Security Target of HHSGG1620I
Version 1.1

Release 1.1, February 2026

Table of Contents

1 Introduction

1.1 Definitions

Term	Description
Application	Instance of an Executable Module after it has been installed and made selectable
Security Domain	On-card entity providing support for the control, security, and communication requirements of an off-card entity (e.g. the Profile Issuer, an Application Provider or a Controlling Authority)
RSP Servers	GSMA-defined SM-DP+ and SM-DS servers. Used to distribute a Profile to the end user

1.2 Abbreviations

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

1.3 References

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

Ref	DocNumber	Title	Version
[10]	[**PP-84**]	Security IC Platform Protection Profile with Augmentation Packages	Version 1.0
[11]	[**PP-117**]	Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile	Version 1.5
[12]	[**GPCS**]	GlobalPlatform Technology Card Specification March 2018	Version 2.3.1
[13]	**[SGP.22]**	RSP Technical Specification	Version 2.2.2
[14]	**[ST-IC]**	Public Security Target IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h G12	R 2.7
[15]	**[MILENAGE]**	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.	Version 11
[16]	**[TUAK]**	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0, release 12, December 2014. • Document 1: Algorithm specification; • Document 2: Implementers' test data; • Document 3: Design conformance test data.	Version 12.1.0
[17]	**[AIS31]**	Functionality classes and evaluation methodology for physical random number generation AIS31	Version 3.0
[18]	**[GPCS]**	Global Platform Card Specification	Version 2.3.1
[19]	**[Amd B]**	Amendment B - Remote Application Management over HTTP	Version 1.1.3
[20]	**[Amd D]**	Amendment D - Secure Channel Protocol 03	v1.2 (GPC_SPE_014)

Ref	DocNumber	Title	Version
[21]	**[JVM]**	The Java Virtual Machine Specification. Lindholm, Yellin. ISBN 0-201-43294-3	ISBN 0-201-43294-3
[22]	**[GUIDES]**	Operational user guidance of HHSGG1620I	V1.9, February 2026

2 Security Target Introduction

2.1 Security Target reference

Name	Security Target of HHSGG1620I v1.1
Version	1.1
Author	BHDC
Reference	BHDC0001
Publication date	25/02/2026

2.2 TOE reference

Product name	HHSGG1620I v1.0
Developer	BHDC
TOE Name	HHSGG1620I v1.0
Reference	HHSGG1620I

3 TOE overview

3.1 TOE description

The eUICC provides a platform for remote provisioning and subscription management as defined by the GSMA. It ensures the data is stored in a safe place and information is given to only authorize applications and people. it can be embedded onto a consumer device, but it can also be removable.

The TOE is the eUICC for Consumer Devices, it includes 3 layers, as shown in Figure 1:

- The hardware layer: Infineon SLC37 IC providing support to the platform layer. The IC is certified in Common Criteria EAL6 augmented *[ST-IC]*.
- The platform layer: eUICC OS including the eUICC GSMA Remote Provisioning composed of set of functions providing support to the application layer.
- The application layer: composed of ISD-R and ECASD privileged applications providing the remote provisioning and administration functionality, encompassing standard and sensitive applications, as well as the security domains.

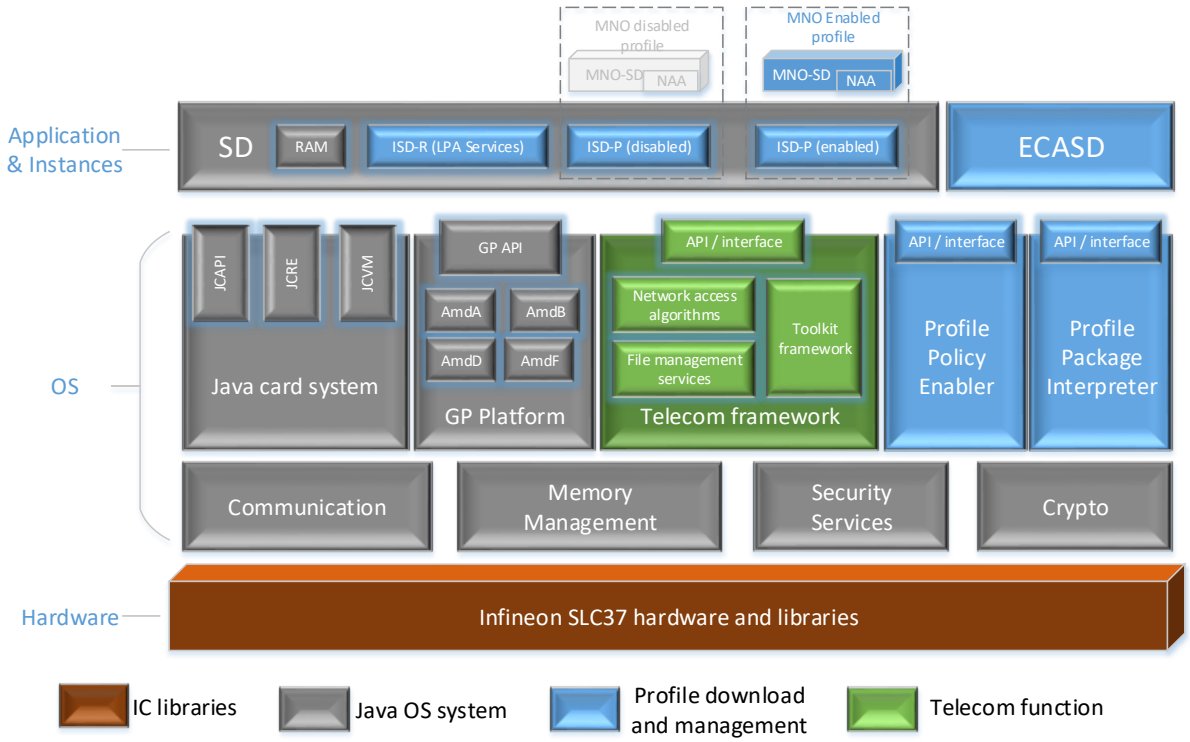

Figure 1 Platform architecture

The Profiles are not part of the TOE.

3.2 TOE type and usage

This is a composite TOE and it consists of the eUICC application layer, the eUICC open platform and the OS on top of a certified IC. Moreover, this TOE is considered to be a final product.

The eUICC is an UICC embedded in a consumer device. The eUICC will contain several MNO Profiles, each of them being associated with a given International Mobile Subscriber Identity (IMSI).The eUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile.

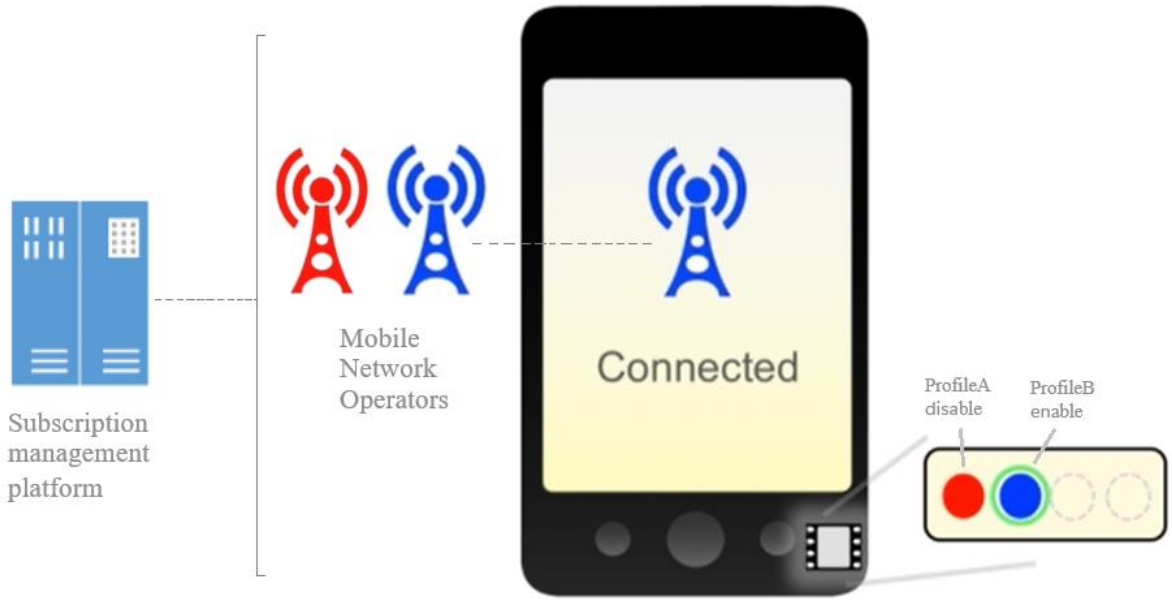

Figure 2 TOE usage scenario

The primary function of the Profile is to authenticate the validity of a Device when accessing the network. The Profile is MNO's property, and stores MNO specific information.

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

3.3 TOE life cycle

This TOE life cycle is conformant to [PP-eUICC]. The TOE life-cycle is composed of 5 phases, the delivery of the TOE to the end user is only performed in phase d.

The life cycle phases and actors of the TOE are summarized in Table 1. For complete details on the TOE life cycle, please refer to [PP-eUICC].

Phase	Name	Actor	Location
a	HHSGG1620I V1.0 SW development Development of Embedded Software	BHDC	Development site of BHDC in Beijing This site is covered by EMVCo site audit
	Development of security IC	Infineon LSI	Development site(s) stated in the IC certificate
b	HHSGG1620I V1.0 storage, pre-perso, test Security IC manufacturing and packaging	Infineon LSI	Development site(s) stated in the IC certificate

c	HHSGG1620I V1.0 storage, pre-perso, test integration of Platform Software (JCOS, GP, policy enforcement module, telecom framework) and Applications (ECASD / ISD-R)	BHDC	Production site of BHDC in Beijing This site is covered by EMVCo site audit
d	eUICC personalization Addition of applications (profiles / ISD-P)	BHDC	Production site of BHDC in Beijing This site is covered by EMVCo and GSMA SAS-UP site audit
e	Operational usage: eUICC device integration and registration, eUICC remote provisioning (optional), and eUICC usage	Profile issuer (SM-DP+ server), Device OEM	On the field, remote access to device manufacturer server

Table 1 Lifecycle stage

The actors:

- The eUICC Manufacturer (EUM), BHDC, is in charge of the eUICC embedded software development, loading, initialization, pre-personalization and personalization in its own premises and proceeds to the delivery of the product directly to customers.
- The IC manufacturer, Infineon LSI, is the developer of the eUICC secure IC.
- The Profile issuer is MNO that has privilege through its OTA Server to perform Remote Card Content Management (CCM) operations within its own profile (ISD-P). And, through its RSP servers, it also can provide Profiles to the end user, but has no privileges to manage profiles remotely without end user consent.
- The Device manufacturer is the Original Equipment Manufacturer (OEM) responsible for integrating the eUICC onto the Device.

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

Non-TOE is same than the ones mentioned in the [PP-EUICC] except for IC and RE, which are in scope of the TOE.

The Bytecode Verifier (BCV) is considered as non-TOE software component.

RMI functions are not implemented by the TOE.

3.4 TOE scope

3.4.1 Physical scope

The TOE consists of the following components:

Category	Component	Version	Delivery form
HW	IFX_CCI_000011h IFX_CCI_00001Bh IFX_CCI_00001Eh IFX_CCI_000025h	G12	Diced wafer (embedding eUICC OS)
FW	IC Firmware	80.201.04.1	Binary file in memory
SW	SCL	2.13.001	Binary file in memory
SW	ACL	3.05.002	Binary file in memory
SW	HHSGG1620I OS	1.0.0015	Software Delivered embedded on the IC
DOC	User guidance	[GUIDES]	Document Electronic document (PDF) via secure email

Table 1 TOE components

3.4.2 Logical scope

The logical boundaries are delimited (dash line in red) in Figure 3.

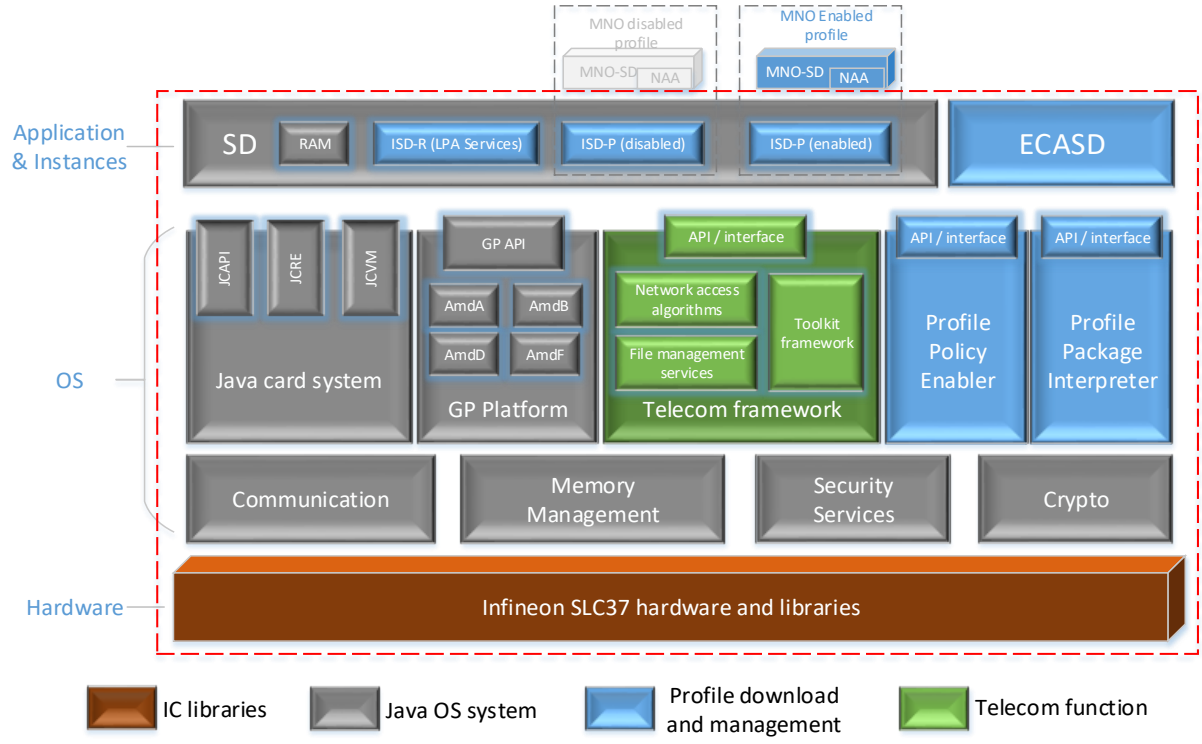

Figure 3 TOE logical boundaries

The TOE consists of the following components:

- An ISD-R, including LPA Services (a module designed to communicate with the LPAd), providing life-cycle management of profiles;
- An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication;

- ISD-P security domains, each one hosting a unique profile;
- A Telecom Framework providing network authentication algorithms, file management, toolkit framework and telecom APIs;
- A Profile Package Interpreter translating Profile Package data into an installed Profile;
- A Profile Policy Enabler which comprises Profile Policy verification and enforcement functions;
- Enforcement of the Javacard Runtime and Firewall mechanism
- Global platform2.3;
- Management and control of the communication between OS and external entities
- Security services as:
    - providing secure cryptographic primitives, algorithms and services
    - ensure the security of assets
    - generating random numbers
- The secure IC platform.

Note: The Java Card API and the GP API included within the scope of the evaluation is limited to the functionalities required by the eUICC.

The TOE supports the following cryptographic algorithms; however, their security is not guaranteed in their use: SHA1 and TDES 112 bits.

4 Conformance Claim

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

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

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

4.2 Assurance package

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

4.3 Protection Profile (PP) conformance claim

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

4.4 Conformance claim rationale

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

- Equivalent (E): The element in the ST is the same as in [PP-eUICC].
- Refinement (R): The element in the ST refines the corresponding [PP-eUICC] element. New names are given between brackets and added to the list of elements.

- Addition (A): The element is newly defined in the ST; it is not present in [PP-eUICC] and does not affect it.
- X: The element is present in [PP-eUICC].

4.4.1 Conformity of the TOE Type

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

The TOE follows the third scenario from the definition in [PP-eUICC] when the embedded eUICC is embedded in a certified IC, but the OS and JCS features have not been certified. The ST additionally fulfils the IC objectives and introduces SFRs in order to meet the objectives for the OS and JCS. This is a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

4.4.2 SPD Consistency

4.4.2.1 Assets consistency

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

Assets	PP-eUICC	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_POLICY_RULES	X	(E)
D.PROFILE_USER_CODES	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)
D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(E)
D.APP_CODE		(A): Added from [PP-JCS].
D.APP_C_DATA		(A): Added from [PP-JCS].
D.APP_I_DATA		(A): Added from [PP-JCS].
D.APP_KEYs		(A): Added from [PP-JCS].

D.PIN		(A): Added from [PP-JCS].
D.API_DATA		(A): Added from [PP-JCS].
D.CRYPTO		(A): Added from [PP-JCS].
D.JCS_CODE		(A): Added from [PP-JCS].
D.JCS_DATA		(A): Added from [PP-JCS].
D.SEC_DATA		(A): Added from [PP-JCS].

Table 3 Assets Consistency table

4.4.2.2 Users and Subjects consistency

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

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

Table 4 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 5 Subjects Consistency table

4.4.2.3 Threats consistency

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

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

Table 6 Threats Consistency table

4.4.2.4 Organizational Security Policies consistency

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

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

Table 7 Organizational Security Policies Consistency table

4.4.2.5 Assumptions consistency

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

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

Table 8 Assumptions Consistency table

4.4.3 Security Objectives Consistency

4.4.3.1 Objective for the TOE consistency

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

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

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

Table 9 Security objectives for the TOE consistency table

4.4.3.2 Objective for Environment consistency

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

OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE-EXE

Table 10 Security objectives for the Operational Environment consistency table

4.4.4 Conformity of the Requirement (SFR/SAR)

4.4.4.1 SFR consistency

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

FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
FCS_RNG.1	X	(E)
FPT_EMS.1	X	(E)
FDP_SDI.1	X	(E)
FDP_RIP.1	X	(E)
FPT_FLS.1	X	(E)
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/PPR	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1	X	(E)
FMT_SMR.1	X	(E)
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.4/Mobile_network	X	(E)
FDP_ACC.2/FIREWALL		(A): Added from [PP-JCS].
FDP_ACF.1/FIREWALL		(A): Added from [PP-JCS].
FDP_IFC.1/JCVM		(A): Added from [PP-JCS].
FDP_IFF.1/JCVM		(A): Added from [PP-JCS].
FDP_RIP.1/OBJECTS		(A): Added from [PP-JCS].
FMT_MSA.1/JCRE		(A): Added from [PP-JCS].
FMT_MSA.1/JCVM		(A): Added from [PP-JCS].
FMT_MSA.2/FIREWALL_JCVM		(A): Added from [PP-JCS].
FMT_MSA.3/FIREWALL		(A): Added from [PP-JCS].
FMT_MSA.3/JCVM		(A): Added from [PP-JCS].
FMT_SMF.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FMT_SMR.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/ECDSA FCS_CKM.1/GP-SCP		(A): Added from [PP-JCS]. Refined with iteraction.

FCS_CKM.4		(A): Added from [PP-JCS].
FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/CRC FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_COP.1/Hash FCS_COP.1/HMAC		(A): Added from [PP-JCS]. Refined with iteraction.
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/JCS		(A): Added from [PP-JCS]. Refined with iteraction.
FPT_TDC.1		(A): Added from [PP-JCS].
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ITC.2/Installer		(A): Added from [PP-JCS].
FMT_SMR.1/Installer		(A): Added from [PP-JCS].
FPT_FLS.1/Installer		(A): Added from [PP-JCS].
FPT_RCV.3/Installer		(A): Added from [PP-JCS].
FDP_ACC.2/ADEL		(A): Added from [PP-JCS].
FDP_ACF.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].
FMT_SMF.1/ADEL		(A): Added from [PP-JCS].

FMT_SMR.1/ADEL		(A): Added from [PP-JCS].
FPT_FLS.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/ODEL		(A): Added from [PP-JCS].
FCO_NRO.2/CM		(A): Added from [PP-JCS].
FDP_IFC.2/CM		(A): Added from [PP-JCS].
FDP_IFF.1/CM		(A): Added from [PP-JCS].
FDP_UIT.1/CM		(A): Added from [PP-JCS].
FIA_UID.1/CM		(A): Added from [PP-JCS].
FMT_MSA.1/CM		(A): Added from [PP-JCS].
FMT_MSA.3/CM		(A): Added from [PP-JCS].
FMT_SMF.1/CM		(A): Added from [PP-JCS].
FMT_SMR.1/CM		(A): Added from [PP-JCS].
FTP_ITC.1/CM		(A): Added from [PP-JCS].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FAU_SAS.1		(A): Added to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added to cover O.IC.RECOVERY.
FPT_RCV.4/OS		(A): Added to cover O.IC.SUPPORT.

Table 11 Security Functional Requirement consistency table

4.4.4.2 SAR consistency

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

5 Security Problem definition

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

5.1 Assets

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

5.2 Users and Subjects

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

5.3 Threats

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

Refined threats description are detailed below:

T.UNAUTHORIZED-PROFILE-MNG

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

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

T.UNAUTHORIZED-PLATFORM-MNG

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

Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA, D.PLATFORM_RAT. By altering the behaviour of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.

T.PROFILE-MNG-INTERCEPTION

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

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

T.PROFILE-MNG-ELIGIBILITY

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

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

T.UNAUTHORIZED-IDENTITY-MNG

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

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

T.IDENTITY-INTERCEPTION

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

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

T.LOGICAL-ATTACK

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

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

5.4 Organizational Security Policies

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

5.5 Assumptions

The definition of assumptions from [PP-eUICC] is not repeated here. See section 4.4.2.5 of this document for complete list of assumptions.

6 Security Objectives

This section introduces the security objectives for the TOE.

6.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [PP-eUICC] are not repeated here. See section 4.4.3 for complete list is Security Objectives for the TOE.

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

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

	○ 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 12 Security Objectives for the TOE

6.2 Security Objectives for the Operational Environment

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

6.3 Security Objectives Rationale

6.3.1 Threats

6.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

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

- O.PPE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP+ and MNO OTA Platform) will access the Security Domains functions and content;
- OE.SM-DPplus and OE.MNO protect the corresponding credentials when used offcard. The on-card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY). The authentication is supported by corresponding secure channels:
- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication with SM-DP+ and a secure channel for communication with MNO OTA Platform. These secure channels rely upon the underlying Runtime

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

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

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

T.UNAUTHORIZED-PLATFORM-MNG

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

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

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

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

T.PROFILE-MNG-INTERCEPTION

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

Consequently, the TSF ensures:

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

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

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

6.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

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

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

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

T.IDENTITY-INTERCEPTION

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

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

6.3.1.3 eUICC cloning

T.UNAUTHORIZED-eUICC

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

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

6.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

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

6.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS

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

6.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

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

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

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

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

The following objectives for the operational environment are also required:

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

T.PHYSICAL-ATTACK

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

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

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

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

6.3.2 Organizational Security Policies

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

6.3.3 Assumptions

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

6.3.4 Rationale Tables

6.3.4.1 Threats Rationale

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

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

Table 13 Threats and Security Objectives- Coverage

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

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

Table 14 Security Objectives and threats

6.3.4.2 Organizational Security Policies Rationale

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

Table 15 Organizational Security Policies and Security Objectives- Coverage

Security Objectives	Organizational Security Policies
O.PPE-PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-DPplus	
OE.MNO	
O.IC.PROOF_OF_IDENTITY	
O.IC.SUPPORT	
O.IC.RECOVERY	
O.RE.PPE-PPI	OSP.LIFE-CYCLE
O.RE.SECURE-COMM	
O.RE.API	
O.RE.DATA-CONFIDENTIALITY	
O.RE.DATA-INTEGRITY	
O.RE.IDENTITY	
O.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd	
OE.APPLICATIONS	
OE.CODE-EVIDENCE	

OE.MNO-SD	

Table 16 Security Objectives and Organizational Security Policies

6.3.4.3 Assumptions Rationale

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

Table 17 Assumptions and Security Objectives for the Operational Environment-Coverage

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

Table 18 Assumptions and Security Objectives for the Operational Environment

7 Extended Components Definition

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

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

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

8 Security Functional requirements

The following conventions are used in the definitions of the SFRs:

- The assignment operations made are marked with **bold** font.
- The selection operations are marked with underlined font.
- The refinement operations are marked with *italic* text.
- The iteration operations on SFR components are marked by a slash ('/') followed by the iteration identifier, placed after the SFR component identifier.

8.1 eUICC Security Functional Requirements

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

8.1.1 Identification and authentication

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **[assignment: 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-DPplus**
- **MNO OID is associated to U.MNO-SD, acting on behalf of U.MNO-OTA.**

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

- **Initial association of SM-DP+ OID and MNO OID requires U.SM-DPplus to be authenticated via "CERT.DPauth.ECDSA".**

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-DPplus to be authenticated via "CERT.DPauth.ECDSA"**
- **change of MNO OID is not allowed.**

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-DPplus**
- **U.MNO-OTA.**

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 U.MNO-SD AID is associated to the S.ISD-P acting on behalf of U.MNO-SD.**

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

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

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 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-DPplus;**
- **MNO OID belonging to U.MNO-OTA;**
- **AID belonging to U.MNO-SD.**

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 to an external entity.

8.1.2 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:**
  - **U.SM-DPplus and S.ISD-R**
  - **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-DPplus and S.ISD-R, with security attribute D.SECRETS**
  - **U.MNO-OTA and U.MNO-SD, with security attribute D.MNO_KEYS**
- **information: transmission of commands**.

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

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

FDP_IFF.1.3/SCP The TSF shall enforce the [assignment: **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-DPplus and S.ISD-R if it is not performed in a SCP-SGP22 secure channel**.

FTP_ITC.1/SCP Inter-TSF trusted channel

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

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

FTP_ITC.1.3/SCP The TSF shall initiate communication via the trusted channel for [assignment: **following 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-DPplus and U.MNO-OTA**
- **Downloaded objects from U.SM-DPplus 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 **ElGamal elliptic curves key agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following: **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)**
- **FRP256V1 (ANSSI ECC FRP256V1).**

Application Note 1: in this TOE, the FRP256V1 (ANSSI ECC FRP256V1) is not supported.

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: **D.MNO_KEYS are distributed during profile download via SCP03t**] that meets the following: [assignment: **SGP.22 standard**].

FCS_CKM.4/SCP-SM Cryptographic key destruction

FCS_CKM.4.1/SCP-SM The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: **wipe the buffer with random bytes**] that meets the following: [assignment: **none**].

FCS_CKM.4/SCP-MNO Cryptographic key destruction

FCS_CKM.4.1/SCP-MNO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: **deletion of the key and removing it from the memory by garbage collection**] that meets the following: [assignment: **none**].

8.1.3 Security Domains

FDP_ACC.1/ISDR Subset access control

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

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

FDP_ACF.1/ISDR Security attribute based access control

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

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

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

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

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

FDP_ACF.1.3/ISDR The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: **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,**
- **objects: S.ECASD,**
- **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"**
- **objects: S.ECASD**
- **operations:**
    - **execution of a ECASD function**
        - **Verification of the off-card entities Certificates (SM-DP+, SM-DS), provided by an ISD-R, with the CI public key (PK.CI.ECDSA)**
        - **Creation of an eUICC signature on material provided by an ISD-R.**
    - **access to output data of these functions**.
- **[assignment: 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, CERT.DP.TLS, CERT.DSauth.ECDSA, or CERT.DS.TLS, provided by an ISD-R, with the CI public key (PK.CI.ECDSA)**
- **Creation of an eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R**.

○ **[assignment: 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**].

8.1.4 Platform Services

FDP_IFC.1/Platform_services Subset information flow control

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

users/subjects:

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

information:

- **D.PROFILE_NAA_PARAMS**
- **D.PROFILE_POLICY_RULES**
- **D.PLATFORM_RAT**

operations:

- **installation of a profile**
- **PPR and RAT enforcement**
- **network authentication.**

FDP_IFF.1/Platform_services Simple security attributes

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

users/subjects:

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

information:

- **D.PROFILE_NAA_PARAMS**
- **D.PROFILE_POLICY_RULES**

- **D.PLATFORM_RAT**

operations:

- **installation of a profile**
- **PPR and RAT enforcement**
- **network authentication.**

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

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

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

8.1.5 Security management

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a [selection: hybrid physical] random number generator [selection: PTG.2 for ECC Key generation, PTG.3 for others] that implements: [assignment:

The implementation of PTG.2 is as follows:

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

The implementation of PTG.3 is as follows:

- **PTG.3.1 A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure has been detected no random numbers will be output.**
- **PTG.3.2 If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.**
- **PTG.3.3 The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test and the seeding of the DRG.3 post-processing algorithm have been finished successfully or when a defect has been detected.**
- **PTG.3.4 The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.**
- **PTG.3.5 The online test procedure checks the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-**

tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

- **PTG.3.6 The algorithmic post-processing algorithm belongs to Class DRG.3 with cryptographic state transition function and cryptographic output function, and the output data rate of the post-rocessing algorithm shall not exceed its input data rate.**]

Application note:

PTG.2 and PTG.3 are implemented according to [AIS31].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment:

The implementation of PTG.2 is as follows:

- **PTG.2.6 Test procedure A, as defined in [6] does not distinguish the internal random numbers from output sequences of an ideal RNG.**
- **PTG.2.7 The average Shannon entropy per internal random bit exceeds 0.997.**

The implementation of PTG.3 is as follows:

- **PTG.3.7 Statistical test suites cannot practically distinguish the internal random numbers from output sequences of an ideal RNG. The internal random numbers must pass test procedure A.**
- **PTG.3.8 The internal random numbers shall use PTRNG of class PTG.2 as random source for the post-processing.**]

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: **side-channels (power consumption, electromagnetic radiation)**] in excess of

[assignment: **IC limits**] enabling access to

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

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

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

FPT_EMS.1.2 The TSF shall ensure [assignment: **users**] are unable to use the following interface [assignment: **secure processor communication**] to gain access to

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

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

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

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1.1 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_POLICY_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 Subset residual information protection

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

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

FPT_FLS.1 Failure with preservation of secure state

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

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

FMT_MSA.1/PLATFORM_DATA Management of security attributes

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

- **ISD-P state**

to

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

FMT_MSA.1/PPR Management of security attributes

FMT_MSA.1.1/PPR The TSF shall enforce the **Security Channel protocol information flow SFP, ISD-P content access control SFP and ISD-R access control SFP** to restrict the ability to change_default, query, modify and delete the security attributes

- **D.PROFILE_POLICY_RULES**

to

- **S.ISD-R to change_default, via function "ES8.ConfigureISDP"**
- **S.ISD-R to query**
- **S.ISD-P to modify, via function "ES6.UpdateMetadata"**
- **S.ISD-R to delete, via function "ES10c.DeleteProfile".**

FMT_MSA.1/CERT_KEYS Management of security attributes

FMT_MSA.1.1/CERT_KEYS The TSF shall enforce the **Security Channel protocol information flow SFP, ISD-R access control SFP and 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 "ES10c.DeleteProfile"**
- **no actor for other operations.**

FMT_SMF.1 Specification of Management Functions

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

List of management functions:

- **SCP information flow control (roles used: S.ISD-R, S.ISD-P, U.SM-DPplus, U.MNO-SD, U.MNO-OTA)**
- **Platform services information flow control (roles used: S.ISD-P, S.ISD-R, S.TELECOM, S.PPE, S.PPI, U.MNO-SD)**
- **ISD-R access control (roles used: S.ISD-R, S.ISD-P, U.SM-DPplus)**
- **ISD-P content access control (roles used: S.ISD-P, U.MNO-SD, U.MNO-OTA)**
- **ECASD access control (roles used: S.ECASD, S.ISD-R)**

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **External users:**
  - **U.SM-DPplus**
  - **U.MNO-SD**
  - **U.MNO-OTA**
- **Subjects:**
  - **S.ISD-R**
  - **S.ISD-P**
  - **S.ECASD**
  - **S.PPI**
  - **S.PPE**
  - **S.TELECOM.**

FMT_SMR.1.2 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 and ISD-R access control SFP** to restrict the ability to query the security attributes

- **D.PLATFORM_RAT**

to

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

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **Security Channel Protocol information flow control SFP, ISD-P content access control SFP, ISD-R access control SFP and ECASD access 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.

8.1.6 Mobile Network authentication

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, Tuak, [selection:** no other algorithm**]** and cryptographic key sizes **according to the corresponding standard** that meet the following:

- **MILENAGE according to standard [MILENAGE] with the following restrictions:**
  - **Only use 128-bit AES as the kernel function - do not support other choices**
  - **Allow any value for the constant OP**
  - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [MILENAGE]**
- **Tuak according to [TUAK] with the following restrictions:**
  - **Allow any value of TOP**
  - **Allow multiple iterations of Keccak**
  - **Support 256-bit K as well as 128-bit**
  - **To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.**

FCS_CKM.2/Mobile_network Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: **cryptographic keys are distributed during profile download via SCP03t**] that meets the following: [assignment: **SGP.22 standard**].

FCS_CKM.4/Mobile_network Cryptographic key destruction

FCS_CKM.4.1/Mobile_network The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: **deletion of the key and removing it from the memory by garbage collection**] that meets the following: [assignment: **none**].

8.2 Runtime Environment Security Requirements

The Subjects (prefixed with an "S"), the Objects (prefixed with an "O"), Information (prefixed with an "I") are defined and described in [PP-JCS] section 7.2. Security attributes linked to these subjects, objects and information are also defined in [PP-JCS] section 7.2. Finally, Operations (prefixed with "OP") definition and description are present in [PP-JCS] section 7.2.

8.2.1 CoreLG Security Functional requirements

8.2.1.1 Firewall Policy

FDP_ACC.2/FIREWALL Complete access control

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

Refinement:

The operations involved in the policy are:

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

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

Application Note:

It should be noticed that accessing array's components of a static array, and more generally fields and methods of static objects, is an access to the corresponding O.JAVAOBJECT.

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:

Subjects	Security attributes
S.CAP_FILE	LC Selection Status
S.JCVM	Active Applets, Currently Active Context
S.JCRE	Selected Applet Context
O.JAVAOBJECT	Sharing, Context, Life Time

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

- **R.JAVA.1 ([JCRE3], §6.2.8): S.CAP_FILE may freely perform, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS upon any O.JAVAOBJECT whose Sharing attribute has value "JCRE entry point" or "global array".**
- **R.JAVA.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: FDP_ACF.1.4/FIREWALL:

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).

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: no additional information flow control SFP rules]**.

FDP_IFF.1.4/JCVM The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: 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 control 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 PERSISTENT-LifeTime 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.3.2/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/JC The TSF shall be capable of performing the following management functions:

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

FMT_SMR.1/JC Security roles

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

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

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

8.2.1.2 Application Programming Interface

FCS_CKM.1/ECDSA Cryptographic key generation

FCS_CKM.1.1/ECDSA The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: ECDSA Key Pair Generation]** and specified cryptographic key sizes **[assignment: P ranging from 160 to 521 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_256 TYPE_EC_FP_PRIVATE LENGTH_EC_FP_384 TYPE_EC_FP_PUBIC LENGTH_EC_FP_256 TYPE_EC_FP_PUBIC LENGTH_EC_FP_384
javacard.security.KeyPair	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 see the table below]** and specified cryptographic key sizes **[assignment: cryptographic key size see the table below]** that meet the following: **[assignment: cryptographic standard see the table below]**.

SCP protocol	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP02	TDES 2-keys	112 bits	[GPCS] section E.4.1
SCP03	AES	128, 192 or 256 bits	[Amd D] section 6.2.1
SCP81	AES	128 bits	[Amd B] section 3.3.2

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: see application note]** 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.

FCS_COP.1/TDES_CIPHER Cryptographic operation

FCS_COP.1.1/TDES_CIPHER The TSF shall perform **[assignment: encryption and decryption of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: Triple DES 3 Keys with cipher modes mentioned in the application note below]** and cryptographic key sizes **[assignment: 168 bits]** that meet the following: **[assignment: FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5]**.

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

Mode	Field name in [JCAPI3] Cipher class
CBC	ALG_DES_CBC_NOPAD
CBC	ALG_DES_CBC_ISO9797_M1
CBC	ALG_DES_CBC_ISO9797_M2
CBC	ALG_DES_CBC_PKCS5
ECB	ALG_DES_ECB_NOPAD
ECB	ALG_DES_ECB_ISO9797_M1

ECB	**ALG_DES_ECB_ISO9797_M2**
ECB	**ALG_DES_ECB_PKCS5**

FCS_COP.1/AES_CIPHER Cryptographic operation

FCS_COP.1.1/AES_CIPHER The TSF shall perform **[assignment: encryption and decryption of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: AES with cipher modes mentioned in the application note below]** and cryptographic key sizes **[assignment: 128, 192 and 256 bits]** that meet the following: **[assignment: FIPS PUB 197, NIST SP800-38A, NIST SP800-38D, ISO/IEC 9797-1, PKCS#5]**.

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

Mode	Field name in [JCAPI3] Cipher class
CBC	**ALG_AES_BLOCK_128_CBC_NOPAD**
CBC	**ALG_AES_CBC_ISO9797_M1**
CBC	**ALG_AES_CBC_ISO9797_M2**
CBC	**ALG_AES_CBC_PKCS5**
ECB	**ALG_AES_BLOCK_128_ECB_NOPAD**
ECB	**ALG_AES_ECB_ISO9797_M1**
ECB	**ALG_AES_ECB_ISO9797_M2**
ECB	**ALG_AES_ECB_PKCS5**
CTR	**ALG_AES_CTR**
CMAC	**ALG_AES_CMAC_128**

FCS_COP.1/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 or CRC32]** 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 and ALG_ISO3309_CRC32 (class Checksum of javacard.security).

FCS_COP.1/ECDSA_SIGN Cryptographic operation

FCS_COP.1.1/ECDSA_SIGN The TSF shall perform **[assignment: signature generation and signature verification of applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: ECDSA as mentioned in the application note below]** and cryptographic key sizes **[assignment: P ranging from 160 to 521 bits]** that meet the following: **[assignment: FIPS PUB 186-4]**.

Application note:

the following ECDSA signatures from [JCAPI3] are implemented:

Hash algorithm	Field name in [JCAPI3] Signature class
SHA256	ALG_ECDSA_SHA_256

FCS_COP.1/ECKA_EG Cryptographic operation

FCS_COP.1.1/ECKA_EG The TSF shall perform **[assignment: key agreement]** in accordance with a specified cryptographic algorithm **[assignment: ECKA-EG algorithm]** and cryptographic key sizes **[assignment: NIST P-256, brainpoolP256r1]** that meet the following: **[assignment: FIPS PUB 186-3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639]**.

FCS_COP.1/Hash Cryptographic operation

FCS_COP.1.1/Hash The TSF shall perform **[assignment: computation of a hash value for applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: see application note]** and cryptographic key sizes **[assignment: none]** that meet the following: **[assignment: see application note]**.

Application note:

the following hash algorithms from [JCAPI3] are implemented for integrity checking:

Hash algorithm	Field name in [JCAPI3] MessageDigest class	Related Standard
SHA-256	ALG_SHA_256	FIPS 180-4

FCS_COP.1/HMAC Cryptographic operation

FCS_COP.1.1/HMAC The TSF shall perform **[assignment: computation of a HMAC value for applet instance's data]** in accordance with a specified cryptographic algorithm **[assignment: HMAC with hash algorithms mentioned in the application note below]** and cryptographic key sizes **[assignment: see application note]** that meet the following: **[assignment: rfc2104]**.

Application note:

the following HMAC algorithms from [JCAPI3] are implemented Only use for integrity checking:

Hash algorithm used in HMAC computation	Field name in [JCAPI3] Signature class
SHA256	**ALG_HMAC_SHA_256**

As mentioned in [JCAPI3] the key can be of any length, but it is strongly recommended that the key is not shorter than the byte length of the hash output used in the HMAC implementation. Keys with length greater than the hash block length are first hashed with the hash algorithm used for the HMAC implementation. As required, the implementation also supports an HMAC key length equal to the length of the supported hash algorithm block size.

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.**

Application Note:

The events that provoke the de-allocation of a transient object are described in [JCRE3], §5.1. FIA_AFL

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.**

Application Note:

The allocation of a resource to the APDU buffer is typically performed as the result of a call to the process() method of an applet.

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.**

Application Note:

A resource is allocated to the bArray object when a call to an applet's install() method is performed. There is no conflict with FDP_ROL.1 here because of the bounds on the rollback mechanism (FDP_ROL.1.2/FIREWALL): the scope of the rollback does not extend outside the execution of the install() method, and the de-allocation occurs precisely right after the return of it.

FDP_RIP.1/GlobalArray Subset residual information protection

FDP_RIP.1.1/GlobalArray [*Refined*]

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

Application Note:

An array resource is allocated when a call to the API method JCSystem.makeGlobalArray is performed. The Global Array is created as a transient JCRE Entry Point Object ensuring that reference to it cannot be retained by any application. On return from the method which called JCSystem.makeGlobalArray, the array is no longer available to any applet and is deleted and the memory in use by the array is cleared and reclaimed in the next object deletion cycle.

FDP_RIP.1/KEYS Subset residual information protection

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

Application Note:

- The javacard.security & javacardx.crypto packages do provide secure interfaces to the cryptographic buffer in a transparent way. See javacard.security.KeyBuilder and Key interface of [JCAPI3].

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.**

Application Note:

- The events that provoke the de-allocation of any transient object are described in [JCRE3], §5.1.
- The clearing of CLEAR_ON_DESELECT objects is not necessarily performed when the owner of the objects is deselected. In the presence of multiselectable applet instances, CLEAR_ON_DESELECT memory segments may be attached to applets that are active in different logical channels. Multiselectable applet instances within a same CAP file must share the transient memory segment if they are concurrently active ([JCRE3], §4.3[8].

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].**

Application Note:

Transactions are a service offered by the APIs to applets. It is also used by some APIs to guarantee the atomicity of some operation. This mechanism is either implemented in Java Card platform or relies on the transaction mechanism offered by the underlying platform. Some operations of the API are not conditionally updated, as documented in [JCAPI3] (see for instance, PIN-blocking, PIN-checking, update of Transient objects).

8.2.1.3 Card Security Management

FAU_ARP.1 Security alarms

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

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

upon detection of a potential security violation.

Refinement:

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

- *CAP file inconsistency,*

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

FDP_SDI.2/DATA Stored data integrity monitoring and action

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

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

FPR_UNO.1 Unobservability

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

FPT_FLS.1/JCS Failure with preservation of secure state

FPT_FLS.1.1/JCS 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.**

Application Note:

The Java Card RE Context is the Current context when the Java Card VM begins running after a card reset ([JCRE3], §6.2.3) or after a proximity card (PICC) activation sequence ([JCRE3]). Behavior of the TOE on power loss and reset is described in [JCRE3], §3.6 and §7.1. Behavior of the TOE on RF signal loss is described in [JCRE3], §3.6.1.

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.

8.2.1.4 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.**

Refinement:

"Individual users" stand for applets.

FIA_UID.2/AID User identification before any action

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

Application Note:

- By users here it must be understood the ones associated to the CAP files (or applets) that act as subjects of policies. In the Java Card System, every action is always performed by an identified user interpreted here as the currently selected applet or the CAP file that is the subject's owner. Means of identification are provided during the loading procedure of the CAP file and the registration of applet instances.
- The role Java Card RE defined in FMT_SMR.1 is attached to an IT security function rather than to a "user" of the CC terminology. The Java Card RE does not "identify" itself to the TOE, but it is part of it.

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

FIA_USB.1.3/AID The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: The initially assigned Package AID is unchangeable]**.

FMT_MTD.1/JCRE Management of TSF data

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

Application Note:

- The installer and the Java Card RE manage other TSF data such as the applet life cycle or CAP files, but this management is implementation specific. Objects in the Java programming language may also try to query AIDs of installed applets through the lookupAID(...) API method.
- The installer, applet deletion manager or even the card manager may be granted the right to modify the list of registered applets' AIDs in specific implementations (possibly needed for installation and deletion; see #.DELETION and #.INSTALL).

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.**

8.2.2 INSTG Security Functional requirements

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

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

FDP_ITC.2.1/Installer The TSF shall enforce the **CAP FILE LOADING information flow control SFP** when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.2.3/Installer 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/Installer 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/Installer The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE:

CAP file loading is allowed only if, for each dependent package, its AID attribute is equal to a resident package AID attribute, the major version attribute associated to the dependent package file is equal to the major version attribute of the resident package and the minor version attribute is equal to or less than the minor version attribute associated to the resident package ([JCVM3], §4.5.2).

Application Note:

FDP_ITC.2.1/Installer:

- The most common importation of user data is CAP file loading and applet installation on the behalf of the installer. Security attributes consist of the shareable flag of the class component, AID and version numbers of the CAP file and the package or packages contained within the CAP file, maximal operand stack size and number of local variables for each method, and export and import components (accessibility).

FDP_ITC.2.3/Installer:

- The format of the CAP file is precisely defined in [JCVM3] specifications; it contains the user data (like applet's code and data) and the security attributes altogether. Therefore there is no association to be carried out elsewhere.

FDP_ITC.2.4/Installer:

- Each CAP file and all the packages contained within a CAP file contain a Version attribute, which is a pair of major and minor version numbers ([JCVM3], §4.5). With the AID, it describes the package defined in the CAP file. When an export file is used during preparation of a CAP file, the version numbers and AIDs of imported packages indicated in the export file are recorded in the CAP files ([JCVM3], §4.5.2): the dependent packages' Version and AID attributes allow the retrieval of these identifications. Implementation-dependent checks may occur on a case-by-case basis to check that packages are binary compatible. Packages have "package Version Numbers" ([JCVM3]) that indicate binary compatibility or incompatibility between successive implementations of a package, which directly concern this requirement.

FDP_ITC.2.5/Installer:

- A package may depend on (import or use data from) other packages already installed. This dependency is explicitly stated in the loaded package in the form of a list of package AIDs.

- The intent of this rule is to ensure the binary compatibility of the package with those already on the card ([JCVM3], §4.4).
- The installation (the invocation of an applet's install method by the installer) is implementation dependent ([JCRE3], §11.2).
- Other rules governing the installation of an applet, that is, its registration to make it SELECTable by giving it a unique AID, are also implementation dependent (see, for example, [JCRE3], §11).

FMT_SMR.1/Installer Security roles

FMT_SMR.1.1/Installer The TSF shall maintain the roles: **Installer**.

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

FPT_FLS.1/Installer Failure with preservation of secure state

FPT_FLS.1.1/Installer The TSF shall preserve a secure state when the following types of failures occur: **the installer fails to load/install a CAP file/applet as described in [JCRE3] §11.1.5.**

Application Note:

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

FPT_RCV.3/Installer Automated recovery without undue loss

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

FPT_RCV.3.2/Installer For **[assignment: a failure during load/installation of a package/applet and deletion of a package/applet/object]**, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

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

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

8.2.3 ADELG Security Functional Requirements

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

FDP_ACC.2/ADEL Complete access control

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], §11.3.4.2.1[10], 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 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.16 ([JCRE3], §11.3.4.3[11], 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], §11.3.4.4[12], 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.

Application Note:

FDP_ACF.1.2/ADEL:

- This policy introduces the notion of reachability, which provides a general means to describe objects that are referenced from a certain applet instance or CAP file.
- S.ADEL calls the "uninstall" method of the applet instance to be deleted, if implemented by the applet, to inform it of the deletion request. The order in which these calls and the dependencies checks are performed are out of the scope of this protection profile.

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.**

Application Note:

Deleted freed resources (both code and data) may be reused, depending on the way they were deleted (logically or physically). Requirements on de-allocation during applet/CAP file deletion are described in [JCRE3], §11.3.4.1, §11.3.4.2 and §11.3.4.3.

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**.

Application Note:

- The TOE may provide additional feedback information to the card manager in case of a potential security violation (see FAU_ARP.1).
- The CAP file/applet instance deletion must be atomic. The "secure state" referred to in the requirement must comply with Java Card specification ([JCRE3], §11.3.4.)

8.2.4 RMIG Security Functional Requirements

The product does not support RMI features.

8.2.5 ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

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().**

Application Note:

- Freed data resources resulting from the invocation of the method javacard.framework.JCSystem.requestObjectDeletion() may be reused. Requirements on de-allocation after the invocation of the method are described in [JCAPI3].
- There is no conflict with FDP_ROL.1 here because of the bounds on the rollback mechanism: the execution of requestObjectDeletion() is not in the scope of the rollback because it must be performed in between APDU command processing, and therefore no transaction can be in progress.

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).

8.2.6 CARG Security Functional Requirements

FCO_NRO.2/CM Enforced proof of origin

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

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

FCO_NRO.2.3/CM The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given **[assignment: at the time the Executable load files are received]**.

FDP_IFC.2/CM Complete information flow control

FDP_IFC.2.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** on **S.INSTALLER, S.BCV, S.CAD and I.APDU** and all operations that cause that information to flow to and from subjects covered by the SFP.

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

Application Note:

- The subjects covered by this policy are those involved in the loading of an application CAP file by the card through a potentially unsafe communication channel.
- The operations that make information to flow between the subjects are those enabling to send a message through and to receive a message from the communication channel linking the card to the outside world. It is assumed that any message sent through the channel as clear text can be read by an attacker. Moreover, an attacker may capture any message sent through the communication channel and send its own messages to the other subjects.
- The information controlled by the policy is the APDUs exchanged by the subjects through the communication channel linking the card and the CAD. Each of those messages contain part of an application CAP file that is required to be loaded on the card, as well as any control information used by the subjects in the communication protocol.

FDP_IFF.1/CM Simple security attributes

FDP_IFF.1.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** based on the following types of subject and information security attributes: **[assignment:**

- **Subjects:**
  - **S.CAD receiving the Card Content Management commands (through APDUs or APIs).**
- **Information:**
  - **executable load file, in case of application loading;**
  - **applications or SD privileges, in case of application installation or registry update;**
  - **personalization keys and/or certificates, in case of application or SD personalization.]**.

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

- **Runtime behavior rules defined by GlobalPlatform for:**
  - **loading (Section 9.3.5 of [GPCS]);**
  - **installation (Section 9.3.6 of [GPCS]);**
  - **extradition (Section 9.4.1 of [GPCS]);**

- **registry update (Section 9.4.2 of [GPCS]);**
- **content removal (Section 9.5 of [GPCS])].]**.

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

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

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

- **The TOE fails to verify the integrity and authenticity evidences of the application package**
- **[assignment: When at least one of those listed in the element FDP_IFF.1.2 does not hold].**

FDP_UIT.1/CM Data exchange integrity

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

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

FIA_UID.1/CM Timing of identification

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

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

FMT_MSA.1/CM Management of security attributes

FMT_MSA.1.1/CM The TSF shall enforce the **CAP FILE LOADING information flow control SFP** to restrict the ability to **[selection:** modify**]** the security attributes **[assignment:**

- **Key Set,**
- **Security Level,**
- **Secure Channel Protocol,**
- **Session Keys,**
- **Sequence Counter,**
- **ICV.] to [assignment:**

the actor associated with the according security domain:
- **The Card Issuer for ISD,**
- **The Application Provider for APSD].**

FMT_MSA.3/CM Static attribute initialisation

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

FMT_MSA.3.2/CM 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_SMF.1/CM Specification of Management Functions

FMT_SMF.1.1/CM The TSF shall be capable of performing the following management functions: **[assignment: Management functions specified in GlobalPlatform specifications:**
- **card locking (Section 9.6.3 of [GPCS])**
- **application locking and unlocking (Section 9.6.2 of [GPCS])**
- **card termination (Section 9.6.4 of [GPCS])**
- **card status interrogation (Section 9.6.6 of [GPCS])**
- **application status interrogation (Section 9.6.5 of [GPCS])].**

FMT_SMR.1/CM Security roles

FMT_SMR.1.1/CM The TSF shall maintain the roles **[assignment: Issuer, Users (e.g. AP, CA) owning SDs]**.

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

FTP_ITC.1/CM Inter-TSF trusted channel

FTP_ITC.1.1/CM 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/CM [*Refined*] The TSF shall permit ***the CAD placed in the card issuer secured environment*** to initiate communication via the trusted channel.

FTP_ITC.1.3/CM The TSF shall initiate communication via the trusted channel for **loading/installing a new application CAP file on the card.**

Application Note:

There is no dynamic CAP file loading on the Java Card platform. New CAP files can be installed on the card only on demand of the card issuer.

8.2.7 Card Content Management Security Functional requirements

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.

8.2.8 Underlying platform IC Security Functional Requirements

FAU_SAS.1 Audit Storage

FAU_SAS.1.1 The TSF shall provide **the test process before TOE Delivery** with the capability to store **[selection:** the Initialisation Data, Pre-personalisation Data, **[assignment: 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 **none,** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

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

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

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

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

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

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

FPT_RCV.4/OS Function recovery

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

8.3 Security Functional Requirements Rationale

8.3.1 SFRs for eUICC rationale

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

8.3.2 SFRs for Runtime Environment rationale

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

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

O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT
O.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE, OE.VERIFICATION, OE.CAP_FILE.

Table 19 Runtime environment objectives conversion for SFR rationale.

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

8.3.3 SFRs for Underlying platform IC rationale

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

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

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

8.3.4 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
FIA_UAU.4/EXT	No dependencies	
FIA_UID.1/MNO-SD	No dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1	No dependencies	
FIA_API.1	No dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFF.1) and (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	No dependencies	

FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP, FPT_TDC.1/SCP
FPT_TDC.1/SCP	No dependencies	
FDP_UCT.1/SCP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM, FCS_COP.1/ECKA_EG, FCS_COP.1/GP-SCP
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/SCP-MNO
FCS_CKM.4/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FCS_CKM.4/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_services	No dependencies	
FCS_RNG.1	No dependencies	
FPT_EMS.1	No dependencies	
FDP_SDI.1	No dependencies	
FDP_RIP.1	No dependencies	
FPT_FLS.1	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, FMT_SMR.1

FMT_MSA.1/PPR	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_IFC.1/SCP, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_IFC.1/SCP, FDP_ACC.1/ECASD, FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ECASD, FMT_SMR.1/CM, FMT_SMF.1/CM
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/PPR, FMT_MSA.1/CERT_KEYS, FMT_SMR.1
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/Mobile_networK
FCS_CKM.2/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/SCP-MNO
FCS_CKM.4/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	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/JC, See rationale
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_SMF.1/JC, FMT_SMR.1/JC

FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1/JC
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1/JC
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM, FMT_SMR.1/JC
FMT_SMF.1/JC	No dependencies	
FMT_SMR.1/JC	(FIA_UID.1)	FIA_UID.2/AID
FCS_CKM.1/ECDSA FCS_CKM.1/GP-SCP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/CRC FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_COP.1/Hash FCS_COP.1/HMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM, FDP_ITC.2/SCP, FCS_CKM.1/ECDSA, FCS_CKM.1/GP-SCP
FDP_RIP.1/ABORT	No dependencies	
FDP_RIP.1/APDU	No dependencies	
FDP_RIP.1/bArray	No dependencies	
FDP_RIP.1/GlobalArray	No dependencies	
FDP_RIP.1/KEYS	No dependencies	
FDP_RIP.1/TRANSIENT	No dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAS.1)	FAU_SAS.1
FDP_SDI.2/DATA	No dependencies	

FPR_UNO.1	No dependencies	
FPT_FLS.1/JCS	No dependencies	
FPT_TDC.1	No dependencies	
FIA_ATD.1/AID	No dependencies	
FIA_UID.2/AID	No dependencies	
FIA_USB.1/AID	No dependencies	
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/JC, FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ITC.2/Installer	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FPT_TDC.1, FTP_ITC.1/CM
FMT_SMR.1/Installer	(FIA_UID.1)	FIA_UID.1
FPT_FLS.1/Installer	No dependencies	
FPT_RCV.3.1/Installer	(AGD_OPE.1)	AGD_OPE.1
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL, FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	See rationale
FPT_FLS.1/ADEL	No dependencies	
FDP_RIP.1/ODEL	No dependencies	
FPT_FLS.1/ODEL	No dependencies	
FCO_NRO.2/CM	(FIA_UID.1)	FIA_UID.1/GP
FDP_IFC.2/CM	(FDP_IFF.1)	FDP_IFF.1/CM
FDP_IFF.1/CM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/CM, FMT_MSA.3/CM
FDP_UIT.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FTP_ITC.1/CM
FIA_UID.1/CM	No dependencies	

FMT_MSA.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/CM, FMT_SMR.1/CM, FMT_SMF.1/CM
FMT_MSA.3/CM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/CM, FMT_SMR.1/CM
FMT_SMF.1/CM	No dependencies	
FMT_SMR.1/CM	(FIA_UID.1)	FIA_UID.1/GP
FTP_ITC.1/CM	No dependencies	
FIA_AFL.1/GP	(FIA_UAU.1)	FIA_UAU.1/GP
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No dependencies	
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FTP_ITC.1/CM
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/CM, FTP_ITC.1/CM
FAU_SAS.1	No dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No dependencies	

Table 20 SFRs dependency rationale.

Rationale for the exclusion of dependencies:

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

8.4 Security Assurance Requirements Rationale

8.4.1 SAR - Evaluation Assurance Level Rationale

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

8.4.2 SAR - Dependency rationale.

SAR-Dependency rationale is the same than the one present in section 6.3.3.2 from [PP-eUICC].

9 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.

9.1 eUICC security functions

9.1.1 Cryptographic support (BHDC_EUICC_FCS)

The following cryptographic keys and certificates are used for common mutual authentication and protection of profile data.

SK.EUICC.ECDSA: Private key of the eUICC used to generate eUICC signatures.

otPK.EUICC.ECKA and **otSK.EUICC.ECKA**: one-time key pair used to generate the session keys (S-ENC and S-MAC) and the initial MAC chaining value.

PK.CI.ECDSA: Public key of the CI used to verify SM-DP+ Certificates (CERT.DPauth.ECDSA and CERT.DPpb.ECDSA) and Certificate Revocation List (CRL).

CERT.EUM.ECDSA: The Certificate(s) of the EUM for eUICC authentication, it signed and issued by a GSMA CI.

CERT.EUICC.ECDSA: The eUICC's Certificate(s) for eUICC authentication containing the eUICC's public key (PK.EUICC.ECDSA), it signed and issued by the EUM.

The above key generation and certificate signature are all based on elliptic curves algorithms. ECKA is used in RSP for the establishment of any session keys specified cryptographic key sizes 256 between the eUICC and the SM-DP+. ECDSA is used to compute to signatures as defined in GlobalPlatform Card Specification Amendment E. The two following sets of elliptic curve parameters preloaded by the EUM during eUICC manufacturing:

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

The MNO-SD is the part of profile, it contains the Operator's Over-The-Air (OTA) keys and provides a secure OTA channel.

NAA parameters is also the part of profile, include cryptographic keys for network authentication algorithms, this eUICC supports Milenage and TUAK network authentication algorithms.

TOE complies with the requirements of SGP.22 and Java card platform, and implements the secure management of various types of cryptographic keys, including generation, distribution, access, and destruction.

Cryptographic operation	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP02 – MAC verification or generation	TDES	112 bits	[GPCS] section E
SCP02 – Symmetric Encryption/Decryption	TDES	112 bits	[GPCS] section E
SCP03 – MAC verification or generation	CMAC AES	128, 192, or 256 bits	NIST 800 38B
SCP03 – Symmetric Encryption/Decryption	AES	128, 192, or 256 bits	NIST 800 38B
SCP80 – Secure communication channel with OTA server	TDES or AES	TDES: 112 bits, AES: 128, 192, or 256 bits	TS 102 225, TS 102 226
SCP81 – Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_AES_128_CBC_SHA256		[Amd B] section 3.3.2
SCP03t – Secure communication channel with the SM-DP+ for profile download	AES	AES: 128	SGP.02
SCP-SGP22 – Secure communication channel with the SM-DP+ for mutual authentication	ECKA-EG	NIST P- 256, brainpoo lP256r1	SGP.22 FIPS PUB 186- 3 Digital Signature Standard, BSI TR-03111 Version 1.11 RFC 5639

Table 21 Cryptographic operation

9.1.2 User data protection (BHDC_EUICC_FDP)

9.1.2.1 Security channel

The eUICC maintains secure channels between

- ISD-R and SM-DP+;
- MNO-SD and MNO OTA Platform.

Once these secure channels are built, all commands are transmitted in secure channels. Then the TOE can ensure at any time:

- that incoming messages are properly provided unaltered to the corresponding Security Domain;
- that any response messages are properly returned to the off-card entity.

The secure channels between ISD-R and SM-DP+ use SCP-SGP22 secure channels. According to SGP.22, mutual authentication is performed first. Once authenticated, the remote entities shall negotiate session keys for further communication, and session keys are generated using Perfect Forward Secrecy.

The eUICC can ensure:

- Not reveal any private data to an unauthenticated Server.
- Not generate any signed material before having authenticated the Server.

The secure channels between MNO-SD and MNO OTA Platform use SCP80 or SCP81 secure channels. And OTA keys are distributed along with the profile.

9.1.2.2 Security domains

ECASD

ECASD is responsible for secure storage of credentials required to support the required Security Domains on the eUICC. Credentials include CERT.EUICC.ECDSA, CERT.EUM.ECDSA, SK.EUICC.ECDSA and PK.CI.ECDSA.

The ECASD provide the following services only for the ISD-R:

- eUICC signature creation on material provided by an ISD-R
- Verification of the off-card entities Certificates (e.g. SM-DP+), provided by an ISD-R, with the CI public key (PK.CI.ECDSA)

ISD-R

The ISD-R is responsible for the creation of new ISD-Ps and lifecycle management of all ISD-Ps. The ISD-R is used for the Profile download and installation, in collaboration with the Profile Package Interpreter for the decoding/interpretation of the received Profile Package, and with an ISD-P as a target.

The LPA Services is the subset of ISD-R functionalities that provide the necessary access to the services and data required by LPA.

ISD-P

The ISD-P is a secure container (Security Domain) for the hosting of a Profile. The ISD-P is also used for updating the Profile Metadata on behalf of the MNO.

The ISD-P hosts a unique Profile. A Profile component shall not have any visibility of, or access to, components outside its ISD-P. An ISD-P shall not have any visibility of, or access to, any other ISD-P.

MNO-SD

The MNO-SD is the part of the Profile as the on-card representative of the Operator. It contains the MNO Over-The-Air (OTA) keys and provides a secure OTA channel to the Operator's OTA Platform.

9.1.2.3 Platform services

Platform services include the Profile Policy Enabler (PPE), the Profile Package Interpreter (PPI) and Telecom Framework. And only ISD-R, ISD-P and MNO-SD may be authorized to access PPE, PPI and Telecom Framework.

9.1.3 Identification and authentication (BHDC_EUICC_FIA)

Users must be successfully identified before performing any security-controlled action, TOE can identify users by the following Identifiers.

- SM-DP+'s Identifier is the SM-DP+ OID
- MNO-OTA platform's Identifier is the MNO OID
- MNO-SD's Identifier is the AID

The SM-DP+ binds Protected Profile Packages to the respective EID and securely downloads these Bound Profile Packages to the LPA of the respective eUICC. These operations shall be based on a secure channel and therefore mutual authentication is required. eUICC shall authenticate SM-DP+ using CERT.DPauth.ECDSA. SM-DP+ shall authenticate eUICC using CERT.EUICC.ECDSA and CERT.EUM.ECDSA.

The MNO-SD is the on-card representative of the MNO-OTA Platform. In order to perform operations such as PPR update based on a secure channel, MNO-OTA Platform also need to be authenticated via SCP80/81 using the keyset loaded in the MNO profile.

In addition, TOE has provided relevant algorithms and interfaces to perform the above identification and authentication.

9.1.4 Security management (BHDC_EUICC_FMT)

9.1.4.1 Security attributes

TOE has some security attributes, and the access to security attributes shall be protected and restricted.

The eUICC life-cycle state of the ISD-P security domain must be modified by ISD-R via interface functions. The ISD-P states include ENABLED, DISABLED, INSTALLED and SELECTABLE. ISD-R can modify ISD-P state from "INSTALLED" to "SELECTABLE" via function "ES8.ConfigureISDP", from " DISABLED " to "ENABLED" via function "ES10c. ENABLED", from "ENABLED" to "DISABLED" via function "ES10c.DisableProfile".

The Profile Policy Rules are associated to a given ISD-P and are used by the TOE to assess whether an ISD-P disabling or deletion is authorized. This security attribute can only be modified by ISD-P via function "ES6.UpdateMetadata", deleted by ISD-R via function "ES10c.DeleteProfile".

All other security attributes, like those above, must be accessed in accordance with the SGP.22 standard.

9.1.4.2 Security roles and security functions

Users and subjects are the security roles of the RSP ecosystem. Users are entities external to the TOE that may access its services or interfaces. Subjects are specific parts of the TOE performing specific operations.

Users include U.SM-DPplus, U.MNO-OTA and U.MNO-SD. Subjects include S.ISD-R, ISD-Ps, S.ISD-P, S.ECASD, S.PPI, S.PPE and S.TELECOM. TOE security functions shall maintain these roles, and be able to associate users with subjects. List of security functions:

- SCP information flow control
- Platform services information flow control
- ISD-R access control
- ISD-P content access control
- ECASD access control

9.1.5 Protection of the TSF (BHDC_EUICC_FPT)

The RSP ecosystem provides the corresponding error or failure handling mechanism, and the eUICC performs as required when an error or failure occurs.

On any error during the processing of a Profile Element, the Profile installation shall be stopped and the ISD-P and all the related Profile Components shall be deleted. Any failure shall be indicated by an `installFailedDueToDataMismatch` error. The secure state will not be changed.

The Profile Policy Enabler on the eUICC has two functions:

- Verification that a Profile containing PPRs is authorised by the RAT, if the verification results in the Profile not being allowed, then the Profile installation shall be rejected and a Profile Installation Result shall be generated and returned to the LPA.
- Enforcement of the PPRs of a Profile when a Local Profile Management Operation is requested upon this Profile. If any failure occurs, the eUICC terminates the command with preservation of secure state.

Error handling mechanism also preserves a secure state when the following types of failures occur:

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

9.1.6 Trusted path/channels (BHDC_EUICC_FTP)

In terms of channels, as described in the section 9.1.2.1 Secure Channels, the secure channels to SM-DP+ must be SCP-SGP22 secure channels. SCP80 or SCP81 must be provided to build secure channels to MNO OTA Platform.

In terms of commands, all commands are transmitted based on the above secure channels.

9.2 Runtime Environment security functions

9.2.1 Security warning function (BHDC_FAU)

The TOE has the ability to throw exceptions for potential safety hazard events during operation, and initialize the TOE system and data. Specific potential safety hazard events are detailed below:

a) a CAP file does not match, returning an alert message;

b) input errors encounter in bytecode operands, throwing exceptions;

c) the life cycle of the applet does not match, returning an alert message;

d) an exception occurs during transaction processing, returning an alert message and performing a transaction rollback;

e) a violation of the firewall policy or the Java Card Virtual Machine security policy occurs, throwing an exception;

f) there is an array out of bounds, throwing an exception;

g) resources are invalid, throwing an exception;

h) other runtime errors related to small application failures, such as uncaught exceptions, return thrown exceptions;

i) the command is wrong, throw an exception;

j) entering wrong PIN values returns an alert message, and if the password entry fails three times in a row, it will be password locked;

k) entering wrong PUK values returns an alarm message after password locking, and PUK will be locked after 10 times of error;

l) entering wrong ADM values returns an alarm message;

m) the Card contact or the voltage is abnormal, throwing an exception.

9.2.2 Key support function (BHDC_FCS)

The following keys are used in this card:

1) PIN: TOE provides a personal authentication key, PIN, which is used as a general user authentication verification and can be assigned different privileges. The password characters acceptable to TOE are taken from the hexadecimal number, and the length of the password is 1-8 bytes.

(2) Java Card GP Security Domain Root Key: TOE has four groups of GP security domain keys. Each group has three keys, which are used for GP download application related operations. TOE stipulates that the GP security domain key characters are taken from hexadecimal numbers, and the length of the passphrase is 16 bytes. The algorithm specified according to the actual application uses all 16 bytes of the selected key.

(3) Java Card 0348 Key: TOE supports up to 16 groups of 0348 keys, with up to 3 keys in each group, which are used for 0348 download application operations. TOE specifies that the 0348 key characters are taken from hexadecimal numbers.

Algorithms utilized by this card:

3DES: Used for data encryption/decryption and MAC calculation. Algorithm mode can be CBC or ECB. The card automatically selects DES/3DES algorithm when key length is 168 bits.

All keys and passphrases in TOE are generated confidentially and securely in the encryption machine. The encryption machine does not provide an interface for obtaining the plaintext of the keys, and none of the key values can be exported from the encryption machine. The keys for the personalization process are loaded with the personalization device automatically decrypted and written to the TOE in a secure environment to ensure that they cannot be stolen by an intermediary. Writing to the TOE requires successful authentication with the old key before the key content can be modified.

TOE in line with JCAPI3.0.2 specification implements the classes and their operations defined in the JAVA card security package and crypto package.

TOE's Security package mainly implements the following functions:

1) the realization of key management of different kinds of encryption algorithms, including generation, distribution, access, destruction and so on;

2) key establishment function;

3) data hash calculation;

4) random number generation;

5) Data signing using encryption keys;

6) session key interaction.

TOE's crypto package includes the key encryption class and the cipher class. The key can be realized in a secure end-to-end way of updating, encryption and decryption algorithms.

The main algorithms implemented in the crypto package include: DES, 3DES, etc. The algorithm modes include CBC, ECB, Pad and no Pad in different ways.

9.2.3 User data protection function (BHDC_FDP)

9.2.3.1 State of safety and safety conditions

The security status refers to the security level of the card at present, and there are different security statuses in the main control directory and the current directory of the card. The security state of each application directory does not affect each other and does not affect the security state of the main control directory. The security state of the current directory can only be changed after the password of the current directory has been verified correctly or after successful external authentication.

A security condition is a security state that must be achieved when a certain operation is performed on a file. Security conditions are realized by mapping them to access conditions, whose establishment is determined when the file is created. The security conditions of the file can only be established if it reaches a certain security state, and follows a certain data format. An operation can be performed only if the security state fulfills the requirements of the security condition. This means that if a file security condition is Always, operations on the file are not subject to security restrictions. If the file security condition is Never, no operations are allowed on that file. In addition to Always and Never, different levels of access conditions are defined and mapped using different PIN indexes.

The security state can be changed by means of both checking the password and external authentication. The transition from any one security state to another can be realized by means of changing the security state. After authentication failure, the security state before authentication remains unchanged when the card is not locked. Similarly, keep the original security state unchanged after performing other operations (such as read/write files, write or modify the key and password) fail.

The TOE can determine whether to accept the access based on the current security state, and the security level of the accessed object, in order to control the flow of information. The security policy is enforced within the card, and access to card data is only allowed through the TOE. The security policy cannot be bypassed.

9.2.3.2 Phase security management

TOE is managed in stages according to the different stages of the card. The main stages of TOE are divided into: R&D stage, production and personalization stage, and use stage. The R&D phase is managed in accordance with the relevant management regulations. The following focuses on the card security management of TOE's production and personalization phases as well as the usage phase.

There is a GP life cycle status byte within TOE that identifies the security stage that the card is currently in, and this flag is valid for any period of time. Many of the processes of card life cycle transition are irreversible.

The card life cycle breakdown includes the following states:

1) OP_READY

2) INITIALIZED

3) SECURED

4) CARD_LOCKED

5) TERMINATED

Among them, OP_READY and INITIALIZED are applicable to the pre-personalization and personalization stages; SECURED, CARD_LOCKED and TERMINATED are applicable to the card usage stage.

(1) Card production and personalization stage

1) Smart card embedded software download

Empty cards first download the embedded software program. Generation of embedded software programs that can be downloaded must be generated using special software and special keys provided by the chip supplier, using the FlashLoader program in the chip ROM.

2) Pre-personalized card

After the card program is loaded, the card is pre-personalized. The pre-personalization process mainly involves allocating space in the memory area, installing the application, creating the file data required by the application, defining the personalization key and managing the Java status. The personalization key memory can only be written once and cannot be read out. After the card is pre-personalized, the life cycle switches to the INITIALIZED state.

3) Personalized card

The card needs to be verified by the personalization key before personalization. The personalization process mainly involves the writing of various passwords and application data for the card. The generation of all keys in the card is done externally. After the card is personalized, the life cycle switches to the SECURED state. The switch from the INITIALIZED state to the SECURED state is unidirectional and irreversible.

After entering the SECURED state, the card enters the use phase. In this phase, most of the card's standby commands, i.e., private/management commands, are forbidden to be used.

The significance of the parameters of the individual commands (such as create file) in the SECURED state and the personalized stage are different even if they can be used in the SECURED state. This also indicates that all standby commands and their parameters used in the personalization phase are not available in the usage phase.

（2）Card use phase

Cards have three states during the usage phase: SECURED, CARD_LOCKED, and TERMINATED. SECURED and CARD_LOCKED states can be directly converted to TERMINATED state. SECURED and CARD_LOCKED are interchangeable. But the transition from CARD_LOCKED state to TERMINATED state is unidirectional and irreversible.

When a card is in the SECURED state, all operations on the card must be controlled by the card issuer's established security policy. After power-on reset, the card automatically selects the master control file and the default security state, and clears or sets default values for various data variables and object. If the card has been accidentally powered down or other accidental data inconsistencies in the storage area before this reset, it is also necessary to carry out operations related to the recovery of data in the storage area. Before the user selects the application in the card, the card ISD is responsible for card management (including: installation and deletion of small applications, etc.), and the management operation needs to comply with the relevant security requirements of the ISD. After the user selects the application, the selected application is responsible for the management of the application.

The card can only be unlocked by the authorized administrator after it is locked. Once the card is terminated, it is impossible to re-activate it.

Different commands can be executed in different life cycles on the TOE. See the table below for details.

Life cycle / Command	OP READY	INITIALIZED	SECURED	CARD LOCKED	TERMINATED
DELETE Application	√	√	√		
GET DATA	√	√	√	√	√
GET STATUS	√	√	√	√	
INSTALL(for load)	√	√	√		
INSTALL(for make selectable)	√	√	√		
PUT KEY	√	√	√		

SELECT	√	√	√	√	
SET STATUS	√	√	√	√	
STORE DATA	√	√	√		

Table 22 Commands in different life cycle state

9.2.3.3 User data entry with security attributes

When TOE installs a package, the installation data conforms to the CAP format, which contains user data, the AID and version number of the package, and the AID of the applet in the CAP file. The CAP file conforms to the definition of the JCVM standard. Consistent interpretation of data security attributes is ensured by the package AID and version number during installation. During the package loading process, if the package AID on which the currently downloaded package has a dependency is not found on the card, or the version number does not match, the loading process will return an error.

9.2.3.4 Firewall

TOE is equipped with applet firewall function, which automatically performs security check at runtime to realize security isolation between applets and shared access to data objects. The lifecycle of a JAVA applet instance on the card starts when it is successfully registered in JCRE and ends when it is successfully deleted by the applet deletion manager. During the real-time operation of the card, JCRE instantiates, selects, deselects, and executes operations on the applet through the install, select, deselect, and process methods. There can be multiple packages in the card, and each package may contain multiple applets. The firewall divides the object system of a Java card into separate protected object spaces called contexts. JCRE assigns and manages a context for each Java API package, which is shared by all instances of the applet within the package. The firewall is able to efficiently isolate applets under different contexts, and makes it impossible for an applet to access another applet under different context without providing shared access to the interfaces. There is no firewall between small application instances in the same package, which means that one small application instance can access the objects of another small application instance in the same package. At installation, JCRE assigns a context for each Java API package, represented by one byte, where the higher four bits indicate the package ID, and the lower four bits indicate the applet ID. JCRE has its own context, which has special system priorities. JCRE context is 0, and can access any small application instance of the context. The one-byte variable represents the currently active context, where the high four bits represent the currently active context's package ID, and the low four bits represent the currently active context's applet ID. At any

given time, there can only be one active context, which is either a JCRE context or the context of a small application.

9.2.3.5 Transaction and atom

In order to protect the consistency and security of data, TOE can perform atomic operations when updating permanent objects, classes or arrays stored in non-volatile memory in the JAVA card system, and can perform transactions for processes containing multiple update operations. That is, the entire update process is atomic, and either all updates are successful, or none of them are successful. The transaction should only contain permanent objects, and temporary objects and global arrays are not included in the transaction. If the update operation in the transaction is unsuccessful, the entire transaction is rolled back.

9.2.3.6 Installation

TOE supports the installation of CAP-formatted files conforming to the JAVA 3.0.2 specification. TOE loads and installs packages and small application data through a secure channel with trusted entities outside the card. During the loading process, the packages are divided into fixed-size blocks, and the P1 and P2 parameters of the LOAD command are used to ensure the order of the loading block transfers, so that the entire loading process is correct and complete.

9.2.3.7 Deletion

TOE supports small application instance deletion and object deletion compliance with the JAVA CARD 3.0.2 specification.

9.2.3.8 Subset residual information protection

The TOE, when allocating resources to JAVA arrays, APDU objects, numeric objects, temporary objects, key-related objects, class instances and arrays, any reference instances of objects created during abort interactions, resources released by deleted packages or small application instances, objects owned by the context of the small application instance that triggered the execution of the javacard.framework.JCSystem.requestObjectDeletion() method, regardless of whether the resources to be allocated are unallocated or reclaimed after allocation, content initialization is performed to ensure that the previous content of the allocated resources is not reusable.

9.2.4 Identification and authentication functions (BHDC_FIA)

In TOE, administrators and general users have different passwords and different

privileges, and they are distinguished into different security roles.

Users are allowed to perform actions that do not require authentication or identification and to make password entries before they are authenticated or identified. Following the GP specification, TOE uses secure channel authentication for user identification. For actions controlled by security functions, the user is required to have been successfully identified before TOE can be used, otherwise no information can be fed back to the user.

TOE stores and manages each package, registered applet and its related information, such as the CAP file AID, package AID, applet version number, the AID of each registered applet, and whether a registered applet is the currently selected program for execution. The AID of an applet must be recognized before any action can be taken on it. The user's security attributes are associated with the package AID during download and loading.

9.2.5 Security management function (BHDC_FMT)

9.2.5.1 Security function data

The security function data of JCRE on TOE is the list of registered applet AIDs. The length of AIDs is required to be 5-16 bytes. The installer and the applet deletion manager have the right to modify the list of AIDs of registered applets.

The security function data of GP in TOE is the static key used to establish the security channel, which can be modified by the Put Key command. There are four groups of GP security domain keys in TOE, and each group has three keys. It is stipulated that the key characters are taken from the hexadecimal number, and the length is 16 bytes.

9.2.5.2 Security attribute

The security attribute of JCRE in TOE is the active context, and the context security attribute can be modified by selecting the applet. The active context needs to meet the requirements of JCRE and JCVM specifications and satisfy the requirement of being in the range of one byte (0x00~0xff). The registered applets need to satisfy the requirement of being in the range of 5~16 bytes. The list of activated applets indicates the currently activated applets on each logical channel, with two states: unactivated and activated.

The security attribute of GP in TOE is the static key used to establish the secure channel, which can be added or modified by the Put Key command.

The security attribute of CMGR in TOE is the life cycle of GP, which can be modified by the Set Status command. The GP life cycle is divided into five stages: OP READY, INITIALIZED, SECURED, CARD LOCKED and TERMINATED.

9.2.5.3 Withdrawal rule

TOE performs different commands in different life cycles, and the operations performed in a specific cycle can be revoked until the next cycle.

9.2.5.4 Security role

The TOE security feature maintains various security roles and associates the users with these roles.

9.2.6 TSF protective function (BHDC_FPT)

(1) The security functions provided by the hardware chip are as follows:

1) The chip used by the TOE contains a MED (Memory Encryption and Decryption Unit) module. The MED unit encrypts and decrypts the data in-line when accessing the contents of the memory data (RAM, ROM, FLASH) in order to realize the protection of the memory data units.

2) The chip used in TOE contains multiple sensors and filters to prevent attacks by voltage, frequency and light, and has the ability to resist power attacks.

3) The chip used in TOE contains MPU (Memory Management Unit) module, which can realize the mapping between physical address and logical address. The access of code and data can be realized by using the logical address to access the physical address. It realizes the segmented access to code and data by providing access privilege grading mode to protect the code and data. That is, at one time, the code and data segments accessible to different levels of privileged users are different.

4) In order to ensure the randomness of code execution time, the chip supports random timing jitter function, so that the same code is executed at different times each time.

(2) The security features provided by the embedded software are as follows:

1) TOE has a different time period for each access to the sensitive information in the card, which can ensure that the operation of the sensitive information cannot be observed.

2) TOE can continue to complete the operation through the mechanism of power-down protection in case of reset or power-down, so that the card reaches the security state of successful operation. If the operation fails, it can be rolled back to restore to the security state before the operation. Within the security control range (4608 bytes) of the transaction operation and power-down protection, it ensures that the security function data or object is restored to the initial security state without excessive loss (i. e., restore the data to the pre-operation value to ensure overall data consistency).

3) TOE in the whole IC card memory, there is firewall protection between different applications, and different applications cannot access security data to each other. The applications are realized to be physically and logically isolated from each other. TOE separates the various TSF security domains by the execution context during execution.

4) TOE is able to interpret CAP files, bytecode and data parameters when sharing data with other trusted entities, and it is able to interpret data using appropriate specifications and rules for data from other trusted entities.

5) TOE will perform self-tests during startup initialization to ensure the correct operation of security functions. When writing or modifying the key, with the Put Key command, the command can be encrypted or with MAC checksum to ensure the integrity of the data.

6) Power-down recovery: TOE generates an update status flag before updating the data in the storage area, indicating whether the data has been updated completely and successfully. Before updating the Flash data, the new data will be backed up in a dedicated area of Flash, and any unexpected situation such as power failure or backup failure during the backup process will not affect the original data in the storage area in any way. After successful backup, it starts to update the data in the storage area. If power failure or other unexpected accidents occurs at this time, the embedded software automatically judges the data update flag bit during the next power-on or reset, and writes the data in the backup area into the storage area to complete the update. This data update process effectively ensures the integrity of the data in the storage area. Meanwhile, the registers that save the security status are cleared after power-down, and all security certifications must be re-executed.

9.2.7 Trusted channel (BHDC_FTP)

TOE can provide a secure communication channel between the card and the off-card entity during an application session, which ensures that the card communicates securely with the off-card entity. A secure channel session consists of three parts in sequence: secure channel initialization, secure channel operation, and secure channel termination. The off-card entity is authenticated by the card through the process of initializing the secure channel session and ensures that it is the authenticated entity that is communicating with the card. If any of the steps in the authentication process fails, the entire process is initialized and restarted. Secure channel operation is the exchange of data between a card application and an entity outside the card under the cryptographic protection of a secure channel session. Secure channel termination occurs in two situations, when the card or off-card entity determines that further communication is no longer necessary, and when the card or off-card entity is not allowed to establish a secure channel session.

To specifically implement secure communication channels, TOE supports Secure Channel Protocol 02 (SCP02). Both protocols provide three levels of security assurance: mutual authentication of card and off-card entities, integrity and proof of data origin, and data privacy.

TOE uses the GP Security Domain (ISD) root key for secure channel protocol session key production and operations. The data operation processes and the algorithms used for session key computation, data encryption and decryption, as well as the generation of MACs and checksums, vary depending on the type of secure channel protocol and the type of protocol parameters. The main algorithms used include DES and 3DES, and the algorithm modes ECB and CBC. The specific protocol definitions are in accordance with the relevant sections of the GP specification.

9.3 TSS Rationale

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

9.3.1 eUICC SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	This SFR is covered by BHDC_EUICC_FIA
FIA_UAU.1/EXT	This SFR is covered by BHDC_EUICC_FIA
FIA_USB.1/EXT	This SFR is covered by BHDC_EUICC_FIA
FIA_UAU.4/EXT	This SFR is covered by BHDC_EUICC_FIA
FIA_UID.1/MNO-SD	This SFR is covered by BHDC_EUICC_FIA
FIA_USB.1/MNO-SD	This SFR is covered by BHDC_EUICC_FIA
FIA_ATD.1	This SFR is covered by BHDC_EUICC_FIA
FIA_API.1.1	This SFR is covered by BHDC_EUICC_FIA
FDP_IFC.1/SCP	This SFR is covered by BHDC_EUICC_FDP
FDP_IFF.1/SCP	This SFR is covered by BHDC_EUICC_FDP
FTP_ITC.1/SCP	This SFR is covered by BHDC_EUICC_FDP
FDP_ITC.2/SCP	This SFR is covered by BHDC_EUICC_FDP
FPT_TDC.1/SCP	This SFR is covered by BHDC_EUICC_FDP
FDP_UCT.1/SCP	This SFR is covered by BHDC_EUICC_FDP
FDP_UIT.1/SCP	This SFR is covered by BHDC_EUICC_FDP
FCS_CKM.1/SCP-SM	This SFR is covered by BHDC_EUICC_FCS
FCS_CKM.2/SCP-MNO	This SFR is covered by BHDC_EUICC_FCS
FCS_CKM.4/SCP-SM	This SFR is covered by BHDC_EUICC_FCS
FCS_CKM.4/SCP-MNO	This SFR is covered by BHDC_EUICC_FCS

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.1/ISDR	This SFR is covered by BHDC_EUICC_FDP
FDP_ACF.1/ISDR	This SFR is covered by BHDC_EUICC_FDP
FDP_ACC.1/ECASD	This SFR is covered by BHDC_EUICC_FDP
FDP_ACF.1/ECASD	This SFR is covered by BHDC_EUICC_FDP
FDP_IFC.1/Platform_services	This SFR is covered by BHDC_EUICC_FDP
FDP_IFF.1/Platform_services	This SFR is covered by BHDC_EUICC_FDP
FPT_FLS.1/Platform_services	This SFR is covered by BHDC_EUICC_FDP
FCS_RNG.1	This SFR is covered by BHDC_EUICC_FCS
FPT_EMS.1	This SFR is covered by BHDC_FPT
FDP_SDI.1	This SFR is covered by BHDC_EUICC_FDP
FDP_RIP.1	This SFR is covered by BHDC_EUICC_FDP
FPT_FLS.1	This SFR is covered by BHDC_EUICC_FPT
FMT_MSA.1/PLATFORM_DATA	This SFR is covered by BHDC_EUICC_FMT
FMT_MSA.1/PPR	This SFR is covered by BHDC_EUICC_FMT
FMT_MSA.1/CERT_KEYS	This SFR is covered by BHDC_EUICC_FMT
FMT_SMF.1	This SFR is covered by BHDC_EUICC_FMT
FMT_SMR.1	This SFR is covered by BHDC_EUICC_FMT
FMT_MSA.1/RAT	This SFR is covered by BHDC_EUICC_FMT
FMT_MSA.3	This SFR is covered by BHDC_EUICC_FMT
FCS_COP.1/Mobile_network	This SFR is covered by BHDC_EUICC_FCS
FCS_CKM.2/Mobile_network	This SFR is covered by BHDC_EUICC_FCS
FCS_CKM.4/Mobile_network	This SFR is covered by BHDC_EUICC_FCS

Table 23 eUICC SFRs coverage

9.3.2 Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	This SFR is covered by BHDC_FDP
FDP_ACF.1/FIREWALL	This SFR is covered by BHDC_FDP
FDP_IFC.1/JCVM	This SFR is covered by BHDC_FDP
FDP_IFF.1/JCVM	This SFR is covered by BHDC_FDP
FDP_RIP.1/OBJECTS	This SFR is covered by BHDC_FDP
FMT_MSA.1/JCRE	This SFR is covered by BHDC_FDP and BHDC_FMT
FMT_MSA.1/JCVM	This SFR is covered by BHDC_FMT
FMT_MSA.2/FIREWALL_JCVM	This SFR is covered by BHDC_FMT

FMT_MSA.3/FIREWALL	This SFR is covered by BHDC_FMT
FMT_MSA.3/JCVM	This SFR is covered by BHDC_FMT
FMT_SMF.1/JC	This SFR is covered by BHDC_FMT
FMT_SMR.1/JC	This SFR is covered by BHDC_FMT
FCS_CKM.1	This SFR is covered by BHDC_FCS
FCS_CKM.4	This SFR is covered by BHDC_FCS
FCS_COP.1	This SFR is covered by BHDC_FCS
FDP_RIP.1/ABORT	This SFR is covered by BHDC_FDP
FDP_RIP.1/APDU	This SFR is covered by BHDC_FDP
FDP_RIP.1/bArray	This SFR is covered by BHDC_FDP
FDP_RIP.1/GlobalArray	This SFR is covered by BHDC_FDP
FDP_RIP.1/KEYS	This SFR is covered by BHDC_FDP
FDP_RIP.1/TRANSIENT	This SFR is covered by BHDC_FDP
FDP_ROL.1/FIREWALL	This SFR is covered by BHDC_FDP
FAU_ARP.1	This SFR is covered by BHDC_FAU
FDP_SDI.2/DATA	This SFR is covered by BHDC_FDP
FPR_UNO.1	This SFR is covered by BHDC_FPT
FPT_FLS.1/JCS	This SFR is covered by BHDC_FDP and BHDC_FPT
FPT_TDC.1	This SFR is covered by BHDC_FPT
FIA_ATD.1/AID	This SFR is covered by BHDC_FIA
FIA_UID.2/AID	This SFR is covered by BHDC_FIA
FIA_USB.1/AID	This SFR is covered by BHDC_FIA
FMT_MTD.1/JCRE	This SFR is covered by BHDC_FMT
FMT_MTD.3/JCRE	This SFR is covered by BHDC_FMT
FDP_ITC.2/Installer	This SFR is covered by BHDC_FDP
FMT_SMR.1/Installer	This SFR is covered by BHDC_FMT
FPT_FLS.1/Installer	This SFR is covered by BHDC_FPT
FPT_RCV.3.1/Installer	This SFR is covered by BHDC_FPT
FDP_ACC.2/ADEL	This SFR is covered by BHDC_FDP
FDP_ACF.1/ADEL	This SFR is covered by BHDC_FDP
FDP_RIP.1/ADEL	This SFR is covered by BHDC_FDP
FMT_MSA.1/ADEL	This SFR is covered by BHDC_FMT
FMT_MSA.3/ADEL	This SFR is covered by BHDC_FMT
FMT_SMF.1/ADEL	This SFR is covered by BHDC_FMT
FMT_SMR.1/ADEL	This SFR is covered by BHDC_FMT

FPT_FLS.1/ADEL	This SFR is covered by BHDC_FPT
FDP_RIP.1/ODEL	This SFR is covered by BHDC_FDP
FPT_FLS.1/ODEL	This SFR is covered by BHDC_FPT
FCO_NRO.2/CM	This SFR is covered by BHDC_FTP.
FDP_IFC.2/CM	This SFR is covered by BHDC_FDP
FDP_IFF.1/CM	This SFR is covered by BHDC_FDP
FDP_UIT.1/CM	This SFR is covered by BHDC_FDP
FIA_UID.1/CM	This SFR is covered by BHDC_FIA
FMT_MSA.1/CM	This SFR is covered by BHDC_FMT
FMT_MSA.3/CM	This SFR is covered by BHDC_FMT
FMT_SMF.1/CM	This SFR is covered by BHDC_FMT
FMT_SMR.1/CM	This SFR is covered by BHDC_FMT
FTP_ITC.1/CM	This SFR is covered by BHDC_FTP
FIA_AFL.1/GP	This SFR is covered by BHDC_FAU
FIA_UAU.1/GP	This SFR is covered by BHDC_FIA
FIA_UAU.4/GP	This SFR is covered by BHDC_FIA
FDP_UIT.1/GP	This SFR is covered by BHDC_FTP
FDP_UCT.1/GP	This SFR is covered by BHDC_FTP
FAU_SAS.1	This SFR is covered by BHDC_FAU
FPT_RCV.3/OS	This SFR is covered by BHDC_FPT
FPT_RCV.4/OS	This SFR is covered by BHDC_FPT

Table 24 Runtime Environment SFRs coverage

10 IC Composition

The current TOE is a composite product relaying on a certified undelaying platform. This platform is a chipset compliant to [PP-84] and identified with Cert-ID: BSI-DSZ-CC-1025-V6-2024.

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

10.1 Statement of compatibility – Threats part

IC threats	Rationale
T.Leak-Inherent	Considered during TOE evaluation
T.Phys-Probing	Considered during TOE evaluation
T.Malfunction	Considered during TOE evaluation
T.Phys-Manipulation	Covered by IC evaluation

T.Leak-Forced	Covered by IC evaluation
T.Abuse-Func	Considered during TOE evaluation
T.RND	Covered by IC evaluation
T.Mem-Access	Considered during TOE evaluation
T.Masquerade_TOE	Covered by IC evaluation
T.Open_Samples_Diffusion	Considered during TOE evaluation

Table 25 IC threats

10.2 Statement of compatibility – OSPs part

IC OSPs	Rationale
P.Process-TOE	Covered by IC evaluation
P.Lim_Block_Loader	Considered during TOE evaluation
P.Ctlr_loader	Considered during TOE evaluation
P.Add-Functions	Considered during TOE evaluation
P.Crypto-Service	Considered during TOE evaluation

Table 26 IC OSPs

10.3 Statement of compatibility – Assumptions part

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

Table 27 IC Assumptions

10.4 Statement of compatibility – Security objectives part

IC Security objectives	Rationale
O.Phys-Probing	Considered during TOE evaluation
O.Malfunction	Considered during TOE evaluation
O.Phys-Manipulation	Considered during TOE evaluation
O.Leak-Forced	Covered by IC evaluation
O.Abuse-Func	Considered during TOE evaluation
O.Identification	Considered during TOE evaluation
O.RND	Covered by IC evaluation
O.Mem-Access	Considered during TOE evaluation
O.Cap_Avail_Loader	Considered during TOE evaluation
O.Ctrl_Auth_Loader	Considered during TOE evaluation

O.TDES	Covered by IC evaluation
O.AES	Covered by IC evaluation
O.Authentication	Considered during TOE evaluation
O.Prot_TSF_Confidentiality	Considered during TOE evaluation
O.Add-Functions	Covered by IC evaluation
O.Leak-Inherent	Considered during TOE evaluation

Table 28 IC Security objectives

10.5 Statement of compatibility – Security objectives for the environment part

IC OEs are separated in the following groups:

- **IrOE**: The objectives for the environment being not relevant for the Composite-ST, e.g. the objectives for the environment about the developing and manufacturing phases of the platform.
- **CfPOE**: The objectives for the environment being fulfilled by the Composite-ST automatically. Such objectives of the environment of the Platform-ST can always be assigned to the TOE security objectives of the Composite-ST. Due to this fact they will be fulfilled either by the Composite-SFR or by the Composite-SAR automatically.
- **SgOE**: The remaining Objectives for the environment of the Platform-ST belonging neither to the group IrOE nor CfPOE. Exactly this group makes up the significant objectives for the environment for the Composite-ST, which shall be addressed in the Composite-ST.

IC OEs	Rationale
OE.Resp-Appl	Considered during TOE evaluation CfPOE
OE.Lim_Block_Loader	Considered during TOE evaluation CfPOE
OE.Loader_Usage	Considered during TOE evaluation CfPOE
OE.TOE_Auth	Considered during TOE evaluation CfPOE
OE.Process-Sec-IC	Considered during TOE evaluation CfPOE

Table 29 IC OEs

10.6 Statement of compatibility – SFRs part

The SFR are categorized according the following types:

- 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.

IC SFRs	Rationale
FPT_FLS.1	RP_SFR-MECH
FRU_FLT.2	RP_SFR-MECH
FMT_LIM.1	RP_SFR-MECH
FMT_LIM.2	RP_SFR-MECH
FAU_SAS.1	RP_SFR-SERV
FDP_SDC.1	RP_SFR-MECH
FDP_SDI.2	RP_SFR-MECH
FPT_PHP.3	RP_SFR-MECH
FDP_ITT.1	RP_SFR-SERV
FPT_ITT.1	IP_SFR
FDP_IFC.1	RP_SFR-SERV
FCS_RNG.1/HPRG	RP_SFR-SERV
FCS_RNG.1/TRNG	RP_SFR-SERV
FCS_RNG.1/DRNG	IP_SFR
FCS_RNG.1/KSG	IP_SFR
FDP_ACC.1	RP_SFR-SERV
FDP_ACF.1	RP_SFR-SERV
FMT_MSA.1	RP_SFR-SERV
FMT_MSA.3	RP_SFR-SERV
FMT_SMF.1	RP_SFR-SERV
FCS_COP.1/TDES	RP_SFR-SERV
FCS_COP.1/TDSCL	IP_SFR
FCS_COP.1/AES	RP_SFR-SERV
FCS_COP.1/AESCL	RP_SFR-SERV
FCS_COP.1/CMAC	RP_SFR-SERV
FCS_COP.1/RMAC	IP_SFR
FCS_COP.1/RSA-1	IP_SFR
FCS_COP.1/RSA-2	IP_SFR
FCS_COP.1/RSA-3	IP_SFR
FCS_COP.1/ECDSA-1	RP_SFR-SERV
FCS_COP.1/ECDSA-2	RP_SFR-SERV
FCS_COP.1/ECDSA-3	RP_SFR-SERV

FCS_COP.1/ECDH-1	RP_SFR-SERV
FCS_COP.1/ECDH-2	RP_SFR-SERV
FCS_COP.1/ECDH-3	RP_SFR-SERV
FCS_COP.1/CCL	IP_SFR
FCS_CKM.1/RSA-1	IP_SFR
FCS_CKM.1/RSA-2	IP_SFR
FCS_CKM.1/RSA-3	IP_SFR
FCS_CKM.1/EC-1	RP_SFR-SERV
FCS_CKM.1/EC-2	RP_SFR-SERV
FCS_CKM.1/EC-3	RP_SFR-SERV
FCS_CKM.1/CCL	IP_SFR
FCS_CKM.4/TDES	RP_SFR-SERV
FCS_CKM.4/AES	RP_SFR-SERV
FCS_CKM.4/CCL	IP_SFR
FMT_LIM.1/Loader	IP_SFRoe.r
FMT_LIM.2/Loader	IP_SFR
FTP_ITC.1	RP_SFR-SERV
FDP_UCT.1	RP_SFR-SERV
FDP_UIT.1	RP_SFR-SERV
FDP_ACC.1/Loader	IP_SFR
FDP_ACF.1/Loader	IP_SFR
FIA_API.1	RP_SFR-SERV
FPT_TST.2	IP_SFR

Table 30 IC SFRs

Annex A Document History

Version	Date	Description of the modification
0.1	02/01/2025	Initial draft of Security Target
0.2	12/02/2025	Add 8.3.4 SFRs dependency rationale and 8.4 Security Assurance Requirements Rationale
0.3	26/03/2025	Minor modifications
0.4	31/03/2025	Minor modifications
0.5	01/04/2025	Minor modifications

0.6	25/04/2025	Minor modifications
0.7	27/05/2025	Minor modifications
0.8	31/10/2025	Minor modifications
0.9	31/12/2025	Minor modifications
1.0	04/02/2026	Minor modifications
1.1	25/02/2026	Minor modifications