[3.3.1 Non-TOE HW/SW/FW available to the TOE 6](#_Toc133402609)

[3.4 TOE scope 7](#_Toc133402610)

[3.4.1 Physical scope 7](#_Toc133402611)

[3.4.2 Logical scope 7](#_Toc133402612)

[4 Conformance Claim 8](#_Toc133402613)

[4.1 Common Criteria version and conformance with CC part 2 and 3 8](#_Toc133402614)

[4.2 Assurance package 8](#_Toc133402615)

[4.3 Protection Profile (PP) conformance claim 8](#_Toc133402616)

[4.4 Conformance claim rationale 8](#_Toc133402617)

[4.4.1 Conformity of the TOE Type 8](#_Toc133402618)

[4.4.2 SPD Consistency 9](#_Toc133402619)

[4.4.3 Security Objectives Consistency 12](#_Toc133402620)

[4.4.4 Conformity of the Requirement (SFR/SAR) 14](#_Toc133402621)

[5 Security Problem definition 18](#_Toc133402622)

[5.1 Assets 18](#_Toc133402623)

[5.2 Users and Subjects 18](#_Toc133402624)

[5.3 Threats 18](#_Toc133402625)

[5.4 Organizational Security Policies 20](#_Toc133402626)

[6 Security Objectives 21](#_Toc133402627)

[6.1 Security Objectives for the TOE 21](#_Toc133402628)

[6.2 Security Objectives for the Operational Environment 22](#_Toc133402629)

[6.3 Security Objectives Rationale 22](#_Toc133402630)

[6.3.1 Threats 22](#_Toc133402631)

[6.3.2 Organizational Security Policies 26](#_Toc133402632)

[6.3.3 Assumptions 26](#_Toc133402633)

[6.3.4 Rationale Tables 26](#_Toc133402634)

[7 Extended Components Definition 31](#_Toc133402635)

[8 Security Functional requirements 32](#_Toc133402636)

[8.1 eUICC Security Functional Requirements 33](#_Toc133402637)

[8.1.1 Identification and authentication 33](#_Toc133402638)

[8.1.2 Communication 34](#_Toc133402639)

[8.1.3 Security Domains 37](#_Toc133402640)

[8.1.4 Platform Services 39](#_Toc133402641)

[8.1.5 Security management 40](#_Toc133402642)

[8.1.6 Mobile Network authentication 42](#_Toc133402643)

[8.2 Runtime Environment Security Requirements 43](#_Toc133402644)

[8.2.1 CoreLG Security Functional requirements 43](#_Toc133402645)

[8.2.2 INSTG Security Functional requirements 48](#_Toc133402646)

[8.2.3 ADELG Security Functional Requirements 49](#_Toc133402647)

[8.2.4 RMIG Security Functional Requirements 50](#_Toc133402648)

[8.2.5 ODELG Security Functional Requirements 50](#_Toc133402649)

[8.2.6 CARG Security Functional Requirements 51](#_Toc133402650)

[8.2.7 Card Content Management Security Functional requirements 54](#_Toc133402651)

[8.2.8 Underlying platform IC Security Functional Requirements 55](#_Toc133402652)

[8.3 Security Functional Requirements Rationale 56](#_Toc133402653)

[8.3.1 SFRs for eUICC rationale 56](#_Toc133402654)

[8.3.2 SFRs for Runtime Environment rationale 56](#_Toc133402655)

[8.3.3 SFRs for Underlying platform IC rationale 57](#_Toc133402656)

[9 TOE Summary Specification 58](#_Toc133402657)

[9.1 eUICC security functions 58](#_Toc133402658)

[9.2 Runtime Environment security functions 58](#_Toc133402659)

[9.3 TSS Rationale 58](#_Toc133402660)

[9.3.1 eUICC SFRs coverage 58](#_Toc133402661)

[9.3.2 Runtime Environment SFRs coverage 59](#_Toc133402662)

[Annex B Document Management 62](#_Toc133402663)

[B.1 Document History 62](#_Toc133402664)

[B.2 Other Information 62](#_Toc133402665)

# Introduction

## Scope

## Definitions

| Term  | Description |
| --- | --- |
|  |  |

## Abbreviations

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

## 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 |
| 1.
 | [**CC-2**] | Common Criteria for Information Technology Security Evaluation Part 2: Security functional components | Version 3.1 Revision 5 |
|  | [**CC-3**] | Common Criteria for Information Technology Security Evaluation Part Part 3: Security assurance components | Version 3.1 Revision 5 |
|  | [**PP-eUICC**] | Embedded UICC for Consumer Devices Protection Profile  | Version 1.0 |
|  | [**PP-JCS**] | Java Card System – Open Configuration Protection Profile  | Version 3.1 |
|  | [**PP-GP**] | Global Platform – Secure Element Protection Profile | Version 1.0 |
|  | [**JCRE3**] | Java Card Platform version 2.2.2, Runtime Environment Specification | March 2006 |
|  | [**JCVM3**] | Java Card Platform - Classic Edition, Virtual Machine (Java Card VM) Specification.  | Version 3.0 to 3.0.5 |
|  | [**JCAPI3**] | Java Card Platform - Classic Edition, Application Programming Interface. | Versions 3.0 up to 3.0.5, |
|  | [**JCRE3**] | Java Card Platform - Classic Edition, Runtime Environment (Java Card RE) Specification.  | Versions 3.0 up to 3.0.5, |
|  | [**JCRE**] | Java Card Platform- Runtime Environment Specification | Versions 2.2 through 3.1  |
|  | [**JCAPI**] | Java Card Platform- Application Programming Interface  | Versions 2.2 through 3.1  |
|  | [**JCVM**] | Java Card Platform- Virtual Machine Specification  | Versions 2.2 through 3.1 |
|  | [**PP-84**] | Security IC Platform Protection Profile with Augmentation Packages | Version 1.0 |
|  | [**PP-117**] | Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile | Version 1.5 |
|  | [**GPCS**] | GlobalPlatform Technology Card Specification March 2018  | Version 2.3.1 |
|  | [**CC-1**] | Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model | Version 3.1 Revision 5 |

# 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.

]

## Security Target reference

|  |  |
| --- | --- |
| **Name** | [ST name] |
| **Version** | [ST version] |
| **Reference** | [ST reference] |

## TOE reference

|  |  |
| --- | --- |
| **Name** | [TOE name] |
| **Version** | [TOE version] |
| **Reference** | [TOE reference] |

## References

[

Guideline to be deleted by ST writer

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

]

# 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].

]

## TOE description

## TOE type and usage

## TOE life cycle

### 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.

## TOE scope

### 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] |

### 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.

]

#  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.

]

## 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.

## Assurance package

This Security target conforms to the assurance package EAL4 augmented with ALC\_DVS.2 and AVA\_VAN.5.

## Protection Profile (PP) conformance claim

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

## 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].

### 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.

### 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.

]

####  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]. |

1. Assets Consistency table

#### 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) |

1. 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]. |

1. Subjects Consistency table

#### 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) |

1. Threats Consistency table

#### 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) |

1. Organizational Security Policies Consistency table

#### 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) |

1. Assumptions Consistency table

### 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.

]

#### 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) |

1. Security objectives for the TOE consistency table

#### 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 |

1. Security objectives for the Operational Environment consistency table

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

#### 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. |

1. Security Functional Requirement consistency table

#### 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.

# 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.

## 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.

## 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.

## 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.

## 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.

# 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.

## 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: * load of a package file, o installation of a package file,
* extradition of a package file or an application,
* personalization of an application or a Security Domain,
* deletion of a package file or an application,
* privileges update of an application or a Security Domain,
* 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. |

## 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.

## Security Objectives Rationale

### Threats

#### 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.

#### 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.

#### 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).

#### LPAd impersonation

**T.LPAd-INTERFACE-EXPLOIT**

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

#### 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.

#### 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).

### Organizational Security Policies

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

### Assumptions

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

### Rationale Tables

#### 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,OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY | Section 6.3.1.1 |
| 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 |

1. 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  |

1. Security Objectives and threats

#### 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 |

1. 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  |  |

1. Security Objectives and Organizational Security Policies

#### 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 |

1. 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  |  |

1. Assumptions and Security Objectives for the Operational Environment

# 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.

# 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.

]

## eUICC Security Functional Requirements

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

### 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.

### 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].

### 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”**
1. **objects:** **S.ECASD**
2. **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*].

### 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]**.

### 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.

### 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].

## 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.

### CoreLG Security Functional requirements

#### 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.

#### 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.

#### 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.

#### 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.

### 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.

### 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.

### 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].

### 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.

### 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.

### 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.

### 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.

## Security Functional Requirements Rationale

### SFRs for eUICC rationale

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

### 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 |

1. 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.

### 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.

# 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.

## eUICC security functions

## Runtime Environment security functions

## 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.

### 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** |  |
| **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** |  |

### 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** |  |

1. Document Management
	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 eUICCCR0002R00 - GSMA eSA ST template for Consumer eUICCCR0004R00 - ST template contains a few minor errors | ISAG | Gloria Trujillo, GSMA |

* 1. 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.