EPT 3355U
Security Target

Version 1.3

May 2026

Eastcompeace Technology Co., Ltd.

Document History

Version	Date	Comment	Author
V0.0.1	2025-09-25	Initial version	wangnannan
V0.0.2	2025-11-19	Addressed actionitems after review	He Haorun
V0.0.3	2025-12-15	Modification	He Haorun
V0.0.4	2026-01-30	Modification	He Haorun
V0.0.5	2026-03-10	Modification	He Haorun
V0.0.6	2026-04-07	Modification	He Haorun
V1.0	2026-04-20	Modification	He Haorun
V1.1	2026-04-28	Update version	He Haorun
V1.2	2026-05-09	Modification	He Haorun
V1.3	2026-05-28	Modification	He Haorun

Table of Contents

1 Security Target Introduction 5
1.1 Security Target reference 5
1.2 TOE reference 5
1.3 References 5
2 TOE overview 7
2.1 TOE description 7
2.2 TOE type and usage 8
2.3 TOE life cycle 8
2.4 Non-TOE HW/SW/FW available to the TOE 10
2.5 TOE scope 11
2.5.1 Physical scope 11
2.5.2 Logical scope 11
3 Conformance Claim 12
3.1 Common Criteria version and conformance 12
3.2 Assurance package 12
3.3 Protection Profile (PP) conformance claim 12
3.4 Conformance claim rationale 12
3.4.1 Conformity of the TOE Type 12
3.4.2 SPD Consistency 12
3.4.3 Security Objectives Consistency 15
3.4.4 Conformity of the Requirement (SFR/SAR) 16
4 Security Problem definition 19
4.1 Assets 19
4.2 Users and Subjects 19
4.3 Threats 19
4.4 Organizational Security Policies 20
4.5 Assumptions 20
5 Security Objectives 21
5.1 Security Objectives for the TOE 21
5.2 Security Objectives for the Operational Environment 21
5.3 Security Objectives Rationale 22
5.3.1 Threats 22
5.3.2 Organizational Security Policies 24
5.3.3 Assumptions 24
5.3.4 Rationale Tables 25
6 Extended Components Definition 28
7 Security Functional requirements 29
7.1 eUICC Security Functional Requirements 29
7.1.1 Operation identification method 29
7.1.2 Identification and authentication 29
7.1.3 Communication 31
7.1.4 Security Domains 35

7.1.5 Platform Services 36
7.1.6 Security management 37
7.1.7 Mobile Network authentication 41
7.2 Runtime Environment Security Requirements 41
7.2.1 CoreLG Security Functional requirements 41
7.2.2 INSTG Security Functional requirements 44
7.2.3 ADELG Security Functional Requirements 45
7.2.4 RMIG Security Functional Requirements 45
7.2.5 ODELG Security Functional Requirements 45
7.2.6 CARG Security Functional Requirements 46
7.2.7 Card Content Management Security Functional requirements 47
7.2.8 Underlying platform IC Security Functional Requirements 48
7.3 Security Assurance Requirements Rationale 48
7.3.1 SAR – Evaluation Assurance Level Rationale 48
7.3.2 SAR – Dependency rationale 48
7.4 Security Functional Requirements Rationale 49
7.4.1 SFRs for eUICC rationale 49
7.4.2 SFRs for Runtime Environment rationale 49
7.4.3 SFRs for Underlying Platform IC rationale 50
7.4.4 SFR dependency rationale 50
8 TOE Summary Specification 54
8.1 eUICC security functions 54
8.2 Runtime Environment security functions 55
8.3 TSS Rationale 56
8.3.1 eUICC SFRs coverage 56
8.3.2 Runtime Environment SFRs coverage 56
9 Statement of Compatibility 57
9.1 Statement of compatibility – ASE_SPD 57
9.2 Statement of compatibility – ASE_OBJ 58
9.3 Statement of compatibility – ASE_REQ 58

1 Security Target Introduction

1.1 Security Target reference

Name	EPT 3355U Security Target
Version	V1.3
Reference	EPT_3355U_ST_1.3

1.2 TOE reference

Name	EPT 3355U
Version	V1.0
Reference	EPT_3355U_1.0

1.3 References

ID	Reference	Title	Version
[1]	[**CC-1**]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model	2022r1
[2]	[**CC-2**]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components	2022r1
[3]	[**CC-3**]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components	2022r1
[4]	[**CC-5**]	Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements	2022r1
[5]	[**CC-Errata**]	Errata and Interpretation for CC:2022(Release 1) and CEM:2022(Release 1)	V1.2
[6]	[**PP-eUICC**]	eUICC for Consumer and IoT Devices Protection Profile	V2.1
[7]	[**PP-JCS**]	Java Card System – Open Configuration Protection Profile	v3.2
[8]	[**PP-GP**]	Global Platform – Secure Element Protection Profile	v1.0
[9]	[**JCVM3**]	Java Card Platform - Classic Edition, Virtual Machine (Java Card VM) Specification.	v3.0.4
[10]	[**JCAPI3**]	Java Card Platform - Classic Edition, Application Programming Interface.	v3.0.4
[11]	[**JCRE3**]	Java Card Platform - Classic Edition, Runtime Environment (Java Card RE) Specification.	v3.0.4
[12]	[**PP-84**]	Security IC Platform Protection Profile with Augmentation Packages	v1.0
[13]	[**GPCS**]	GlobalPlatform Technology Card Specification March 2018	v2.3.1
[14]	[**GP Amd B**]	GlobalPlatform technology. Remote Application Management over HTTP, Card specification v2.3 – Amendment B	V2.3
[15]	**[GPC-Gui]**	GlobalPlatform Card Composition Model Security Guidelines for Basic Applications. GPC_GUI_050.	v2.0
[16]	**[AIS31]**	Functionality classes and evaluation methodology for physical random number generators AIS31	v3.0
[17]	**[MILENAGE]**	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 18): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; • Document 1: General; • Document 2: Algorithm Specification; • Document 3: Implementers Test Data; • Document 4: Design Conformance Test Data; • Document 5: Summary and results of design and evaluation.	Rel. 18
[18]	**[TUAK]**	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, "Specification of the	Rel. 18

ID	Reference	Title	Version
		TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; • Document 1: Algorithm specification; • Document 2: Implementers' test data; • Document 3: Design conformance test data.	
[19]	**[SGP21]**	Remote SIM Provisioning (RSP) Architecture,	V2.5
[20]	**[SGP22]**	Remote SIM Provisioning (RSP) Technical Specification	V2.5
[21]	**[ST-IC]**	Security target lite of HED Secure Chip CIU98M50 V1.0 with IC Dedicated Software V1.1, V1.1	V1.1
[22]	**[SGP31]**	eSIM IoT Architecture and Requirements	V1.2
[23]	**[SGP32]**	GSMA SGP.32–eSIMIoT Technical Specification	V1.2
[24]	**[CC-4]**	Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities	2022r1
[25]	**[CIC]**	Common Implementation Configuration v2.1, July 2018 Ref: GPC_GUI_080.	V2.1
[26]	**[FIPS PUB 186-4]**	Digital Signature Standard (DSS) FIPS PUB 186-4	July 2013
[27]	**[FIPS197]**	Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology, November 26, 2001.	November 26, 2001.
[28]	**[FIPS 198]**	National Institute of Standards and Technology (2008) The Keyed-Hash Message Authentication Code (HMAC). (U.S. Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication	(FIPS) 198-1, July 2008.
[29]	**[NIST 880-67]**	Barker EB, Mouha N (2017) Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. (National Institute of Standards and Technology, Gaithersburg, Maryland), NIST Special Publication (SP)	800-67, Rev. 2, November 2017.
[30]	**[NIST 800 38A]**	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication	May 2005
[31]	**[SP800-38b]**	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005.	May 2005
[32]	**[NIST 800-108]**	Recommendation for Key Derivation Using Pseudorandom Functions (Revised)	October 2009.
[33]	**[TS 102 225]**	Smartcards; Secured packet structure for UICC based applications.	V12.1.0
[34]	**[TS 102 226]**	Smart Cards; Remote APDU structure for UICC based applications	V13.0.0
[35]	**[ISO 10118-3]**	IT Security techniques – Hash-functions Part 3: Dedicated hash-functions	Edition 4, 2018
[36]	**[SGP22 V3.1]**	Remote SIM Provisioning (RSP) Technical Specification	V3.1

2 TOE overview

This section presents the architecture and common usages of the Target of Evaluation (TOE).

The TOE is an eUICC open platform with multi-application support, such as Java Card, Global Platform, that implements:

- GSMA RSP Architecture Specification [SGP21] and Technical Specification [SGP22] for Consumer Devices(MEP functionality is implemented based on [SGP22 V3.1]) and
- GSMA eSIM IoT Architecture and Requirements [SGP31] and eSIM IoT Technical Specification [SGP32] for IoT Devices.

2.1 TOE description

The TOE is a eUICC and it follows an architecture as depicted below:

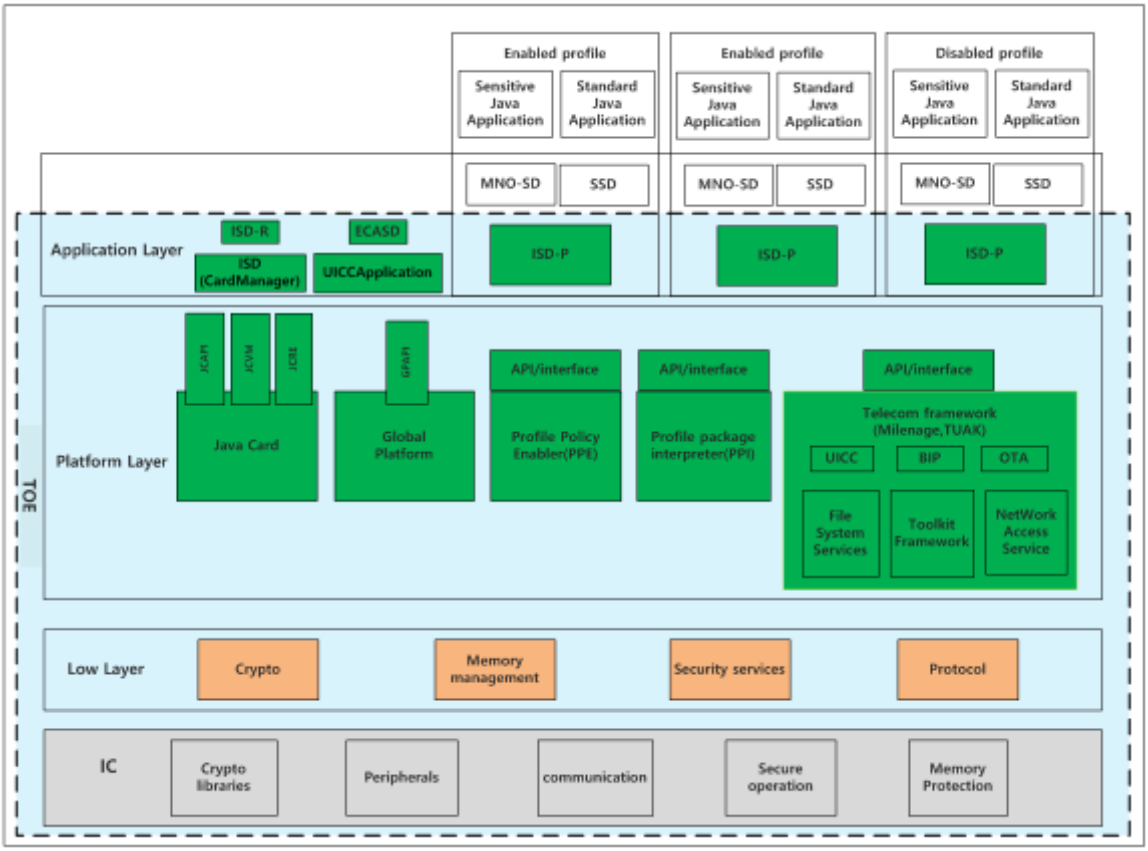

Figure 1TOE Architecture

The TOE includes:

- The Application Layer: privileged applications, such as Security Domains, providing the remote provisioning and administration functionality (the notion of Security Domain follows the definition given by [GPCS]):
  - An ISD-R, including LPA/IPA Services, providing life-cycle management of profiles.
  - An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication.
  - An ISD-P security domain, each one hosting a unique profile. MEP (Multiple Enabled Profile) functionality is supported by the TOE, which enables the simultaneous activation of 2 ISD-Ps. MEP functionality is implemented based on [SGP22 V3.1].

  - An ISD Issuer Security Domain, providing card content management
  - A UICCApplication, providing UICC command management, file system management and UICC net authentication.

  The ISD and UICCApplication have no impact on the overall security.

- The Platform Layer: a set of functions providing support to the Application Layer:
  - A Telecom Framework providing network authentication algorithms.
  - A Profile Package Interpreter translating Profile Package data into an installed Profile.
  - A Profile Policy Enabler, which comprises Profile Policy verification and enforcement, functions.
  - A runtime environment based on JavaCard.
- The Low Layer: a set of services to communicate with Hardware and cryptographic libraries.
- The secure IC and its embedded software.

The Profiles are not part of the TOE.

2.2 TOE type and usage

The TOE is an UICC embedded in a consumer or IoT device, and it could be removable once it is rolled out. The eUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile.

During pre-personalization the TOE is configured either for consumer or IoT device. This process is not reversible.

The eUICC will contain several MNO Profiles, each of them being associated with a given International Mobile Subscriber Identity (IMSI). The primary function of the Profile is to authenticate the validity of a Device when accessing the network. The Profile is MNO's property, and stores MNO specific information.

A eUICC with an enabled operational Profile provides the same functionality as a SIM or USIM card.

TOE major and security features are the ones described in section 1.2.1 of [PP-eUICC].

2.3 TOE life cycle

The TOE life cycle is based on a smartcard life cycle with differences in its post-issuance provisioning functionality.

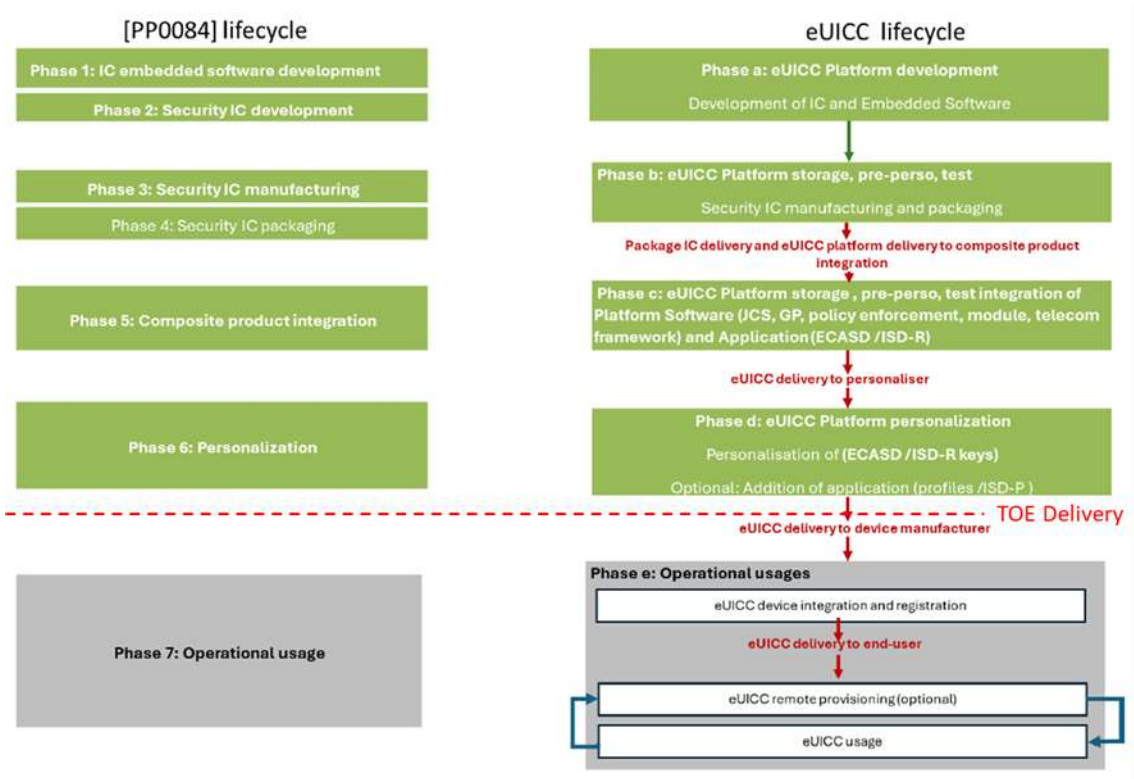

Figure 2TOE Life Cycle

The reader may refer to [PP-84] for a thorough description of Phases 1 to 7:

- **Phases 1 and 2** compose the product development: Embedded Software (IC Dedicated Software, OS, RE, applications, other Platform components such as PPI, PRE, and Applications) and IC development.
- **Phases 3 and 4** correspond to IC manufacturing and packaging, respectively. Some IC pre-personalization steps may occur in Phase 3.
- **Phase 5** concerns the embedding of software components within the IC.
- **Phase 6** is dedicated to the product personalization prior final use.
- **Phase 7** is the product operational phase.

The eUICC life cycle is composed of the following stages:

- **Phase a**: Development corresponds to the first two stages of the IC development.
- **Phase b**: Storage, pre-personalization and test cover the stages related to manufacturing and packaging of the IC.
- **Phase c**: eUICC platform storage, pre-personalization, test covers the stage of the embedding of software products onto the eUICC.
- **Phase d**: eUICC personalization covers the insertion of provisioning Profiles and Operational Profiles onto the eUICC.
    - TOE Delivery: At this phase the TOE is delivered to the customer of the eUICC manufacturer.
- **Phase e**: operational usage of the TOE covers the following steps:
    - eUICC integration onto the Device is performed by the Device Manufacturer. The Device Manufacturer and/or the eUICC Manufacturer also register the eUICC in a given SM-DS.

- The eUICC is then used to provide connectivity to the Device end-user. The eUICC may be provisioned again, at post-issuance, using the remote provisioning infrastructure.

For additional details refer to section 1.2.3 of [PP-eUICC].

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

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

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

In this TOE, LPAe/IPAe is not implemented and is therefore outside the scope of evaluation.

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

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

• The TOE is intended to be plugged in an IoT device or consumer is not part of the TOE, but it provides power and communication means to external world.

• The provisioning system and relevant network infrastructure are not part of TOE, but they interact with it to manage profile provisioning and administration. It includes at least remote servers of:

o SM-DP+, which provides Profile management commands and Profile,

o MNO OTA Platforms.

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

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

2.5 TOE scope

2.5.1 Physical scope

Category	Component	Version	Delivery form
Hardware	CIU98M50	V1.0	Module via certified delivery method under GSMA-CB-CH-25TRE00181-01
IC dedicated Software	CMS	V1.0	Binary file in memory
	Cryptographic and functional library	V1.1	Binary file in memory
	Lib file API library	V1.0	Binary file in memory
Software	JCES	V3.0	Binary file in memory
Document	EPT 3355U User Guidance	V1.2	PDF

2.5.2 Logical scope

TOE major and security features are the ones described in section 1.2.1 of [PP-eUICC]. Included features are as listed below:

- The Application Layer:
  - An ISD-R, including LPA/IPA Services, providing life-cycle management of profiles.
  - An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication.

    The ECASD is the representative of the off-card entity CI root. the ECASD has the following properties:
    a) There can only be one ECASD on an eUICC.
    b) It is installed and personalized by the EUM during the eUICC manufacturing.
    c) It has eUICC private key(s) for creating signatures.
    d) It has associated certificate(s) for eUICC authentication.
    e) It has the Certificate Issuers' (CI) root public key(s) for verifying SM-DP+ and SM-DS certificates.
    f) It has the certificate of the EUM.
    g) It MAY have the eIM public key(s) or certificate(s) for verifying eIM messages (SGP.32)
  - ISD-P security domains, each one hosting a unique profile. MEP (Multiple Enabled Profile) functionality is supported by the TOE, which enables the simultaneous activation of 2 ISD-Ps.
  - An ISD Issuer Security Domain, providing card content management
  - A UICCApplication, providing UICC command management, file system management and UICC net authentication.
- The Platform Layer
  - A Telecom Framework providing network authentication algorithms.
  - A Profile Package Interpreter translating Profile Package data into an installed Profile.
  - A Profile Policy Enabler which comprises Profile Policy verification and enforcement functions.
  - Java Card system; including the JCVM [JCVM3], JCAPI [JCAPI3] and JCRE [JCRE3].
  - GlobalPlatform system; including Card Content Management system [GPCS].
- The Low Layer:
  - including Cryptographic primitives, Memory management and Communication protocol management.

3 Conformance Claim

3.1 Common Criteria version and conformance

This Security Target conforms to Common Criteria 2022 release 1 [CC-1], [CC-2], [CC-3], [CC-4], [CC-5] and [CC-Errata].

This Security Target is CC Part 2 [CC-2] extended and CC Part 3 [CC-3] conformant of Common Criteria 2022 release 1.

3.2 Assurance package

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2, AVA_VAN.5 and the composite product package (COMP) defined in [CC-5].

ADV_ARC is refined to add a particular set of verifications on top of the existing requirement.

3.3 Protection Profile (PP) conformance claim

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

3.4 Conformance claim rationale

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

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

3.4.1 Conformity of the TOE Type

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

The TOE follows the third scenario from the definition in [PP-eUICC] when the embedded eUICC is embedded in a certified IC (**GSMA-CB-CH-25TRE00181-01** as described in [ST-IC]), but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs to meet the objectives for the OS and JCS.

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

3.4.2 SPD Consistency

3.4.2.1 Assets consistency

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

Assets	PP-eUICC	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_RULES	X	(E)
D.PROFILE_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.PK.EIM.ECDSA (SGP.32)	X	(E)
D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(R): Optional element not added in the current ST.
D.APP_CODE		(A): Added from [PP-JCS].
D.APP_C_DATA		(A): Added from [PP-JCS].
D.APP_I_DATA		(A): Added from [PP-JCS].
D.APP_KEYs		(A): Added from [PP-JCS].
D.PIN		(A): Added from [PP-JCS].
D.API_DATA		(A): Added from [PP-JCS].
D.CRYPTO		(A): Added from [PP-JCS].
D.JCS_CODE		(A): Added from [PP-JCS].
D.JCS_DATA		(A): Added from [PP-JCS].
D.SEC_DATA		(A): Added from [PP-JCS].

Table 1Assets Consistency table

3.4.2.2 Users and Subjects consistency

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

User	PP-eUICC	Security Target
U.SM-DPplus	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.EIM (SGP.32)	X	(E)
U.End-User (SGP.22)	X	(E)

Table 2User 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.PRE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A): Added from [PP-JCS].

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

Table 3Subjects Consistency table

3.4.2.3 Threats consistency

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

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

Table 4Threats Consistency table

3.4.2.4 Organizational Security Policies consistency

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

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

Table 5Organizational Security Policies Consistency table

3.4.2.5 Assumptions consistency

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

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

Table 6Assumptions Consistency table

3.4.3 Security Objectives Consistency

3.4.3.1 Objective for the TOE consistency

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

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

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

Table 7Security objectives for the TOE consistency table

The security objectives for the operational environment that are addressed by the underlying platform are translated into objectives for the TOE, as indicated in section 3.4.3.2.

3.4.3.2 Objective for Environment consistency

O.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.MNO	X	(E)
OE.EIM(SGP.32)	X	(E)
OE.TRUSTED-PATHS-LPAd-IPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.VERIFICATION		(A): Added from [PP-JCS].
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.PRE-PPI	X	Removed and replaced by O.RE.PRE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY

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

Table 8Security objectives for the Operational Environment consistency table

3.4.4 Conformity of the Requirement (SFR/SAR)

3.4.4.1 SFR consistency

SFR	PP-eUICC	Security Target
FIA_UID.1/EXT	X	(E)
FIA_UAU.1/EXT	X	(E)
FIA_USB.1/EXT	X	(E)
FIA_UAU.4/EXT	X	(E)
FIA_UID.1/MNO-SD	X	(E)
FIA_USB.1/MNO-SD	X	(E)
FIA_ATD.1/Base	X	(E)
FIA_API.1	X	(E)
FDP_IFC.1/SCP	X	(E)
FDP_IFF.1/SCP	X	(E)
FTP_ITC.1/SCP	X	(E)
FDP_ITC.2/SCP	X	(E)
FPT_TDC.1/SCP	X	(E)
FDP_UCT.1/SCP	X	(E)
FDP_UIT.1/SCP	X	(E)
FCS_CKM.1/SCP-SM	X	(E)
FCS_CKM.2/SCP-MNO	X	(E)
FCS_CKM.6/SCP-SM	X	(E)
FCS_CKM.6/SCP-MNO	X	(E)
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	(E)
FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
FCS_RNG.1	X	(E)
FPT_EMS.1/Base	X	(E)
FDP_SDI.1/Base	X	(E)
FDP_RIP.1/Base	X	(E)
FPT_FLS.1/Base	X	(E).
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/RULES	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1/Base	X	(E)
FMT_SMR.1/Base	X	(E)
FMT_MSA.1/RAT	X	(E)

FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.6/Mobile_network	X	(E)
FDP_ACC.2/FIREWALL		(A): Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A): Added from [PP-JCS].
FDP_IFC.1/JCVM		(A): Added from [PP-JCS].
FDP_IFF.1/JCVM		(A): Added from [PP-JCS].
FDP_RIP.1/OBJECTS		(A): Added from [PP-JCS].
FMT_MSA.1/JCRE		(A): Added from [PP-JCS].
FMT_MSA.1/JCVM		(A): Added from [PP-JCS].
FMT_MSA.2/FIREWALL_JCVM		(A): Added from [PP-JCS].
FMT_MSA.3/FIREWALL		(A): Added from [PP-JCS].
FMT_MSA.3/JCVM		(A): Added from [PP-JCS].
FMT_SMF.1/JC		(A): Added from [PP-JCS].
FMT_SMR.1/JC		(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_UIT.1/CM		(A): Added from [PP-JCS].
FIA_UID.1/GP		(A): Added from [PP-GP].
FTP_ITC.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
FCS_COP.1/GP-SCP		(A): Added from [PP-GP]
FDP_ROL.1/GP		(A): Added from [PP-GP]
FDP_ITC.2/GP-KL		(A): Added from [PP-GP]
FDP_IFC.2/GP-KL		(A): Added from [PP-GP]
FDP_IFF.1/GP-KL		(A): Added from [PP-GP]
FPR_UNO.1/GP		(A): Added from [PP-GP]
FPT_TDC.1/GP		(A): Added from [PP-GP]
FIA_AFL.1/GP		(A): Added from [PP-GP]
FMT_MSA.3/GP		(A): Added from [PP-GP]
FMT_MSA.1/GP		(A): Added from [PP-GP]
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP]
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP]
FMT_SMF.1/GP		(A): Added from [PP-GP].
FMT_SMR.1/GP		(A): Added from [PP-GP].

Table 9Security Functional Requirement consistency table

3.4.4.2 SAR consistency

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

4 Security Problem definition

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

4.1 Assets

The definition of the assets from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.1 for complete list is assets.

4.2 Users and Subjects

The definition of users and subjects from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.2 for complete list is users and subjects.

4.3 Threats

The definition of threats from [PP-eUICC] where no refinements are made is not repeated here. See section 3.4.2.3 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.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, and D.PLATFORM_RAT.By altering the behavior of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.

- **T.PROFILE-MNG-INTERCEPTION**
  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.APP_CODE,

D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA,D.PK.EIM.ECDSA (SGP.32).

- **T.IDENTITY-INTERCEPTION**
  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_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.

4.4 Organizational Security Policies

The definition of organizational security policies from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.4 for complete list is organizational security policies.

4.5 Assumptions

The definition of assumptions from [PP-eUICC] and [PP-JCS] is not repeated here. See section 3.4.2.5 for complete list is assumptions.

5 Security Objectives

This section introduces the security objectives for the TOE.

5.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 3.4.3 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 3.4.3.2 and their description are listed below:

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.PRE, S.PPI, and S.TELECOM). (3) It allows the S.PRE, S.PPI, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection). (4) It provides a means to perform memory operations atomically for S.PRE, 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.PRE-PPI	The Runtime Environment shall provide secure means for card management activities, including: ○ load of a package file, ○ installation of a package file, ○ extradition of a package file or an application, ○ personalization of an application or a Security Domain, ○ deletion of a package file or an application, ○ privileges update of an application or a Security Domain,
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication.
O.RE.API	The Runtime Environment shall ensure that native code can be invoked only via an API.
O.RE.DATA-CONFIDENTIALITY	The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes.
O.RE.DATA-INTEGRITY	The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.
O.RE.IDENTITY	The Runtime Environment shall ensure the secure identification of the applications it executes.
O.RE.CODE-EXE	The Runtime Environment shall prevent unauthorized code execution by applications.

Table 10 Security Objectives for the TOE

5.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the Operation Environment from [PP-eUICC] and [PP-JCS] are not repeated here. See section 3.4.3.2 for complete list is Security Objectives for the Operational Environment.

5.3 Security Objectives Rationale

5.3.1 Threats

5.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

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

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

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

The authentication is supported by corresponding secure channels:

- O.SECURE-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.PRE.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) by means of RPM requests from Profile owner to ISD-R (UpdateMetadataRequest), or by means of PSMO commands from eIM to ISD-R (SGP.32)..

Consequently, the TSF ensures:

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

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

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

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

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

5.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

- O.PRE.PPI and O.eUICC-DOMAIN-RIGHTS covers this threat by providing an access control policy for ECASD content and functionality.
- The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY).
- O.RE.IDENTITY ensures that at the Java Card level, the applications cannot impersonate other actors or modify their privileges.

T.IDENTITY-INTERCEPTION

- O.INTERNAL-SECURE-CHANNELS ensures the secure transmission of the shared secrets from the ECASD to ISD-R and ISD-P. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).
- OE.CI ensures that the CI root will manage securely its credentials off-card.

5.3.1.3 eUICC cloning

T.UNAUTHORIZED-eUICC

- O.PROOF_OF_IDENTITY guarantees that the off-card actor can be provided with a cryptographic proof of identity based on an EID.
- O.PROOF_OF_IDENTITY guarantees this EID uniqueness by basing it on the eUICC hardware identification (which is unique due to O.IC.PROOF_OF_IDENTITY).

5.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

- OE.TRUSTED-PATHS-LPAd ensures that the interfaces ES10a, b, c (SGP.22) are trusted paths to the LPAd/IPA.

5.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS

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

5.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

- by the APIs provided by the Runtime Environment (O.RE.API);

- by the APIs of the TSF (O.API); the APIs of Telecom Framework, 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 PRE, PPI and Telecom Framework (O.OPERATE), and
- PRE, PPI and Telecom Framework must protect the confidentiality and integrity of the sensitive data they process, while applications must use the protection mechanisms provided by the Runtime Environment (O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY).

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).

5.3.2 Organizational Security Policies

The OSP defined is OSP.LIFE-CYCLE as in [PP-eUICC] section 4.3.2 and OSP.VERIFICATION in [PP-JCS] section 6.3.2.

5.3.3 Assumptions

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

A.APPLICATIONS

This assumption is directly upheld by **OE.CODE-EVIDENCE** and **OE.APPLICATIONS**

A.VERIFICATION

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

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

5.3.4 Rationale Tables

5.3.4.1 Threats Rationale

Threats	Sec. Objectives	Rationale
T.UNAUTHORIZEDPROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO,O.PRE.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	Sec.5.3.1.1
T.UNAUTHORIZEDPLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE.PPI,OE.EIM (SGP.32) ,OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Sec. 5.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD,OE.EIM (SGP.32)	Sec. 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+, OE.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Sec. 5.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE.PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Sec. 5.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Sec. 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Sec. 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	Sec. 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Sec. 5.3.1.5
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	Sec. 5.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Sec. 5.3.1.6

Table 11Threats and Security Objectives-Coverage

Sec. Objectives	Threats
O.PRE.PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DP+	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.PRE-PPI	N/A
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.CODE-EVIDENCE	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION

Table 12 Security Objectives and threats

5.3.4.2 Organizational Security Policies Rationale

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

Table 13 Organizational Security Policies and Security Objectives- Coverage

Sec. Objectives	Organizational Security Policies
O.PRE.PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	N/A
O.SECURE-CHANNELS	N/A
O.INTERNAL-SECURE-CHANNELS	N/A
O.PROOF_OF_IDENTITY	N/A
O.OPERATE	OSP.LIFE-CYCLE
O.API	N/A
O.DATA-CONFIDENTIALITY	N/A
O.DATA-INTEGRITY	N/A
O.ALGORITHMS	N/A
OE.CI	N/A
OE.SM-DP+	N/A
OE.MNO	N/A
O.IC.PROOF_OF_IDENTITY	N/A
O.IC.SUPPORT	N/A
O.IC.RECOVERY	N/A

O.RE.PRE-PPI	OSP.LIFE-CYCLE
O.RE.SECURE-COMM	N/A
O.RE.API	N/A
O.RE.DATA-CONFIDENTIALITY	N/A
O.RE.DATA-INTEGRITY	N/A
O.RE.IDENTITY	N/A
O.RE.CODE-EXE	N/A
OE.TRUSTED-PATHS-LPAd	N/A
OE.APPLICATIONS	N/A
OE.CODE-EVIDENCE	N/A
OE.MNO-SD	N/A
OE.SM-DS	N/A

Table 14Security Objectives and Organizational Security Policies

5.3.4.3 Assumptions Rationale

Assumptions	Sec. Objectives for the OE	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd	Sec. 5.3.3
A.ACTORS	OE.CI, OE.SM-DP+, OE.MNO ,OE.EIM (SGP.32)	Sec. 5.3.3
A.APPLICATIONS	OE.APPLICATIONS,OE.CODE-EVIDENCE	Sec. 5.3.3
A.VERIFICATION	OE.VERIFICATION, OE.CODE-EVIDENCE	Sec. 5.3.3

Table 15Assumptions and Security Objectives for the Operational Environment- Coverage

Sec. Objectives for the OE	Assumptions
OE.CI	A.ACTORS
OE.SM-DP+	A.ACTORS
OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd-IPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.VERIFICATION	A.VERIFICATION
OE.CODE-EVIDENCE	A.APPLICATIONS , A.VERIFICATION
OE.MNO-SD	N/A

Table 16Assumptions and Security Objectives for the Operational Environment

6 Extended Components Definition

The extended component FAU_SAS.1 from [PP-84], section 5.3 has been taken with no modification.

7 Security Functional requirements

7.1 eUICC Security Functional Requirements

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

7.1.1 Operation identification method

All operations reproduced from [PP-eUICC], [PP-JCS] are marked using the same notation as in the source document. Operations defined by the ST author are indicated by identifying the operation type with bold text.

Example: **[Assignment: value]**

7.1.2 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: initializing a secure channel with the card].**

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: initializing a secure channel with the card]**

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

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

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

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

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

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

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

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

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

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow

[assignment:
- **application selection**
- **requesting data that identifies the eUICC]**

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/Base User attribute definition

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

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

FIA_API.1 Authentication Proof of Identity

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

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **[selection: 1]** 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**.

7.1.3 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 [Editorially Refined] The TSF shall enforce **[assignment: no additional information flow control SFP rules].**

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

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

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

FDP_IFF.1/GP-KL Simple security attributes

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

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

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, SCP03, SCP80, SCP81], each equipped with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**

- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the S.OPEN checks that the requesting S.SD has no restrictions for personalisation.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and prior to the command forwarding to the targeted Application or SD.**
- **[assignment: S.OPEN verifies that the targeted application implements a personalization interface].**

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

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

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

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

FDP_IFC.2/GP-KL Complete information flow control

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

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.

Refinement:

FTP_ITC.1.3/SCP The TSF shall **permit the SM-DP+ to open a SCP-SGP22 secure channel to [assignment: transmit the following operations:**

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

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

- **ES10a.GetEuiccConfiguredAddresses**
- **ES10a.SetDefaultDpAddress(SGP.22)**
- **ES10b.SetDefaultDpAddress(SGP.32)**
- **ES10b.PrepareDownload**
- **ES10b.LoadBoundProfilePackage**
- **ES10b.GetEUICCChallenge**
- **ES10b.GetEUICCInfo**
- **ES10b.ListNotification**
- **ES10b.RetrieveNotificationsList**

- **ES10b.RemoveNotificationFromList**
- **ES10b.AuthenticateServer**
- **ES10b.CancelSession**
- **ES10b.LoadEuiccPackage (SGP.32)**
- **ES10b.AddInitialEim (SGP.32)**
- **ES10b.GetCerts (SGP.32)**
- **ES10b.ImmediateEnable (SGP.32)**
- **ES10b.ProfileRollback (SGP.32)**
- **ES10b.ConfigureImmediateProfileEnabling (SGP.32)**
- **ES10b.GetEimConfigurationData (SGP.32)**
- **ES10b.GetProfilesInfo (SGP.32)**
- **ES10b.GetRAT**
- **ES10c.GetProfilesInfo(SGP.22)**
- **ES10c.EnableProfile(SGP.22)**
- **ES10c.DisableProfile (SGP.22)**
- **ES10c.DeleteProfile(SGP.22)**
- **ES10c.eUICCMemoryReset(SGP.22)**
- **ES10c.GetEID(SGP.22)**
- **ES10c.GetEID (SGP.32)**
- **ES10c.SetNickname(SGP.22)**

The TSF shall permit the remote OTA Platform to open a SCP80 or SCP81 secure channel to transmit the following operation: ES6.UpdateMetadata.].

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FPT_TDC.1.1/SCP The TSF shall provide the capability to consistently interpret

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

when shared between the TSF and another trusted IT product.

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

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

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

when shared between the TSF and another trusted IT product.

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

FDP_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

FCS_CKM.1.1/SCP-SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curves Key agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following:

[assignment: **ECKA using one of the following standards:**

- **NISTP-256 (FIPS PUB 186-5 Digital Signature Standard)**
- **brainpoolP 256r1 (BSITR-03111, Version2.10, RFC5639)**

FCS_CKM.2/SCP-MNO Cryptographic key distribution

FCS_CKM.2.1/SCP-MNO The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[assignment: distribution method from SGP22 (SCP03t)**] that meets the following: **[assignment: SGP.22]**.

FCS_CKM.6/SCP-SM Cryptographic key destruction

FCS_CKM.6.1/SCP-SM The TSF shall destroy **D.SECRETS, CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, CERT.DSauth.ECDSA, D.CERT.EUICC.ECDSA, D.SK.EUICC.ECDSA and D.PK.CI.ECDSA** when [selection: *no longer needed*].

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

FCS_CKM.6/SCP-MNO Cryptographic key destruction

FCS_CKM.6.1/SCP-MNO The TSF shall destroy **D.MNO_KEYS** when **[selection: no longer needed]**.

FCS_CKM.6.2/SCP-MNO The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-MNO in accordance with a specified cryptographic key destruction method **[assignment: overwrite the keys with zeros]**that meets the following: **[assignment:**

none].

7.1.4 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:**
  - **SO.ISD-P with security attributes "state" "PPR", and [Selection: no additional attributes].**
- **operations:**
  - **Create and configure profile**
  - **Store profile meta data**
  - **Enable profile**
  - **Disable profile**
  - **Delete profile**
  - **Perform a Memory reset.**

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

- **Enabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "DISABLED" and**
  - **in case a currently enabled S.ISD-P has to be disabled, the PPR data of this S.ISD-P allows its disabling, and**
  - **[Selection: no additional attributes].**
- **Disabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "ENABLED" and**
  - **the corresponding S.ISD-P's PPR data allows its disabling.**
- **Deleting a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is not in the state "ENABLED" and**
  - **the corresponding S.ISD-P's PPR data allows its deletion.**
- **Performing a S.ISD-P Memory reset is authorized regardless of the involved S.ISD-P's state or PPR attribute.**

FDP_ACF.1.3/ISDR The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[assignment:**

- **ES8+.ConfigureISDP (Create and configure profile)**
- **ES8+.StoreMetadata (Store profile metadata)**
- **ES10c.EnableProfile (Enable profile)**
- **ES10c.DisableProfile (Disable profile)**
- **ES10c.DeleteProfile (Delete profile)**
- **ES10c.eUICCMemoryReset (Perform a Memory reset)**

based on Profile "state" and profile policy rules "PPR"].

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

FDP_ACC.1/ECASD Subset access control

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

- **subjects: S.ISD-R, S.ECASD**

- **objects: data and attributes of ECASD,,**
- **operations:**
  - **execution of a ECASD function**
  - **access to output data of these functions,**
  - **[assignment: additional operations defined by the interfaces ES8+ (SM-DP+ – eUICC), and ES10a,b,c (LPA – eUICC)**
  - **creation of a eUICC signature on material provided by an ISD-R].**

FDP_ACF.1/ECASD Security attribute based access control

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

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

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

- **Authorized users: only S.ISD-R, identified by its AID, shall be authorized to execute the following S.ECASD functions:**
  - **Verification of a certificate CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, or CERT.DSauth. ECDSA provided by an ISD-R, with the eSIM CA public key (D.PK.CI.ECDSA),**
  - **Creation of a eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R.**
- **[assignment: Rules defined in GSMA SGP.22 Specification].**

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

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

FDP_ROL.1/GP Basic rollback

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

7.1.5 Platform Services

FDP_IFC.1/Platform_services Subset information flow control

FDP_IFC.1.1/Platform_services The TSF shall enforce the **Platform services information flow control SFP** on

- **users/subjects:**
  - **S.ISD-R, S.ISD-P,U.MNO-SD**
  - **Platform code (S.PRE, S.PPI, S.TELECOM)**
- **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_RULES**
  - **D.PLATFORM_RAT**
- **operations**:

- **installation of a profile**
- **PPR and RAT enforcement**
- **network authentication**.
- **[Selection: no additional attributes].**

FDP_IFF.1/Platform_services Simple security attributes

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

- **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"**
- **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_RULES**
  - **D.PLATFORM_RAT**
- **operations:**
  - **installation of a profile**
  - **PPR and RAT enforcement**
  - **network authentication.**
  - **[Selection: no additional operations].**

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

- **D.PROFILE_NAA_PARAMS shall be transmitted only:**
  - **by U.MNO-SD to S.TELECOM in order to execute the network authentication function**
  - **by S.ISD-R to S.PPI using the profile installation function**
- **D.PROFILE_RULES shall be transmitted only**
  - **by S.ISD-R to S.PRE in order to execute the PPR enforcement function**
  - **[Selection: no additional information flows].**
- **D.PLATFORM_RAT shall be transmitted only**
  - **by S.ISD-R to S.PRE in order to execute the RAT enforcement function.**

FDP_IFF.1.3/Platform_services [Editorially Refined] The TSF shall enforce **[assignment: no additional information flow control SFP rules].**

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

FDP_IFF.1.5/Platform_services The TSF shall explicitly deny an information flow based on the following rules: **[assignment: none].**

FPT_FLS.1/Platform_services Failure with preservation of secure state

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

- **failure that lead to a potential security violation during the processing of a S.PRE, S.PPI or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **PPR and RAT enforcement**
  - **Network authentication**
  - **[Selection: no additional functions].**
- **[assignment: none].**

7.1.6 Security management

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **[selection: physical]** random number generator **[selection: Class PTG.2 according to [AIS31]]** that implements: **[assignment:**

- **PTG.2.1: A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.**
- **PTG.2.2: If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.**
- **PTG.2.3: The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.**
- **PTG.2.4: The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.**
- **PTG.2.5: The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.]**

FCS_RNG.1.2 The TSF shall provide **[assignment: octets of bits]** that meet **[assignment:**

- **PTG.2.6: Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.**
- **PTG.2.7: The average Shannon entropy per internal random bit exceeds 0.997.].**

FPT_EMS.1/Base TOE Emanation

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

ID	Emission	Attack surface	TSF data	User data
1	**[assignment: variations in power consumption or timing during command execution]**	**Any**	**-**	**o D.SECRETS;** **o D.SK.EUICC.ECDSA** **and the secret keys which are part of the following keysets:** **o D.MNO_KEYS,** **o D.PROFILE_NAA_PARAMS.**

Table 1 FPT_EMS.1 factors

FDP_SDI.1/Base Stored data integrity monitoring

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

FDP_RIP.1/Base Subset residual information protection

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

FPT_FLS.1/Base 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/RULES Management of security attributes

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

- **D.PROFILE_RULES**

to

- **S.ISD-R for change default, via function "ES8+.ConfigureISDP"**
- **S.ISD-R for query**
- **S.ISD-P for modify, via function "ES6.UpdateMetadata"**
- **[selection:**
  - **S.ISD-R to delete, via function "ES10c.DeleteProfile"(SGP.22),**
  - **S.ISD-R to delete, via function "ESep.Delete"(SGP.32)**

  ]

FMT_MSA.1/CERT_KEYS Management of security attributes

FMT_MSA.1.1/CERT_KEYS The TSF shall enforce the **ECASD access control SFP** to restrict the ability to **query and delete** the security attributes

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

to

- **S.ISD-R for:**
  - **query D.PK.CI.ECDSA**
  - **delete D.MNO_KEYS, via function [selection: ES10c.DeleteProfile (SGP.22), ESep.Delete (SGP.32)]**

no actor for other operations

FMT_SMF.1/Base Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[assignment: Profile Management functions specified in GSMA SGP.22 and SGP.32]**.

FMT_SMR.1/Base Security roles

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

FMT_SMR.1/GP Security roles

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

FMT_SMF.1/GP Specification of Management Functions

The definition of this SFR is present in [PP-GP] 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.

FCS_COP.1/GP-SCP Cryptographic Operation

FCS_COP.1.1/GP-SCP The TSF shall perform **[assignment: list of cryptographic operations in table below]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm in table below]** and cryptographic key sizes **[assignment:**

cryptographic key sizes in table below] that meet the following: **[assignment: list of standards in table below]**.

SCP Protocol	Cryptographic Operation	Cryptographic Algorithm	Supported Key Size	Standards
SCP02	MAC Generation/ Verification	CBC MAC using TDES	112 bits	[FIPS 198]
SCP02	Symmetric Encryption/ Decryption	TDES in CBC mode	112 bits	[NIST 880-67] [NIST 800 38A]
SCP02	Key Derivation	HMAC-based KDF, CMAC-based KDF using TDES	112 bits	[NIST 800-108] [FIPS 198]
SCP03	Symmetric Encryption/Decryption	AES in CBC mode	128, 192, or 256 bits	[FIPS 197] [NIST 800 38A]
SCP03	MAC Generation/Verification	CMAC AES	128, 192, or 256 bits	[NIST 800 38B]
SCP03	Key Derivation	CMAC-based KDF using AES	128, 192, or 256 bits	[NIST 800 108] [NIST 800 38B]
SCP03	Hash Computing	SHA-256, SHA-384, SHA-512		[ISO 10118-3] [FIPS 180-4]
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 112 bits AES: 128, 192, or 256 bits	[TS 102 225] [TS 102 226]
SCP81	Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_AES_128_CBC_SHA256		[GP Amd B] section 3.3.2
SCP-SGP22	Secure communication channel with the SM-DP+ for mutual authentication	ECKA	NIST P-256, brainpoolP256r1	[SGP.22]
SCP-SGP22 (SCP03t)	Secure communication channel with the SM-DP+ for profile download	AES CMAC AES	AES: 128	[SGP.22]
SCP-SGP22	Secure mutual authentication with the SM-DP+ for PrepareDownload	ECDSA signature generation ECDSA signature verification	NIST P-256	[FIPS PUB 186-4]

FMT_MSA.3 Static attribute initialization

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

FMT_MSA.1/GP Static attribute initialization

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

FMT_MSA.3/GP Static attribute initialization

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

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

7.1.7 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, Tuak, [selection: none]** and cryptographic key sizes **according to the corresponding standard** that meet the following:

- **MILENAGE according to standard [MILENAGE] with the following restrictions:**
  - **Only use 128-bit AES as the kernel function. Do not support other choices.**
  - **Allow any value for the constant OP.**
  - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [MILENAGE].**
- **Tuak according to [TUAK] with the following restrictions:**
  - **Allow any value of TOP.**
  - **Allow multiple iterations of Keccak.**
  - **Support 256-bit K as well as 128-bit.**
  - **To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.**
- **[selection: no additional 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: distribution method from SGP22 (SCP03t)]** that meets the following: **[assignment: SGP.22].**

FCS_CKM.6/Mobile_network Cryptographic key destruction

FCS_CKM.6.1/ Mobile_network The TSF shall destroy **[assignment: MILENAGE keys, TUAK keys and [selection: no other keys of the cryptographic algorithm]]** when **[selection: no longer needed]**.

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

7.2 Runtime Environment Security Requirements

The Subjects (prefixed with an "S"), the Objects (prefixed with an "O"), Information (prefixed with an "I") are defined and described in [PP-JCS] section 7.1. 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.

7.2.1 CoreLG Security Functional requirements

7.2.1.1 Firewall Policy

FDP_ACC.2/FIREWALL Complete access control

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

FDP_ACF.1/FIREWALL Security attribute based access control

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

FDP_IFC.1/JCVM Subset information flow control

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

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes
S.JCVM	Currently Active Context

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

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

FDP_IFF.1.3/JCVM The TSF shall enforce the **[assignment: no additional information flow control SFP rules].**

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

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **[assignment: none].**

FDP_RIP.1/OBJECTS Subset residual information protection

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 initialization

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

FMT_MSA.3/JCVM Static attribute initialization

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] defined as FMT_SMF.1. Its formulation is unchanged within this ST.

FMT_SMR.1/JC Security roles

The definition of this SFR is present in [PP-JCS] defined as FMT_SMR.1. Its formulation is unchanged within this ST.

7.2.1.2 Application Programming Interface

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.

7.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take one of the following actions:

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

upon detection of a potential security violation.

Refinement:

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

- CAP file inconsistency,
- typing error in the operands of a bytecode,
- applet life cycle inconsistency,
- card tearing (unexpected removal of the Card out of the CAD) and power failure, abort of a transaction in an unexpected context, (see abortTransaction(), [JCAPI3] and ([JCRE3], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow
- **[assignment: none].**

FDP_SDI.2/DATA Stored data integrity monitoring and action

FDP_SDI.2.1/DATA The TSF shall monitor user data stored in containers controlled by the TSF for **[assignment: integrity errors]**on all objects, based on the following attributes:**[assignment: integrity protected data].**

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

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **[assignment: all users]** are unable to observe the operation **[assignment: all operations]** on **[assignment: D.APP_KEYs, D.PIN]** by**[assignment: another user].**

FPR_UNO.1/GP Unobservability

FPR_UNO.1.1/GP The TSF shall ensure that **SDs and Applications** are unable to observe the operation: **keys or data import (PUT KEY or STORE DATA), encryption, decryption,**

signature generation and verification, [assignment: none] on **keys and data** by **the OPEN or any other SD or Application**.

FPT_FLS.1 Failure with preservation of secure state

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

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use

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

when interpreting the TSF data from another trusted IT product.

7.2.1.4 AID Management

FIA_ATD.1/AID User attribute definition

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: Each uploaded package is associated with a unique Package AID].**

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: The initially assigned Package AID is unchangeable].**

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.

7.2.2 INSTG Security Functional requirements

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

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

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

FMT_SMR.1/Installer Security roles

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

FPT_FLS.1/Installer Failure with preservation of secure state

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

FPT_RCV.3/Installer Automated recovery without undue loss

FPT_RCV.3.1/Installer When automated recovery from**[assignment: 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/Installer For**[assignment: a failure during load/installation of a package/applet and deletion of a package/applet/object]**, 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: 0%]** 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.

7.2.3 ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

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 initialization

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.

7.2.4 RMIG Security Functional Requirements

The TOE does not support RMI features.

7.2.5 ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

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.

7.2.6 CARG Security Functional Requirements

FCO_NRO.2/CM Enforced proof of origin

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

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

Refinement:

FCO_NRO.2.3/CM The TSF shall provide a capability to verify the evidence of origin of information to **originator** given **[assignment: at the time the Executable load files are received as no evidence is kept on the card for future verification**].

FDP_IFC.2/GP-ELF Complete information flow control

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

FDP_IFF.1/GP-ELF Simple security attributes

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

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

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, SCP03, SCP80, SCP81], each with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **On receipt of INSTALL or LOAD commands, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **S.OPEN accepts an ELF only if its integrity and authenticity has been verified.**
- **[assignment: S.OPEN accepts an ELF only if its AID is not already registered by the TSF].**

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

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

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

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- **S.OPEN fails to verify the Card Life Cycle state**
- **S.OPEN fails to verify the SD privileges.**
- **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**

- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.SD fails to unwrap INSTALL or LOAD commands.**
- **[assignment: The ELF AID is already registered within the card].**

FDP_UIT.1/CM Data exchange integrity

Refinement:

FDP_UIT.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP to [selection: receive]** user data in a manner protected from **[selection: modification, deletion and 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/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **[assignment:**

- **application selection**
- **initializing a secure channel with the card**
- **requesting data that identifies the card or the Card Issuer]**

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

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

FTP_ITC.1/GP Inter-TSF trusted channel

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

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

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

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

7.2.7 Card Content Management Security Functional requirements

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: receive]** user data in a manner protected from **modification, deletion, insertion, replay** errors**.**

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

FDP_UCT.1/GP Basic data exchange confidentiality

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

7.2.8 Underlying platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide**[assignment: the test process before TOE Delivery]**with the capability to store **[assignment: the Initialization Data, Pre-personalization Data, Smartcard Embedded Software]** in the **[assignment: chip non-volatile memory].**

FPT_RCV.3/OS Automated recovery without undue loss

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

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

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

[assignment:

- **the contents of Java Card static fields, instance fields, and array positions that fall under the scope of an open transaction;**
- **the Java Card objects that were allocated into the scope of an open transaction;**
- **the contents of Java Card transient objects;**
- **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**[assignment: reading from and writing to static and objects' fields interrupted by power loss]**have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

7.3 Security Assurance Requirements Rationale

7.3.1 SAR – Evaluation Assurance Level Rationale

The security assurance requirements rationale is the same than the ones present in section 6.3.4 from [PP-eUICC].

7.3.2 SAR – Dependency rationale

SAR	CC dependencies	Satisfied dependencies

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

Table 17 SAR dependency mapping

The table here-above shows that all SAR dependencies are met.

7.4 Security Functional Requirements Rationale

7.4.1 SFRs for eUICC rationale

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

7.4.2 SFRs for Runtime Environment rationale

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 [PP-JCS] and [PP-GP]
O.RE.PRE-PPI	O.INSTALL, O.DELETION, O.LOAD, O.CARD-MANAGEMENT
O.RE.SECURE-COMM	O.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT,O.SID, O.OPERATE, O.FIREWALL, OE.VERIFICATION, 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, OE.VERIFICATION
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, OE.VERIFICATION
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE, OE.VERIFICATION
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT
O.RE.CODE-EXE	O.FIREWALL, O.NATIVE, OE.VERIFICATION

Table 18Runtime 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.

7.4.3 SFRs for Underlying Platform IC rationale

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

O.IC.RECOVERY coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for recovery operations as dealt with in FPT_RCV.3/OS and FPT_RCV.4/OS.

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.

7.4.4 SFR dependency rationale

SFR	CC dependencies	Satisfied dependencies
FIA_UID.1/EXT	No dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_UAU.4/EXT	No dependencies	
FIA_UID.1/MNO-SD	No dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1/Base	No dependencies	
FIA_API.1	No dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP FMT_MSA.3
FTP_ITC.1/SCP	No dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP FTP_ITC.1/SCP FPT_TDC.1/SCP
FPT_TDC.1/SCP	No dependencies	
FDP_UCT.1/SCP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/SCP FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_COP.1) , (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_CKM.6/SCP-SM FCS_RNG,1 FCS_COP.1/GP-SCP
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP FCS_CKM.6/SCP-

SFR	CC dependencies	Satisfied dependencies
	and (FCS_CKM.6)	MNO
FCS_CKM.6/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP FCS_CKM.1/SCP-SM
FCS_CKM.6/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP FCS_CKM.1/SCP-SM
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services FMT_MSA.3
FPT_FLS.1/Platform_Services	No dependencies	
FCS_RNG.1	No dependencies	
FPT_EMS.1/Base	No dependencies	
FDP_SDI.1/Base	No dependencies	
FDP_RIP.1/Base	No dependencies	
FPT_FLS.1/Base	No dependencies	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FMT_SMF.1/Base FMT_SMR.1/Base
FMT_MSA.1/PPR	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_IFC.1/SCP FMT_SMF.1/Base FMT_SMR.1/Base
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_IFC.1/SCP FDP_ACC.1/ECASD FMT_SMF.1/Base FMT_SMR.1/Base
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA FMT_MSA.1/PPR FMT_MSA.1/CERT_KEYS FMT_SMR.1/Base
FMT_SMF.1/Base	No dependencies	
FMT_SMR.1/Base	(FIA_UID.1)	FIA_UID.1/EXT FIA_UID.1/MNO-SD
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FDP_ITC.2/SCP FCS_CKM.6/Mobile_network
FCS_CKM.2/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.6)	FDP_ITC.2/SCP FCS_CKM.6/Mobile_network
FCS_CKM.6/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP
FDP_ITC.2/Installer	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1 FTP_ITC.1/GP
FPT_RCV.3/Installer	(AGD_OPE.1)	AGD_OPE.1
FMT_SMR.1/Installer	(FIA_UID.1)	FIA_UID.1/GP
FPT_FLS.1/Installer	No dependencies	
FPT_TDC.1	No dependencies	
FTP_ITC.1/GP	No dependencies	
FCO_NRO.2/CM	(FIA_UID.1)	FIA_UID.1/GP
FIA_UID.1/GP	No dependencies	
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FTP_ITC.1/GP
FDP_UIT.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FTP_ITC.1/GP
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FTP_ITC.1/GP
FPR_UNO.1	No dependencies	
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No dependencies	
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ECASD FMT_SMR.1/GP FMT_SMF.1/GP
FDP_ACC.2/FIREWALL	(FDP_ACF.1)	FDP_ACF.1/FIREWALL
FDP_ACF.1/FIREWALL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/FIREWALL FMT_MSA.3/FIREWALL
FDP_IFC.1/JCVM	(FDP_IFF.1)	FDP_IFF.1/JCVM
FDP_IFF.1/JCVM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/JCVM FMT_MSA.3/JCVM
FDP_RIP.1/OBJECTS	No dependencies	
FMT_MSA.1/JCRE	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FMT_SMR.1/JC

SFR	CC dependencies	Satisfied dependencies
		See rationale
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM FMT_SMF.1/JC FMT_SMR.1/JC
FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_SMR.1/JC
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_SMR.1/JC
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM FMT_SMR.1/JC
FMT_SMF.1/JC	No dependencies	
FMT_SMR.1/JC	(FIA_UID.1)	FIA_UID.2/AID
FDP_RIP.1/ABORT	No dependencies	
FDP_RIP.1/APDU	No dependencies	
FDP_RIP.1/GlobalArray	No dependencies	
FDP_RIP.1/bArray	No dependencies	
FDP_RIP.1/KEYS	No dependencies	
FDP_RIP.1/TRANSIENT	No dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAS.1)	**See rationale**
FDP_SDI.2/DATA	No dependencies	
FIA_ATD.1/AID	No dependencies	
FIA_UID.2/AID	No dependencies	
FIA_USB.1/AID	(FIA_ATD.1)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/JC FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL FMT_SMF.1/ADEL FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	**See rationale**
FPT_FLS.1/ADEL	No dependencies	
FDP_RIP.1/ODEL	No dependencies	
FPT_FLS.1/ODEL	No dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No dependencies	
FAU_SAS.1	No dependencies	
FMT_MSA.1/RULES	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FMT_SMR.1/Base FMT_SMF.1/Base
FCS_COP.1/GP-SCP	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FCS_CKM.6/SCP-SM FDP_ITC.2/SCP
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-KL
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL, FDP_TDC.1/GP, FTP_ITC.1/GP
FDP_IFC.2/GP-KL	(FDP_IFF.1)	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-KL and FMT_MSA.3/GP
FPR_UNO.1/GP	No dependencies	
FPT_TDC.1/GP	No dependencies	
FIA_AFL.1/GP	FIA_UAU.1	FIA_UAU.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FMT_MSA.1/GP	(FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control) FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_SMR.1/GP	FIA_UID.1	FIA_UID.1/GP
FMT_SMF.1/GP	No dependencies	
FDP_IFC.2/GP-ELF	FDP_IFF.1	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2/GP-ELF FMT_MSA.3/GP

Table 19SFR dependency mapping

Rationale for the exclusion of dependencies:

- The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is unsupported.
  - The dependency between FMT_MSA.1/JCRE and FMT_SMF.1 is not satisfied because no management functions are required for the Java Card RE.
- The dependency FIA_UID.1 of FMT_SMR.1/ADEL is unsupported
  - This ST does not require the identification of the “deletion manager” since it can be considered as part of the TSF.
- The dependency FAU_SAA.1 of FAU_ARP.1 is unsupported.

  The dependency of FAU_ARP.1 on FAU_SAA.1 assumes that a "potential security violation" generates an audit event. On the contrary, the events listed in FAU_ARP.1 are self-contained (arithmetic exception, ill-formed bytecodes, access failure) and ask for a straightforward reaction of the TSFs on their occurrence at runtime. The JCVM or other components of the TOE detect these events during their usual working order. Thus, there is no mandatory audit recording in this ST.

8 TOE Summary Specification

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.

8.1 eUICC security functions

Security Functions (SF)	Description
SF.EUICC.CRYPTO	The TOE implements RSP features as described in SGP.22. Part of the features is to support additional crypto algorithms, which are part of the services provided by the Java Card system. The algorithms in scope are: • TUAK • MILENAGE
SF.EUICC.PROFILEMANAGEMENT	The TOE implements RSP features as described in SGP.22. This implementation is an extension from the features implemented according [GPCS] and grouped in **SF.GP.CM**. Extended features provide support for Profile management: • Profile downloading • Profile elements installation • Profile deletion • Profile management (enable/disable) • MEP feature The **SF.GP.CM** enforces the use of secure channel protocols to provide authentication and integrity and confidentiality features for data being transmitted.
SF.EUICC.SD	The TOE implements RSP features as described in SGP.22.This security function provides secure domain installation, distribution and management for the TOE. It includes the following security domains: • ISD-R • ECASD • ISD-P The ISD-R is responsible for the creation of new ISD-Ps. The ECASD is used for secure storage of credentials required to support the required Security Domains on the eUICC. The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile.
SF.EUICC.SCP	The TOE implements RSP features as described in SGP.22. Part of these features is support for additional secure protocol channels which are part of the services provided by the TOE. The SCP in scope are: • ES6 • ES8+ • ES10a • ES10b • ES10c

Table 20 eUICC security functions

8.2 Runtime Environment security functions

Security Functions (SF)	Description
SF.JC.FW	The TOE is based on a Java Card system as defined in [JCRE3]. Java Card provides isolation of user spaces by means of a firewall.
SF.JC.RIP	The TOE is based on a Java Card system as defined in [JCAPI3], [JCRE3] and [JCVM3]. The Java Card system provides a number features of to guarantee information from different sources made unavailable after destruction. A list of type of data and feature is listed below: • Objects: Garbage Collector • Transient data: Logical channels • Persistent data: Transaction mechanism • Packages/CAP files: Card Manager • Keys: Cryptographic containers
SF.JC.CRYPTO	The TOE is based on a Java Card system as defined in [JCAPI3]. And it provides a number of API which links to cryptographic support (key management, cryptographic operations, etc.) and PIN features. The cryptographic algorithms in scope are only the ones supporting SF.GP.SCP and SF.EUICC.SCP.
SF.JC.ROLLBACK	The TOE is based on a Java Card system as defined in [JCRE3]. Java Card provides features to provide atomic operation in the context of a transaction. For these operations, recovery of data is warrantied with rollback and roll forward operations.
SF.JC.APDU	The TOE is based on a Java Card system as defined in [JCAPI3]. This security function provides a standardized format for data exchange between Java Card and external terminals, enabling data transmission within security boundaries.
SF.JC.EXCEPTION	The TOE is based on a Java Card system as defined in [JCRE3].It implements full-lifecycle management of exception through the Java Card Runtime Environment.
SF.GP.CM	The TOE implements GlobalPlatform as defined in [GPCS]. The implementation include an application that provides functionalities to manage Java Card applets, including: • Packages/CAP downloading • Packages/CAP elements installation • Packages/CAP deletion The card manager enforces the use of secure channel protocols to provide authentication and integrity and confidentiality features for data being transmitted. Additionally, specific roles are considered in the form of ISD and SSD.

SF.GP.SCP	The TOE implements GlobalPlatform as defined in [GPCS]. The card manager enforces the use of secure channel protocols to provide authentication and integrity and confidentiality features for data being transmitted.
	The SCP in scope are:
	• SCP02
	• SCP03
	• SCP03t
	• SCP80
	• SCP81
	  • TLS_PSK_WITH_AES_128_CBC_SHA256
	  • TLS_PSK_WITH_NULL_SHA
	  • TLS_PSK_WITH_3DES_EDE_CBC_SHA
	  • TLS_PSK_WITH_AES_128_CBC_SHA
	  • TLS_PSK_WITH_NULL_SHA256

Table 21Runtime Environment security functions

8.3 TSS Rationale

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

8.3.1 eUICC SFRs coverage

Security Functions (SF)	SFR Mapping Rationale
SF.EUICC.CRYPTO	FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network and FCS_CKM.6/Mobile_network
SF.EUICC.PROFILEMANAGEMENT	FMT_SMF.1/Base , FPT_FLS.1/Base , FDP_RIP.1/Base, FDP_IFC.1/SCP , FCS_CKM.6/SCP-MNO, FDP_IFC.1/Platform_services,FDP_IFF.1/Platform_services,FPT_FLS.1/Platform_services, FMT_MSA.1/CERT_KEYS, FMT_SMR.1/Base
SF.EUICC.SD	FDP_SDI.1/Base, 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/Base, FIA_API.1, FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD,FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RAT, FMT_MSA.3,FMT_SMR.1/Base
SF.EUICC.SCP	FIA_UAU.1/EXT, FIA_USB.1/EXT, FIA_ATD.1/Base ,FIA_API.1, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FMT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS , 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.6/SCP-SM and FCS_CKM.6/SCP-MNO.

Table 22 eUICC SFRs coverage

8.3.2 Runtime Environment SFRs coverage

Security Functions (SF)	SFR Mapping Rationale
SF.JC.FW	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JC, FMT_SMR.1/JC, FDP_ROL.1/FIREWALL,FMT_MTD.1/JCRE and FMT_MTD.3/JCRE.
SF.JC.RIP	FCS_CKM.6/SCP-SM ,FCS_CKM.6/SCP-MNO ,FDP_RIP.1/Base ,FDP_RIP.1/ADEL,FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/APDU, FDP_RIP.1/bArray, FDP_RIP.1/GlobalArray, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT and FDP_RIP.1/Base.
SF.JC.CRYPTO	FCS_CKM.1/SCP-SM,FCS_CKM.2/SCP-MNO,FCS_COP.1/GP-SCP, FPR_UNO.1, FPR_UNO.1/GP, FCS_RNG.1 andFPT_EMS.1/Base.
SF.JC.ROLLBACK	FDP_ROL.1/FIREWALL, FDP_RIP.1/ABORT, FPT_RCV.3/OS, FPT_RCV.4/OS
SF.JC.APDU	FDP_IFC.1/JCVM, FDP_RIP.1/APDU
SF.JC.EXCEPTION	FAU_ARP.1, FPT_FLS.1
SF.GP.CM	FPT_RCV.3/Installer, FAU_ARP.1, FDP_SDI.2/DATA, FPT_FLS.1/Base, FPT_TDC.1, FPT_TDC.1/GP, FIA_ATD.1/AID, FIA_UID.2/AID, FIA_USB.1/AID, FDP_ITC.2/Installer, FMT_SMR.1/Installer, FPT_FLS.1/Installer, FPT_RCV.3.1/Installer, FPT_FLS.1/ADEL, 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, FDP_RIP.1/ODEL, FPT_FLS.1/ODEL, FIA_UAU.1/GP, FIA_UAU.4/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FAU_SAS.1,FMT_SMF.1/GP, FMT_SMR.1/GP, FMT_MSA.1/GP, FMT_MSA.3/GP, FCO_NRO.2/CM, FDP_ITC.2/GP-KL, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FDP_ROL.1/GP, FIA_AFL.1/GP, FMT_MSA.1/GP, FMT_MSA.3/GP
SF.GP.SCP	FIA_UAU.4/EXT,FCS_COP.1/GP-SCP,FMT_SMF.1/GP, FCO_NRO.2/CM, FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_UIT.1/CM, FIA_UID.1/GP, FMT_MSA.1/GP, FMT_MSA.3/CM,FTP_ITC.1/GP and FMT_SMR.1/GP

Table 23 Runtime Environment SFRs coverage

9 Statement of Compatibility

The current TOE is a composite product relaying on a certified undelaying platform. This platform is a chipset compliant to [PP-84] and identified with Cert-ID: **GSMA-CB-CH-25TRE00181-01**.

The statement of compatibility has taken Threats, OSP, Assumptions and Objectives and Requirements from the applicable ST as identified by Cert-ID

9.1 Statement of compatibility – ASE_SPD

Threats	Rationale
T.Phys-Manipulation	This threat is related to physical manipulation of the Security IC. Covered by IC evaluation
T.Phys-Probing	This threat is related to physical probing of the TOE to disclose relevant information. Considered during TOE evaluation
T.Malfunction	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. Considered during TOE evaluation
T.Leak-Inherent	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. Considered during TOE evaluation
T.Leak-Forced	This threat is related to information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the composite TOE. Covered by IC evaluation
T.Abuse-Func	This threat is related to the usage of functions of the TOE that are not allowed once the TOE Delivery and can impact the security of the TOE. Considered during TOE evaluation
T.RND	This threat is related to the deficiency of random numbers. Covered by IC evaluation
T.Unauthorized-Access	Covered by IC evaluation and TOE evaluation

Table 24 Threats

OSP	Rationale
P.Process-TOE	This policy is related to the accurate unique identification during IC Development and Production. Covered by IC evaluation
P.Crypto-Service	Considered during TOE evaluation

Table 25 OSP

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

Table 26 Assumptions

9.2 Statement of compatibility – ASE_OBJ

O.TOE	Rationale
O.Phys-Manipulation	Covered by IC evaluation
O.Phys-Probing	This objective is covered by TOE evaluation.
O.Malfunction	This objective is covered by TOE evaluation.
O.Leak-Inherent	This objective is covered by TOE evaluation.
O.Leak-Forced	Covered by IC evaluation
O.Abuse-Func	This objective is covered by TOE evaluation.
O.Identification	This objective is covered by TOE evaluation.
O.RND	Covered by IC evaluation
O.TDES	Covered by IC evaluation and TOE evaluation
O.AES	Covered by IC evaluation and TOE evaluation
O.RSA	Covered by IC evaluation
O.ECC	Covered by IC evaluation and TOE evaluation
O.X25519	Covered by IC evaluation
O.Mem Access	This objective is covered by TOE evaluation.

Table 27 O.TOE

O.ENV	Rationale
OE.Resp-Appl	Covered by IC evaluation and TOE evaluation
OE.Process-Sec-IC	Covered by IC evaluation and TOE evaluation

Table 28 O.ENV

9.3 Statement of compatibility – ASE_REQ

The SFR are categorized according the following types:

- IP_SFR: Irrelevant and not used by current TOE
- RP_SFR-SERV: Relevant and used by current TOE to implement a Security Service with associated TSFI.
- RP_SFR-MECH: Relevant and used by current TOE to implement a Security Mechanism and addressed in ADV_ARC.

SFR	Rationale
FDP_ACC.1	RP_SFR-SERV; FDP_ACC.1/ISDR, FDP_ACC.1/ECASD
FDP_ACF.1	RP_SFR-SERV; FDP_ACF.1/ISDR, FDP_ACF.1/ECASD, FDP_ACF.1/FIREWALL, FDP_ACF.1/ADEL
FRU_FLT.2	RP_SFR-MECH
FPT_FLS.1	RP_SFR-MECH
FMT_LIM.1	RP_SFR-MECH
FMT_LIM.2	RP_SFR-MECH
FAU_SAS.1	RP_SFR-SERV; FAU_SAS.1
FDP_SDC.1	RP_SFR-MECH

SFR	Rationale
FDP_SDI.2	RP_SFR-MECH
FPT_PHP.3	RP_SFR-MECH
FDP_ITT.1	RP_SFR-MECH
FPT_ITT.1	IP_SFR
FDP_IFC.1	RP_SFR-SERV; FDP_IFC.1/SCP, FDP_IFC.1/Platform_services, FDP_IFC.1/JCVM
FCS_RNG.1	RP_SFR-SERV; FCS_RNG.1
FCS_RNG.1[PTG.2]	RP_SFR-SERV; FCS_RNG.1
FCS_RNG.1[DRG.3]	IP_SFR
FCS_COP.1[TDES]	RP_SFR-SERV; FCS_COP.1/GP-SCP
FCS_COP.1[AES]	RP_SFR-SERV; FCS_COP.1/GP-SCP
FCS_COP.1[RSA]	IP_SFR
FCS_COP.1[ECC]	RP_SFR-SERV; FCS_COP.1/GP-SCP
FCS_CKM.4[ECC]	RP_SFR-SERV; FCS_CKM.6/SCP-MNO
FCS_CKM.4[TDES]	RP_SFR-SERV; FCS_CKM.6/SCP-MNO
FCS_CKM.4[AES]	RP_SFR-SERV; FCS_CKM.6/SCP-MNO
FCS_CKM.4[RSA]	IP_SFR
FCS_COP.1[X25519]	IP_SFR
FCS_CKM.4[X25519]	IP_SFR

Table 29SFR