CTD 1514A Security Target
Version 1.12
Chutian Dragon Co., Ltd.

Table of Contents

1 Security Target Introduction

1.1 Security Target reference

Name	CTD 1514A Security Target
Version	1.12
reference	CTD_1514A_ST v1.12

1.2 TOE reference

Name	CTD 1514A
Version	1.7
Reference	CTD_1514A_1.7

1.3 References

Ref	DocNumber	Title	Version
[1]	[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model	Version 2022
[2]	[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components	Version 2022
[3]	[CC-3]	Common Criteria for Information Technology Security Evaluation Part Part 3: Security assurance components	Version 2022
[4]	[CC-5]	Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements	Version 2022
[5]	[CC-COMP]	Composite product evaluation for Smart Cards and similar devices	Version 1.5.1 May 2018
[6]	[PP-eUICC]	eUICC for Consumer and IoT Devices Protection Profile	Version 2.1
[7]	[PP-JCS]	Java Card System – Open Configuration Protection Profile	Version 3.2
[8]	[PP-GP]	Global Platform – Secure Element Protection Profile	Version 1.0
[9]	[PP-84]	Security IC Platform Protection Profile with Augmentation Packages	Version 1.0
[10]	[PP-USIM]	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations	Version 2.0.2, July 2010, ANSSI-CC-PP-2010/05.

Ref	DocNumber	Title	Version
[11]	[JCVM3]	Java Card Platform - Classic Edition, Virtual Machine (Java Card VM) Specification.	Version 3.0.4
[12]	[JCAPI3]	Java Card Platform - Classic Edition, Application Programming Interface.	Version 3.0.4
[13]	[JCRE3]	Java Card Platform - Classic Edition, Runtime Environment (Java Card RE) Specification.	Version 3.0.4
[14]	[GPCS]	GlobalPlatform Technology Card Specification March 2018 • [Amd A] Amendment A - Confidential Card Content Management, v1.1 - July 2019 (GPC_SPE_007) • [Amd B] Amendment B - Remote Application Management over HTTP, v1.1.3 - May 2015 (GPC_SPE_011) – ref [13] in [PP/0100]	Version 2.3.1
[15]	[GP-BASIC]	Security Guidelines for Basic Applications	Version 2.0 November 2014
[16]	[3GPP-MIL]	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; • 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.	Release 11
[17]	[3GPP-TUAK]	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233 • Document 1: Algorithm specification; • Document 2: Implementers' test data; Document 3: Design conformance test data.	Release 12, December 2014
[18]	[SGP.22]	Remote SIM Provisioning (RSP) Technical Specification	V2.6
[19]	[ST-IC]	IFX_CCI_000068h/80h/97h/99h G12 and IFX_CCI_000093h R11/R12 Security Target	Rev. 2.8

Ref	DocNumber	Title	Version
[20]	[EUPP]	TCA eUICC Profile Package Interoperable Format Test Specification	V3.3.1
[21]	[TS 102.225]	ETSI TS 102 225 V16.0.0 (2020-06), Smart Cards; Secured packet structure for UICC based applications (Release 16).	V16.0.0 (2020-06)
[22]	[TS 102.226]	ETSI TS 102 226 V16.0.1 (2020-12), Smart Cards; Remote APDU structure for UICC based applications (Release 16).	V16.0.1 (2020-12)
[23]	[AIS31]	A Proposal for Functionality Classes for Random Number Generators	Version 2.0, 18 September 2011

2 TOE overview

This section presents the architecture and common usages of the TOE.

2.1 TOE description

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

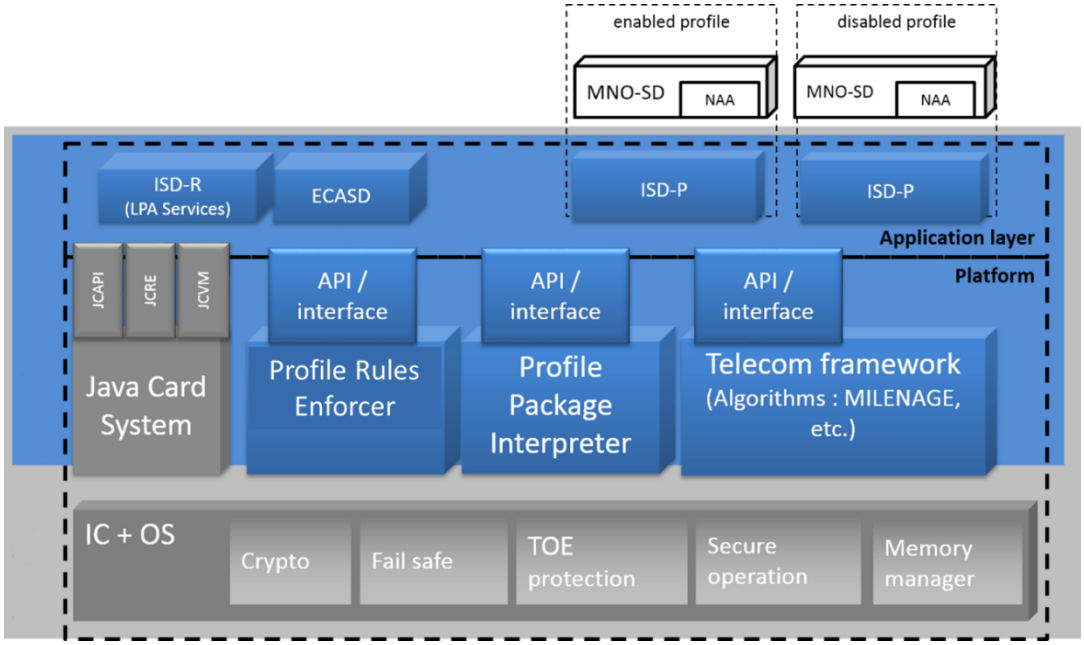


Figure 1 TOE architecture

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 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.

- 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.
- Runtime Environment: A Java Card System built on top of an certified Integrated Circuit providing support to the Platform layer and Application Layer.

Specifically, Profiles are not part of the TOE as defined in [PP-eUICC]. Additionally, LPAe is not in the TOE.

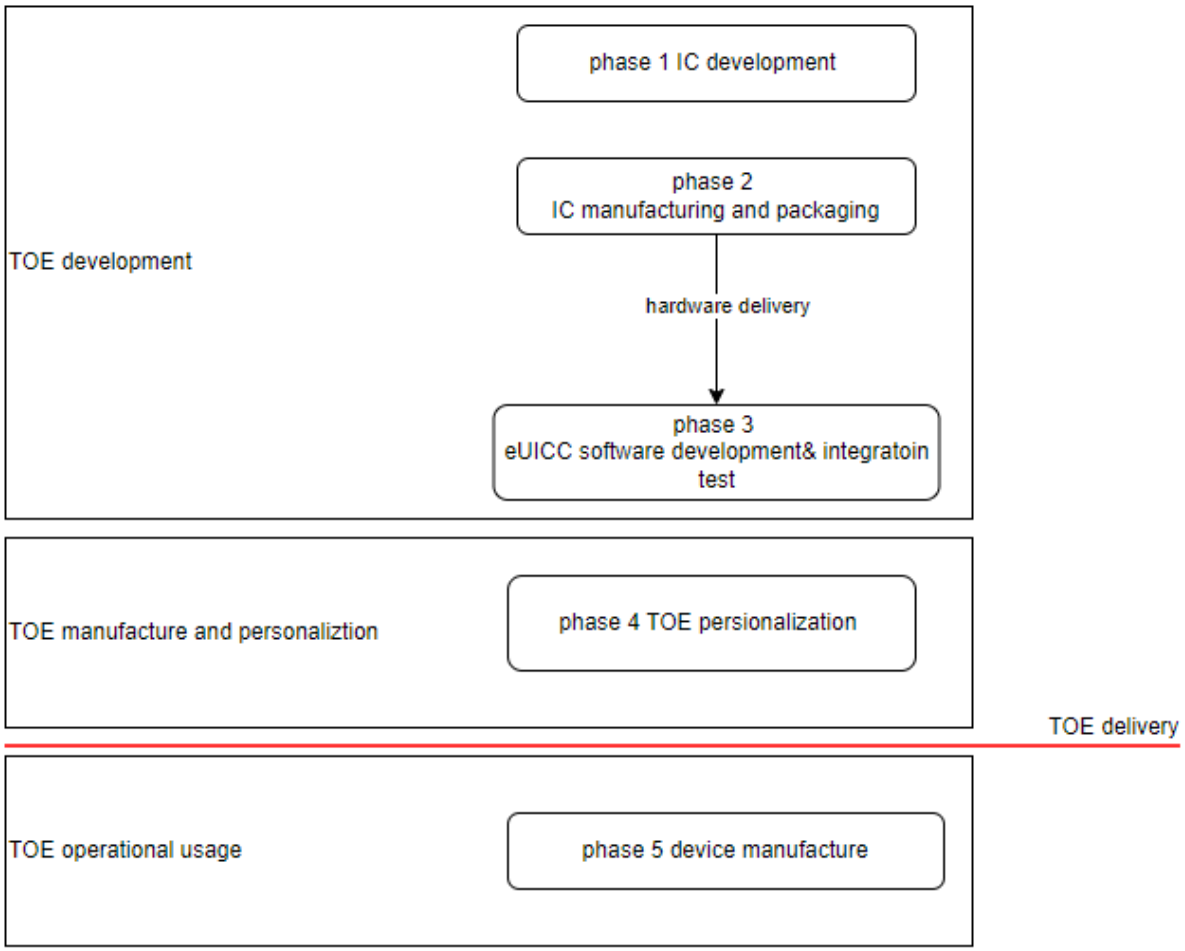
2.2 TOE type and usage

TOE is an eUICC embedded device in a consumer terminal device. The eUICC is connected to a specific mobile network through its currently enabled mobile network operator Profile.

TOE can be applied to smartphones, tablets, Internet of Things (IoT) devices, cars (V2X), wearable devices, etc. Through remote SIM Profile management, it supports downloading, installing, enabling, disabling and deleting Profiles through the SM-DP+ remote management platform to achieve dynamic network switching.

2.3 TOE life cycle

The life cycle of the TOE shows as follow. The self-protected TOE is delivered at the end of phase 4



Actor:

- eUICC Manufacturer, Chutian Dragon is in charge of eUICC software development and eUICC personalization
- IC manufacturer, Infineon, is in charge of the IC development and manufacture
- Device manufacturer is the user of TOE

Phase	Content	Actor
1	IC development including hardware design and IC dedicated software development	IC manufacturer, Infineon
2	IC manufacture including wafer manufacture and test, and module packaging IC delivery including Flash Loader component. Flash loader is provided to IC user for OS image download.	IC manufacturer, Infineon
3	eUICC software (including OS) development Integration testing between the eUICC module and the IC platform Functional testing of TOE	eUICC Manufacturer, Chutian Dragon (Beijing)
4	TOE personalization and quality testing TOE is self-protected and delivered at the end of this	eUICC Manufacturer, Chutian Dragon

	phase.	(Dongguan, Guangdong)
5	Integrate TOE into a consumer device, ensuring proper functionality	Device manufacturer

Figure 2 TOE life-cycle

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

Non-TOE is same as the ones mentioned in the [PP-eUICC] except for IC, Embedded software (ES) and Runtime Environment (RE), which are in scope of the TOE, including:

- LPAd,
- Consumer Device,
- MNO-SD and applications,
- Remote provisioning infrastructure.

Besides, bytecode verifier is non-TOE software. The TOE supports post-issuance application loading; Bytecode Verifier is considered part of the IT environment (Non-TOE) due to the resource constraints of the smart card. The security model of the Java Card architecture relies on off-card bytecode verification combined with a cryptographic signature mechanism. The verification is performed by an off-card tool which digitally signs the verified file. The TOE validates the integrity and authenticity of the loaded code by verifying this signature, thereby obtaining indirect assurance that the code has successfully passed bytecode verification without the need for resource-intensive on-card execution.

2.5 TOE scope

2.5.1 Physical scope

The physical boundaries define the area within the IC's hardware where the eSIM software operates. Other components are not included in this evaluation.

The TOE consists of the following components:

- **Hardware:**
  - Developer: Infineon
  - Certification ID: **BSI-DSZ-CC-1206-V5-2025**.
  - IC certified name: IFX_CCI_000080h
  - IC design step G12
  - IC firmware: 80.505.04.1
  - IC Libraries:
    - HSL version 04.05.0040,
    - Crypto Suite 5.02.002
    - UMSLC 02.01.0040
  - Delivery form: wafer/QFN/DFN
- **eUICC OS:**
  - Developer: Chutian Dragon Co., Ltd.

- Name and version: CTD 1514A eUICC V1.7
- Form of delivery: Binary in memory

- **eUICC guidance's:**
  - Developer: Chutian Dragon Co., Ltd.
  - Item:
    - CTD_1514A_AGD_OPE v1.6
    - CTD_1514A_AGD_PRE v1.8
  - Form of delivery: Documents protected by PGP encryption and sent via email

NOTE:

The TOE's IC supports only Class C voltage mode as defined in ISO/IEC 7816-3, operating within the range of 1.62V to 1.98V. This limitation ensures low-power consumption suitable for eUICC applications but restricts compatibility with Class A (5V) and Class B (3V) modes. The TOE assumes a stable power supply within this range to support TSF execution, with voltage deviations may cause chip malfunctions.

2.5.2 Logical scope

The logical scope of the TOE covers a comprehensive set of services designed to support the security features. Specifically, it provides at least the following services:

- Remote SIM Provisioning Service:

Supports remote configuration and management of SIM card features, enabling dynamic profile installation, activation, deactivation, and deletion by interacting with external entities such as the Subscription Manager - Data Preparation (SM-DP+).

- Communication Management Service:

Manages secure and reliable communications between the operating system and external entities such as the MNO and SM-DP+. This service ensures data integrity and confidentiality during transmission.

-Operating System Security Services:

- Cryptographic Primitives, Algorithms, and Services: Provides standard cryptographic operations and key management services.
- Secure Asset Protection: Ensures the integrity and confidentiality of critical security assets through secure storage and access control.
- Random Number Generation: Provides hardware-compliant, high-quality random numbers for cryptographic operations and authentication.

- JavaCard Runtime and Firewall Enforcement:

Implements a JavaCard runtime environment and firewall mechanism to enforce applet isolation and resource access control, preventing unauthorized interference between applets and protecting sensitive data.

- Standard API Support:

Provides a set of standardized application programming interfaces (APIs) to enable interoperability and functionality:

- Telecom API: Provides SIM-related support functions.
- JavaCard API: Provides a secure execution environment and standard API for applets.

- GlobalPlatform API: Standard API for secure content management and lifecycle operations.

Profiles are not part of the TOE as defined in [PP-eUICC]. Additionally the TOE does not support LPAe and RMI functions of JCS is not implemented

3 Conformance Claim

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

This Security Target conforms to CC version 2022 [CC-1], [CC-2] ,[CC-3] and [CC-5].

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

3.2 Assurance package

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

Besides, as TOE is a composite product. Composite product package from CC2022 part 5 [CC5] are added as augmented set of SARs including ASE_COMP.1, ADV_COMP.1, ALC_COMP.1, ATE_COMP.1 and AVA_COMP.1.

3.3 Protection Profile (PP) conformance claim

This Security Target claims demonstrable conformance to the following protection profile:

- SGP.25 Base PP [PP-eUICC].

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.
- 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] which does not contain LPAe.

The TOE follows the third scenario from the definition in [PP-eUICC] when the embedded eUICC is embedded in a certified IC (BSI-DSZ-CC-1206-V5-2025) 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 in order to meet the objectives for the OS and JCS. This is a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

3.4.2 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_POLICY_RULES	X	(E)
D.PROFILE_USER_CODES	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)
D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(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].

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-DP+	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.End-User	X	(E)

Table 1 User consistency table

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

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

Table 2 Subjects 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	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-PLATFORM-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PROFILE-MNG-ELIGIBILITY	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-IDENTITY-MNG	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.IDENTITY-INTERCEPTION	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.UNAUTHORIZED-eUICC	X	(E)
T.LPAd-INTERFACE-EXPLOIT	X	(E)
T.UNAUTHORIZED-MOBILE-ACCESS	X	(E)
T.LOGICAL-ATTACK	X	(R): Assets added from [PP-JCS] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)

Table 3 Threats 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)

Table 4 Organizational 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.

TOE is an open platform and support applet download after TOE delivery. A.CAP_FILE is added to prevent other applet containing native method which may compromise TOE SF. It aims at regulating the applet developer and they do not affect the original security problem.

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

A.APPLICATIONS	X	(E)
A.CAP_FILE		(A): Added from [PP-JCS].

Table 5 Assumptions Consistency table

A.CAP_FILE is added from [PP-JCS] without modification.

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.PPE-PPI	X	(E)
O.eUICC-DOMAIN-RIGHTS	X	(E)
O.SECURE-CHANNELS	X	(E)
O.INTERNAL-SECURE-CHANNELS	X	(E)
O.PROOF_OF_IDENTITY	X	(E)
O.OPERATE	X	(E)
O.API	X	(E)
O.DATA-CONFIDENTIALITY	X	(E)
O.DATA-INTEGRITY	X	(E)
O.ALGORITHMS	X	(E)
O.IC.PROOF_OF_IDENTITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.IC.SUPPORT		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.IC.RECOVERY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.PPE-PPI		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.

O.RE.SECURE-COMM		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.API		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.DATA-CONFIDENTIALITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.DATA-INTEGRITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.IDENTITY		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.
O.RE.CODE-EXE		(A): Added as Security Objective for the TOE instead of Security Objective for the Operational Environment.

Table 6 Security objectives for the TOE consistency table

3.4.3.2 Objective for Environment consistency

TOE is an open platform and support applet download after TOE delivery. OE.VERIFICATION and OE.CODE-EVIDENCE are added to ensure other applets can be installed. TOE user must verify the their bytecode and promise its integrity after verification.

OE.CAP_FILE is added to fulfil A.CAP_FILE. prevent other applet containing native method which may compromise TOE SF.

Therefore, the added objectives for environment aims at regulating the applet developer and they do not affect the original set of security objectives for the TOE nor the security objectives for the operational environment.

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.TRUSTED-PATHS-LPAd-IPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.CODE-EVIDENCE		(A): Added from [PP-JCS].
OE.VERIFICATION		(A): Added from [PP-JCS].
OE.MNO-SD	X	(E)
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PPE-PPI	X	Removed and replaced by O.RE.PPE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE
OE.CAP_FILE		(A): Added from [PP-JCS].

Table 7 Security objectives for the Operational Environment consistency table

3.4.4 Conformity of the Requirement (SFR/SAR)

As shown in TOE physical scope, except eUICC, java card platform code is also involved in TOE. Therefore, some SFRs are added from [PP-JCS] for java card platform. Then the total set of SFRs in the ST is more restrictive than the set of SFRs in 错误!未找到引用源。.

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]. Refined with iteration.
FMT_SMR.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/EC FCS_CKM.1/GP-SCP		(A): Added from [PP-JCS]. Refined with iteration. (A): Added from [PP-GP].
FCS_CKM.6		(A): Added from [PP-JCS].
FCS_COP.1/JC_TDES_MAC FCS_COP.1/JC_AES_MAC FCS_COP.1/JC_ECDSA_SIGN FCS_COP.1/GP-SCP FCS_COP.1/JC_TDES_CIPHER FCS_COP.1/JC_AES_CIPHER FCS_COP.1/JC_Hash FCS_COP.1/JC_CRC		(A): Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A): Added from [PP-JCS].
FDP_RIP.1/APDU		(A): Added from [PP-JCS].
FDP_RIP.1/bArray		(A): Added from [PP-JCS].
FDP_RIP.1/GlobalArray		(A): Added from [PP-JCS].
FDP_RIP.1/KEYS		(A): Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A): Added from [PP-JCS].
FAU_ARP.1		(A): Added from [PP-JCS].
FDP_SDI.2/DATA		(A): Added from [PP-JCS].

FPR_UNO.1		(A): Added from [PP-JCS].
FPT_FLS.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FPT_TDC.1		(A): Added from [PP-JCS].
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ACC.2/ADEL		(A): Added from [PP-JCS].
FDP_ACF.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].
FMT_SMF.1/ADEL		(A): Added from [PP-JCS].
FMT_SMR.1/ADEL		(A): Added from [PP-JCS].
FPT_FLS.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/ODEL		(A): Added from [PP-JCS].
FDP_ROL.1/GP		(A): Added from [PP-GP].
FCO_NRO.2/GP		(A): Added from [PP-GP].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP].
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP].
FMT_MSA.1/GP		(A): Added from [PP-GP].
FMT_MSA.3/GP		(A): Added from [PP-GP].
FMT_SMR.1/GP		(A): Added from [PP-GP].
FMT_SMF.1/GP		(A): Added from [PP-GP].
FDP_ITC.2/GP-KL		(A): Added from [PP-GP].
FTP_ITC.1/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-KL		(A): Added from [PP-GP].
FDP_IFF.1/GP-KL		(A): Added from [PP-GP].

FIA_UID.1/GP		(A): Added from [PP-GP].
FPT_TDC.1/GP		(A): Added from [PP-GP].
FPT_RCV.3/GP		(A): Added from [PP-GP].
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP].
FPT_FLS.1/GP		(A): Added from [PP-GP].
FPR_UNO.1/GP		(A): Added from [PP-GP].
FAU_SAS.1		(A): Added to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added to cover O.IC.RECOVERY.
FPT_RCV.4/OS		(A): Added to cover O.IC.SUPPORT.

Table 8 Security 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 of 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 of 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 of threats.

Refined threats description is detailed below, where assets in **bold** come from [PP-JCS] and/or [PP-GP].:

Threat	Refined description
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, D.PROFILE_*, **D.APP_C_DATA, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_CODE.**
T.UNAUTHORIZED-PLATFORM-MNG	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behaviour of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.

T.PROFILE-MNG-INTERCEPTION	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatens the assets: D.MNO_KEYS, D.TSF_CODE, D.PROFILE_*., **D.APP_C_DATA, D.PIN and D.APP_KEYs**.
T.PROFILE-MNG-ELIGIBILITY	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatens the assets: D.TSF_CODE, D.DEVICE_INFO, D.EID, D.APP_C_DATA, D.PIN, **D.APP_KEYs, D.APP_CODE and D.APP_I_DATA**.
T.UNAUTHORIZED-IDENTITY-MNG	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, **D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA.**
T.IDENTITY-INTERCEPTION	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatens the assets: D.SECRETS, D.EID, **D.APP_C_DATA, D.PIN and D.APP_KEYs.**
T.IDENTITY-INTERCEPTION	Directly threatens the assets: D.SECRETS, D.EID, **D.APP_C_DATA, D.PIN and D.APP_KEYs.**
T.UNAUTHORIZED-eUICC	
T.LPAd-INTERFACE-EXPLOIT	
T.UNAUTHORIZED-MOBILE-ACCESS	

T.LOGICAL-ATTACK	The definition of this threat is present in [PP-eUICC]. The mapping against assets has been refined as detailed below. Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_POLICY_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, **D.JCS_CODE, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_C_DATA**.
T.PHYSICALATTACK	

Table 9 Refined threats description

4.4 Organizational Security Policies

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

4.5 Assumptions

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

5 Security Objectives

This section introduces the security objectives for the TOE.

5.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 3.4.3 for complete list of Security Objectives for the TOE.

Some objectives from the environment have been converted to objectives of the TOE, specifically the ones from [PP-eUICC] related to OE.RE* and OE.IC*. The replaced objectives from 3.4.3.2 and their description are listed next:

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

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

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 TOE from [PP-eUICC] and [PP-JCS] are not repeated here. See section 3.4.3.2 for complete list of 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.PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP+ and MNO OTA Platform) will access the Security Domains functions and content;
- OE.SM-DP+ and OE.MNO protect the corresponding credentials when used offcard. The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY). The authentication is supported by corresponding secure channels:
- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication with SM-DP+ and a secure channel for communication with MNO OTA Platform. These secure channels rely upon the underlying Runtime

Environment, which protects the applications communications (O.RE.SECURE-COMM).

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

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

T.UNAUTHORIZED-PLATFORM-MNG

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

- O.PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.
- OE.SM-DP+ protects 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, OE.VERIFICATION and O.RE.DATA-INTEGRITY).

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

T.PROFILE-MNG-INTERCEPTION

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

Consequently, the TSF ensures:

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

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

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

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

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

T.IDENTITY-INTERCEPTION

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

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

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, ES10b and ES10c are trusted paths to the LPAd.

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 PPE, PPI, the Telecom Framework or any native/OS part of the TOE. As such it is covered:

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

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

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

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

The following objectives for the operational environment are also required:

- compliance to security guidelines for applications (OE.APPLICATIONS, OE.VERIFICATION 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.

5.3.3 Assumptions

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

A.TRUSTED-PATHS-LPAd-IPAd, A.ACTORS and A.CAP_FILE are defined the same as the one in [PP-eUICC]and [PP-JCS]. Then they are not repeated here.

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

5.3.4 Rationale Tables

5.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD,	Section 5.3.1.1

	OE.CODE-EVIDENCE, OE.VERIFICATION,	
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.SM-DP+ OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.RE.DATA- CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.VERIFICATION	Section 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	Section 5.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+, O.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 5.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 5.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 5.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 5.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 5.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 5.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.VERIFICATION	Section 5.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 5.3.1.6

Table 11 Threats and Security Objectives- Coverage

Security Objectives	Threats
O.PPE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG

O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-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.PPE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd-IPAd	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

Organizational Security Policies	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PPE-PPI, O.RE.PPE-PPI, O.OPERATE	Section 5.3.2

Table 13 Organizational Security Policies and Security Objectives- Coverage

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

O.RE.DATA-CONFIDENTIALITY	
O.RE.DATA-INTEGRITY	
O.RE.IDENTITY	
O.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd	
OE.APPLICATIONS	
OE.CODE-EVIDENCE	
OE.MNO-SD	
OE.SM-DS	
OE.CAP_FILE	

Table 14 Security Objectives and Organizational Security Policies

5.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd	Section 5.3.3
A.ACTORS	OE.CI, OE.SM-DP+, OE.MNO, OE.SM-DS	Section 5.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.VERIFICATION, OE.CODE-EVIDENCE	Section 5.3.3
A.CAP_FILE	OE.CAP_FILE	Section 5.3.3

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

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-DP+	A.ACTORS
OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd-IPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.VERIFICATION	A.APPLICATIONS
OE.MNO-SD	
OE.CAP_FILE	A.CAP_FILE

Table 16 Assumptions and Security Objectives for the Operational Environment

6 Extended Components Definition

There is no extend components defined in [PP-eUICC]. The ST does not define any extended components for eUICC part either.

There are no extended components defined in the [PP-JCS]. The ST defines an additional extended component FAU_SAS.1 defined in [PP-84] without any modification. Thus, it is not repeated here.

7 Security Functional requirements

The following conventions are used in the definition of the SFRs

- Selections and assignment that have already been made in [PP-eUICC], [PP-GP] and [PP-JCS] are in **bold**, and the original text on which the selection or assignment has been made is not reminded.
- Selections and assignment made in this ST are in **bold and underlined**.
- Iteration operations on SFR components are denoted by showing a slash"/" and the iteration indicator after the SFR component identifier.

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 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: no other algorithm]** and cryptographic key sizes **according to the corresponding standard** that meet the following:

- **MILENAGE according to standard [3GPP-MIL] 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 [3GPP-MIL]**
- **Tuak according to [3GPP-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: following key distribution methods**] that meets the following: [**assignment: following standards**]:

Item	Method	Standard
Milenage	distribution method from SCP-SGP22 (SCP03t)	[SGP.02]
Tuak	distribution method from SCP-SGP22 (SCP03t)	[SGP.02]

FCS_CKM.6/Mobile_network Cryptographic key destruction

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

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: write random number**] that meets the following: [**assignment: none**].

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: none].**

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: none]**

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 of U.MNO-OTA;**
- **SM-DS OID is associated to S.ISD-R, acting on behalf of U.SM-DS;**
- **[selection: no other associations].**

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 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: no other initial associations].**

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: no other changes]**

FIA_UAU.4/EXT Single-use authentication mechanisms

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

- **U.SM-DP+**
- **U.MNO-OTA**
- **[Selection: none]**

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow

[**assignment: none**] on behalf of the user to be performed before the user is identified.

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

FIA_USB.1/MNO-SD User-subject binding

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

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

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

FIA_ATD.1/Base User attribute definition

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

- **CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-DP+;**
- **MNO OID belonging to U.MNO-OTA;**
- **AID belonging to U.MNO-SD;**
- **CERT.DSauth.ECDSA and SM-DS OID belonging to U.SM-DS;**
- **[selection: no additional attributes].**

FIA_API.1 Authentication Proof of Identity

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

7.1.3 Communication

FDP_IFC.1/SCP Subset information flow control

FDP_IFC.1.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** on

- **users/subjects/objects:**
  - **U.SM-DP+ and SO.ISD-R, SO.ISD-P**
  - **U.MNO-OTA and U.MNO-SD**
- **information: transmission of commands**.

FDP_IFF.1/SCP Simple security attributes

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

- **users/subjects:**
  - **U.SM-DP+, SO.ISD-P and SO.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.MNO-SD in a SCP80 or SCP81 secure channel**.

FDP_IFF.1.3/SCP The TSF shall enforce the [**assignment: none**].

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

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

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

FTP_ITC.1/SCP Inter-TSF trusted channel

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

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

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

The TSF shall permit the SM-DP+ to open a SCP-SGP22 secure channel to transmit the following operations:

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

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

- **ES10a.GetEuiccConfiguredAddresses**
- **ES10a.SetDefaultDpAddress**
- **ES10b.PrepareDownload**
- **ES10b.LoadBoundProfilePackage**
- **ES10b.GetEUICCChallenge**
- **ES10b.GetEUICCInfo**
- **ES10b.ListNotification**
- **ES10b.RetrieveNotificationsList**
- **ES10b.RemoveNotificationFromList**
- **ES10b.AuthenticateServer**
- **ES10b.CancelSession**
- **ES10c.GetProfilesInfo**
- **ES10c.EnableProfile**
- **ES10c.DisableProfile**
- **ES10c.DeleteProfile**
- **ES10c.eUICCMemoryReset**
- **ES10c.GetEID**
- **ES10c.SetNickname**
- **ES10c.GetRAT.**

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

- **ES6.UpdateMetadata**

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

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

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

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

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

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

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

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

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

when shared between the TSF and another trusted IT product.

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

FDP_UCT.1/SCP Basic data exchange confidentiality

FDP_UCT.1.1/SCP The TSF shall enforce the **Secure Channel Protocol information flow control SFP** to **receive** user data in a manner protected from unauthorised disclosure.

FDP_UIT.1/SCP Data exchange integrity

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

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

FCS_CKM.1/SCP-SM Cryptographic key generation

FCS_CKM.1.1/SCP-SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curves Key agreement**

(ECKA) and specified cryptographic key sizes **256** that meet the following: **[assignment: ECKA-EG using one of the following standards:**

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard)**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639)]**

FCS_CKM.2/SCP-MNO Cryptographic key distribution

FCS_CKM.2.1/SCP-MNO The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**assignment: distribution method from SCP-SGP22 (SCP03t)**] that meets the following: [**assignment: SGP.02 standard**].

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: [assignment: The profile was downloaded successfully or an error occurred during the download process]**].

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: write random number]** 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: [assignment: profile deletion]**].

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: write random number**] that meets the following: [**assignment: none**].

7.1.4 Security Domains

FDP_ACC.1/ISDR Subset access control

FDP_ACC.1.1/ISDR The TSF shall enforce the **ISD-R content access control SFP** on

- **subjects: S.ISD-R**
- **objects: SO.ISD-P**
- **operations:**
  - **Create and configure profile**
  - **Store profile metadata**

- **Enable profile**
- **Disable profile**
- **Delete profile**
- **Perform a Memory reset**.

FDP_ACF.1/ISDR Security attribute based access control

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

- **subjects: S.ISD-R**
- **objects:**
  - **S.ISD-P with security attributes "state" and "PPR" and [Selection*:* no additional attributes]**
  -
- **operations:**
  - **Create and configure profile**
  - **Store profile metadata**
  - **Enable profile**
  - **Disable profile**
  - **Delete profile**
  - **Perform a Memory reset**.

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

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

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

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

FDP_ACC.1/ECASD Subset access control

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

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

FDP_ACF.1/ECASD Security attribute based access control

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

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

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

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

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

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

7.1.5 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

- o **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD**
  - **Platform code (S.PRE, S.PPI, S.TELECOM)**
- o **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_RULES**
  - **D.PLATFORM_RAT**
- o **operations**:
  - **installation of a profile**
  - **PPR and RAT enforcement**
  - **network authentication**.
  - **[selection: no additional operations]**

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:

- o **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"**
  - **Platform code (S.PRE, S.PPI, S.TELECOM)**
- o **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_POLICY_RULES**
  - **D.PLATFORM_RAT**
- o **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_POLICY_RULES shall be transmitted only**
  - **by S.ISD-R to S.PPE 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.PPE in order to execute the RAT enforcement function**.

FDP_IFF.1.3/Platform_services The TSF shall enforce the [**assignment: none**].

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorise 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.PPE, S.PPI or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **PPR and RAT enforcement**
  - **Network authentication**
  - **[selection: none]**
- **[assignment: none]**.

7.1.6 Security management

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **[selection: hybrid physical]** random number generator that implements: [**assignment: backward secrecy & forward secrecy**].

FCS_RNG.1.2 The TSF shall provide [**selection: byte string represented in hexadecimal**] random numbers that meet [**assignment: [AIS31] test procedure A**].

Refinement: The TOE implements a PTG.3-compliant random-number generator

FPT_EMS.1/Base TOE Emanation of TSF and User data

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

ID	Emission	Attack surface	TSF data	User data
1	[**assignment: side channels (power consumptions and electromagnetic fluctuations)**]	**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.**

FDP_SDI.1/Base Stored data integrity monitoring

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

Refinement:

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

- D.MNO_KEYS
- Profile data
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE_RULES
  - D.PROFILE_USER_CODES
- Management data
  - D.PLATFORM_DATA
  - D.DEVICE_INFO
  - D.PLATFORM_RAT
- Identity management data
  - D.SK.EUICC.ECDSA
  - D.CERT.EUICC.ECDSA
  - D.PK.CI.ECDSA
  - D.EID
  - D.SECRETS
  - D.CERT.EUM.ECDSA

- D.CRLs if existing

FDP_RIP.1/Base Subset residual information protection

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

- o **D.SECRETS;**
- o **D.SK.EUICC.ECDSA;**
- o **The secret keys which are part of the following keysets:**
  - **D.MNO_KEYS,**
  - **D.PROFILE_NAA_PARAMS**.

FPT_FLS.1/Base Failure with preservation of secure state

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

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

FMT_MSA.1/PLATFORM_DATA Management of security attributes

FMT_MSA.1.1/PLATFORM_DATA The TSF shall enforce the **ISD-R content access control policy** to restrict the ability to **modify** the security attributes **the following parts of D.PLATFORM_DATA of:**

- o **ISD-P state**

to

- o **S.ISD-R**

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

- o **D.PROFILE_RULES**

to

- o **S.ISD-Rfor change_default, via function "ES8+.ConfigureISDP"**
- o **S.ISD-R for query**
- o **S.ISD-P for modify, via function "ES6.UpdateMetadata"**

- **[selection:**
  - **S.ISD-R to delete, via function "ES10c.DeleteProfile" (SGP.22)**

  ]

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)]**
- **no actor for other operations**.

FMT_SMF.1/Base Specification of Management Functions

FMT_SMF.1.1/Base The TSF shall be capable of performing the following management functions: **[assignement:**

- **ISD-R access control,**
- **Security Channel protocol information flow control (for roles: S.ISD-R and S.ISD_P),**
- **ECASD access control (for role S.ECASD and S.ISD-R),**
- **Platform services information flow control (for roles S.ISD-R and S.PRE)]**

FMT_SMR.1/Base Security roles

FMT_SMR.1.1/Base The TSF shall maintain the roles

- **External users:**
  - **U.SM-DP+**
  - **U.MNO-SD**
  - **U.MNO-OTA**
  - **U.SM-DS**
  - **[selection: none]**
- **Subjects:**
  - **S.ISD-R**
  - **S.ISD-P**

- **S.ECASD**
- **S.PPI**
- **S.PRE**
- **S.TELECOM**.

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

FMT_MSA.1/RAT Management of security attributes

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

- o **D.PLATFORM_RAT**
- o **D.PROFILE_NAA_PARAMS**
- o **D.PROFILE_RULES**

to

- o **S.ISD-R for query**
- o **S.PRE for query**.

FMT_MSA.3 Static attribute initialisation

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

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

7.2 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

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

Refinement:

The operations involved in the policy are:

- o OP.CREATE,
- o OP.INVK_INTERFACE,
- o OP.INVK_VIRTUAL,
- o OP.JAVA,
- o OP.THROW,
- o OP.TYPE_ACCESS.
- o OP.ARRAY_LENGTH
- o OP.ARRAY_T_ALOAD
- o OP.ARRAY_T_ASTORE
- o OP.ARRAY_AASTORE

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

FDP_ACF.1/FIREWALL Security attribute based access control

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

Subject/Object	Security attributes
S.CAP_FILE	LC Selection Status
S.JCVM	Active Applets, Currently Active Context
S.JCRE	Selected Applet Context
O.JAVAOBJECT	Sharing, Context, LifeTime

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

- o **R.JAVA.1 ([JCRE3], §6.2.8): S.CAP_FILE may freely perform, OP.INVK_VIRTUAL,** OP.**INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS upon any O.JAVAOBJECT whose Sharing attribute has value "JCRE entry point" or "global array".**
- o **R.JAVA.2 ([JCRE3], §6.2.8): S.CAP_FILE may freely perform**

OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE or OP.THROW upon any O.JAVAOBJECT whose Sharing attribute has value "Standard" and whose Lifetime attribute has value "PERSISTENT" only if O.JAVAOBJECT's Context attribute has the same value as the active context.

- **R.JAVA.3 ([JCRE3], §6.2.8.10): S. CAP_FILE may perform OP.TYPE_ACCESS upon an O.JAVAOBJECT with Context attribute different from the currently active context, whose Sharing attribute has value "SIO" only if O.JAVAOBJECT is being cast into (checkcast) or is being verified as being an instance of (instanceof) an interface that extends the Shareable interface.**
- **R.JAVA.4 ([JCRE3], §6.2.8.6): S.CAP_FILE may perform OP.INVK_INTERFACE upon an O.JAVAOBJECT with Context attribute different from the currently active context, whose Sharing attribute has the value "SIO", and whose Context attribute has the value "CAP File AID", only if the invoked interface method extends the Shareable interface and one of the following conditions applies:**

a) The value of the attribute Selection Status of the CAP file whose AID is "CAP File AID" is "Multiselectable",

b) The value of the attribute Selection Status of the CAP file whose AID is "CAP File AID" is "Non-multiselectable", and either "CAP File AID" is the value of the currently selected applet or otherwise "CAP File AID" does not occur in the attribute Active Applets.

- **R.JAVA.5: S.CAP_FILE may perform OP.CREATE upon O.JAVAOBJECT only if the value of the Sharing parameter is "Standard" or “SIO”.**
- **R.JAVA.6 ([JCRE3], §6.2.8): S.CAP_FILE may freely perform OP.ARRAY_ACCESS or OP.ARRAY_LENGTH upon any O.JAVAOBJECT whose Sharing attribute has value "global array".**

FDP_ACF.1.3/FIREWALL The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

- **1) The subject S.JCRE can freely perform OP.JAVA(") and OP.CREATE, with the exception given in FDP_ACF.1.4/FIREWALL, provided it is the Currently Active Context.**
- **2) The only means that the subject S.JCVM shall provide for an application to execute native code is the invocation of a Java Card API method (through OP.INVK_INTERFACE or OP.INVK_VIRTUAL).**

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

- **1) Any subject with OP.JAVA upon an O.JAVAOBJECT whose LifeTime attribute has value "CLEAR_ON_DESELECT" if O.JAVAOBJECT's Context attribute is not the same as the Selected Applet Context.**
- **2) Any subject attempting to create an object by the means of OP.CREATE and a "CLEAR_ON_DESELECT" LifeTime parameter if the active context is not the same as the Selected Applet Context.**
- **3) S.CAP_FILE performing OP.ARRAY_AASTORE of the reference of an O.JAVAOBJECT whose sharing attribute has value “global array” or**

“Temporary”.

- **4) S.CAP_FILE performing OP.PUTFIELD or OP.PUTSTATIC of the reference of an O.JAVAOBJECT whose sharing attribute has value “global array” or “Temporary”**
- ~~**5) R.JAVA.7 ([JCRE3], §6.2.8.2): S.CAP_FILE performing OP.ARRAY_T_ASTORE into an array view without ATTR_WRITABLE_VIEW access attribute.**~~
- ~~**6) R.JAVA.8 ([JCRE3], §6.2.8.2):S.CAP_FILE performing OP.ARRAY_T_ALOAD into an array view without ATTR_READABLE_VIEW access attribute.**~~

Application Note:

- The deletion of applets may render some O.JAVAOBJECT inaccessible, and the Java Card RE may be in charge of this aspect. This can be done, for instance, by ensuring that references to objects belonging to a deleted application are considered as a null reference. Such a mechanism is implementation-dependent.

In the case of an array type, fields are components of the array ([JVM], §2.14, §2.7.7), as well as the length; the only methods of an array object are those inherited from the Object class.

The Sharing attribute defines five categories of objects:

- Standard ones, whose both fields and methods are under the firewall policy,
- Shareable interface Objects (SIO), which provide a secure mechanism for inter-applet communication,
- JCRE entry points (Temporary or Permanent), who have freely accessible methods but protected fields,
- Global arrays, having both unprotected fields (including components; refer to JavaCardClass discussion above) and methods.
- Array Views, having fields/elements access controlled by access control attributes,ATTR_READABLE_VIEW and ATTR_WRITABLE_VIEW and methods.

When a new object is created, it is associated with the Currently Active Context. But the object is owned by the applet instance within the Currently Active Context when the object is instantiated ([JCRE3], §6.1.3). An object is owned by an applet instance, by the JCRE or by the library where it has been defined (these latter objects can only be arrays that initialize static fields of CAP files).

([JCRE3], Glossary) Selected Applet Context. The Java Card RE keeps track of the currently selected Java Card applet. Upon receiving a SELECT command with this applet's AID, the Java Card RE makes this applet the Selected Applet Context. The Java Card RE sends all APDU commands to the Selected Applet Context.

While the expression "Selected Applet Context" refers to a specific installed applet, the relevant aspect to the policy is the context (CAP file AID) of the selected applet. In this policy, the "Selected Applet Context" is the AID of the selected CAP file.

([JCRE3], §6.1.2.1) At any point in time, there is only one active context within the Java Card VM (this is called the Currently Active Context).

It should be noticed that the invocation of static methods (or access to a static field) is not considered by this policy, as there are no firewall rules. They have no effect on the active context as well and the "acting CAP File" is not the one to which the static method belongs to in this case.

It should be noticed that the Java Card platform, version 2.2.x and version 3.x.x Classic Edition, introduces the possibility for an applet instance to be selected on multiple logical channels at the same time, or accepting other applets belonging to the same CAP file being selected simultaneously. These applets are referred to as multiselectable applets. Applets that belong to a same CAP file are either all multiselectable or not ([JCVM3], §2.2.5). Therefore, the selection mode can be regarded as an attribute of CAP files. No selection mode is defined for a library CAP file.

An applet instance will be considered an active applet instance if it is currently selected in at least one logical channel. An applet instance is the currently selected applet instance only if it is processing the current command. There can only be one currently selected applet instance at a given time ([JCRE3], §4).

The TOE is architected upon the Java Card Platform version 3.0.4 runtime environment. In this specific version, the fundamental bytecode instructions astoreand aload, which handle array operations, are designed to function without requiring explicit access control attributes (such as ATTR_WRITABLE_VIEW) for reading from or writing to array views. Consequently, the last two items (Items 5 and 6) of security functional requirements FDP_ACF.1.4/FIREWAL are not supported.

FDP_IFC.1/JCVM Subset information flow control

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

Application Note:

It should be noticed that references of temporary Java Card RE entry points, which cannot be stored in class variables, instance variables or array components, are transferred from the internal memory of the Java Card RE (TSF data) to some stack through specific APIs (Java Card RE owned exceptions) or Java Card RE invoked methods (such as the process (APDU apdu)); these are causes of OP.PUT(S1,S2,I) operations as well.

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes

S.JCVM	Currently Active Context

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

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

FDP_IFF.1.3/JCVM The TSF shall enforce the **[assignment: none]**.

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

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

FDP_RIP.1/OBJECTS Subset residual information protection

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

Application Note:

The semantics of the Java programming language requires for any object field and array position to be initialized with default values when the resource is allocated [JVM], §2.5.1.

FMT_MSA.1/JCRE Management of security attributes

FMT_MSA.1.1/JCRE The TSF shall enforce the **FIREWALL access contro**l SFP to restrict the ability to **modify** the security attributes **Selected Applet Context to the Java Card RE**.

Application Note:

The modification of the Selected Applet Context should be performed in accordance with the rules given in [JCRE3], §4 and [JCVM3], §3.4.

FMT_MSA.1/JCVM Management of security attributes

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

Application Note:

The modification of the Currently Active Context should be performed in accordance with the rules given in [JCRE3], §4 and [JCVM3], §3.4.

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

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

Application Note:

The following rules are given as examples only. For instance, the last two rules are motivated by the fact that the Java Card API defines only transient arrays factory methods. Future versions may allow the creation of transient objects belonging to arbitrary classes; such evolution will naturally change the range of "secure values" for this component.

- The Context attribute of an O.JAVAOBJECT must correspond to that of an installed applet or be "Java Card RE".
- An O.JAVAOBJECT whose Sharing attribute is a Java Card RE entry point or a global array necessarily has "Java Card RE" as the value for its Context security attribute.
- Any O.JAVAOBJECT whose Sharing attribute value is not "Standard" has a PERSISTENTLifeTime attribute's value.
- Any O.JAVAOBJECT whose LifeTime attribute value is not PERSISTENT has an array type as JavaCardClass attribute's value.

FMT_MSA.3/FIREWALL Static attribute initialisation

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

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

Application Note:

FMT_MSA.3.1/FIREWALL

- Objects' security attributes of the access control policy are created and initialized at the creation of the object or the subject. Afterwards, these attributes are no longer mutable (FMT_MSA.1/JCRE). At the creation of an object (OP.CREATE), the newly created object, assuming that the FIREWALL access control SFP permits the operation, gets its Lifetime and Sharing attributes from the parameters of the operation; on the contrary, its Context attribute has a default value, which is its creator's Context attribute and AID respectively ([JCRE3], §6.1.3). There is one default value for the Selected Applet Context that is the default applet identifier's Context, and one default value for the Currently Active Context that is "Java Card RE".
- The knowledge of which reference corresponds to a temporary entry point object or a global array and which does not is solely available to the Java Card RE (and the Java Card virtual machine).

FMT_MSA.3.1/FIREWALL

- The intent is that none of the identified roles has privileges with regard to the default values of the security attributes. It should be noticed that creation of objects is an operation controlled by the FIREWALL access control SFP. The operation shall fail anyway if the created object would have had security attributes whose value violates FMT_MSA.2.1/FIREWALL_JCVM.

FMT_MSA.3/JCVM Static attribute initialisation

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

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

FMT_SMF.1/JC Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

o **modify the Currently Active Context, the Selected Applet Context and the Active Applets.**

FMT_SMR.1/JC Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

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

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

7.2.1.2 Application Programming Interface

FCS_CKM.1/EC Cryptographic key generation

FCS_CKM.1.1/EC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: EC Key Pair Generation]** and specified cryptographic key sizes **[assignment: P ranging from 192 to 384 bits]** that meet the following: **[assignment: see application note]**.

Application note:

- The keys are generated and diversified in accordance with [JCAPI3] in classes KeyBuilder (buildKey method) and KeyPair (genKeyPair method).
- The TOE implements elliptic curve cryptography over GF(p), supporting the following [JCAPI3] key types:

[JCAPI3] Class	Supported Parameters
javacard.security.KeyBuilder	TYPE_EC_FP_PRIVATE LENGTH_EC_FP_192 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_224 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_256 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_384
javacard.security.KeyPair	ALG_EC_FP LENGTH_EC_FP_192 ALG_EC_FP LENGTH_EC_FP_224 ALG_EC_FP LENGTH_EC_FP_256 ALG_EC_FP LENGTH_EC_FP_384

FCS_CKM.1/GP-SCP Cryptographic key generation

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

SCP protocol	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP02	TDES 2-keys	112 bits	[GPCS] section E.4.1
SCP81	TDES 3-keys	168 bits	[Amd B] section 3.3.2
SCP81	AES	128 bits	[Amd B] section 3.3.2

FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy **[assignment: ECC Key, AES Key, TDES Key]** when **[selection: no longer needed]**.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **[assignment: clearKey method]** that meets the following: **[assignment: JCAPI3 standard]**.

Application Note:

- The keys are reset as specified in [JCAPI3] Key class, with the method clearKey(). Any access to a cleared key for ciphering or signing shall throw an exception.
- This component shall be instantiated according to the version of the Java Card API applicable to the security target and the implemented algorithms [JCAPI3].

FCS_COP.1/JC_TDES_MAC Cryptographic operation

FCS_COP.1.1/JC_TDES_MAC The TSF shall perform **[assignment: MAC computation of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: MAC algorithms mentioned in the application note below]** and cryptographic key sizes **[assignment: 112 bits for TDES 2 Keys, 168 bits for TDES 3 Keys]** that meet the following: **[assignment:FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5]**.

Application note: the following TDES MACs from [JCAPI3] are implemented:

MAC length	MAC algorithm	Field name in [JCAPI3] Signature class
4bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC4_ISO9797_1_M1_ALG3

4bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC4_ISO9797_1_M2_ALG3
4bytes	3DES in outer CBC mode	ALG_DES_MAC4_ISO9797_M1
4bytes	3DES in outer CBC mode	ALG_DES_MAC4_ISO9797_M2
4bytes	3DES in outer CBC mode	ALG_DES_MAC4_NOPAD
4bytes	3DES in outer CBC mode	ALG_DES_MAC4_PKCS5
8bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC8_ISO9797_1_M1_ALG3
8bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC8_ISO9797_1_M2_ALG3
8bytes	3DES in outer CBC mode	ALG_DES_MAC8_ISO9797_M1
8bytes	3DES in outer CBC mode	ALG_DES_MAC8_ISO9797_M2
8bytes	3DES in outer CBC mode	ALG_DES_MAC8_NOPAD
8bytes	3DES in outer CBC mode	ALG_DES_MAC8_PKCS5

FCS_COP.1/JC_AES_MAC Cryptographic operation

FCS_COP.1.1/JC_AES_MAC The TSF shall perform **[assignment: MAC computation of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: MAC algorithms mentioned in the application note below]** and cryptographic key sizes **[assignment: 128bits]** that meet the following: **[assignment: FIPS PUB 197, NIST SP800-38A]**.

Application note: the following AES MACs from [JCAPI3] are implemented:

MAC length	MAC algorithm	Field name in [JCAPI3] Signature class
16bytes	AES in CBC mode, block size 128 bits	ALG_AES_MAC_128_NOPAD

FCS_COP.1/JC_ECDSA_SIGN Cryptographic operation

FCS_COP.1.1/JC_ECDSA_SIGN The TSF shall perform **[assignment: signature generation and verification]** in accordance with a specified cryptographic algorithm **[assignment: ECDSA algorithm shown below]** and cryptographic key sizes **[assignment: NIST P-256, brainpoolP256r1]** that meet the following: **[assignment: FIPS PUB 186-4 Digital Signature Standard, RFC 5639 standard]**.

[JCAPI3] class	MAC algorithm
Signature	
	ALG_ECDSA_SHA_224
	ALG_ECDSA_SHA_256
	ALG_ECDSA_SHA_384
	ALG_ECDSA_SHA_512

FCS_COP.1/GP-SCP Cryptographic operation

FCS_COP.1.1/GP-SCP The TSF shall perform **[assignment: cryptographic operations shown blow]** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithms shown blow]** and cryptographic key sizes **[assignment: cryptographic key sizes shown blow]** that meet the following: **[assignment: cryptographic standards shown blow]**.

SCP protocol	Cryptographic Operation	Cryptographic Algorithm	Supported key sizes	Standards
SCP02	MAC Generation/ Verification	HMAC, CMAC using TDES	112 bits	FIPS 198
SCP02	Symmetric Encryption/ Decryption	TDES in CBC mode	112 bits	NIST 800 67 NIST 800 38A
SCP02	Key Derivation	HMAC-based KDF, CMAC-based KDF using TDES	112 bits	NIST 800 108 FIPS 198
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 112 bits AES: 128 bits	TS 102 225 TS 102 226

SCP81	Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_3DES_EDE_CBC_SHA TLS_PSK_WITH_AES_128_CBC_SHA TLS_PSK_WITH_AES_128_CBC_SHA256		[Amd B] section 3.3.2
SCP SGP22	Secure communication channel with the SM-DP+ for mutual authentication	ECKA-EG	NIST P-256, brainpoolP256r1	SGP.22 FIPS PUB 186 3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639
SCP SGP22 (SCP03t)	Secure communication channel with the SM-DP+ for profile download	AES	AES: 128	SGP.02

FCS_COP.1/JC_TDES_CIPHER Cryptographic operation

FCS_COP.1.1/JC_TDES_CIPHER The TSF shall perform **[assignment: encryption and decryption]** in accordance with a specified cryptographic algorithm **[assignment: TDES 2 Keys or TDES 3 Keys with cipher modes shown below]** and cryptographic key sizes **[assignment: 112 bits for TDES 2 Keys, 168 bits for TDES 3 Keys]** that meet the following: **[assignment: FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5 standards]**.

[JCAPI3] class	Implemented algorithm	Mode
Cipher	ALG_DES_CBC_ISO9797_M1	CBC
	ALG_DES_CBC_ISO9797_M2	CBC
	ALG_DES_CBC_NOPAD	CBC

	ALG_DES_CBC_PKCS5	CBC
	ALG_DES_ECB_ISO9797_M1	ECB
	ALG_DES_ECB_ISO9797_M2	ECB
	ALG_DES_ECB_NOPAD	ECB
	ALG_DES_ECB_PKCS5	ECB

FCS_COP.1/JC_AES_CIPHER Cryptographic operation

FCS_COP.1.1/JC_AES_CIPHER The TSF shall perform **[assignment: encryption and decryption]** in accordance with a specified cryptographic algorithm **[assignment: AES with cipher modes]** and cryptographic key sizes **[assignment: 128bits]** that meet the following: **[assignment: FIPS PUB 197, NIST SP800-38A, NIST SP800-38D, ISO/IEC 9797-1, PKCS#5]**.

[JCAPI3] class	Implemented algorithm	Mode
Cipher	ALG_AES_BLOCK_128_CBC_NOPAD	CBC
	ALG_AES_BLOCK_128_ECB_NOPAD	ECB
	ALG_AES_CBC_ISO9797_M1	CBC
	ALG_AES_CBC_ISO9797_M2	CBC
	ALG_AES_CBC_PKCS5	CBC
	ALG_AES_ECB_ISO9797_M1	ECB

	ALG_AES_ECB_ISO9797_M2	ECB
	ALG_AES_ECB_PKCS5	ECB

FCS_COP.1/JC_Hash Cryptographic operation

FCS_COP.1.1/JC_Hash The TSF shall perform **[assignment: computation of a hash value]** in accordance with a specified cryptographic algorithm **[assignment: hash algorithms shown below]** and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: cryptographic standards]**.

[JCAPI3] class	Implemented algorithm	Standard
MessageDigest		
	ALG_SHA_224	FIPS 180-4
	ALG_SHA_256	FIPS 180-4
	ALG_SHA_384	FIPS 180-4
	ALG_SHA_512	FIPS 180-4

FCS_COP.1/JC_CRC Cryptographic operation

FCS_COP.1.1/CRC The TSF shall perform **[assignment: Computation of checksum of applet instance's data]** in accordance with a specified cryptographic algorithm [**assignment: CRC16**] and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: ISO/IEC 3309]**.

Application note: the related algorithms in [JCAPI3] are ALG_ISO3309_CRC16 (class Checksum of javacard.security).

FDP_RIP.1/ABORT Subset residual information protection

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

FDP_RIP.1/APDU Subset residual information protection

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

FDP_RIP.1/bArray Subset residual information protection

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

FDP_RIP.1/GlobalArray Subset residual information protection

FDP_RIP.1.1/GlobalArray [Refined]

The TSF shall ensure that any previous information content of a resource is made unavailable upon **deallocation of the resource from** the applet as a result of returning from the process method to the following objects: **a user Global Array**.

FDP_RIP.1/KEYS Subset residual information protection

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

FDP_RIP.1/TRANSIENT Subset residual information protection

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

FDP_ROL.1/FIREWALL Basic rollback

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

FDP_ROL.1.2/FIREWALL The TSF shall permit operations to be rolled back within the **scope of a select(), deselect(), process(), install() or uninstall() call, notwithstanding the restrictions given in [JCRE3], §7.7, within the bounds of the Commit Capacity ([JCRE3], §7.8), and those described in [JCAPI3].**

7.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

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

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

Refinement:

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

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

FDP_SDI.2/DATA Stored data integrity monitoring and action

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

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

FPR_UNO.1 Unobservability

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

FPT_FLS.1/JC Failure with preservation of secure state

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

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use

- **the rules defined in [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

FIA_ATD.1.1/AID The TSF shall maintain the following list of security attributes belonging to

individual users:

- **CAP File AID**,
- **Package AID**,
- **Applet's version number**,
- **Registered applet AID**,
- **Applet Selection Status**.

FIA_UID.2/AID User identification before any action

FIA_UID.2.1/AID The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1/AID User-subject binding

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

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: CAP file AID is defined during loading by the associated value and context identifier]**.

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

FMT_MTD.1/JCRE Management of TSF data

FMT_MTD.1.1/JCRE The TSF shall restrict the ability to **modify** the **list of registered applets' AIDs** to **the JCRE**.

FMT_MTD.3/JCRE Secure TSF data

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

7.2.2 INSTG Security Functional requirements

Refer the following SFRs from [PP GP], which is defined in the Global Platform Security Functional requirements in Section 7.2.6 of this ST.

- FDP_ITC.2/GP-ELF replaces FDP_ITC.2/Installer of [PP-JCS]
- FMT_SMR.1/GP replaces FMT_SMR.1/Installer of [PP-JCS]
- FPT_RCV.3/GP replaces FPT_RCV.3/Installer of [PP-JCS]
- FPT_FLS.1/GP replaces FPT_FLS.1/Installer of [PP-JCS]

7.2.3 ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

FDP_ACC.2.1/ADEL The TSF shall enforce the **ADEL access control SFP** on **S.ADEL, S.JCRE, S.JCVM, O.JAVAOBJECT, O.APPLET and O.CODE_CAP_FILE** and all operations among subjects and objects covered by the SFP.

Refinement:

The operations involved in the policy are:

- OP.DELETE_APPLET,
- OP.DELETE_CAP_FILE,
- OP.DELETE_CAP_FILE_APPLET.

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

FDP_ACF.1/ADEL Security attribute based access control

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

Subject/Object	Attributes
S.JCVM	Active Applets
S.JCRE	Selected Applet Context, Registered Applets, Resident CAP files
O.CODE_CAP_FILE	CAP file AID, AIDs of packages within a CAP file, Dependent package AID, Static References
O.APPLET	Applet Selection Status
O.JAVAOBJECT	Owner, Remote

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

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

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

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

- **R.JAVA.14 ([JCRE3], §11.3.4.29 , Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon an O.APPLET only if,**

(1) S.ADEL is currently selected,

(2) there is no instance in the context of O.APPLET that is active in any logical channel and

(3) there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance distinct from O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.

- R.JAVA.15 ([JCRE3], §11.3.4.2.110 , Multiple Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon several O.APPLET only if,

  (1) S.ADEL is currently selected,

  (2) there is no instance of any of the O.APPLET being deleted that is active in any logical channel and

  (3) there is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a CAP file P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.

- R.JAVA.16 ([JCRE3], §11.3.4.311 , Applet/Library CAP file Deletion): S.ADEL may perform OP.DELETE_CAP_FILE upon an O.CODE_CAP_FILE only if,

  (1) S.ADEL is currently selected,

  (2) no reachable O.JAVAOBJECT, from a CAP file distinct from O.CODE_CAP_FILE that is an instance of a class that belongs to O.CODE_CAP_FILE, exists on the card and

  (3) there is no resident package on the card that depends on O.CODE_CAP_FILE.

- R.JAVA.17 ([JCRE3], §11.3.4.412 , Applet CAP file and Contained Instances Deletion):S.ADEL may perform OP.DELETE_CAP_FILE_APPLET upon an O.CODE_CAP_FILE only if,

  (1) S.ADEL is currently selected,

  (2) no reachable O.JAVAOBJECT, from a CAP file distinct from O.CODE_CAP_FILE, which is an instance of a class that belongs to O.CODE_CAP_FILE exists on the card,

(3) there is no CAP file loaded on the card that depends on O.CODE_CAP_FILE, and

(4) for every O.APPLET of those being deleted it holds that: (i) there is no instance in the context of O.APPLET that is active in any logical channel and (ii) there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance not being deleted, or O.JAVAOBJECT is reachable from a CAP file not being deleted, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.

FDP_ACF.1.3/ADEL The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/ADEL The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

any subject but S.ADEL to O.CODE_PKG or O.APPLET for the purpose of deleting them from the card.

FDP_RIP.1/ADEL Subset residual information protection

FDP_RIP.1.1/ADEL The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects: **applet instances and/or CAP files when one of the deletion operations in FDP_ACC.2.1/ADEL is performed on them**.

FMT_MSA.1/ADEL Management of security attributes

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

FMT_MSA.3/ADEL Static attribute initialisation

FMT_MSA.3.1/ADEL The TSF shall enforce the **ADEL access control SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ADEL The TSF shall allow the **following role(s): none**, to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/ADEL Specification of Management Functions

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

FMT_SMR.1/ADEL Security roles

FMT_SMR.1.1/ADEL The TSF shall maintain the roles: **applet deletion manager**.

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

FPT_FLS.1/ADEL Failure with preservation of secure state

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

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

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

FPT_FLS.1/ODEL Failure with preservation of secure state

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

Application Note:

The TOE may provide additional feedback information to the card manager in case of potential security violation (see FAU_ARP.1).

7.2.6 Global Platform Security Functional requirements

FDP_ROL.1/GP Basic rollback

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

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

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

FCO_NRO.2/GP Enforced proof of origin

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

Refinement

The TSF shall be able to generate an evidence of origin at all times for 'Executable Load Files, SD/Application data and keys' received from the off-card entity (originator of transmitted data) that communicates with the card

FCO_NRO.2.2/GP The TSF shall be able to relate the **[assignment: identity]** of the originator of the information, and the **[assignment: Executable Load Files, SD/Application data and keys]** the information to which the evidence applies.

Refinement

The TSF shall be able to load 'Executable Load Files, SD/Application data and keys' to the card with associated security attributes (the identity of the originator, the destination) such that the evidence of origin can be verified.

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

FIA_AFL.1/GP Authentication failure handling

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

FIA_UAU.1/GP Timing of authentication

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

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

FDP_UIT.1/GP Basic data exchange integrity

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

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

FDP_UCT.1/GP Basic data exchange confidentiality

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

FDP_IFC.2/GP-ELF Complete information flow control

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

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

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

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

FDP_IFF.1/GP-ELF Complete information flow control

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

[assignment:

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

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, 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 only accepts ELFs whose AIDs have not been registered by TSF].**

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

FDP_IFF.1.4/GP-ELF The TSF shall explicitly authorise 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 AID of this ELF is registered in the card].**

FMT_MSA.1/GP Management of security attributes

FMT_MSA.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to restrict the ability to **[selection: [assignment: perform the actions listed in the table]]** the security attributes **[assignment: mentioned in the table]** to **[assignment: the authorised identified roles mentioned in the table]**.

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorised Identified Roles with Privileges
DELETE Executable Load File	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Executable Load File and related Application(s)	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Application	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Key	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
INSTALL	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
INSTALL [for personalisation]	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
LOAD	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
PUT KEY	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD

SELECT	OP_READY, INITIALIZED, SECURED, or ~~CARD_LOCKED (If an SD does have the Final~~ Application privilege)	ISD, AM SD, DM SD, SD with Final Application privilege
SET STATUS	OP_READY, INITIALIZED, SECURED, or ~~CARD_LOCKED~~	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, ~~CARD_LOCKED, or TERMINATED~~	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, or ~~CARD_LOCKED~~	ISD, AM SD, DM SD, SD

Table 17 GlobalPlatform Common Operations, Security Attributes, and Roles

Operations: SCP02 Commands	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
INITIALIZE UPDATE	OP_READY, INITIALIZED, SECURED~~, or CARD_LOCKED~~	None	ISD, AM SD, DM SD, SD
EXTERNAL AUTHENTICATE		C-MAC	

Table 18 SCP02 Operations, Security Attributes, and Roles

Operations: SCP80 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges

Remote File Management Commands SELECT UPDATE BINARY UPDATE RECORD SEARCH RECORD INCREASE VERIFY PIN CHANGE PIN DISABLE PIN ENABLE PIN UNBLOCK PIN DEACTIVATE FILE ACTIVATE FILE READ BINARY READ RECORD CREATE FILE DELETE FILE RESIZE FILE	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]
Remote Applet Management Commands DELETE SET STATUS INSTALL LOAD PUT KEY GET STATUS GET DATA STORE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]

Table 19 SCP80 Operations, Security Attributes, and Roles

Operations: SCP81 Command	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges

PUT KEY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, ~~CARD_LOCKED, or TERMINATED~~	None	ISD, AM SD, DM SD, SD

Table 20 SCP81 Operations, Security Attributes, and Roles

FMT_MSA.3/GP Security attribute initialization

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

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

FMT_SMR.1/GP Security roles

FMT_SMR.1.1/GP The TSF shall maintain the roles:

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

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

FMT_SMF.1/GP Specification of Management Functions

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

- **Card and Application Security Management as defined in [GPCS]: Life Cycle, Privileges, Application/SD Locking and Unlocking, Card Locking and Unlocking, Card Termination, Application Status interrogation, Card Status Interrogation, command dispatch, Operational Velocity Checking, and Tracing and Event Logging.**

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

FDP_ITC.2/GP-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: none].**

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].**

FDP_IFC.2/GP-KL Complete information flow control

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

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

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

FDP_IFF.1/GP-KL Complete information flow control

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

- Subjects: S.SD, S.OPEN
- Information: GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys
- Security attributes: card Life Cycle State, Application and SD Life Cycle states, Secure Channel Security Level, SD and Application privileges.

].

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

- **S.SD implements one or more Secure Channel Protocols, namely [selection: SCP02, 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 verify that the target application implements the personalized interface].**

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

FDP_IFF.1.4/GP-KL The TSF shall explicitly authorise 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 target application implements the personalized interface].**

FIA_UID.1/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **[assignment: SD selection, application selection, initialization of a secure channel with the card, request for data identifying the card or off-card entities]** on behalf of the user to be performed before the user is identified.

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

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.

FPT_RCV.3/GP Automated recovery without undue loss

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

FPT_RCV.3.2/GP For **[assignment: The integrity of the executable loader file was compromised during transfer;The ELF installation process was aborted;A fatal error**

occurred when linking ELF with an existing executable file] the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/GP The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **[assignment: 0% of the executable load file loaded or installed]** for loss of TSF data or objects under the control of the TSF.

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

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

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

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

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

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

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

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

FPT_FLS.1/GP Failure with preservation of secure state

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

- **S.OPEN fails to load/install an Executable Load File / Application instance.**
- **S.SD fails to load SD/Application data and keys.**
- **S.OPEN fails to verify/change the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**

- **S.SD fails to verify the security level applied to protect APDU commands.**
- **[assignment: none].**

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.**

7.2.7 Underlying platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **the test process before TOE Delivery** with the capability to store **[selection: the Initialisation Data, Pre-personalisation Data, [assignment: none]]** 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 Functional Requirements Rationale

7.3.1 SFRs for eUICC rationale

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

7.3.2 SFRs for Runtime Environment rationale

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

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

O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, OE.VERIFICATION, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION Note: ADV_ARC "non-bypassability" refinement is applicable.
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, OE.VERIFICATION, 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, OE.CODE-EVIDENCE, O.LOAD, O.NATIVE, ,
O.RE.IDENTITY	O.CARD-MANAGEMENT, O.FIREWAL, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, OE.SCP.RECOVERY, O.INSTALL, O.SID, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.OPERATE
O.RE.CODE-EXE	OE.VERIFICATION, O.FIREWALL, OE.CAP.FILEO.NATIVE

Table 21 Runtime environment objectives conversion for SFR rationale.

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

7.3.3 SFRs for Underlying platform IC rationale

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

O.IC.RECOVERY coverage: the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for recovery operations as dealt with in FPT_RCV.3/OS and FPT_RCV.4/OS, for secure state preservation against security violations as in FPT_FLS.1/Platform_services.

O.IC.SUPPORT the IC is a part of the TOE supporting TSFs of the upper layer of the TOE, especially for secure low-level cryptographic processing as in FCS_CKM.1/EC, FCS_CKM.1/GP-SCP, FCS_CKM.1/SCP-SM, FCS_COP.1/JC_TDES_MAC, FCS_COP.1/JC_AES_MAC, FCS_COP.1/JC_ECDSA_SIGN, FCS_COP.1/GP-SCP,

FCS_COP.1/JC_TDES_CIPHER, FCS_COP.1/JC_AES_CIPHER, FCS_COP.1/JC_Hash ,, FCS_COP.1/ JC_CRC

7.3.4 **SFRs dependency rationale**

SFR	CC Dependencies	Satisfied dependencies
FIA_UID.1/EXT	No dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_UAU.4/EXT	No Dependencies	
FIA_UID.1/MNO-SD	No Dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_ATD.1/Base	No Dependencies	
FIA_API.1	No Dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	No Dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP, FPT_TDC.1/SCP
FPT_TDC.1/SCP	No Dependencies	
FDP_UCT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1/GP-SCP FCS_CKM.6/SCP-SM, FCS_RNG.1
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-SM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP

	or FCS_CKM.5)	
FCS_CKM.6/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) or FCS_CKM.5)	FDP_ITC.2/SCP
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	
FCS_RNG.1	No Dependencies	
FPT_EMS.1/Base	No Dependencies	
FDP_SDI.1/Base	No Dependencies	
FDP_RIP.1/Base	No Dependencies	
FPT_FLS.1/Base	No Dependencies	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.1/RULES	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_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/ECASD, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_SMF.1/Base	No Dependencies	
FMT_SMR.1/Base	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.1/Platform_services, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS,

		FMT_SMR.1/Base, FMT_MSA.1/RAT
FCS_COP.1/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and FCS_CKM.6	FDP_ITC.2/SCP, FCS_CKM.6/Mobile_network
FCS_CKM.2/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) or FCS_CKM.5)	FDP_ITC.2/SCP
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
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, FMT_SMR.1
FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_IFC.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1/JC FDP_ACC.2/FIREWALL
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1
FMT_MSA.3/JCVM	FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM, FMT_SMR.1
FMT_SMF.1/JC	No Dependencies	
FMT_SMR.1/JC	(FIA_UID.1)	FIA_UID.2/AID
FCS_CKM.1/EC FCS_CKM.1/GP-SCP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.6)	FCS_COP.1/JC_ECDSA_SIGN FCS_COP.1/GP-SCP

		FCS_CKM.6 FCS_RNG.1
FCS_CKM.6	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1/EC FCS_CKM.1/GP-SCP
FCS_COP.1/JC_TDES_MAC FCS_COP.1/JC_AES_MAC FCS_COP.1/JC_ECDSA_SIGN FCS_COP.1/GP-SCP FCS_COP.1/JC_TDES_CIPHER FCS_COP.1/JC_AES_CIPHER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FCS_CKM.1/EC FCS_CKM.1/GP-SCP, FCS_CKM.6
FDP_RIP.1/ABORT	No Dependencies	
FDP_RIP.1/APDU	No Dependencies	
FDP_RIP.1/bArray	No Dependencies	
FDP_RIP.1/GlobalArray	No Dependencies	
FDP_RIP.1/KEYS	No Dependencies	
FDP_RIP.1/TRANSIENT	No Dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAS.1)	FAU_SAS.1
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPT_FLS.1/JC	No Dependencies	
FPT_TDC.1	No Dependencies	
FIA_ATD.1/AID	No Dependencies	
FIA_UID.2/AID	No Dependencies	
FIA_USB.1/AID	(FIA_ATD.1)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
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	FDP_ACC.2/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL

	(FMT_SMR.1), 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)	
FPT_FLS.1/ADEL	No Dependencies	
FDP_RIP.1/ODEL	No Dependencies	
FPT_FLS.1/ODEL	No Dependencies	
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_AFL.1/GP	(FIA_UAU)	FIA_UAU.1/GP
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No Dependencies	
FDP_UIT.1/GP	(FDP_ACC.1, or FDP_IFC.1) (FTP_ITC.1, or FTP_TRP.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FDP_UCT.1/GP	(FTP_ITC.1, or FTP_TRP) (FDP_ACC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FDP_IFC.2/GP-ELF	(FDP_IFF.1)	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FMT_MSA.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FMT_SMR.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/GP	No Dependencies	
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL FPT_TDC.1/GP FTP_ITC.1/GP
FTP_ITC.1/GP	No Dependencies	
FDP_IFC.2/GP-KL	FDP_IFF.1	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	(FDP_IFC.1 and FMT_MSA.3)	FDP_IFC.2/GP-KL FMT_MSA.3/GP

FIA_UID.1/GP	No Dependencies	
FPT_TDC.1/GP	No Dependencies	
FPT_RCV.3/GP	(AGD_OPE.1)	AGD_OPE.1
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF, FTP_ITC.1/GP, FPT_TDC.1/GP
FPT_FLS.1/GP	No Dependencies	
FPR_UNO.1/GP	No Dependencies	
FAU_SAS.1	No Dependencies	
FPT_RCV.3/OS	No Dependencies	
FPT_RCV.4/OS	No Dependencies	

The rationale for 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 dependencies of FCS_COP.1/JC_Hash are unsupported

Hash operation does not require any key.

- The dependencies of FCS_COP.1/JC_CRC are unsupported

CRC operations do not require any key

7.4 Rationale for the Security Assurance Requirements

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 defined in [PP-eUICC] without extension. Therefore, the rationale for Security Assurance Requirements is the same in section 6.2 in [PP-eUICC]. It is repeated here.

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

8.1.1 SF.EUICC.ProfileManagement

The SF.EUICC.ProfileManagement is responsible for the secure management of profiles throughout their lifecycle. This security function implements the controls related to profile management defined in [SGP.22] and [EUPP] including .

- Profile downloading
- Profile installation
- Profile deletion
- Profile enable and disable

8.1.2 SF.EUICC.ISDR

This SF.EUICC.ISDR is responsible for access control and management of the eUICC's internal root security domain, ensuring that only properly identified and authorized entities can perform root security domain-related operations as defined in [SGP.22].

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

8.1.3 SF.EUICC.ECASD

eUICC Controlling Authority Security Domain is responsible for secure storage of credentials to support the required Security Domains on the eUICC. The security functions follows [SGP.22] .

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

8.1.4 SF.EUICC.ISDP

This security function handles the management of the ISD-P as defined in [SGP.22]. The ISD-P is the on-card representative of the SM-DP+ and is the secure container (security domain) used to host profiles. Profile. The ISD-P is used for the Profile download and installation in collaboration with the Profile Package Interpreter for the decoding/interpretation of the received Profile Package.

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

8.1.5 SF.EUICC.PPR

This security function manages Profile Policy Rules (PPRs) as defined in [SGP.22]. The PPRs are defined by the Profile Owners and set by the SM-DP+ in the Profile Metadata.Upon downloading a profile with defined PPR, eUICC is required to follow these defined rules.

Secure management and processing of the PPRs are covered.

8.2 Runtime Environment security functions

8.2.1 SF.GP.CardContentManagement

This security function provides the capability and a dedicated flow control for loading, installing, extracting, updating the registry, selecting, and removing card content, especially executable files and application instances.

1. Core Capabilities

Lifecycle Management: Controls loading, installation, extraction, registry updates, selection, and deletion of card content (e.g., applets, executable files).

State-Based Command Enforcement: Only permits commands allowed in the smart card's current lifecycle state (e.g., INSTALLED, PERSONALIZED, SECURED). Ill-formed commands are rejected with error codes.

2. Delegated Management (DM) & Authorized Management (AM)

Delegated Management (DM): Allows third parties (e.g., mobile network operators, service providers) to manage content on the card under predefined rules.

Authorized Management (AM): Restricts management to entities with explicit authorization (e.g., the card issuer).

3. DAP Verification & Reception Tokens

Data Authentication Pattern (DAP): Ensures the integrity and authenticity of loaded content.

Content must be signed by a trusted authority (e.g., card issuer). The card cryptographically validates the content before installation. Reception Token is generated upon successful DAP verification to confirm legitimacy of the content.

4. Security Domain (SD) Privileges

Privilege-Based Access Control.

Each Security Domain (a privileged applet) holds cryptographic keys for.

Secure Channel Protocol (SCP): Encrypted communication (e.g., SCP02).

Platform Management: Authorized updates.

Operations require prior authentication (e.g., mutual authentication via SCP).

8.2.2 SF.GP.KeyManagement

Key management provides the capability and a dedicated flow control for loading keys and other sensitive data using GlobalPlatform's STORE DATA and PUT KEY APDUs (ISO 7816-4 commands) or GlobalPlatform APIs for loading and storing data and keys.
Dedicated Flow Control enforces strict sequencing (e.g., pre-authentication, key derivation, and validation before storage).

8.2.3 SF.GP.SecurityDomain

This security function manages security domains, including creation, selection, privilege setting, and deletion within the SD hierarchy. It enables the association or extradition of an application to or from a security domain to provide services (such as secure channels) to the dedicated application without sharing the related keys stored in the SD.

The function also manages key sets within security domains, including creation, deletion, importation, replacement, and deletion of keys within key sets.

Security Domains are privileged applications as defined in [GPCS], holding cryptographic keys to be used to support Secure Channel Protocol operations and/or to authorize card content management functions.

The are different types of Security Domains with dedicated privileges and associated operations: ISD Security Domain, Supplementary Security Domains and Controlling Authority Security Domains.

8.2.4 SF.GP.SecureChannel

Establishing a secure communication session is divided into initialization, operation and termination phases, and supports multiple SCP protocols (SCP02/80/81).

Trusted channels protect against unauthorized disclosure, modification, or replay. The security function ensures that incoming messages are transmitted unaltered to the corresponding Security Domain and that response messages are properly returned to the off-card entity.

Applications may use the Secure Channel Protocols supported by their associated Security Domain to securely exchange information with the off-card entity.

This security function provides APDU flow control, checking command security levels based on the Card Life Cycle and APDU type.

A Secure Channel Session is divided into three sequential phases:

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

The following services are provided by the Secure Channel:

- Entity authentication in which the card or the off-card entity proves its authenticity to the other entity through a cryptographic exchange, based on session ley generation and a dedicated flow control. For SCP80, envelope APDU shall contain secured packet structure defined in [TS 102.225] and Anti-replay mechanism is proposed using a counter defined in [TS 102.225].

- Integrity and authentication in which the receiving entity (the card or the off-card entity) ensures that the data being received from the sending entity (respectively the off-card entity or the card) came from an authenticate entity in the correct sequence and has not been altered.

- Confidentiality is which data being transmitted from the sending entity (the off-card entity or card) to the receiving entity (respectively the card or the off-card entity) is not viewable by an unauthenticated entity.

The following Secure Channel Protocols are supported by the TOE: SCP02, SCP03t, SCP80 and SCP81.

8.2.5 SF.GP.GPRegistry

The Security function provides management and access to the GlobalPlatform Registry used for:

- Store card management information.
- Store relevant application management information (AID, associated Security Domain and Privileges).
- Support card resource management data.

- Store Application Life Cycle information.
- Store card Life Cycle information.
- Track any counters associated with logs.

The content of the GlobalPlatform Registry may be accessed by administrative command or by applet using a dedicated GlobalPlatform API. Only secure values are accepted for the information stored in the GlobalPlatform registry (including Life Cycle states, Security Levels and Privileges)

8.2.6 SF.JCS.APDUBuffer

The Security function maintains a byte array buffer accessible from any applet context. This buffer is used to transfer incoming APDU header and data bytes as well as outgoing data according to [JCAPI3]. The APU class API is designed to be transport protocol independent T=0 (as defined in ISO 7816-3).

APDU buffer is a JCRE temporary entry point object where no associated reference can be stored in a variable or an array component

8.2.7 SF.JCS.ByteCodeExecution

This security function handles applet bytecode execution according to the rules defined in [JCAPI3]. The JCVM execution involves JCVM interpreter startup, bytecode execution, and the JCVM interpreter loop. The applet bytecode execution loop consists of:

- Fetching the next bytecode to be executed by the applet to make a flow control.
- Decoding the next bytecode.
- Executing the fetched bytecode.

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

8.2.8 SF.JCS.Firewall

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

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

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

8.2.9 SF.JCS.Package

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

8.2.10 SF.JCS.CryptoAPI

The Security Function offers the following cryptographic services to applets through Javacard API:

- Generation of random numbers as defined in [JCAPI3] to be used for key values or challenges during external exchanges. The RNG (Random Number Generator) is a hybrid physical random number generator conformant to [AIS31] PTG.3 conformant to [AIS31], providing enhanced backward secrecy & enhanced forward secrecy. It passes [AIS31] test procedure A.
- Encryption and decryption using TDES algorithm as defined in [JCAPI3] Cipher class. TDES 2-keys (112 bits key length) is supported.
- Encryption and decryption using AES (128bits key length) algorithm as defined in [JCAPI3] Cipher class.
- Generation of 16 bytes MAC using AES algorithm (128bits key length) in CBC mode as defined in [JCAPI3] Signature class.
- Computation of checksum CRC16 conformant with ISO3309, as defined in [JCAPI3] Checksum class. ALG_ISO3309_CRC16 are supported and implemented in a secure way.
- Data hash computation as defined in [JCAPI3] MessageDigest class.
- Generation and verification of ECDSA signatures as defined in [JCAPI3] Signature class. Elliptic curve cryptographic over GF(p) is considered here, with P ranging from 192/224/256/384 bits.

These operations are performed in a way that avoids revealing key values. If the applet specifies an algorithm that the platform does not support, the JCRE will refuse to perform the cryptographic operation and generate an exception.

8.2.11 SF.JCS.KeyManagement

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

- Key generation implemented through KeyBuilder and/or KeyPair classes :
  - ECDSA Key Pair Generation (P ranging from 192,224,256,384bits).
- Key importation and exportation is done using method protecting confidentiality and integrity of key.

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

8.2.12 SF.JCS.OwnerPIN

This security function provides applets with the capability to perform user identification and authentication using the OwnerPIN class, as defined in [JCAPI3].

It enables the creation and secure storage of a PIN in persistent memory. Access to the PIN value is restricted to secure comparisons between the stored PIN and a received parameter.

The method returns a positive result if a valid PIN has been presented during the current session. If the PIN is not blocked and the comparison is successful, the validated flag is set to true, and the try counter is set to its maximum. Otherwise, authentication fails, and the associated try counter is decreased. When the validated flag is set, it is assumed that the user is authenticated.

If the try counter reaches zero, the PIN is blocked, and further authentication is not possible until the PIN is unblocked.

8.2.13 SF.JCS.ClearResidualData

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

Secure Deletion of Packages and Applications

- Secure Deletion of Objects and , transient object at reset or allocation and persistent object are erased at allocation for new object.
- Secure Clearing of Temporary Buffers：temporary buffers (transient object, bArray object, Global Array object, APDU buffer, Cryptographic buffer) are securely cleared after their usage) are securely cleared after use, respecting their lifecycle and interface.

8.2.14 SF.JCS.ResidualInfoProtection

This security function ensures that sensitive data are locked until postponed erasure on the following operations:

Deletion of persistent and transient objects according to [JCRE3].

8.2.15 SF.JCS.RunTimeExecution

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

- Instance registration or deletion,

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

8.2.16 SF.JCS.Exception

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

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

8.2.17 SF.OS.Atomic

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

8.2.18 SF.OS.MemoryManagement

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

8.3 TSS Rationale

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

8.3.1 eUICC SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	SF.EUICC.ISDR
FIA_UAU.1/EXT	SF.EUICC.ECASD and SF.GP.SecureChannel
FIA_USB.1/EXT	SF.EUICC.ECASD and SF.GP.SecurityDomain
FIA_UAU.4/EXT	SF.EUICC.ECASD and SF.GP.SecureChannel
FIA_UID.1/MNO-SD	SF.GP.SecurityDomain
FIA_USB.1/MNO-SD	SF.GP.SecurityDomain, SF.EUICC.ISDP, SF.EUICC.ECASD
FIA_ATD.1/Base	SF.GP.SecurityDomain and SF.EUICC.ECASD
FIA_API.1.1	SF.EUICC.ECASD
FDP_IFC.1/SCP	SF.EUICC.ProfileManagement SF.GP.SecureChannel
FDP_IFF.1/SCP	SF.EUICC.ProfileManagement SF.GP.SecureChannel
FTP_ITC.1/SCP	SF.EUICC.ProfileManagement SF.GP.SecureChannel
FDP_ITC.2/SCP	SF.EUICC.ProfileManagement SF.GP.SecureChannel
FPT_TDC.1/SCP	SF.EUICC.ProfileManagement
FDP_UCT.1/SCP	SF.EUICC.ProfileManagement
FDP_UIT.1/SCP	SF.EUICC.ProfileManagement
FCS_CKM.1/SCP-SM	SF.EUICC.ProfileManagement SF.JCS.KeyManagement
FCS_CKM.2/SCP-MNO	SF.JCS.CryptoAPI SF.JCS.KeyManagement
FCS_CKM.6/SCP-SM	SF.JCS.KeyManagement
FCS_CKM.6/SCP-MNO	SF.JCS.KeyManagement
FDP_ACC.1/ISDR	SF.EUICC.ISDR
FDP_ACF.1/ISDR	SF.EUICC.ISDR
FDP_ACC.1/ECASD	SF.EUICC.ECASD
FDP_ACF.1/ECASD	SF.EUICC.ECASD
FDP_IFC.1/Platform_services	SF.EUICC.ProfileManagement
FDP_IFF.1/Platform_services	SF.EUICC.ProfileManagement
FPT_FLS.1/Platform_services	SF.EUICC.ProfileManagement
FCS_RNG.1	SF.JCS.CryptoAPI

Security Functional Requirement	Coverage by TSS Security Function(s)
FPT_EMS.1/Base	SF.JCS.CryptoAPI ,SF.JCS.KeyManagement
FDP_SDI.1/Base	SF.EUICC.ProfileManagement SF.GP.SecureChannel SF.JCS.RunTimeExecution
FDP_RIP.1/Base	SF.EUICC.ProfileManagement
FPT_FLS.1/Base	SF.EUICC.ProfileManagement
FMT_MSA.1/PLATFORM_DATA	SF.EUICC.ISDR SF.EUICC.ISDP
FMT_MSA.1/RULES	SF.EUICC.ISDR SF.EUICC.ISDP
FMT_MSA.1/CERT_KEYS	SF.EUICC.ProfileManagement
FMT_SMF.1/Base	SF.EUICC.ProfileManagement,SF.EUICC.ISDR, SF.EUICC.ISDP,SF.EUICC.ECASD, SF.EUICC.PPR
FMT_SMR.1/Base	SF.EUICC.ProfileManagement,SF.EUICC.ISDR, SF.EUICC.ISDP,SF.EUICC.ECASD, SF.EUICC.PPR
FMT_MSA.1/RAT	SF.EUICC.ISDR
FMT_MSA.3	SF.EUICC.ISDR,SF.EUICC.ISDP, SF.EUICC.ECASD
FCS_COP.1/Mobile_network	SF.JCS.CryptoAPI
FCS_CKM.2/Mobile_network	SF.JCS.CryptoAPI SF.JCS.KeyManagement
FCS_CKM.6/Mobile_network	SF.JCS.KeyManagement

8.3.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	SF.JCS.Firewall
FDP_ACF.1/FIREWALL	SF.JCS.Firewall
FDP_IFC.1/JCVM	SF.JCS.Firewall, SF.JCS.APDUBuffer
FDP_IFF.1/JCVM	SF.JCS.Firewall
FDP_RIP.1/OBJECTS	SF.JCS.ResidualInfoProtection, SF.JCS.ClearResidualData This SFR is covered by JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data)

FMT_MSA.1/JCRE	SF.JCS.RunTimeExecution covering context switch and application selection
FMT_MSA.1/JCVM	SF.JCS.ByteCodeExecution, requiring context switch for specific code execution and SF.JCS.RunTimeExecution covering context switch and modification of the Currently Active Context according to given rules
FMT_MSA.2/FIREWALL_JCVM	SF.JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/FIREWALL	SF.JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/JCVM	SF.JCS.RunTimeExecution covering object sharing.
FMT_SMF.1/JC	SF.JCS.RunTimeExecution covering context management and instance registration
FMT_SMR.1/JC	SF.JCS.RunTimeExecution covering JCVM and JCRE roles.
FCS_CKM.1/EC	SF.JCS.KeyManagement,
FCS_CKM.1/GP-SCP	SF.GP.SecureChannel
FCS_CKM.6	SF.JCS.KeyManagement
FCS_COP.1/JC_TDES_MAC	SF.JCS.CryptoAPI
FCS_COP.1/JC_AES_MAC	SF.JCS.CryptoAPI
FCS_COP.1/JC_ECDSA_SIGN	SF.JCS.CryptoAPI
FCS_COP.1/GP-SCP	SF.GP.SecureChannel
FCS_COP.1/JC_TDES_CIPHER	SF.JCS.CryptoAPI
FCS_COP.1/JC_AES_CIPHER	SF.JCS.CryptoAPI
FCS_COP.1/JC_Hash	SF.JCS.CryptoAPI
FCS_COP.1/JC_CRC	SF.JCS.CryptoAPI
FDP_RIP.1/ABORT	SF.JCS.ClearResidualData covering data erasure.
FDP_RIP.1/APDU	SF.JCS.ClearResidualData covering data erasure.
FDP_RIP.1/bArray	SF.JCS.ResidualInfoProtection, SF.JCS.ClearResidualData covering data erasure.
FDP_RIP.1/GlobalArray	SF.JCS.ClearResidualData covering data erasure.
FDP_RIP.1/KEYS	SF.JCS.ClearResidualData covering data erasure.
FDP_RIP.1/TRANSIENT	SF.JCS.ResidualInfoProtection managing the access control to transient object to be erased prior the erasure of the content in memory.

FDP_ROL.1/FIREWALL	SF.JCS.RunTimeExecution covering transaction rollback during specific operations.
FAU_ARP.1	SF.JCS.RunTimeExecution, SF.JCS.Exception,SF.JCS.Firewall, SF.OS.MemoryManagement covering exception handling with different specific operations.
FDP_SDI.2/DATA	SF.JCS.OwnerPIN,SF.JCS.KeyManagement, SF.OS.Atomic, SF.OS.MemoryManagement covering integrity handling with specific operations.
FPR_UNO.1	SF.JCS.OwnerPIN,SF.JCS.KeyManagement, SF.JCS.CryptoAPI, SF.OS.MemoryManagement covering data handling with specific operations avoiding observation.
FPT_FLS.1/JC	SF.JCS.Exception, SF.JCS.ByteCodeExecution, SF.JCS.RunTimeExecution, SF.OS.Atomic preserving a secure state when unexpected events occur during specific operations
FPT_TDC.1	SF.JCS.Package enforcing export check, CAP file translation and link specific operations.
FIA_ATD.1/AID	SF.JCS.RunTimeExecution, SF.GP.GPRegistry controlling applet registration and uninstallation.
FIA_UID.2/AID	SF.GP.GPRegistry, SF.JCS.RunTimeExecution managing user identity (package AID) during applet selection and identify associated context provided.
FIA_USB.1/AID	SF.GP.GPRegistry, SF.JCS.RunTimeExecution managing registration of each applet and associated pac kage during its installation with its AID.
FMT_MTD.1/JCRE	SF.JCS.RunTimeExecution offering services for applet registration and uninstallation managing associated access rights.
FMT_MTD.3/JCRE	SF.JCS.RunTimeExecution managing presence and legacy of AID with ISO rules.
FDP_ACC.2/ADEL	SF.GP.CardContentManagement,SF.GP.GPRegistry, SF.JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_ACF.1/ADEL	SF.GP.CardContentManagement,SF.GP.GPRegistry, SF.JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_RIP.1/ADEL	SF.GP.CardContentManagement, SF.JCS.ResidualInfoProtection checking operations to avoid access to freed resources prior to its reuse.
FMT_MSA.1/ADEL	SF.GP.GPRegistry,SF.GP.CardContentManagement, SF.JCS.RunTimeExecution responsible of checking rules concerning applet attributes, implicit and explicit selection rules prior to authorize deletion operation.

FMT_MSA.3/ADEL	SF.JCS.RunTimeExecution, SF.GP.CardContentManagement dealing with Security Attributes initialization, providing secure, restrictive default values for the security attributes of subject and objects involved in applet deletion.
FMT_SMF.1/ADEL	SF.GP.CardContentManagement,SF.GP.SecurityDomain, SF.JCS.RunTimeExecution
FMT_SMR.1/ADEL	SF.GP.SecurityDomain, maintaining the ISD and SDD roles responsible of applet deletion. SF.JCS.RunTimeExecution maintaining the JCRE role for applet uninstallation
FPT_FLS.1/ADEL	SF.GP.GPRegistry, SF.JCS.RunTimeExecution, SF.OS.Atomic preserving a secure state when unexpected events occur during package or instance deletion, managing the transaction part of the deletion operation by either rolling back, or completing it.
FDP_RIP.1/ODEL	SF.JCS.ClearResidualData, SF.OS.MemoryManagement ensuring that the content of deleted objects is erased upon the deletion, SF.JCS.ResidualInfoProtection making unavailable for disclosure upon further reallocation of the freed space.
FPT_FLS.1/ODEL	SF.JCS.RunTimeExecution, SF.OS.MemoryManagement performing memory management to release no more used memory on unreferenced objects and preserves a secure state when unexpected events occur during object deletion.
FDP_ROL.1/GP	SF.GP.CardContentManagement, SF.GP.KeyManagement, SF.OS.Atomic
FCO_NRO.2/GP	SF.GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading: * mutual authentication between the external entity (Issuer or Application provider) and the selected security Domain, including creation of a session key, * by the verification of a (chained) MAC that the Issuer or Application provider attaches to each file or data block sent, * by the erase of the session key at the end of the session.
FIA_AFL.1/GP	SF.GP.SecureChannel
FIA_UAU.1/GP	SF.JCS.RunTimeExecution, SF.GP.SecurityDomain
FIA_UAU.4/GP	SF.GP.SecureChannel
FDP_UIT.1/GP	SF.GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
FDP_UCT.1/GP	SF.GP.SecureChannel which provides confidentiality protection for sensitive data (such as secret keys).
FDP_IFC.2/GP-ELF	SF.GP.CardContentManagement managing flow control for loading and installing application instances.

FDP_IFF.1/GP-ELF	SF.GP.CardContentManagement managing flow control for loading and installing application instances.
FMT_MSA.1/GP	SF.GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.
FMT_MSA.3/GP	SF.GP.SecureChannel providing setting of the default value.
FMT_SMR.1/GP	SF.JCS.RunTimeExecution, SF.GP.SecurityDomain managing the roles: S.OPEN, issuer, application provider, verification authority and controlling authority.
FMT_SMF.1/GP	SF.GP.SecurityDomain, SF.GP.SecureChannel
FDP_ITC.2/GP-KL	SF.GP.KeyManagement
FTP_ITC.1/GP	SF.GP.SecureChannel
FDP_IFC.2/GP-KL	SF.GP.KeyManagement, SF.GP.SecurityDomain, SF.GP.SecureChannel
FDP_IFF.1/GP-KL	SF.GP.KeyManagement, SF.GP.SecurityDomain, SF.GP.SecureChannel
FIA_UID.1/GP	SF.JCS.RunTimeExecution, SF.GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
FPT_TDC.1/GP	SF.GP.CardContentManagement, SF.GP.SecureChannel, SF.GP.KeyManagement
FPT_RCV.3/GP	SF.JCS.RunTimeExecution,SF.OS.MemoryManagement,SF .GP.GPRegistry, SF.GP.CardContentManagement covering the applet instance erasure when applet instance regist ration operation fails.
FDP_ITC.2/GP-ELF	SF.JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations.
FPT_FLS.1/GP	SF.JCS.Package JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FPR_UNO.1/GP	SF.JCS.RunTimeExecution, SF.JCS.CryptoAPI
FAU_SAS.1	SF.OS.MemoryManagement
FPT_RCV.3/OS	SF.OS.Atomic
FPT_RCV.4/OS	SF.OS.MemoryManagement

9 COMPOSITION WITH IC

9.1 Statement of compatibility – Threats part

Threats	Rationale

T.Phys-Manipulation	Covered by IC evaluation
T.Phys-Probing	Considered during TOE evaluation
T.Malfunction	Considered during TOE evaluation
T.Leak-Inherent	Considered during TOE evaluation
T.Leak-Forced	Considered during TOE evaluation
T.Abuse-Func	Considered during TOE evaluation
T.RND	Covered by IC evaluation
T.Masquerade_TOE	Covered by IC evaluation

9.2 Statement of compatibility – OSPs part

OSP	Rationale
P.Process-TOE	Covered by IC evaluation
P.Crypto-Service	Covered by IC evaluation
P.Lim_Block_Loader	This policy is used to permanently shut down the Loader and prevent it from being used again, thus preventing the chip from loading illegal firmware. it is covered by ALC_IMP.1 of TOE evaluation.
P.Ctrl_Loader	This policy conditionally enables the Loader function in a secure production environment. The Loader will be permanently disabled before delivery to users. it is covered by ALC_IMP.1 of TOE evaluation.
P.Firewall	This policy is about the end-user embedded software to manage and control access to regions in memory. It is covered by the ADV_IMP.1 activity of the TOE evaluation.

9.3 Statement of compatibility – Assumptions part

Assumptions	Rationale
A.Process-Sec-IC	Considered during TOE evaluation
A.Resp-Appl	Considered during TOE evaluation

9.4 Statement of compatibility – Security objectives for the environment part

According to the definition in Appendix 1.1 of [CC-COMP], IC OEs are divided into the following groups:

IrOE: IC OE being not relevant for the current TOE.

CfPOE: IC OE being fulfilled by the current TOE automatically.

SgOE: The remaining IC OE which shall be addressed by the current TOE.

O.ENV	Rationale
OE.Resp-Appl	This objective deals with the treatment of TOE user data by the TOE itself. It is covered by the ADV_IMP.1 activity of the TOE evaluation. • CfPOE
OE.Process-Sec-IC	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation • During phases 2,3: CfPOE • During phase 4: SgOE
OE.Lim_Block_Loader	This objective is covered by the IC evaluation and by the ADV_IMP.1 activity of the TOE evaluation • During phases 3: CfPOE •
OE.Loader_Usage	This objective is covered by the IC evaluation and by the ADV_IMP.1 activity of the TOE evaluation • During phases 3: CfPOE •
OE.TOE_Auth	This objective is covered by the IC evaluation and by the ADV_IMP.1 activity of the TOE evaluation • During phases 3: CfPOE
OE.Secure_Delivery	OE.Secure_Delivery is only applicable when the IC is delivered with the Flash Loader deactivated. In the context of the TOE, the IC is delivered with the Flash Loader activated as it is used during TOE development and production. Therefore, as the OE is not applicable, it results as irrelevant for the composite TOE. IrOE

9.5 Statement of compatibility – Security objectives part

O.TOE	Rationale
O.Phys-Manipulation	Considered during TOE evaluation

	This objective maps to O.IC.SUPPORT. It provides low-level physical attack resistant function to fulfil non-bypassibility and integrity requirement in O.IC.SUPPORT.
O.Phys-Probing	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides low-level physical attack resistant function to fulfil non-bypassibility and integrity requirement in O.IC.SUPPORT.
O.Malfunction	Considered during TOE evaluation This objective maps to O.IC.Recovery. It provides low-level robustness to contributes to remain a secure state facing abnormal operation environment described in O.IC.Recovery.
O.Leak-Inherent	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides low-level physical attack resistant function to fulfil non-bypassibility and integrity requirement in O.IC.SUPPORT.
O.Leak-Forced	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides low-level physical attack resistant function to fulfil non-bypassibility and integrity requirement in O.IC.SUPPORT.
O.Abuse-Func	Covered by IC evaluation This objective aims at blocking IC test features in order to achieve non-passibility. Before IC is delivered to the TOE developer, the capabilities have already been disabled, so it is not covered in this TOE evaluation.
O.Identification	Considered during TOE evaluation This objectives maps to O.IC.PROOF_OF_IDENTITY since it provides IC identification function contributing to IC identification requirement in O.IC.PROOF_OF_IDENTITY.
O.RND	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides the low-level random number generator contributing to the TOE secure function in O.IC.SUPPORT.
O.Cap_Avail_Loader	Covered by IC evaluation This objective is about loader capability limitation. which is disabled after the TOE delivery. Therefore, it is irrelevant to the TOE evaluation.

O.Ctrl_Auth_Loader	Covered by IC evaluation This objective is about trust communication channel during OS download, whereas the loader is disabled after the TOE delivery. Therefore, it is irrelevant to the TOE evaluation.
O.Authentication	Considered in IC evaluation This objective contributes to IC identity authentication when OS update. However, OS update is out of the TOE evaluation scope. Thus, this objective is irrelevant.
O.AES	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides the AES function contributing to the TOE cryptographic function in O.IC.SUPPORT.
O.TDES	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides the TDES function contributing to the TOE cryptographic function in O.IC.SUPPORT.
O.Firewall	Covered by IC evaluation This objective is about memory separation between IC dedicated software and IC user software. After TOE is delivered, this mechanism has been enforced. Thus, it is irrelevant to the TOE evaluation.
O.FFC	Covered by IC evaluation This objective aims at FFC algorithm which is not used in the TOE.
O.RSA	Covered by IC evaluation This objective aims at RSA algorithm which is not used in the TOE.
O.ECC	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides the ECC function contributing to the TOE cryptographic function in O.IC.SUPPORT.
O.HMAC	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides the HMAC function contributing to the TOE cryptographic function in O.IC.SUPPORT.
O.Hash	Considered during TOE evaluation This objective maps to O.IC.SUPPORT. It provides the hash function contributing to the TOE secure feature in O.IC.SUPPORT.
O.MISE	Covered by IC evaluation

	This objective aims at ecure cryptographic services implemented with the MISE instructions which is not used in the TOE.

9.6 Statement of compatibility – SFRs part

IC SFRs are separated in the following groups as defined in appendix 1.1 of [CC-COMP]:

- IP_SFR: Irrelevant IC SFR not being used by the current TOE.
- RP_SFR-SERV: Relevant IC SFR being used by the current TOE to implement a security service with associated TSFI.
- RP_SFR-MECH: Relevant IC SFR being used by the current evaluation because of its security properties providing protection attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the IC.

SFR	Rationale
FCS_RNG.1/TRNG	IP_SFR-MECH This IC SFR is used to generate random number used in security mechanism to protect the TOE from SCA and FI attack.
FCS_COP.1/AES	IP_SFR This IC SFR is about hardware AES and not used by TOE
FCS_CKM.4	IP_SFR This IC SFR is not used by TOE when keys are destroyed.
FCS_COP.1/SHA2	IP_SFR This IC SFR is about SHA256 MISE algorithm and is not used in the TOE.
FCS_COP.1/ASCON	IP_SFR ASCON algorithm is not in the scope of the TOE.
FPT_TST.1	RP_SFR-MECH This IC SFR contributes to security initialization of the TOE.
FAU_SAS.1	RP_SFR-SERV This IC SFR is used to support identification function in FAU_SAS.1.
FDP_SDC.1	RP_SFR-MECH This IC SFR contributes to secure storage mechanism of the TOE against physical manipulation and probing.

FDP_SDI.2	RP_SFR-MECH This IC SFR contributes to secure storage mechanism of the TOE against physical manipulation and probing.
FDP_ACC.2/AF	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FDP_ACF.1/AF	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FMT_MSA.3/AF	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FMT_MSA.1/AF/S	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FMT_MSA.1/AF/NS	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FMT_SMF.1/AF	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FMT_SMR.1/AF	RP_SFR-MECH This IC SFR contributes to access control mechanism of the TOE against unauthorized access.
FIA_API.1	IP_SFR IP_SFR is used to enforce IC identification authentication process during OS update which is not claimed in the TOE evaluation scope.
FMT_LIM.1/Loader	IP_SFR This IC SFR contributes to limit the capability of Flash Loader, which is enforced before TOE delivery. Thus it is irrelevant to the TOE secure feature to its customers.
FMT_LIM.2/Loader	IP_SFR

	This IC SFR contributes to limit Flash Loader availability, which is enforced before TOE delivery. Thus it is irrelevant to the TOE secure feature to its customers..
FTP_ITC.1	IP_SFR This IC SFR is used to enforce secure communication between TOE and the IC during Flash image download. Since this function is completed before the TOE delivered, this SFR is irrelevant to the TOE secure feature to its customers.
FDP_ACC.1/Loader	IP_SFR This IC SFR is used to enforce Flash loader used by authorized user during Flash image download. Since this function is enforced before the TOE delivered, this SFR is irrelevant to the TOE secure feature to its customers.
FDP_ACF.1/Loader	IP_SFR This IC SFR is used to enforce Flash loader used by authorized user during Flash image download. Since this function is enforced before the TOE delivered, this SFR is irrelevant to the TOE secure feature to its customers.
FMT_MTD.1/Loader	IP_SFR This IC SFR is used to enforce the ability of authorized roles who can download Flash image. Before TOE is delivered, the Flash Loader is deactivated, so this SFR is irrelevant to the TOE secure feature to its customers.
FMT_SMR.1/Loader	IP_SFR This IC SFR is used to define the authorized roles who can operate Flash image. Before TOE is delivered, the Flash Loader is deactivated, so this SFR is irrelevant to the TOE secure feature to its customers.
FMT_SMF.1/Loader	IP_SFR This IC SFR is used to define the Flash Loader operation of authorized roles Before TOE is delivered, the Flash Loader is deactivated, so this SFR is irrelevant to the TOE secure feature to its customers.
FIA_UID.2/Loader	IP_SFR This IC SFR is used to enforce user identification before Flash image download. Before TOE is delivered, the Flash Loader is deactivated, so this

	SFR is irrelevant to the TOE secure feature to its customers.
FCS_COP.1/CS/AES	RP_SFR-SERV This IC SFR is used by TOE to implement AES algorithm in FCS_COP.1/JC_AES_CIPHER and FCS_COP.1/JC_AES_MAC.
FCS_CKM.4/CS/AES	RP_SFR-SERV This IC SFR is used by TOE when keys are destroyed.
FCS_COP.1/CS/TDES/<iter>	RP_SFR-SERV This IC SFR is used by TOE to implement AES algorithm in FCS_COP.1/JC_TDES_CIPHER and FCS_COP.1/JC_TDES_MAC.
FCS_CKM.4/CS/TDES	RP_SFR-SERV This IC SFR is used by TOE when keys are destroyed.
FCS_COP.1/CS/HMAC/<iter>	RP_SFR-SERV This IC SFR is used by TOE to implement HMAC algorithm in FCS_COP.1/GP-SCP.
FCS_COP.1/CS/FFC	IP_SFR FFC algorithm is not used in the TOE.
FCS_COP.1/CS/RSA	IP_SFR RSA algorithm is not used in the TOE.
FCS_CKM.1/CS/RSA	IP_SFR RSA algorithm is not used in the TOE.
FCS_COP.1/CS/ECC	RP_SFR-SERV This IC SFR is used by TOE to implement ECC algorithm in FCS_COP.1/JC_ECDSA_SIGN.
FCS_CKM.1/CS/ECC	RP_SFR-SERV This IC SFR contributes to implement ECC key generation in FCS_CKM.1/EC.
FCS_COP.1/CS/Hash	RP_SFR-SERV This IC SFR contributes to implement FCS_COP.1/JC_Hash.
FCS_RNG.1/CS/PTG2	RP_SFR-MECH This IC SFR contributes to implement low level security mechanism of the TOE.
FCS_RNG.1/CS/PTG3	RP_SFR-SERV

	This IC SFR contributes to implement random number generator in FCS_RNG.1.
FCS_RNG.1/CS/DRG3	IP_SFR The TOE does not involve a DRG.3 level random number generator.
FCS_RNG.1/CS/DRG4	IP_SFR The TOE does not involve a DRG.4 level random number generator.
FDP_IFC.1	RP_SFR-MECH This IC SFR contributes to protect the TOE from information leakage and physical attack.
FDP_ITT.1	RP_SFR-MECH This IC SFR contributes to protect the TOE from information leakage and physical attack.
FDP_UCT.1	RP_SFR-SERV This IC SFR is used to enforce secure communication between TOE and the IC during Flash image download.
FDP_UIT.1	RP_SFR-SERV This IC SFR is used to enforce secure communication between TOE and the IC during Flash image download.
FPT_FLS.1	RP_SFR-MECH This IC SFR contributes to protect the TOE from malfunction.
FPT_ITT.1	RP_SFR-MECH This IC SFR contributes to protect the TOE from information leakage and physical attack.
FPT_PHP.3	RP_SFR-MECH This IC SFR contributes to implement physical attack resistance mechanism to providing protection against attacks to the TOE.
FRU_FLT.2	RP_SFR-MECH This IC SFR contributes to protect the TOE from malfunction.
FMT_LIM.1	RP_SFR-MECH This IC SFR contributes sperate IC hardware from the TOE software to prevent abuse of IC functionality.
FMT_LIM.2	RP_SFR-MECH

	This IC SFR contributes sperate IC hardware from the TOE software to prevent abuse of IC functionality.

9.7 Statement of compatibility – SAR part

This ST claims the same evaluation assurance level as [PP-eUICC], i.e., EAL4 augmented with ALC_DVS.2 and AVA_VAN.5. While IC assurance level is EAL6 with augmentation ALC_FLR.1 based on [PP-84] and [PP-84] has already involved ALC_DVS.2 and AVA_VAN.5

Therefore, TOE SARs is a subset of IC SARs.