eUICC V1.0 with MCOS V3.8 on

CIU98N70 Secure Element Security Target

Version 1.0

CEC Huada Electronic Design Co., Ltd.

2025

REVISION HISTORY

Version	Date	Author	Remark
0.1	08/05/2025	[HED]	First draft release
0.2	29/05/2025	[HED]	1. Revised chapter 1.3.2 to remove Bootloader, HCI, GMI1.3 software modules from the TOE software architecture diagram, which are not in the scope of TOE. In addition, added GP2.3.1 AmdA and AmdF, which are implemented in the TOE software. 2. OS Upgrade Security Functional requirements are elaborated separately as chapter 6.2.8. 3. Revise the "FAU_SAS.1 Audit Storage" in section 6.2.9, the Initialization Data, Pre-personalization Data are stored in the flash of CIU98N70, not in the ROM. 4. Revise section 6.3.4 "Rationale for the exclusion of dependencies", remove the description of "FMT_MSA.3/OS Update". 5. Revised section 7.2.4 by adding "AmdA and AmdC should be followed in the process of 'secure communication channel'. 6. Revised section 8.1 to include the latest names and versions of some specifications. 7. Revised some layout problems and text errors in the document.
0.3	12/06/2025	[HED]	Update the TOE Life-Cycle.
0.4	03/07/2025	[HED]	1. Revised the TOE software architecture diagram in section 1.3.2 and the TOE logical boundary diagram in section 1.4.2. 2. Revised section 1.3.2 and modified the functional descriptions of the software modules in the HAL layer, platform layer, and application layer based on the TOE software architecture diagram.
0.5	25/07/2025	[HED]	1. Modified ST Reference and TOE Reference 2. Add caption to charts and tables.
0.6	30/07/2025	[HED]	1. Modified ST Reference and TOE Reference
0.7	23/08/2025	[HED]	1. Fixed some typos and document formatting. 2. Change "OS Update" to "OS Upgrade". 3. Modify section 6.2.1.2, revise parameters related to the algorithm, and ensure consistency with the code.
0.8	01/09/2025	[HED]	Revise Section 6.2.1.2: 1. SCP80 supports 256-bit length. 2. AES does not advertise CCM support. 3. Does not advertise support for SHA3 and MD5 4. Modify the key size of ECC.
0.9	15/10/2025	[HED]	1.Amend PP-eUICC to eUICC for Consumer and IoT Devices Protection Profile Version 2.1, 3 February 2025; 2.Remove all descriptions related to [PP-GP]. 3.Revise Chapters 2, 3, and 4 to ensure consistent descriptions of assets, users and subjects, threats, organizational security policies and assumptions. 4.Revise the content of Section 5.1 to align with the description in SGP.25 v2.1.
0.A	06/11/2025	[HED]	1.Change OS-UPGRADE to OS-UPDATE; 2.Add AGD-PRE as a reference to [eUICC Guidence]. 3.Change T.UNAUTH-LOAD-UPDATE-IMAGE to T.UNAUTH-UPDATE-IMAGE.LOAD 4.Sections 4.2 and 4.3: Add content related to OE.OS-UPDATE-ENCRYPTION 5.Re-add [PP-GP] related content.
0.B	08/12/2025	[HED]	1.Remove CAVE from ST.
0.C	04/01/2026	[HED]	1.The start size of RSA algorithm keys has been changed from 512 to 1024; 2.Modify the algorithm used for storing sensitive data; 3.Modify the algorithm used to ensure integrity during OS upgrades; 4.Remove the sections related to FCS_COP.1/CRC, as well as the descriptions concerning CRC in JCAPI. 5.Modify sections 6.2.10.JCS.CryptoAPI and 6.2.11.JCS.KeyManagement to incorrect

			key lengths and unsupported algorithms. 6.Remove descriptions related to SHA1 and SHA224; 7.Refine Section 1.4.2 to detail the descriptions of eUICC and UICC-related modules.
0.D	15/01/2026	[HED]	1.Delete Section 2.3, the statement description regarding PP-0084. 2.Revise Section 5.3.2 to add SFR rationale for O.SECURE_LOAD_ACODE, O.SECURE_AC_ACTIVATION and O.TOE_IDENTIFICATION. 3.Remove OE.OS-UPDATE-ENCRYPTION and OE.PROCESS_SEC_IC. 4.Add Chapter 7: Composition with IC.
0.E	19/01/2026	[HED]	1.Supplement the missing table of contents; 2.Revise Section 2.3: Change 'OS Upgrade' PP-Module to 'OS Update' PP-Module; 3.Revise Chapter 5: Correct the chapter citation error; 4.Remove content related to Enterprise Rules; 5.Revise Section 5.1 to clarify the assignment section content and adjust font colors as specified in the documentation requirements.
0.F	22/01/2026	[HED]	1.Remove the content description related to A.PROCESS-SEC-IC; 2.Remove content related to OE.OS-UPDATE-EVIDENCE and OE.SECURE_ACODE_MANAGEMENT. This content falls under the PP-GP specification and is not supported. 3.Fix assignment issue in FPT_FLS.1/Platform_services SFR.
0.G	23/01/2026	[HED]	1.Remove content related to OE.IC* and OE.RE* from certain tables. 2.Add content related to OE.VERIFICATION, OE.CAP_FILE, A.VERIFICATION, A.CAP_FILE and O.LOAD. 3.Rename O.PRE-PPI to O.PPE-PPI.
0.H	04/02/2026	[HED]	1.Adjust the software architecture diagrams in sections 1.3.2 and 1.4.2, adding CASD and ECASD along with their related descriptions; 2.Revise section 1.3.2 to specify that the IC hardware of CIU98N70_SE is within the TOE scope; 3.Change ES10a.VerifySmdsResponse to ES10b.VerifySmdpResponse; 4.Delete content related to FCS_CKM.4; 5.Add content related to the three SFRs for OS upgrades: 'FTP_TRP.1/OSU', 'FCS_COP.1/OSU-DEC', and 'FCS_COP.1/OSU-VER'; 6.Modify the key length of certain algorithms.
0.I	11/02/2026	[HED]	Section 1.3.1, further clarify the product scope;
0.J	27/02/2026	[HED]	1.Revise Chapter 7 to include O.RSA and the SFRs for RSA; 2.Remove unsupported algorithms.
0.K	04/03/2026	[HED]	1.Revise Section 2.2 to include relevant descriptions concerning the CC2022 Part 5 COMP assurance requirment package; 2.Section 1.3.4: Add relevant explanations concerning Bytecode Verification; 3.Section 1.3.2: Revised Description of TOE Type; 4.Add descriptions for A.PERSONLIZATION-SEC and OE.PERSONLIZATION_SEC.
0.L	13/03/2026	[HED]	1.Section 1.2: Revised TOE Name and added TOE Version; 2.Section 1.3.4: Clearly specify in tabular form that the BCV component forms part of the TOE;
0.M	30/03/2026	[HED]	1.Revise Section 1.3.2 to further clarify that TOE does not support LPAe; 2.Revise Section 5.3.4 to synchronise the CC dependencies of SFRs in the table in accordance with the [CC-E&I] specification;
0.N	02/04/2026	[HED]	Revise the version numbers for [JC-PP]、GP AmdB. and GP AmdF.
1.0	09/04/2026	[HED]	Official release.

HED

Table of Contents

REVISION HISTORY 2
1. ST INTRODUCTION 8
1.1. ST Reference 8
1.2. TOE Reference 8
1.3. TOE Overview 8
1.3.1. TOE Description 8
1.3.2. TOE Type and Usage 8
1.3.3. TOE Life-cycle 10
1.3.4. Non-TOE HW/SW/FW available to the TOE 12
1.4. TOE scope 12
1.4.1. Physical scope 12
1.4.2. Logical scope 13
2. CONFORMANCE CLAIMS(ASE_CCL) 14
2.1. CC Conformance claim 14
2.2. Assurance package claim 15
2.3. PP conformance claim 15
2.4. Conformance claim rationale 15
2.4.1. Conformity of the TOE Type 15
2.4.2. SPD Consistency 15
2.4.3. Security Objectives Consistency 18
2.4.4. Conformity of the Requirement (SFR/SAR) 19
3. SECURITY PROBLEM DEFINITION(ASE_SPD) 22
3.1. Assets 22
3.2. Users and Subjects 24
3.3. Threats 26
3.4. Organizational Security Policies 27
3.5. Assumptions 27
4. SECURITY OBJECTIVES 28
4.1. Security Objectives for the TOE 28
4.2. Security Objectives for the Operational Environment 30
4.3. Security Objectives Rationale 31
4.3.1. Threats 31
4.3.2. Organizational Security Policies 34
4.3.3. Assumptions 34
4.3.4. Rationale tables 35
5. SECURITY REQUIREMENTS(ASE_REQ) 38
5.1. eUICC Security Functional Requirements 38
5.1.1. Identification and authentication 39
5.1.2. Communication 42
5.1.3. Security Domains 47
5.1.4. Platform Services 49
5.1.5. Security management 51
5.1.6. Mobile Network authentication 55
5.2. Runtime Environment Security Requirements 56
5.2.1. CoreLG Security Functional requirements 56
5.2.2. INSTG Security Functional requirements 70
5.2.3. ADELG Security Functional Requirements 70
5.2.4. RMIG Security Functional Requirements 73
5.2.5. ODELG Security Functional Requirements 73
5.2.6. CARG Security Functional Requirements 73
5.2.7. Global Platform Security Functional requirements 73
5.2.8. OS Upgrade Security Functional requirements 82
5.2.9. Underlying platform IC Security Functional Requirements 85
5.3. Security Functional Requirements Rationale 86
5.3.1. SFRs for eUICC rationale 86
5.3.2. SFRs for Runtime Environment rationale 86
5.3.3. SFRs for underlying platform IC rationale 87

5.3.4. SFRs dependency rationale 87
6. TOE SUMMARY SPECIFICATION 91
6.1. eUICC security functions 91
6.1.1. GSMA.ProfileManagement 91
6.1.2. GSMA.ECASD 91
6.1.3. GSMA.ISDR 91
6.1.4. GSMA.ISDP 91
6.1.5. GSMA.PPR 92
6.2. Runtime Environment security functions 92
6.2.1. GP.CardContentManagement 92
6.2.2. GP.KeyLoading 92
6.2.3. GP.SecurityDomain 92
6.2.4. GP.SecureChannel 92
6.2.5. GP.GPRegistry 93
6.2.6. JCS.APDUBuffer 93
6.2.7. JCS.ByteCodeExecution 94
6.2.8. JCS.Firewall 94
6.2.9. JCS.Package 94
6.2.10. JCS.CryptoAPI 94
6.2.11. JCS.KeyManagement 95
6.2.12. JCS.OwnerPIN 95
6.2.13. JCS.EraseResidualData 95
6.2.14. JCS.OutOfLifeDataUndisclosure 95
6.2.15. JCS.RunTimeExecution 95
6.2.16. JCS.Exception 96
6.2.17. OS.Atomicity 96
6.2.18. OS.MemoryManagement 96
6.2.19. OS.OS Update 96
6.3. TSS Rationale 96
6.3.1. eUICC SFRs coverage 96
6.3.2. Runtime Environment SFRs coverage 97
7. Composition with IC 102
7.1. Statement of compatibility 102
7.1.1. Threats 102
7.1.2. Organizational Security Policies 102
7.1.3. Assumptions 103
7.1.4. Security Objectives for the environment 103
7.1.5. Security Objectives 103
7.1.6. Security Functional Requirements 104
8. BIBLIOGRAPHY 105
8.1. External references 105
8.2. Internal references 106
8.3. Glossary 106
8.4. Abbreviations 107

TABLE OF FIGURES

Figure 1 - Product environment 9
Figure 2 - CIU98N70 Software Architecture 9
Figure 3 - TOE Life-cycle and actors 10
Figure 4 - Product environment - TOE Physical boundaries 12
Figure 5 - TOE Logical boundaries 13

TABLE OF TABLES

Table 1 - TOE Life-cycle(manufacturing flow) 11
Table 2 - TOE Life-cycle (OS Upgrade flow) 11
Table 3 - Non-TOE components List 12
Table 4 - TOE Components 13

Table 5 - Assets Consistencytable 16
Table 6 - User Consistencytable 16
Table 7 - Subjects Consistencytable 17
Table 8 - Threats Consistencytable 17
Table 9 - Organizational Security Policies Consistencytable 17
Table 10 - Assumptions Consistencytable 18
Table 11 - Security objectives for the TOE Consistencytable 19
Table 12 - Security objectives for the Operational Environment Consistencytable 19
Table 13 - Security Functional Requirement Consistencytable 22
Table 14 - Security Assets List 24
Table 15 - Users List 25
Table 16 - Subjects List 26
Table 17 - Threats List for the SPD 27
Table 18 - OSP List for the SPD 27
Table 19 - Assumptions List for the SPD 28
Table 20 - Security Objectives List for the TOE 30
Table 21 - Security Objectives List for the Operational Environment 30
Table 22 - T.CONFID-UPDATE-IMAGE.LOAD Threat 33
Table 23 - T.UNAUTH-UPDATE-IMAGE.LOAD Threat 33
Table 24 - T.INTEG-UPDATE-IMAGE.LOAD Threat 34
Table 25 - T.INTERRUPT_OSU Threat 34
Table 26 - OSPs List for the Security Objectives in [PP-eUICC] 34
Table 27 - Assumptions List for the Security Objectives in [PP-eUICC] 35
Table 28 - Threats and Security Objectives - Coverage 36
Table 29 - Security Objectives and threats 37
Table 30 - Organizational Security Policies and Security Objectives-Coverage 37
Table 31 - Security Objectives and Organizational Security Policies 37
Table 32 - Assumptions and Security Objectives for the Operational Environment-Coverage 38
Table 33 - Assumptions and Security Objectives for the Operational Environment 38
Table 34 - Base TOE Emanation of TSF and User data List Explanation 52
Table 35 - Mobile network Cryptographic key distribution List Explanation 55
Table 36 - Mobile network Cryptographic key destruction List Explanation 56
Table 37 - Security attribute based access control List Explanation 57
Table 38 - Simple security attributes List Explanation 59
Table 39 - Cryptographic key generation List Explanation 61
Table 40 - GP-SCP Cryptographic key generation List Explanation 61
Table 41 - TDES_MAC Cryptographic operation List Explanation 62
Table 42 - AES_MAC Cryptographic operation List Explanation 62
Table 43 - ECDH Cryptographic operation List Explanation 63
Table 44 - ECDSA_SIGN Cryptographic operation List Explanation 63
Table 45 - ECKA_EG Cryptographic operation List Explanation 63
Table 46 - GP-SCP Cryptographic operation List Explanation 64
Table 47 - TDES_CIPHER Cryptographic operation List Explanation 64
Table 48 - AES_CIPHER Cryptographic operation List Explanation 65
Table 49 - RSA_SIGN Cryptographic operation List Explanation 65
Table 50 - RSA_CIPHER Cryptographic operation List Explanation 66
Table 51 - Hash Cryptographic operation List Explanation 66
Table 52 - HMAC Cryptographic operation List Explanation 66
Table 53 - ADEL-Security attribute based access control List Explanation 71
Table 54 - GP Management of security attributes List Explanation 82
Table 55 - Runtime environment objectives conversion for SFR rationale 86
Table 56 - SFRs dependencytable 90
Table 57 - eUICC SFRs Coverage List 97
Table 58 - Runtime Environment SFRs Coverage List 101
Table 59 - IC Threats compatibility between Composite-ST and IC-ST 102
Table 60 - Organizational Security Policies compatibility between Composite-ST and IC-ST 103
Table 61 - IC Assumptions compatibility between Composite-ST and IC-ST 103
Table 62 - IC OEs compatibility between Composite-ST and IC-ST 103
Table 63 - IC Security Objectives compatibility between Composite-ST and IC-ST 104
Table 64 - IC Security Functional Requirements compatibility between Composite-ST and IC-ST 105

Table 65 - External References List 106
Table 66 - Internal References List 106
Table 67 - Glossary List 107
Table 68 - Abbreviations List 107

1. ST INTRODUCTION

1.1. ST Reference

The ST identification is the following:

- Title: eUICC V1.0 with MCOS V3.8 on CIU98N70 Secure Element Security Target
- Version: 1.0
- Author: HED
- Publication date: 09/04/2026

1.2. TOE Reference

- TOE name: eUICC V1.0 with MCOS V3.8
- TOE Version: 1.0
- Developer: HED
- Software name: MCOS V3.8
- Software version: V3.8
- TOE type: Embedded Secure Element for embedded UICC OS
- TOE hardware part: CIU98N70

1.3. TOE Overview

1.3.1. TOE Description

The product CIU98N70 eUICC V1.0 is a combo eSE/eUICC product addressing the consumer electronics mobile market. Both eSE and eUICC features are isolated logically (via framework) and physically (via interface/protocol).

- As embedded Secure Element (eSE), it ensures the data is stored in a safe place and information is given to only authorized applications. It is also provided security service for payment applications, transportation applications, access control applications, electronic ID applications, etc.
- As embedded UICC (eUICC), it provides a software platform for remote provisioning and subscription management as defined by the GSMA. The eUICC is a tamper-proof chip and embedded in the device. It also ensures the data is stored in a safe place and information is given to only authorize applications.

The TOE is the product in **eUICC and SPE configuration** for Consumer Devices.

The TOE can be upgraded via the OS upgrade module on the SPE side.

The TOE is the **eUICC** open platform with multi-application support, such as Java Card, GlobalPlatform, that implements the GSMA Remote SIM Provisioning (RSP) Architecture for Consumer Devices compliant with the GSMA specifications **[SGP.21] [SGP.22] [SGP.23]** and the Trusted Connectivity Alliance eUICC Profile Package implementing **[EUPP].**

The TOE is able to communicate over [ISO7816] (T=0, T=1) contact protocols and [ISO14443] contactless protocols.

1.3.2. TOE Type and Usage

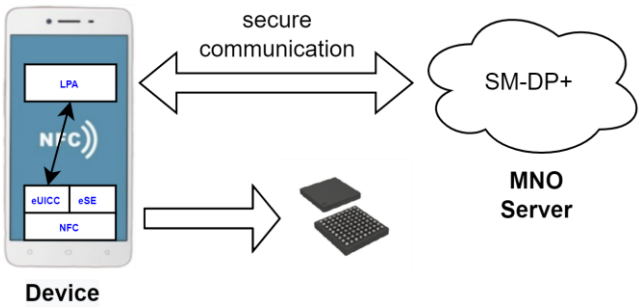


Figure 1 - Product environment

The eUICC is an UICC embedded in a consumer device. The eUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile.

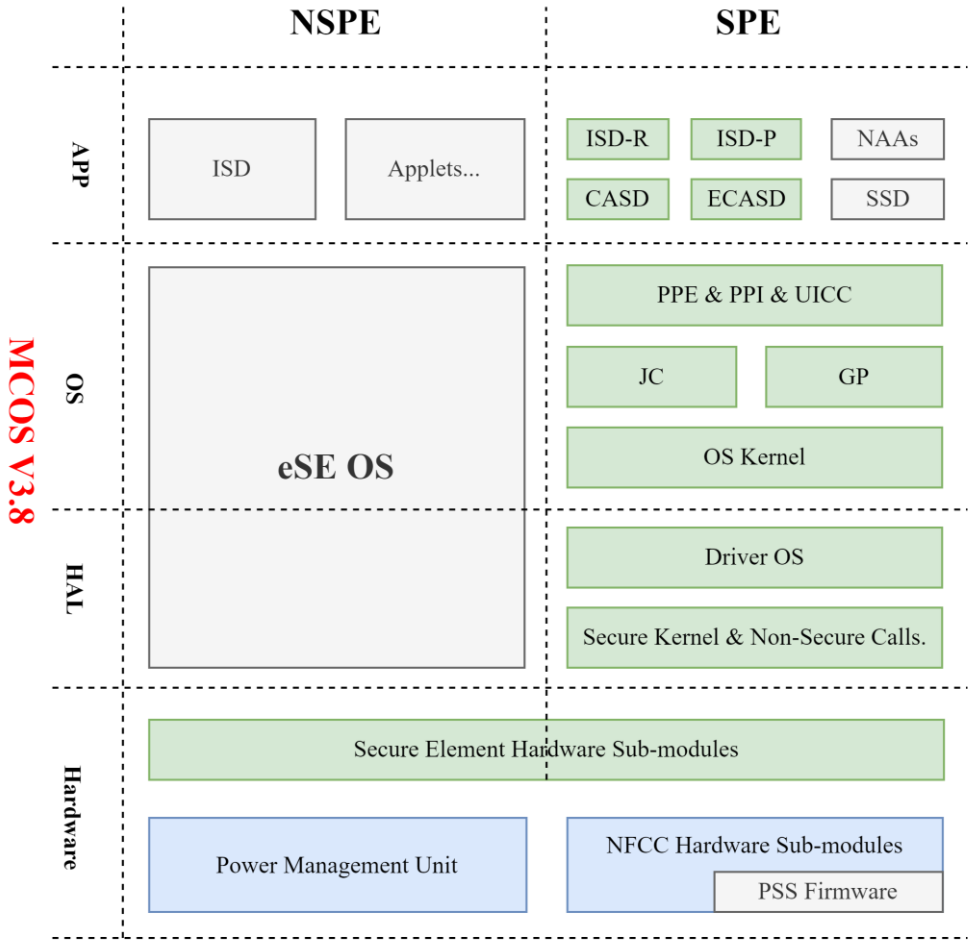


Figure 2 - CIU98N70 Software Architecture

The TOE type is an **embedded UICC** software in a customer device and only relies on **SPE(Secure Processing Environment)** Area on CIU98N70, The gray part in Figure 2, **eSE COS Section of NSPE(Non-secure Processing Environment) is not part of the TOE** .

The TOE relies on a Local Profile Assistant (LPA) component. It can be either be implemented at the application level as LPAe (the case covered by the LPA PP-Module), or it can be implemented as a non-TOE on-device unit called LPAd. In this product, **LPAe is not supported, the LPAe and LPAd is not in the TOE**.

The **Profiles, NAAs, File System and MNO-SD are not part of the TOE**.

The **Third-Party Applets and related SSD are not part of the TOE**.

ISDR , ISD-P, ECASD and CASD are mandatory on the combo product in the scope of this TOE.

The TOE includes 4 layers:

- The hardware layer: **CIU98N70** IC providing support to the hardware platform layer.
- The Hardware Abstraction Layer(HAL): This primarily includes the adaptation of physical interfaces (7816 and SMB interfaces), algorithm interfaces (including DES/3DES, RSA, ECC algorithm interfaces, etc.), and storage interfaces (Flash and RAM) to provide support for the platform layer.
- The platform layer: The **CIU98N70 eUICC V1.0** operating system (OS) includes the JavaCard standard implementation, GP standard and its amendment standard implementation, eUICC GSMA remote configuration functionality, and Profile management functionality implementation, providing support for the application layer.

●The application layer: Composed of privileged applications such as ISD-R and ISD-P, providing remote configuration and management functions (within the TOE scope), as well as NAAs operator applications and third-party Applet applications, and secure domains (outside the TOE scope).

The Secure Element Hardware Sub-module (CIU98N70_SE) falls within the scope of TOE.

1.3.3. TOE Life-cycle

The TOE life-cycle consists of the Phase1、Phase2、Phase3、Phase4 and Phase5 of the PP0084. The TOE lice-cycle is composed of 4 phases of eUICC Life-Cycle (from phase a to c) which are described in Figure 3, in Table 1 and Table 2 with the associated locations. The TOE delivery is mentioned before phase d.

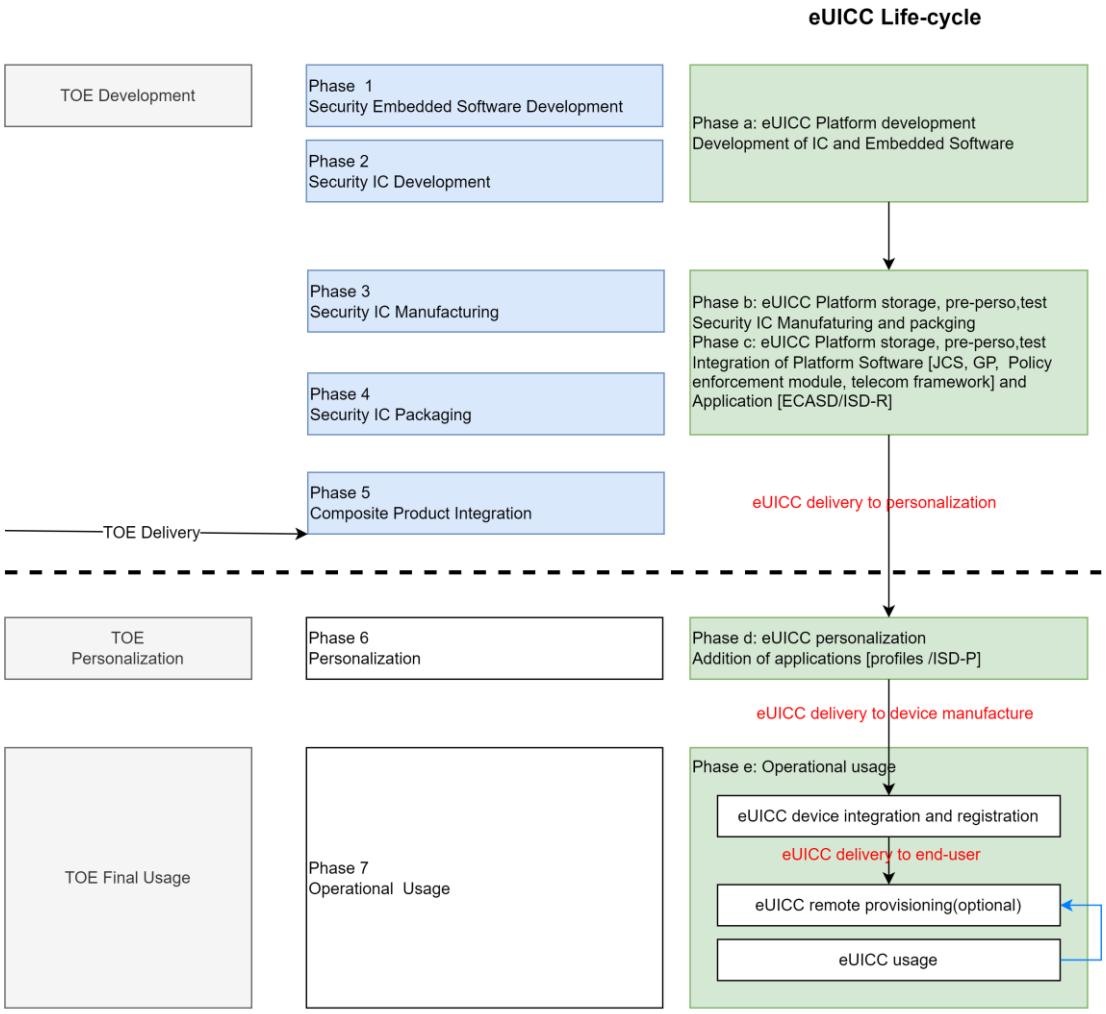


Figure 3 - TOE Life-cycle and actors

The manufacturing flow is described in the following table, the OS software and the application are downloaded in the IC manufacturing(Mask production) of phase b:

Phase	Description	Actor
a	Embedded Software Development	CEC Huada Electronic Design Co., Ltd.
	IC development	CEC Huada Electronic Design Co., Ltd.
b &c	IC manufacturing(Mask production)	Semiconductor Manufacturing International(Shanghai) Corporation.

	IC manufacturing(Wafer production)	Semiconductor Manufacturing North China(Beijing) Corporation (B2)
	IC manufacturing (Wafer testing)	Zhejiang Chipadvanced Technology Co.,Ltd.
	IC packaging (WLCSP package)	JCET Advanced Packaging Co., Ltd.
	IC manufacturing (FT testing)	JCET Advanced Packaging Co., Ltd.
	IC manufacturing (Dicing)	JCET Advanced Packaging Co., Ltd.
***** TOE delivery *****		
d	Personalization of data during wafer test flow	Zhejiang Chipadvanced Technology Co.,Ltd.
Device is delivered to point of sales and is reaching end user		
e	RSP process (Profile loading and activation)	Profile issuer (SM-DP+ server)

Table 1 - TOE Life-cycle(manufacturing flow)

The OS Upgrade flow is described in the following table :

The conditions to trigger OS Upgrade are weakness on eUICC Secure Application (**CIU98N70 eUICC V1.0** OS) at security, or functional, or both -OR- deployment of additional feature.

Phase	Description	Actor
a	MCOS SW (OS and Crypto)	HED
***** TOE delivery ***** **Secure delivery of CIU98N70 eUICC V1.0 embedded software (patch) to DEVICE OEM**		
e	RSP process (Profile loading and activation)	Profile issuer (SM-DP+ server)

Table 2 - TOE Life-cycle (OS Upgrade flow)

The IC Embedded Software Developer is in charge of security embedded software development.
The IC Development is in charge of:

- IC design
- IC Dedicated Software development

The IC Manufacturing is in charge of:

- Integration and photomask fabrication
- IC production
- IC testing
- Preparation and pre-personalization if necessary

The Composite Product life cycle phase 4 and phase 5 are included in the evaluation of the IC:

- The IC Packaging (Phase 4)
- Security IC packaging (and testing)
- Pre-personalization if necessary

The Composite Product finishing process, preparation and shipping to the personalization line for the Composite Product (Composite Product Integration Phase 5)

The Composite Product personalization and testing stage where the User Data is loaded into the Security IC's memory (Personalization Phase 6).
The Composite Product usage by its issuers and consumers (Operational Usage Phase 7) which may include loading and other management of applications in the field.

The MCOS V3.8 software(including image data corresponding to the eSE OS software which is not covered by this TOE, the eUICC OS software which is covered by this TOE and the pre-installed applets which are not covered by this TOE) is downloaded in the IC manufacturing(Mask production) of phase 3.

1.3.4. 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 RTE.

The TOE does not implement the **RMI** functions from JCS.

Here is a description of the non-TOE components and systems:

Component	Required	Description
Bytecode verifier	Mandatory	The bytecode verifier is a program that performs static checks on the bytecodes of the methods of a CAP file prior to the execution of the file on the card. Bytecode verification is a key component of security: applet isolation, for instance, depends on the file satisfying the properties a verifier checks to hold. A method of a CAP file that has been verified shall not contain, for instance, an instruction that allows forging a memory address or an instruction that makes improper use of a return address as if it were an object reference. In other words, bytecodes are verified to hold up to the intended use to which they are defined. Bytecode verification could be performed totally or partially dynamically. No standard procedure in that concern has yet been recognized. Furthermore, different approaches have been proposed for the implementation of bytecode verifiers, most notably data flow analysis, model checking and lightweight bytecode verification, this latter being an instance of what is known as proof carrying code. The actual set of checks performed by the verifier is implementation-dependent, but it is required that it should at least enforce all the " must clauses" imposed in [JCVM] on the bytecodes and the correctness of the CAP files' format.It is required also that the latest available version of the verifier is used.

Table 3 - Non-TOE components List

1.4. TOE scope

1.4.1. Physical scope

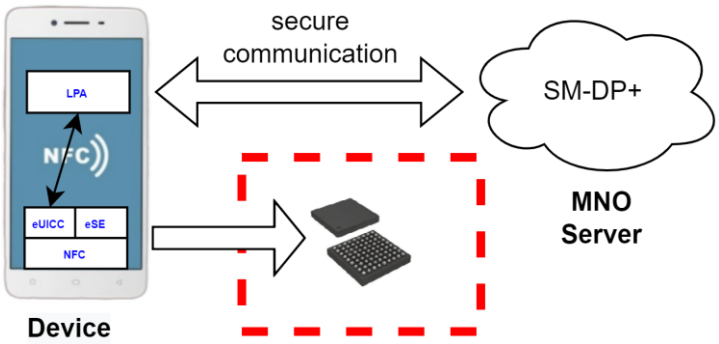


Figure 4 - Product environment - TOE Physical boundaries

The physical boundaries encompass the **CIU98N70 eUICC V1.0** software executed inside the IC hardware. The other items are outside the scope of the evaluation as illustrated in Figure 4 - Product environment.

This TOE is built on the CIU98N70 security element hardware.

IC Certification ID： EUCC-3110-2026-2500106-01.

The TOE consists of the following components:

TOE component	Developer	Item	Identifier	Form of delivery
IC	HED	CIU98N70 hardware	[ST/IC]	Diced wafer (embedding eUICC OS)
eUICC OS	HED	CIU98N70 eUICC V1.0	3640	Software (delivered embedded within the IC)
eUICC Guidances	HED	CIU98N70 eUICC V1.0	[GUIDES]	Document Electronic document (PDF) via secure email

Table 4 - TOE Components

1.4.2. Logical scope

The logical boundaries are delimited (dash line in red) in Figure 5.

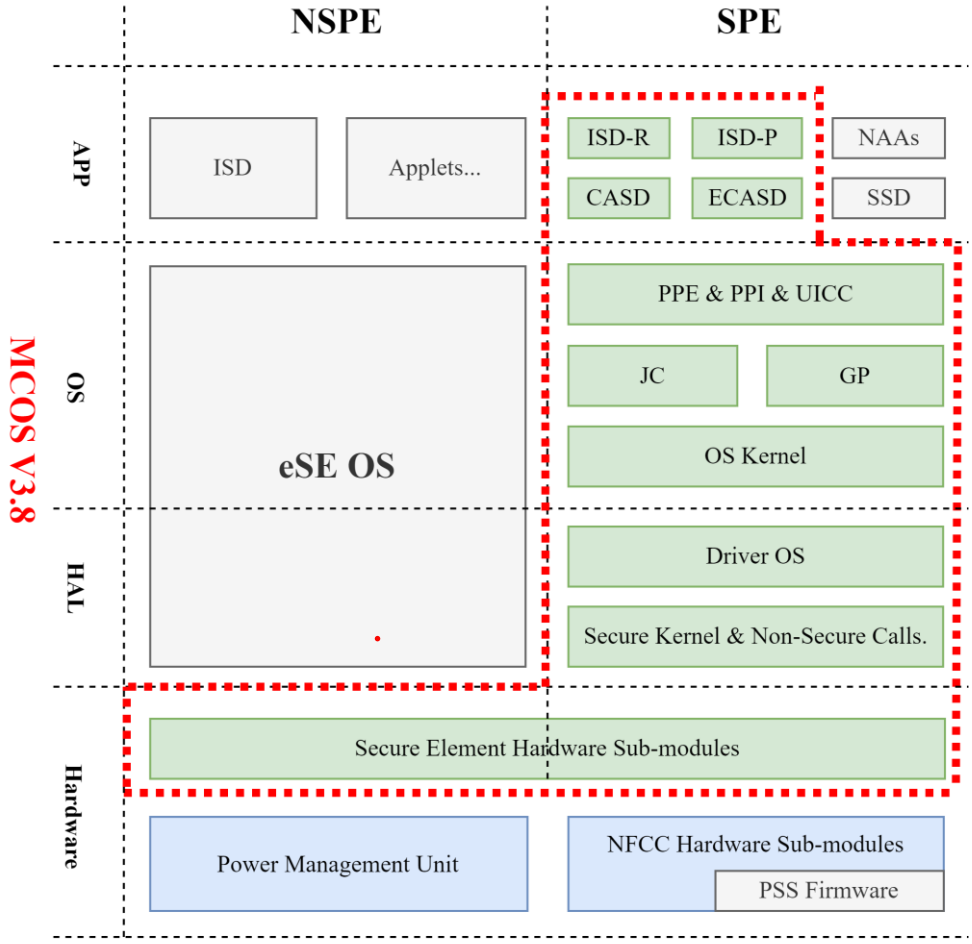


Figure 5 - TOE Logical boundaries

The eUICC OS implements the following services:

- App Layer:
  - ISD-R serves as the Root security domain for the eUICC, responsible for authentication with external SM-DP+ systems and managing card system data;
  - ISD-P serves as the profile management security domain, responsible for managing the operator's MNO-SD and its profile data;
  - The CASD security domain is responsible for managing the card content of the GP;
  - The ECASD is responsible for secure storage of credentials required to support the required Security Domains on the eUICC.
- OS Layer:
  - PPE & PPI & UICC: Remote Sim Provisioning (RSP), Local Profile Management (Enable, Disable, Delete MNO Profiles) and Telecom Framework;

◆PPE Module: Primarily based on the SGP.22 V3.1 specification, it provides policy enforcement and management for Profile;

◆PPI Module: Primarily based on the TCA 3.2 specification, it provides parsing and management of Profile packets;

◆UICC Module: Primarily based on ETSI specifications, it provides the UICC telecom basic framework, including UICC basic commands, telecom file system management, network authentication algorithms, SCP80/SCP81 communication management, RFM/RAM management, and the Toolkit framework.

■JC: Oracle's Java Card 3.1.0 [JC], which consist of the Java Card 3.1.0 Virtual machine, Java Card Run Time Environment 3.1.0 and the Java Card 3.1.0 Application Programming Interface;

■GP: Global Platform 2.3.1, UICC Configuration;

■The OS implements (at least) the following services:

◆Management and control of the communication between OS and external entities

◆OS Security services as follows:

●Checking environmental operating conditions using information provided by the IC

●Checking life cycle consistency

●Providing secure cryptographic primitives, algorithms and services

●Ensuring the security of the PIN and cryptographic key objects

●Generating random numbers

●Handling secure data object and backup mechanisms

●Managing memory content

◆Enforcement of the Javacard Runtime and Firewall mechanism

◆Standard APIs such as Telecom APIs, JC APIs and GP APIs

◆Management of life-cycle information (for the eUICC, Security Domains and Applications)

◆SCP02, SCP03 and SCP11 support

◆Secure loading, installation and deletion of applications within each SD

◆DAP and Mandated DAP verification

◆GlobalPlatform 'Authorized Management' and 'Delegated Management'

◆GlobalPlatform CLFDB

◆PIN verification (GP CVM)

◆Global Services (GS) according to GP

◆Confidential Card Content Management (CCCM) according to GP [Amd A]

◆Remote Application Management over HTTP [Amd B]

◆Contactless Services [Amd C]

■OS Kernel: OS Kernel module, which primarily includes the following functions:

◆OS security upgrade functionality (OS Upgrade feature, called Root Applet)

◆Flash and RAM management functionality

◆Transaction and garbage collection functionality

●HAL Layer:

■Driver OS Module, which primarily includes the following functions:

◆Driver adaptation for physical interfaces (including 7816, and SMB interfaces)

◆Interface adaptation for storage devices such as RAM and Flash

◆Interface adaptation for algorithm interfaces (including DES/3DES, RSA, ECC, etc.)

■Secure Kernel & Non-Secure Calls, which primarily includes the following functions:

◆The Secure Kernel section primarily encompasses the security implementations related to CIU98N70_SE's TrustZone functionality, firmware algorithm libraries, driver libraries, and other associated components.

◆The Non-Secure Calls section primarily includes encapsulated interfaces that need to be provided for NS-side invocation.

2. CONFORMANCE CLAIMS(ASE_CCL)

Evaluation type:

●This is a composite evaluation, which relies on the CIU98N70 IC certificate and evaluation results.

The composite evaluation includes the additional composition tasks defined in the [CC-COMP].

2.1. CC Conformance claim

This Security Target conforms to CC 2022 Revision 1:

●Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022, Revision 1, November 2022, [CCMB-2022-11-001]

- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC:2022, Revision 1, November 2022, [CCMB-2022-11-002]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC:2022, Revision 1, November 2022, [CCMB-2022-11-003]
- Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC:2022, Revision 1, November 2022, [CCMB-2022-11-004]
- Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC:2022, Revision 1, November 2022, [CCMB-2022-11-005]
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 22 July 2024, [CCMB-2024-002]

The assurance requirement of this Security Target is EAL4 augmented. Augmentation results from the selection of:

- ALC_DVS.2 Sufficiency of security measures,
- AVA_VAN.5 Advanced methodical vulnerability analysis,

2.2. Assurance package claim

This Security target conforms to the assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5 and the assurance package from [CCMB-2022-11-005] for COMP .

2.3. PP conformance claim

This Security Target claims demonstrable conformance to the [PP-eUICC] protection profile and ‘OS Update’ PP-Module defined in Annex A of [PP-eUICC].

2.4. 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].

2.4.1. 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], section §1.2.5 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.

2.4.2. SPD Consistency

2.4.2.1. 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].
D.UPDATE_IMAGE	X	(E): Appendix A from [PP-eUICC] to cover OS Update.
D.TOE_IDENTIFIER	X	(E): Appendix A from [PP-eUICC] to cover OS Update.
D.OS-UPDATE_KEY(S)	X	(E): Appendix A from [PP-eUICC] to cover OS Update.

Table 5 - Assets Consistencytable

2.4.2.2. Users and Subjects consistency

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

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

Table 6 - User Consistencytable

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].
S.OSU	X	(E): Appendix A from [PP-eUICC] to cover OS Update.
S.UpdateImageCreator	X	(E): Appendix A from [PP-eUICC] to cover OS Update.

Table 7 - Subjects Consistencytable

2.4.2.3. 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)
T.CONFID-UPDATE-IMAGE.LOAD	X	(E): Appendix A from [PP-eUICC] to cover OS Update.
T.UNAUTH-UPDATE-IMAGE.LOAD	X	(E): Appendix A from [PP-eUICC] to cover OS Update.
T.INTEG-UPDATE-IMAGE.LOAD	X	(E): Appendix A from [PP-eUICC] to cover OS Update.
T.INTERRUPT-OSU	X	(E): Appendix A from [PP-eUICC] to cover OS Update.

Table 8 - Threats Consistencytable

2.4.2.4. Organizational Security Policies consistency

All Organizational Security Policies defined in [PP-eUICC] are relevant for the TOE of this Security Target.

The table below indicates the Organizational Security Policies' consistency.

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

Table 9 - Organizational Security Policies Consistencytable

2.4.2.5. 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)
A.CAP_FILE	X	(A): Added from [PP-JCS].
A.VERIFICATION	X	(A): Added from [PP-JCS].
A.PERSONLIZATION-SEC		(A): Added from [PP-84].

Table 10 - Assumptions Consistencytable

2.4.3. Security Objectives Consistency

2.4.3.1. Objective for the TOE consistency

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

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

O.TOE	PP-eUICC	Security Target
O.PPE-PPI	X	(E)
O.eUICC-DOMAIN-RIGHTS	X	(E)
O.SECURE-CHANNELS	X	(E)
O.INTERNAL-SECURE- CHANNELS	X	(E)
O.PROOF_OF_IDENTITY	X	(E)
O.OPERATE	X	(E)
O.API	X	(E)
O.DATA-CONFIDENTIALITY	X	(E)
O.DATA-INTEGRITY	X	(E)
O.ALGORITHMS	X	(E)
O.IC.PROOF_OF_IDENTITY		(A): Added and replace OE.IC.PROOF_OF IDENTITY from [PP-eUICC].
O.IC.SUPPORT		Added and replace OE.IC.SUPPORT from [PP-eUICC].
O.IC.RECOVERY		(A): Added and replace OE.IC.RECOVERY from [PP-eUICC].
O.RE.PPE-PPI		(A): Added and replace OE.RE.PPE-PPI from [PP-eUICC].
O.RE.SECURE-COMM		Added and replace OE.RE.SECURE-COMM from [PP-eUICC].
O.RE.API		(A): Added and replace OE.RE.API from [PP-eUICC].
O.RE.DATA-CONFIDENTIALITY		(A): Added and replace OE.RE.DATA-CONFIDENTIALITY from [PP-eUICC].
O.RE.DATA-INTEGRITY		(A): Added and replace OE.RE.DATA-INTEGRITY from [PP-eUICC].
O.RE.IDENTITY		(A): Added and replace OE.RE.IDENTITY from [PP-eUICC].
O.RE.CODE-EXE		(A): Added and replace OE.RE.CODE-EXE from [PP-eUICC].
O.SECURE_LOAD_ACODE		(E): Appendix A from [PP-eUICC] to cover OS Update.
O.SECURE AC ACTIVATION		(E): Appendix A from [PP-eUICC] to cover OS Update.
O.TOE IDENTIFICATION		(E): Appendix A from [PP-eUICC] to cover OS Update.
O.CONFID-UPDATE-IMAGE.LOAD		(E): Appendix A from [PP-eUICC] to cover OS Update.

O.AUTH-LOAD-UPDATE-IMAGE		(E): Appendix A from [PP-eUICC] to cover OS Update.
O.LOAD		(A): Added from [PP-JCS].

Table 11 - Security objectives for the TOE Consistencytable

2.4.3.2. Objective for Environment consistency

O.ENV	PP-eUICC	Security Target
OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.MNO	X	(E)
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PPE-PPI	X	Removed and replaced by O.RE.PPE-PPI.
OE.RE.SECURE-COMM	X	Removed and replaced by O.RE.SECURE-COMM.
OE.RE.API	X	Removed and replaced by O.RE.API.
OE.RE.DATA-CONFIDENTIALITY	X	Removed and replaced by O.RE.DATA-CONFIDENTIALITY.
OE.RE.DATA-INTEGRITY	X	Removed and replaced by O.RE.DATA-INTEGRITY
OE.RE.IDENTITY	X	Removed and replaced by O.RE.IDENTITY
OE.RE.CODE-EXE	X	Removed and replaced by O.RE.CODE- EXE
OE.TRUSTED-PATHS-LPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.MNO-SD	X	(E)
OE.CAP_FILE	X	(A) : Added from [PP-JCS]
OE.VERIFICATION	X	(A) : Added from [PP-JCS]
OE.CODE-EVIDENCE	X	(A) : Added from [PP-JCS]
OE.CONFID_UPDATE_IMAGE.CREATE	X	(E)
OE.PERSONLIZATION_SEC		(A): Added from [PP-84].

Table 12 - Security objectives for the Operational Environment Consistencytable

2.4.4. Conformity of the Requirement (SFR/SAR)

2.4.4.1. SFR consistency

SFR	PP-eUICC	Security Target
FIA_UID.1/EXT	X	
FIA_UAU.1/EXT	X	
FIA_USB.1/EXT	X	
FIA_UAU.4/EXT	X	
FIA_UID.1/MNO-SD	X	
FIA_USB.1/MNO-SD	X	
FIA_ATD.1/Base	X	
FIA_API.1	X	
FDP_IFC.1/SCP	X	
FDP_IFF.1/SCP	X	
FTP_ITC.1/SCP	X	
FDP_ITC.2/SCP	X	
FPT_TDC.1/SCP	X	
FDP_UCT.1/SCP	X	

FDP_UIT.1/SCP	X	
FCS_CKM.1/SCP-SM	X	
FCS_CKM.2/SCP-MNO	X	
FCS_CKM.6/SCP-SM	X	
FCS_CKM.6/SCP-MNO	X	
FDP_ACC.1/ISDR	X	
FDP_ACF.1/ISDR	X	
FDP_ACC.1/ECASD	X	
FDP_ACF.1/ECASD	X	
FDP_IFC.1/Platform_services	X	
FDP_IFF.1/Platform_services	X	
FPT_FLS.1/Platform_services	X	
FCS_RNG.1	X	
FPT_EMS.1	X	
FDP_SDI.1/Base	X	
FDP_RIP.1/Base	X	
FPT_FLS.1/Base	X	
FMT_MSA.1/PLATFORM_DATA	X	
FMT_MSA.1/RULES	X	
FMT_MSA.1/CERT_KEYS	X	
FMT_SMF.1	X	
FMT_SMR.1	X	
FMT_MSA.1/RAT	X	
FMT_MSA.3	X	
FCS_COP.1/Mobile_network	X	
FCS_CKM.2/Mobile_network	X	
FCS_CKM.6/Mobile_network	X	
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] and refined
FMT_SMR.1/JC		(A): Added from [PP-JCS] and refined
FCS_CKM.1/ECDSA		(A): Added from [PP-JCS]. Refined with iteration.
FCS_CKM.1/GP-SCP		(A): Added from [PP-GP].
FCS_COP.1/TDES_MAC FCS_COP.1/AES_MAC FCS_COP.1/ECDH FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_COP.1/GP-SCP FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/RSA_SIGN FCS_COP.1/RSA_CIPHER FCS_COP.1/Hash FCS_COP.1/HMAC		(A): Added from [PP-JCS]. Refined with iteration.
FDP_RIP.1/ABORT		(A): Added from [PP-JCS].
FDP_RIP.1/APDU		(A): Added from [PP-JCS].
FDP_RIP.1/bArray		(A): Added from [PP-JCS].
FDP_RIP.1/GlobalArray		(A): Added from [PP-JCS].

FDP_RIP.1/KEYS		(A): Added from [PP-JCS].
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JCS].
FDP_ROL.1/FIREWALL		(A): Added from [PP-JCS].
FAU_ARP.1		(A): Added from [PP-JCS].
FDP_SDI.2/DATA		(A): Added from [PP-JCS].
FPR_UNO.1		(A): Added from [PP-JCS].
FPT_FLS.1/JC		(A): Added from [PP-JCS]. Refined with iteration.
FPT_TDC.1		(A): Added from [PP-JCS].
FIA_ATD.1/AID		(A): Added from [PP-JCS].
FIA_UID.2/AID		(A): Added from [PP-JCS].
FIA_USB.1/AID		(A): Added from [PP-JCS].
FMT_MTD.1/JCRE		(A): Added from [PP-JCS].
FMT_MTD.3/JCRE		(A): Added from [PP-JCS].
FDP_ACC.2/ADEL		(A): Added from [PP-JCS].
FDP_ACF.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.1/ADEL		(A): Added from [PP-JCS].
FMT_MSA.3/ADEL		(A): Added from [PP-JCS].
FMT_SMF.1/ADEL		(A): Added from [PP-JCS].
FMT_SMR.1/ADEL		(A): Added from [PP-JCS].
FPT_FLS.1/ADEL		(A): Added from [PP-JCS].
FDP_RIP.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/ODEL		(A): Added from [PP-JCS].
FPT_FLS.1/GP		(A): Added from [PP-GP].
FDP_ROL.1/GP		(A): Added from [PP-GP].
FCO_NRO.2/GP		(A): Added from [PP-GP].
FMT_SMR.1/GP		(A): Added from [PP-GP].
FMT_SMF.1/GP		(A): Added from [PP-GP].
FDP_ITC.2/GP-ELF		(A): Added from [PP-GP].
FDP_ITC.2/GP-KL		(A): Added from [PP-GP].
FPT_RCV.3/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-ELF		(A): Added from [PP-GP].
FDP_IFF.1/GP-ELF		(A): Added from [PP-GP].
FIA_UID.1/GP		(A): Added from [PP-GP].
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FTP_ITC.1/GP		(A): Added from [PP-GP].
FPR_UNO.1/GP		(A): Added from [PP-GP].
FPT_TDC.1/GP		(A): Added from [PP-GP].
FDP_IFC.2/GP-KL		(A): Added from [PP-GP].
FDP_IFF.1/GP-KL		(A): Added from [PP-GP].
FMT_MSA.1/GP		(A): Added from [PP-GP].
FMT_MSA.3/GP		(A): Added from [PP-GP].
FDP_IFC.2/OSU		(A): Added to cover OS Update.
FDP_IFF.1/OSU		(A): Added to cover OS Update.
FMT_MSA.3/OSU		(A): Added to cover OS Update.
FMT_MSA.1/OSU		(A): Added to cover OS Update.
FMT_SMR.1/OSU		(A): Added to cover OS Update.
FMT_SMF.1/OSU		(A): Added to cover OS Update.
FIA_UID.1/OSU		(A): Added to cover OS Update.
FIA_UAU.1/OSU		(A): Added to cover OS Update.
FIA_UAU.4/OSU		(A): Added to cover OS Update.
FTP_TRP.1/OSU		(A): Added to cover OS Update, refer to [PP-GP].

FCS_COP.1/OSU-DEC		(A): Added to cover OS Update, refer to [PP-GP].
FCS_COP.1/OSU-VER		(A): Added to cover OS Update, refer to [PP-GP].
FPT_FLS.1/OSU		(A): Added to cover OS Update.
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 13 - Security Functional Requirement Consistencytable

2.4.4.2. SAR consistency

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

3. SECURITY PROBLEM DEFINITION(ASE_SPD)

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.

3.1. Assets

The definition of the assets from [PP-eUICC] and [PP-JCS] is not repeated here. See section2.4.2.1 for complete list is assets.

Assets	Description
D.MNO_KEYS	Keys used by MNO OTA Platform to request management operations from the ISD-P. The keys are loaded during provisioning and stored under the control of the MNO SD.
D.PROFILE_NAA_PARAMS	Parameters used for network authentication, including keys. Such parameters may include for example elliptic curve parameters. Parameters are loaded during provisioning and storedunder the control ofthe ISD-P. They may be transmitted to the Telecom Framework, which contains the authentication algorithms. To be protected from unauthorized disclosure and unauthorized modification.
D.PROFILE_IDENTITY	The International Mobile Subscriber Identity is the user credential when authenticating on a MNO′s network via an Authentication algorithm. The IMSI is a representation of the subscriber′s identity and will be used by the MNO as an index for the subscriber in itsHLR. Each IMSI is stored under the control of the ISD-P during provisioning. The IMSI shall be protected from unauthorized modification.
D.PROFILE_POLICY_RULES	Data describing the profile policy rules (PPRs) of a profile. These rules are loaded during provisioning and stored under the control of the ISD-P. They are managed by the MNO OTA Platform. PPRs shall be protected from unauthorized modification.
D.PROFILE_USER_CODES	This asset consists of: ●the optional Activation Code that End User may use to initiate a Profile Download and Installation via the Local User Interface (LUId); ●the hash of the optional Confirmation Code (Hashed Confirmation Code) that End User may use to confirm a Profile Download and Installation via the Local User Interface (LUId). Note that although these codes are input by End User at the LUId, which is outside of the TOE, the codes are sent to the TOE for signature (ex. euiccSigned2 data structure). To be protected from unauthorized modification.
D.PROFILE_CODE	The profile applications include first and second level applications, in particular: ● The MNO-SD and the Security Domains under the control of the MNO-SD (CASD, SSD); ●The other applications that may be provisioned within the MNO-SD (network access applications, and so on). This asset also includes, by convention, the file system of the Profile.

	All these applications are under the control of the MNO SD. These assets have to be protected from unauthorized modification.
D.TSF_CODE	The TSF Code distinguishes between ●the ISD-R, ISD-Ps and ECASD; ●the Platform code. All these assets have to be protected from unauthorized disclosure and modification. Knowledge of this code may allow bypassing the TSF. This concerns logical attacks at runtime in order to gain a read access to executable code, typically by executing an application that tries to read the memory area where a piece of code is stored. Application Note : ●this does not include applications within the MNO-SD, which are part of the user data (Profile applications); ● the notion of unauthorized disclosure and modification is the same as used in [PP-JCS].
D.PLATFORM_DATA	The data of the platform environment, like for instance, ●the identifiers and privileges including SM-DS OID, MNO OID, SM-DP+ OID; ●the eUICC life-cycle state of the ISD-P security domain (see Annex A of [SGP.22]). This data may be partially implemented in the logic of ISD-R and the Platform code, instead of being "data" properly speaking. As a consequence, this asset is strongly linked with D.TSF_CODE. To be protected from unauthorized modification.
D.DEVICE_INFO	This asset includes the security-sensitive elements of Device Information data, such as the device type allocation code (TAC) or the device capabilities (ex. Support for updating of certificate revocation lists (CRLs)), that is provided to the eUICC by the LPAd. To be protected from unauthorized modification.
D.PLATFORM_RAT	Data describing the Rules Authorisation Table (RAT) of the eUICC. These rules are initialised at eUICC manufacturing time or during the initial device setup provided that there is no installed operational profile. The OEM or EUM is responsible for setting the content of the RAT. RAT is stored in the eUICC. To be protected from unauthorized modification.
D.SK.EUICC.ECDSA	The eUICC private key(s), stored in ECASD, used by the eUICC to prove its identity, generate shared secrets with remote actors, and generate signatures. It must be protected from unauthorized disclosure and modification.
D.CERT.EUICC.ECDSA	Certificate(s) issued by the EUM for a specific, individual, eUICC. Certificates contain public keys PK.EUICC.ECDSA and are stored in ECASD. This certificate(s) can be verified using the EUM Certificate. The eUICC certificate(s) has to be protected from unauthorized modification.
D.PK.CI.ECDSA	The ′eSIM CA public key (D.PK.CI.ECDSA) used to verify the certification chain of Euicc and remote actors. It is stored in ECASD. It must be protected from unauthorized modification. ECASD MAY contain several public keys belonging to the same Esim CA or different Esim CA. Each D.PK.CI.ECDSA SHALL be stored with information coming from the CERT.CI.ECDSA the key is included in, at least: ●Certificate serial number: required to manage eSIM CA revocation by CRL; ●eSIM CA Identifier: eSIM CA OID; ●Subject Key Identifier: required to verify the Certification chain of the off-card entity.
D.EID	The EID (eUICC-ID) uniquely identifies the eUICC. This identifier is set by the eUICC manufacturer and does not change during operational life of the eUICC. It is stored in ECASD. The EID is used as a key by SM-DP+ and SM-DS to identify eUICCs in their databases. The EID shall be protected from unauthorized modification.
D.SECRETS	This asset includes: ●the one-time keys of the eUICC and the SM-DP+:

	●tSK.EUICC.ECKA, otPK.EUICC.ECKA, otSK.EUICC.ECKAeac (optional), otPK.EUICC.ECKAeac (optional) and otPK.DP.ECKA; ●the shared secret (ShS) used to protect the Profile download; and ●session keys (S-ENC and S-MAC) and the initial MAC chaining value. These asset shall be protected from unauthorized disclosure and modification.
D.CERT.EUM.ECDSA	The Certificate(s) of the EUM(CERT.EUM.ECDSA). To be protected from unauthorised modification.
D.CRLs	The optional certificate revocation lists (extract) stored in the eUICC. To be protected against unauthorised modification.
D.APP_CODE	The code of the applets and libraries loaded on the card. To be protected from unauthorized modification.
D.APP_C_DATA	Confidentiality - sensitive data of the applications, like the data Zontained in an object, an array view, a static field, a local variable of the currently executed method, or a position of the operand stack. To be protected from unauthorized disclosure.
D.APP_I_DATA	Integrity sensitive data of the applications, like the data contained in an object, an array view and the PIN security attributes (PIN Try limit, PIN Try counter and State). To be protected from unauthorized modification.
D.APP_KEYs	Cryptographic keys owned by the applets. To be protected from unauthorized disclosure and modification.
D.PIN	Any end-user's PIN. To be protected from unauthorized disclosure and modification.
D.API_DATA	Private data of the API, like the contents of its private fields. To be protected from unauthorized disclosure and modification.
D.CRYPTO	Cryptographic data used in runtime cryptographic computations, like a seed used to generate a key. To be protected from unauthorized disclosure and modification.
D.JCS_CODE	The code of the Java Card System. To be protected from unauthorized disclosure and modification.
D.JCS_DATA	The internal runtime data areas necessary for the execution of the Java Card VM, such as, for instance, the frame stack, the program counter, the class of an object, the length allocated for an array, any pointer used to chain data-structures. To be protected from unauthorized disclosure or modification.
D.SEC_DATA	The runtime security data of the Java Card RE, like, for instance, the AIDs used to identify the installed applets, the currently selected applet, the current context of execution and the owner of each object. To be protected from unauthorized disclosure and modification.
Additional D.Asset to cover OS Update	
D.UPDATE_IMAGE	Can be an upgrade data for the COS, as a patch or a component data to be replaced. It is sent to the TOE, received by the COS. It includes executable code, configuration data, as well as a Sequence Number (Received Sequence Number) and Image Type. It has to be protected from unauthorized disclosure and modification. It is decrypted using the Decryption Session Key and its signature is verified using the Verification Session Key.
D.TOE_IDENTIFIER	Identification data to identify the TOE. To be protected from unauthorized modification.
D.OS-UPDATE_KEY(S)	Key(s) used for OS Upgrade. To be protected from unauthorized disclosure and modification.

Table 14 - Security Assets List

3.2. Users and Subjects

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

User	Description

U.SM-DP+	Role that prepares the Profiles and manages the secure download and installation of these Profiles onto the eUICC.
U.SM-DS	Role that securely performs functions of discovery.
U.MNO-OTA	An MNO platform for remote management of UICCs and the content of Enabled MNO Profiles on eUICCs.
U.MNO-SD	A MNO-SD is a Security Domain part of the Profile, owned by the MNO, providing the Secured Channel to the MNO′s OTA Platform (U.MNO-OTA). It is used to manage the content of a Profile once the Profile is enabled. An eUICC can contain more than one MNO-SD.
U.End-User	The person using the Device.

Table 15 - Users List

Subjects	Description
S.ISD-R	The ISD-R is responsible for the creation of new ISD-Ps and life-cycle management of all ISD-Ps. The ISD-R includes LPA Services that provides the necessary access to the services and data required by LPA functions. LPA Services are mandatory, regardless of the fact whether it is LPAe or LPAd which is active. The ISD-R acts also as an object. In this case, it is named S.ISD-R.
S.ISD-P	The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile. The ISD-P acts also as an object. In this case, it is named S.ISD-P.
S.ECASD	The Embedded UICC Controlling Authority Security Domain (ECASD) is responsible for secure storage of credentials required to support the required security domains on the eUICC.
S.PPI	Profile Package Interpreter, an eUICC Operating System service that translates the Profile Package data as defined in eUICC Profile Package Specification into an installed Profile using the specific internal format of the target eUICC.
S.PPE	Profile Rules Enforcer (PRE), which contains the Profile Policy Enabler (PPE). The PPE has two functions: ●Verification that a Profile containing PPRs is authorised by the RAT; ●Enforcement of the PPRs of a Profile.
S.TELECOM	The Telecom Framework is an Operating System service that provides standardised network authentication algorithms to the NAAs hosted in the ISD-Ps.
S.ADEL	The applet deletion manager which also acts on behalf of the card issuer. It may be an applet ([JCRE22], §11), but its role asks anyway for a specific treatment from the security viewpoint.
S.APPLET	Any applet instance.
S.BCV	The bytecode verifier (BCV), which acts on behalf of the verification authority who is in charge of the bytecode verification of the CAP files.
S.CAD	The CAD represents off-card entity that communicates with the S.INSTALLER. If the TOE provides JCRMI functionality, CAD can request RMI services by issuing commands to the card.
S.INSTALLER	The installer is the on-card entity which acts on behalf of the card issuer. This subject is involved in the loading of CAP files and installation of applets.
S.JCRE	The runtime environment under which Java programs in a smart card are executed.
S.JCVM	The bytecode interpreter that enforces the firewall at runtime.
S.LOCAL	Operand stack of a JCVM frame, or local variable of a JCVM frame containing an object or an array of references.
S.MEMBER	Any object's field, static field or array position.
S.CAP_FILE	A CAP file may contain multiple Java language packages. A package is a namespace within the Java programming language that may contain classes and interfaces. A CAP file may contain packages that define either user library, or one or several applets. A CAP file compliant with Java Card Specifications version 3.1 may contain multiple Java language packages. An EXTENDED CAP file as specified in Java Card

	Specifications version 3.1 may contain only applet packages, only library packages or a combination of library packages. A COMPACT CAP file as specified in Java Card Specifications version 3.1 or CAP files compliant to previous versions of Java Card Specification, MUST contain only a single package representing a library or one or more applets.
S.OSU	OS Upgrade provides secure functionality to update the TOE operating system with an image created by a trusted off-card entity (S.UpdateImageCreator)
S.UpdateImageCreator	The off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

Table 16 - Subjects List

3.3. Threats

The definition of threats from [PP-eUICC] where no refinements are made is not repeated here. See section 3.4.2.3 for complete list is threats.

The definition of each threat is present in [PP-eUICC]. The mapping against assets has been refined in the column “refined threats description” where assets in bold come from [PP-JCS].

Threats	Refined threats description
T.UNAUTHORIZED-PROFILE-MNG	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	Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA D.PLATFORM_RAT. By altering the behavior of ISD-R or PPE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-MNG.
T.PROFILE-MNG-INTERCEPTION	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	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	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	Directly threatens the assets: D.SECRETS, D.EID, **D.APP_C_DATA, D.PIN and D.APP_KEYs**.
T.UNAUTHORIZED-eUICC	Directly threatens the assets: D.TSF_CODE (ECASD), D.SK.EUICC.ECDSA,D.EID, D.SECRETS.
T.LPAd-INTERFACE-EXPLOIT	Directly threatened asset: D.DEVICE_INFO, D.PLATFORM_DATA.
T.UNAUTHORIZED-MOBILE- ACCESS	Directly threatens the assets: D.PROFILE_NAA_PARAMS.
T.LOGICAL-ATTACK	Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_POLICY_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT, **D.JCS_CODE, D.API_DATA, D.SEC_DATA, D.JCS_DATA, D.CRYPTO, D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs and D.APP_C_DATA**.
T.PHYSICAL-ATTACK	Directly threatens: all assets.
Additional T.Threat to cover OS Update	
T.CONFID-UPDATE-IMAGE.LOAD	Threat agent: Attacker Adverse action: The attacker discloses (part of) the image used to update the TOE in the field while the image is transmitted to the eUICC for installation. Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, D.JCS_DATA.

T.UNAUTH-UPDATE-IMAGE.LOAD	Threat agent: Attacker Adverse action: The attacker tries to upload an unauthorized Update Image. Directly threatened asset(s): D.JCS_CODE, D.JCS_DATA, D.UPDATE_IMAGE.
T.INTEG-UPDATE-IMAGE.LOAD	Threat agent: Attacker Adverse action: The attacker modifies (part of) the image used to update the TOE in the field while the image is transmitted to the card for installation. Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, D.JCS_DATA.
T.INTERRUPT-OSU	Threat agent: Attacker Adverse action: The attacker tries to interrupt the OS Upgrade procedure (Load Phase through activation of additional code) leaving the TOE in a partially functional state. Directly threatened asset(s): D.JCS_CODE, D.JCS_DATA, D.UPDATE_IMAGE, D.TOE_IDENTIFIER.

Table 17 - Threats List for the SPD

3.4. Organizational Security Policies

The definition of organizational security policies from [PP-eUICC] and [PP-JCS] is not repeated here. See section3.4.2.4 for complete list is organizational security policies.

OSPs	Description
OSP.LIFE-CYCLE	The TOE must enforce the eUICC life-cycle defined in [SGP.22]. In particular: ●There is a limit on the number of ISD-Ps enabled at a time: ■if the eUICC supports MEP, the limit is greater than one ■otherwise, the limit is one ●The eUICC must enforce the profile policy rules (PPR) in case a profile state change is attempted (installation, disabling or deletion of a profile), except during the memory reset or test memory reset functions: in this case, the eUICC may disable and delete the currently enabled profile, even if a PPR states that the profile cannot be disabled or deleted; ●The eUICC must enforce the rules authorisation table (RAT) before a profile containing PPRs is authorised to be installed on the eUICC.
OSP.VERIFICATION	

Table 18 - OSP List for the SPD

3.5. Assumptions

The definition of assumptions from [PP-eUICC] and [PP-JCS] where no refinements are made is not repeated here. See section 3.4.2.5 for complete list is assumptions.

Assumptions	Description
A.TRUSTED-PATHS-LPAd	It is assumed that the interfaces ES10a, ES10b and ES10c (SGP.22) are trusted paths between the eUICC and LPAd, when LPAd is present and active. It is also assumed that the LPAd is a trusted component. It is assumed that LPAd has a means to authenticate the End User (SGP.22). It is assumed that LPAd is protected against misuse. It is assumed that the Device manufacturer is securing the following operations (SGP.32): ●Add of an initial eIM Configuration Data by the IPA. ●Complete removal of eIM Configuration Data by the IPA.
A.ACTORS	Actors of the infrastructure (eSIM CA, EUM, SM-DP+, SM-DS,

	and MNO) securely manage their own credentials and otherwise sensitive data. In particular for the overall mobile authentication mechanism defined in 3GPP TS 33.102 [22] to be secure, certain properties need to hold that are outside the scope of the eUICC. In particular, subscriber keys need to be strongly generated and securely managed. The following assumptions are therefore stated: ●The key K is randomly generated during profile preparation and is securely transported to the Authentication Centre belonging to the MNO; ●The random challenge RAND is generated with sufficient entropy in the Authentication Centre belonging to the MNO; ●The Authentication Centre belonging to the MNO generates unique sequence numbers SQN, so that each quintuplet can only be used once; ●Triplets / Quintets1are communicated securely between MNOs for roaming.
A.APPLICATIONS	The applications shall comply with the security guidelines document for the used platform (operating system). These guideline must substantially describe the application writing style and the platform security mechanisms (e.g. security domains, application firewall) that shall be used to ensure that the applications do not harm the TOE.
A.CAP_FILE	
A.VERIFICATION	
A.PERSONLIZATION-SEC	Protection during Personalisation It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately. The assets to be protected are: The information and material produced and/or processed by the Security IC Embedded Software Developer in Phase 1 and by the Composite Product Manufacturer can be grouped as follows: 1. personalisation data including specifications of formats and memory areas, test related data.

Table 19 - Assumptions List for the SPD

4. SECURITY OBJECTIVES

This section introduces the security objectives for the TOE.

4.1. 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 2.4.3 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 2.4.3.2 and their description are listed next:

O.TOE	Replaced objectives description
O.PPE-PPI	
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE CHANNELS	
O.PROOF OF IDENTITY	
O.OPERATE	
O.API	

O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
O.IC.PROOF_OF_IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: (1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification). (2) It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PPE, S.PPI, and S.TELECOM). (3) It allows the S.PPE, S.PPI, and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection). (4) It provides a means to perform memory operations atomically for S.PPE, S.PPI, and S.TELECOM.
O.IC.RECOVERY	If there is a loss of power while an operation is in progress, the underlying IC must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.
O.RE.PPE-PPI	The Runtime Environment shall provide secure means for card management activities, including: ● Load of a package file, installation of a package file, ● Extradition of a package file or an application, ● Personalization of an application or a Security Domain, ● Deletion of a package file or an application, ● Privileges update of an application or a Security Domain, ● 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.
O.LOAD	
Additional O.TOE to cover OS Update	
O.SECURE_LOAD_ACODE	**Secure loading of the Additional Code** The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure.
O.SECURE_AC_ACTIVATION	**Secure activation of the Additional Code** Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE such as tearing, integrity violation, error case...), the Initial TOE shall remain in its initial state or fail secure.

O.TOE_IDENTIFICATION	**Secure identification of the TOE by the user** The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.
O.CONFID-UPDATE-IMAGE.LOAD	The TOE shall ensure that the encrypted image transferred to the device is not disclosed during the installation. The keys used for decrypting the image shall be kept confidential.
O.AUTH-LOAD-UPDATE-IMAGE	The TOE shall ensure that it is only possible to load an authorized image.

Table 20 - Security Objectives List for the TOE

4.2. 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 2.4.3.2 for complete list is Security Objectives for the Operational Environment.

O.ENV	Description
OE.CI	A.ACTORS
OE.SM-DP+	A.ACTORS
OE.SM-DS	A.ACTORS
OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.MNO-SD	
OE.CAP_FILE	No CAP file loaded post-issuance shall contain native methods.
OE.VERIFICATION	All the bytecodes shall be verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time. See #.VERIFICATION for details. Additionally, the applet shall follow all the recommendations, if any, mandated in the platform guidance for maintaining the isolation property of the platform. Application Note: Constraints to maintain the isolation property of the platform are provided by the platform developer in application development guidance. The constraints apply to all application code loaded in the platform.
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.PERSONLIZATION_SEC	Protection during composite product manufacturing Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.
Additional O.ENV to cover OS Update	
OE.CONFID_UPDATE_IMAGE.CREATE	Confidentiality of Update Image – CREATE The off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

Table 21 - Security Objectives List for the Operational Environment

4.3. Security Objectives Rationale

4.3.1. Threats

4.3.1.1. Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG:

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

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

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

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

T.UNAUTHORIZED-PLATFORM-MNG

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

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

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:

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

T.PROFILE-MNG-INTERCEPTION

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

Consequently, the TSF ensures:

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

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

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

4.3.1.2. 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.

4.3.1.3. 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).

4.3.1.4. LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

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

4.3.1.5. 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.

4.3.1.6. 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).

The following objectives for the operational environment are also required:

- prevention of unauthorized code execution by applications (O.RE.CODE-EXE),
- Compliance to security guidelines for applications (OE.APPLICATIONS, OE.VERIFICATION and OE.CODE-EVIDENCE).

T.PHYSICAL-ATTACK

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

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

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

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

4.3.1.7. OS Upgrade Threats

T.CONFID-UPDATE-IMAGE.LOAD

O.CONFID-UPDATEIMAGE.LOAD	Counters the threat by ensuring the confidentiality of D.UPDATE_IMAGE during installing it on the TOE.
OE.CONFID-UPDATEIMAGE. CREATE	Counters the threat by ensuring that the D.UPDATE_IMAGE is not transfered in plain and that the keys are kept secret.

Table 22 - T.CONFID-UPDATE-IMAGE.LOAD Threat

T.UNAUTH-UPDATE-IMAGE.LOAD

O.SECURE_LOAD_ACODE	Counters the threat directly by ensuring that only authorized (allowed version) images can be installed.
O.AUTH-LOAD-UPDATE- IMAGE	Counters the threat directly by ensuring that only authorized (allowed version) images can be loaded.

Table 23 - T.UNAUTH-UPDATE-IMAGE.LOAD Threat

T.INTEG-UPDATE-IMAGE.LOAD

O.SECURE_LOAD_ACODE	Counters the threat directly by ensuring the authenticity and integrity of D.UPDATE_IMAGE.

Table 24 - T.INTEG-UPDATE-IMAGE.LOAD Threat

T.INTERRUPT_OSU

O.SECURE_LOAD_ACODE	Counters the threat directly by ensuring that the TOE remains in a secure state after interruption of the OS Update procedure (Load Phase).
O.TOE_IDENTIFICATION	Counters the threat directly by ensuring that D.TOE_IDENTIFICATION is only updated after successful OS Update procedure.
O.SECURE_AC_ACTIVATION	Counters the threat directly by ensuring that the update OS is only activated after successful (atomic) OS Update procedure.

Table 25 - T.INTERRUPT_OSU Threat

4.3.2. Organizational Security Policies

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

OSPs	
OSP.LIFE-CYCLE	O.PPE-PPI ensures that there is a single ISD-P enabled at a time. The profile deletion capability relies on the secure application deletion mechanisms provided by OE.RE.PPE-PPI. O.OPERATE contributes to this OSP by ensuring that the Platform security functions are always enforced.
OSP.VERIFICATION	OSP.VERIFICATION is upheld by the security objective of the environment OE.VERIFICATION which guarantees that all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution in order to ensure that each bytecode is valid at execution time. This policy is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that evidences exist that the application code has been verified and not changed after verification, and by the security objective for the TOE O.LOAD which shall ensure that the loading of a CAP file into the card is safe.

Table 26 - OSPs List for the Security Objectives in [PP-eUICC]

4.3.3. Assumptions

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

Assumptions	
A.TRUSTED-PATHS-LPAd	This assumption is upheld by OE.TRUSTED-PATHS-LPAd.
A.ACTORS	This assumption is upheld by objectives OE.CI, OE.SM-DP+, and OE.MNO, which ensure that credentials and otherwise sensitive data will be managed correctly by each actor of the infrastructure.
A.APPLICATIONS	This assumption is directly upheld by objective OE.APPLICATIONS.
A.CAP_FILE	A.CAP_FILE is upheld by the security objective for the operational environment OE.CAP_FILE which ensures that no CAP file loaded post-issuance shall contain native methods.
A.VERIFICATION	This assumption is is upheld by the security objective on the operational environment OE.VERIFICATION which guarantees that all the bytecodes shall be verified at least once, before the loading, before the installation or before the execution in order to ensure that each bytecode is valid at execution time. This assumption is also upheld by the security objective of the environment OE.CODE-EVIDENCE which ensures that

	evidences exist that the application code has been verified and not changed after verification.
A.PERSONLIZATION-SEC	This assumption is directly upheld by objective OE.PERSONLIZATION_SEC.

Table 27 - Assumptions List for the Security Objectives in [PP-eUICC]

4.3.4. Rationale tables

4.3.4.1. Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, OE.VERIFICATION, OE.CODE-EVIDENCE, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Section 4.3.1.1
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.APPLICATIONS, OE.VERIFICATION, OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 4.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD	Section 4.3.1.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DP+, O.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 4.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 4.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 4.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 4.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	Section 4.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 4.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, OE.VERIFICATION, OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 4.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 4.3.1.6
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATE-IMAGE.LOAD, OE.CONFID-UPDATE-IMAGE.CREATE	Section 4.3.1.7
T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE, O.AUTH-LOAD-UPDATE-IMAGE	Section 4.3.1.7
T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE	Section 4.3.1.7
T.INTERRUPT-OSU	O.SECURE_LOAD_ACODE, O.TOE_IDENTIFICATION, O.SECURE_AC_ACTIVATION	Section 4.3.1.7

Table 28 - 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
O.SECURE_LOAD_ACODE	T.UNAUTH-UPDATE-IMAGE.LOAD, T.INTEG-UPDATE-IMAGE.LOAD, T.INTERRUPT-OSU
O.SECURE_AC_ACTIVATION	T.INTERRUPT-OSU
O.TOE_IDENTIFICATION	T.INTERRUPT-OSU
O.CONFID-UPDATE-IMAGE.LOAD	T.CONFID-UPDATE-IMAGE.LOAD
O.AUTH-LOAD-UPDATE-IMAGE	T.UNAUTH-UPDATE-IMAGE.LOAD
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DP+	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
O.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.IC.RECOVERY	T.PHYSICAL-ATTACK
O.RE.PPE-PPI	
O.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.RE.API	T.LOGICAL-ATTACK
O.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
O.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
O.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.VERIFICATION	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.CONFID-UPDATE-IMAGE.CREATE	T.CONFID-UPDATE-IMAGE.LOAD

Table 29 - Security Objectives and threats

4.3.4.2. Organizational Security Policies Rationale

Organizational Security Policies	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PPE-PPI, O.RE.PPE-PPI, O.OPERATE	Section 4.1
OSP.VERIFICATION	OE.VERIFICATION, O.LOAD, OE.CODE-EVIDENCE	Section 4.1

Table 30 - 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	
O.SECURE_LOAD_ACODE	
O.SECURE AC ACTIVATION	
O.TOE IDENTIFICATION	
O.CONFID-UPDATE-IMAGE.LOAD	
O.AUTH-LOAD-UPDATE-IMAGE	
OE.CI	
OE.SM-DP+	
OE.SM-DS	
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	
O.LOAD	OSP.VERIFICATION
OE.TRUSTED-PATHS-LPAd	
OE.APPLICATIONS	
OE.CAP_FILE	
OE.VERIFICATION	OSP.VERIFICATION
OE.CODE-EVIDENCE	OSP.VERIFICATION
OE.MNO-SD	
OE.CONFID_UPDATE_IMAGE.CREATE	

Table 31 - Security Objectives and Organizational Security Policies

4.3.4.3. Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd	OE.TRUSTED-PATHS-LPAd	Section 4.3.3

A.ACTORS	OE.CI, OE.SM-DP+, OE.SM-DS, OE.MNO	Section 4.3.3
A.APPLICATIONS	OE.APPLICATIONS,OE.VERIFICATION OE.CODE-EVIDENCE	Section 4.3.3
A.CAP_FILE	OE.CAP_FILE	Section 4.3.3
A.VERIFICATION	OE.VERIFICATION	Section 4.3.3
A.PERSONLIZATION-SEC	OE.PERSONLIZATION_SEC	Section 4.3.3

Table 32 - Assumptions and Security Objectives for the Operational Environment-Coverage

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-DP+	A.ACTORS
OE.SM-DS	A.ACTORS
OE.MNO	A.ACTORS
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.CAP_FILE	A.CAP_FILE
OE.VERIFICATION	A.VERIFICATION
OE.CODE-EVIDENCE	A.APPLICATIONS
OE.PERSONLIZATION_SEC	A.PERSONLIZATION-SEC
OE.MNO-SD	
OE.CONFID_UPDATE_IMAGE.CREATE	

Table 33 - Assumptions and Security Objectives for the Operational Environment

5. SECURITY REQUIREMENTS(ASE_REQ)

For section 5.1, the following conventions are used in the definitions of the SFRs:

- Selections and assignments that have already been made in the [PP-eUICC] are in bold, and the original text on which the selection or assignment has been made is not reminded.
- Selections and assignments made in this ST are in blue or **bold blue**.
- This convention also applies for section 5.2 for SFRs in light blue (as example below) dedicated to RSP module.

- **example**

Iteration operations on SFR components are denoted by showing a slash "/" and the iteration indicator after the SFR component identifier. For section 5.2, following conventions are used in the definitions of the SFRs :

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

- This convention applies for SFRs in dark blue as example below:

- **example**

5.1. eUICC Security Functional Requirements

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

5.1.1. Identification and authentication

This package describes the identification and authentication measures of the TOE: The TOE must:

- identify the remote user U.SM-DP+ by its SM-DP+ OID;
- identify the remote user U.MNO-OTA by its MNO OID;identify the on-card user U.MNO-SD by its AID, according to [ETSI TS 102 220];

The TOE must:

- authenticate U.SM-DP+ using CERT.DPauth.ECDSA;
- authenticate U.MNO-OTA via SCP80/81 using the keyset loaded in the MNO profile;

U.MNO-SD is not authenticated by the TOE. It is created on the eUICC during the profile download and installation by the U.SM-DP+. For this reason, the U.MNO-SD is bound to the internal subject S.ISD-P and this binding requires the U.SM-DP+ authentication. During the operational life of the TOE, U.MNO-SD acts on behalf of U.MNO-OTA, thus requiring U.MNO-OTA authentication.

The TOE shall bind the off-card and on-card users to internal subjects:

- U.SM-DP+ is bound to S.ISD-R;
- U.MNO-OTA is bound to U.MNO-SD, and U.MNO-SD is bound to the S.ISD-P managing the corresponding MNO profile;

The TOE shall eventually provide a means to prove its identity to off-card users.

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.

Application Note:
This SFR is related to the identification of the following external (remote) users of the TOE:

- U.SM-DP+;
- U.MNO-OTA;

The identification of the only local user (U.MNO-SD) is addressed by the FIA_UID.1/MNO-SD SFR.
Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote 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.

Application Note:

This SFR is related to the authentication of the following external (remote) users of the TOE:

- U.SM-DP+;
- U.MNO-OTA;

As the cryptographic mechanisms used for the authentication may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFRs.

The ST writer shall add FCS_COP.1 requirements to include the requirements stated by [SGP.22]:

- A U.SM-DP+ must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.DPauth.ECDSA and CERT.DPpb.ECDSA), as wellas the public key of the CI (D.PK.CI.ECDSA).
- U.MNO-OTA must be authenticated using a SCP80 secure channel according to [SCP80] using the parameters defined in [SGP.02] section 2.4.3, or optionally SCP81 according to [SCP81] using the parameters defined in [SGP.02] section 2.4.4 (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO).

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with at least one of the elliptic curves referenced for that purpose in SGP.22 [SGP.22].

FIA_USB.1/EXT User-subject binding

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

- **SM-DP+ OID is associated to S.ISD-R, acting on behalf of U.SM-DP+**
- **MNO OID is associated to U.MNO-SD, acting on behalf of U.MNO-OTA**.
- **SM-DS OID is associated to S.ISD-R, acting on behalf of U.SM-DS;**

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

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

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

- **Change of SM-DP+ OID requires U.SM-DP+ to be authenticated via "CERT.DPauth.ECDSA"**
- **change of MNO OID is not allowed.**
- **change of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA";**

Application Note:

This SFR is related to the binding of external (remote) users to local subjects or users of the TOE:

- U.SM-DP+ binds to a subject (S.ISD-R);
- U.SM-DS binds to a subject (S.ISD-R);
- U.MNO-OTA binds to an on-card user (U.MNO-SD);

The ST writer must be aware that U.MNO-SD is not a subject of the TOE, but an external on- card user acting on behalf of U.MNO-OTA, which is an external off-card user; and to apply the correct selections depending on the specification (SGP.22).

This SFR is related to the following commands:

- Initial association of the D.MNO_KEYS keyset is performed by the ES8+.ConfigureISDP command;

FIA_UAU.4/EXT Single-use authentication mechanisms

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

- **U.SM-DP+**
- **U.MNO-OTA**.

Application Note:

This SFR is related to the authentication of external (remote) users of the TOE:

- U.SM-DP+;
- 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.

Application Note:

This SFR is related to the identification of the local user U.MNO-SD only. The identification of remote users is addressed by the FIA_UID.1/EXT SFR.

It should be noted that the U.MNO-SD is identified but not authenticated. However, U.MNO-SD is installed on the TOE by the U.SM-DP+ via the subject S.ISD-R (see FDP_ACF.1/ISDR), and the binding between U.SM-DP+ and S.ISD-R requires authentication of U.SM-DP+, as described in FIA_USB.1/EXT.

FIA_USB.1/MNO-SD User-subject binding

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

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

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

Application Note:

This SFR is related to the identification of the local user U.MNO-SD.

Being a local but external user of the TOE, the U.MNO-SD is bound to the S.ISD-R which is responsible for its installation during the “Profile download and install” . This profile installation is controlled by the ISD-R content access control SFP (see FDP_ACC.1/ISDR). Being performed by the S.ISD-R, it requires authentication of the U.SM-DP+.

In order to perform operations such as PPR update, U.MNO-OTA authenticates, then sends a command to U.MNO-SD, which transmits it to S.ISD-P.

The identification does not depend on direct authentication of the MNO OTA Platform, but on the authentication of the S.ISD-R: The S.ISD-R installs a profile which includes a U.MNO-SD and associated keyset.

FIA_ATD.1/Base User attribute definition

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

- **CERT.DPauth.ECDSA, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-DP+;**
- **MNO OID belonging to U.MNO-OTA;**
- **AID belonging to U.MNO-SD;**
- **CERT.DSauth.ECDSA and SM-DS OID belonging to U.SM-DS;**

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.

Application Note:
This proof is obtained by including the EID value in the eUICC certificate, which is signed by the eUICC Manufacturer.

5.1.2. Communication

This package describes how the TSF shall protect communications with external users. The TSF shall enforce secure channels (FTP_ITC.1/SCP and FTP_ITC.2/SCP):

- between U.SM-DP+ and S.ISD-R;
- between U.MNO-OTA and U.MNO-SD.

These secure channels are used to import commands and objects, thus requiring that these commands and objects are consistently interpreted by the TSF (FPT_TDC. 1/SCP).

These secure channels are established according to a security policy (Secure Channel Protocol Information flow control SFP described in FDP_IFC.1/SCP and FDP_IFF.1/SCP). This policy specifically requires protection of the confidentiality (FDP_UCT.1/SCP) and integrity (FDP_UIT. 1/SCP) of transmitted information.

- The TSF must use cryptographic means to enforce this protection, and securely manage the associated keysets: generation and deletion of D.SECRETS(FCS_CKM.1/SCP-SM and FCS_CKM.6/SCP-SM);
- distribution and deletion of D.MNO_KEYS (FCS_CKM.2/SCP-MNO and FCS_CKM.6/SCP-MNO).

FDP_IFC.1/SCP Subset information flow control

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

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

FDP_IFF.1/SCP Simple security attributes

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

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

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

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

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

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

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

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

Application Note :

More details on the secure channels can be found in [SGP.22]

- For SM-DP+: Section 5.5;
- For MNO-SD: Section 5.4;

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**].

Application Note:

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the requirements stated by [SGP.22]:

- The secure channels to SM-DP+ must be SCP-SGP22 secure channels. Identification of endpoints is addressed by the use of AES according to [GPC v2.3] Amendment F using the parameters defined in [SGP.22], sections 2.6 and 5.5.
- SCP80 must be provided to build secure channels to MNO OTA Platform (section 5.4 of [SGP.22]). The TSF may also permit to use a SCP81 secure channel to perform the same functions than the SCP80 secure channel.

Related keys are:

- either generated on-card (D.SECRETS); see FCS_CKM.1/SCP-SM for further details.
- or distributed along with the profile (D.MNO_KEYS); see FCS_CKM.2/SCP-MNO for further details.

In terms of commands, the TSF shall permit remote actors to initiate communication via a trusted channel in the following cases:

- 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 (SGP.22 v3.1 or higher)
  - ES10a.SetDefaultDpAddress (SGP.22 v2.x)
  - 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 may permit the LPAd to transmit the following operations:
  - ES10b.VerifySmdpResponse (SGP.22 v3.1 or higher)
  - ES10b.PrepareDeviceChange (SGP.22 v3.1 or higher)
  - ES10b.VerifyDeviceChange (SGP.22 v3.1 or higher)

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

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

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

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

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

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

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

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

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

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

When shared between the TSF and another trusted IT product.

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

Application Note:

The commands related to the SFRs FPT_TDC.1/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP and the Downloaded objects related to this SFR FPT_TDC.1/SCP are listed below:

- SM-DP+ commands
  - ES8+.InitialiseSecureChannel

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

- LPAd commands
  - ES10a.GetEuiccConfiguredData (SGP.22 v3.1 or higher)
  - ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.x)
  - ES10a.SetDefaultDpAddress (SGP.22)
  - ES10b.PrepareDownload
  - ES10b.LoadBoundProfilePackage
  - ES10b.GetEUICCChallenge
  - ES10b.GetEUICCInfo
  - ES10b.ListNotification
  - ES10b.RetrieveNotificationsList
  - ES10b.RemoveNotificationFromList
  - ES10b.AuthenticateServer
  - ES10b.CancelSession
  - ES10c.EnableProfile
  - ES10c.DisableProfile
  - ES10c.DeleteProfile
  - ES10c.GetEID (SGP.22)
  - ES10c.SetNickname (SGP.22)
  - ES10b.GetRAT
  - ES10b.VerifySmdpResponse (SGP.22 v3.1 or higher)
  - ES10b.PrepareDeviceChange (SGP.22 v3.1 or higher)
  - ES10b.VerifyDeviceChange (SGP.22 v3.1 or higher)
- Downloaded objects from SM-DP+
  - Session keys
  - Profile Metadata (including PPR data)
- MNO commands
  - ES6.UpdateMetadata
- Downloaded objects from MNO OTA Platform
  - Profile Metadata (including PPR data)

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 unauthorized disclosure.

Application Note:

This SFR is related to the protection of:

- Profiles downloaded from SM-DP+;
- Commands received from SM-DP+ and MNO OTA Platform;
- PPR received from the MNO OTA Platform.

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the requirements stated by [SGP.22].

Related keys are:

- either generated on-card (D.SECRETS): see FCS_CKM.1/SCP-SM for further details;
- or distributed along with the Profile (D.MNO_KEYS); see FCS_CKM.2/SCP-MNO for further details.

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.

Application Note:
This SFR is related to the protection of:

- Profiles downloaded from SM-DP+;
- Commands received from SM-DP+ and MNO OTA Platform;
- PPR received from the MNO OTA Platform.

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the requirements stated by [SGP.22].

Related keys are:

- either generated on-card (D.SECRETS): see FCS_CKM.1/SCP-SM for further details;
- or distributed along with the Profile (D.MNO_KEYS); see FCS_CKM.2/SCP-MNO for further details.

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:
[assignment: ECKA-EG using one of the following standards:

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard)**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639)**
- **FRP256V1 (ANSSI ECC FRP256V1).**

].

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

Application Note:
This key generation mechanism is used to generate

- D.SECRETS keyset via the ES8+.InitialiseSecureChannel command, using the U.SM-DP+ public key otPK.DP.ECKA.

The Elliptic Curve cryptography used for this key agreement may be provided by the underlying Platform. Consequently this PP does not include the corresponding FCS_COP.1 SFR.

FCS_CKM.2/SCP-MNO Cryptographic key distribution

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

Application Note:
This SFR is related to the distribution of

- D.MNO_KEYS during profile download.

Note: this SFR does not apply to the private keys loaded pre-issuance of the TOE (D.SK.EUICC.ECDSA).

FCS_CKM.6/SCP-SM Cryptographic key destruction

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

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

FCS_CKM.6/SCP-MNO Cryptographic key destruction

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

FCS_CKM.6.2/SCP-MNO The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-MNO in accordance with a specified cryptographic key destruction method [assignment: **deletion of the key and removing it from the memory by garbage collection**] that meets the following: [assignment: **none**].

5.1.3. Security Domains

This package describes the specific requirements applicable to the Security Domains belonging to the TOE. In particular it defines:

- The rules under which the S.ISD-R can perform its functions (ISD-R content access control SFP in FDP_ACC.1/ISDR and FDP_ACF.1/ISDR),
- The rules under which the S.ISD-R can perform ECASD functions and obtain output data from these functions (ECASD access control SFP in FDP_ACC.1/ECASD and FDP_ACF.1/ECASD).

FDP_ACC.1/ISDR Subset access control

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

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

Application Note:

- This policy describes the rules to be applied to access Platform Management operations. It covers the access to operations by ISD-R required by sections 5.x of [SGP.22].

FDP_ACF.1/ISDR Security attribute based access control

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

- **subjects: S.ISD-R**
- **objects:**
  - **SO.ISD-P with security attributes "state" and "PPR", and [Selection: none]**
- **operations:**
  - **Create and configure profile**

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

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

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

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

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

Application Note:
This policy describes the rules to be applied to access Platform Management or eUICC Management operations. It covers the access to the following operations by ISD-R required by sections 5.x of [SGP.22]:

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

FDP_ACC.1/ECASD Subset access control

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

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

FDP_ACF.1/ECASD Security attribute based access control

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

- **subjects: S.ISD-R, with security attribute "AID", S.ECASD**
  objects: data and attributes of ECASD
  operations:

- **execution of a ECASD function**
  - **Verification of the off-card entities Certificates (SM-DP+, SM- DS), provided by an ISD-R, with the eSIM CA public key (D.PK.CI.ECDSA)**
  - **Creation of a eUICC signature on material provided by an ISD-R.**
- **access to output data of these functions.**

- **[assignment: none].**

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

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

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

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

5.1.4. Platform Services

This package describes the specific requirements applicable to the Profile Rules Enforcer, Profile Package Interpreter and the Telecom Framework. In particular it defines:

- FDP_IFC.1/Platform_services and FDP_IFF.1/Platform_services: the measures taken to control the flow of information between the Security Domains and PRE, PPI or Telecom Framework;
- FPT_FLS.1/Platform_services: the measures to enforce a secure state in case of failures of PRE, PPI or Telecom Framework.

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.**
  - **[selection: none]**

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)"**
  - **Platform code (S.PRE, 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.**
  - **[selection: none]**

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

- **D.PROFILE_NAA_PARAMS shall be transmitted only:**
  - **by U.MNO-SD to S.TELECOM in order to execute the network authentication function**
  - **by S.ISD-R to S.PPI using the profile installation function**
- **D.PROFILE_POLICY_RULES shall be transmitted only**
  - **by S.ISD-R to S.PPE in order to execute the PPR enforcement function**
  - **[selection: none]**
- **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: **no additional rules**].

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**].

Application Note:
This SFR aims to control which subject is able to transmit Profile Policy Rules, network authentication keys to the PRE, PPI, and Telecom Framework. Differences in implementation are allowed, since this PP requires demonstrable conformance. It is consequently possible for the ST writer to replace this SFR by another instance of FDP_IFF.1 as long as it addresses the control of information flow for these data. Examples of such adaptations could be due to cases such as:

- D.PROFILE_RULES transmitted from S.ISD-P to S.ISD-R, then from S.ISD-R to S.PRE;
- D.PROFILE_NAA_PARAMS transmitted from U.MNO-SD to S.ISD-P, then by S.ISD-P to S.TELECOM.

FPT_FLS.1/Platform_services Failure with preservation of secure state

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

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

Application Note:
The ST writer shall include both:

- this FPT_FLS.1/Platform_services SFR, and

- the FPT_FLS.1 SFR required by the security objectives of [PP-JCS]. The two SFRs may be merged into a single one, but the ST writer must make sure that the merged SFR includes the specific failure cases of this PP and those of [PP-JCS].

5.1.5. Security management

This package includes several supporting security functions:

- Random number generation (FCS_RNG. 1)
- User data and TSF self-protection measures:
  - TOE emanation (FPT_EMS. 1/Base)
  - protection from integrity errors (FDP_SDI. 1/Base)
  - residual data protection (FDP_RIP. 1/Base)
  - preservation of a secure state (FPT_FLS. 1/Base)
- Security management measures:
  - Management of security attributes such as Platform data (FMT_MSA.1/PLATFORM_DATA), (FMT_MSA. 1/RAT) and keys (FMT_MSA. 1/CERT_KEYS) with restrictive default values (FMT_MSA.3);
  - Management of roles and security functions (FMT_SMR.1 and FMT_SMF.1/Base).

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a [selection: **deterministic]** random number generator [selection: **DRG.3**] that implements: [assignment: **Hybrid design, Forward secrecy, Enhanced backward secrecy, Output and mutual difference, Statistical tests**].

FCS_RNG.1.2 The TSF shall provide [**selection: bits, octets of bits, numbers [assignment: format of the numbers that meet the requirements of class DRG.3]**] that meet [assignment: **a defined quality metric of the selected RNG class**].

Application Note:

- Hybrid design: (DRG.3.1) *"If initialized with a random seed using a PTRNG of class PTG.2 as random source, the internal state of the RNG shall have at least 256 bit of entropy".*
- Forward secrecy: (DRG.3.2) *"The RNG provides forward secrecy"* .
- Enhanced backward secrecy: (DRG.3.3) *"The RNG provides enhanced backward secrecy even if the current internal state is known".*
- Output and mutual difference: (DRG.3.4) *"The RNG, initialized with a random seed using a PTRNG of class PTG.2 as random source generates output for which 2^{48} strings of bit length 128 are mutually different with probability at least 1-2^{24}".*
- Statistical tests: (DRG.3.5) *"Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A"* .

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

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

ID	Emission	Attack surface	TSF data	User data

1	[assignment: ***power consumption and electromagnetic fluctuations***]	**Any**	**-**	● **D.SECRETS;** ● **D.SK.EUICC.ECDSA** **and the secret keys which are part of the following keysets:** ● **D.MNO_KEYS,** ● **D.PROFILE_NAA_PARAMS.**

Table 34 - Base TOE Emanation of TSF and User data List Explanation

Application Note:

The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate from internal operation of the TOE or may originate from an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE.

Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE′s electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, and so on.

FDP_SDI.1/Base Stored data integrity monitoring

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

Refinement:

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

- D.MNO_KEYS
- Profile data
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE_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/Base Subset residual information protection

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

- **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/Base Failure with preservation of secure state

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

- **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 content access control policy** to restrict the ability to modify the security attributes **the following parts of D.PLATFORM_DATA of:**

- **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).**

Application Note :

- In case part of the Platform functionality is performed by GlobalPlatform packages, the role of S.PRE may for instance be partly attributed to the OPEN.

FMT_MSA.1/RULES Management of security attributes

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

- **D.PROFILE_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"**
- **[selection:**

S.ISD-R to delete, via function "ES10c.DeleteProfile" (SGP.22)]

Application Note:

The ST writer must choose all options applicable to SGP.22 depending on the technical specification implemented by the TOE.

FMT_MSA.1/CERT_KEYS Management of security attributes

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

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

to

- **S.ISD-R for:**
  - **query D.PK.CI.ECDSA**
  - **delete D.MNO_KEYS, via function [selection: ES10c.DeleteProfile (SGP.22)]**
- **no actor for other operations.**

Application Note :
The modification of D.MNO_KEYS keysets is forbidden. To modify the keysets, one must delete the profile and load another profile.

FMT_SMF.1/Base Specification of Management Functions

FMT_SMF.1.1/Base 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 (linked to roles S.ISD-R, U.SM-DP+, S.ISD-P, U.MNO-SD, U.MNO-OTA)
- Platform services information flow control (linked to roles S.PPI, S.ISD-P, S.ISD-R, U.MNO-SD)
- ISD-R access control (linked to role S.ISD-R, U.SM-DP+)
- ISD-P content access control (linked to roles S.ISD-P, U.MNO-SD, U.MNO-OTA)
- ECASD access control (linked to roles S.ECASD)

FMT_SMR.1/Base Security roles

FMT_SMR.1.1/Base The TSF shall maintain the roles

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

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

Application Note :
The roles defined here correspond to the users and subjects defined in Section 3.2.

FMT_MSA.1/RAT Management of security attributes

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

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

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-R content access control SFP, ECASD access control SFP and Platform services information flow control SFP** to provide restrictive default values for security attributes that are used to enforce the SFP.

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

5.1.6. Mobile Network authentication

This package defines the requirements related to the authentication of the eUICC on MNO networks.

The TSF must implement cryptographic mechanisms for the authentication on the MNO network (FCS_COP. 1/Mobile_network) and manage the keys securely (FCS_CKM.2/Mobile_network and FCS_CKM.6/Mobile_network).

FCS_COP.1/Mobile_network Cryptographic operation

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

- **MILENAGE according to standard [ETSI TS 135 206] 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 [ETSI TS 135 206].**
- **Tuak according to [ETSI TS 135 231] 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.**

Application Note :

The ST writer must list the complete list of algorithms supported by the telecom framework of the TOE (for example Milenage, and so on).

The keys used by these algorithms are distributed within the profiles during provisioning (see FCS_CKM.2/Mobile_network) and must be securely deleted (FCS_CKM.6/Mobile_network).

FCS_CKM.2/Mobile_network Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: **cryptographic key distribution method**] that meets the following: [assignment: **following standards**].

Item	Method	Standard
Milenage	distribution method from SCP-SGP22 (SCP03t)	[SGP.22]
Tuak	distribution method from SCP-SGP22 (SCP03t)	[SGP.22]

Table 35 - Mobile network Cryptographic key distribution List Explanation

Application Note :

The keys in this SFR are the Mobile Network authentication keys included in the asset D.PROFILE_NAA_PARAMS. These keys are distributed as a part of the MNO profile during profile download.

FCS_CKM.6/Mobile_network Cryptographic key destruction

FCS_CKM.6.1/Mobile_network The TSF shall destroy **[assignment: list of cryptographic keys (including keying material)] when [selection: no longer needed] .**

Item	List of Cryptographic keys
Milenage	K, RAND, SQN, AMF
Tuak	K, RAND, SQN, AMF

Table 36 - Mobile network Cryptographic key destruction List Explanation

FCS_CKM.6.2/ Mobile_network The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/Mobile_network in accordance with a specified cryptographic key destruction method **[assignment: deletion of the key and removing it from the memory by garbage collection]** that meets the following: **[assignment: none]**.

Application Note:
The selection of FCS_CKM.6.1/Mobile_network must be done in accordance with the NAA algorithms selected in FCS_COP.1/Mobile_network.

5.2. Runtime Environment Security Requirements

The following conventions for [PP-JCS] are used in the definitions of the SFRs:

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

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

5.2.1. CoreLG Security Functional requirements

5.2.1.1. 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:

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

Table 37 - Security attribute based access control List Explanation

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 (check cast) or is being verified as being an instance of (instance of) 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 authorize 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 Life Time 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" Life Time 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. Nevertheless, 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

Table 38 - Simple security attributes List Explanation

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 **No additional rules** [1].

FDP_IFF.1.4/JCVM The TSF shall explicitly authorize an information flow based on the following rules: **No additional rules** [2].

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **No additional rules** [3].

Application note:

The storage of temporary Java Card RE-owned objects references is runtime-enforced ([JCRE3], §6.2.8.1-3).

It should be noticed that this policy essentially applies to the execution of bytecode. Native methods, the Java Card RE itself and possibly some API methods can be granted specific rights or limitations through the FDP_IFF.1.3/JCVM to FDP_IFF.1.5/JCVM elements. The way the Java Card virtual machine manages the transfer of values on the stack and local variables (returned values, uncaught exceptions) from and to internal registers is implementation-dependent. For instance, a returned reference, depending on the implementation of the stack frame, may transit through an internal register prior to being pushed on the stack of the invoker. The returned bytecode would cause more than one OP.PUT operation under this scheme.

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

[1] [assignment: additional information flow control SFP rules]
[2] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[3] [assignment: rules, based on security attributes, that explicitly deny information flows]

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-Life Time attribute's value.
- Any O.JAVAOBJECT whose Life Time attribute value is not PERSISTENT has an array type as JavaCardClass attribute's value.

FMT_MSA.3/FIREWALL	Static attribute initialization

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).

Application note, 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 initialization

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.

5.2.1.2. 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 **ECDSA Key Pair Generation** [4] and specified cryptographic key sizes **256,384, 521** [5] that meet the following: **see application note** [6].

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	LENGTH_EC_FP_256 LENGTH_EC_FP_384 LENGTH_EC_FP_521 ALG_TYPE_EC_FP_PRIVATE ALG_TYPE_EC_FP_PUBLIC
javacard.security.KeyPair	ALG_EC_FP ALG_EC_F2M

Table 39 - Cryptographic key generation List Explanation

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]** and specified cryptographic key sizes **[assignment: cryptographic key size]** that meet the following: **[assignment: cryptographic standard]**.

SCP protocol	Cryptographic algorithm	Cryptographic key size	Cryptographic standard
SCP02	TDES 2-keys	128 bits	[GPCS] section E.4.1
SCP03	AES	128, 192, 256 bits	[Amd D] section 6.2.1
SCP81	TDES 3-keys	192 bits	[Amd B] section 3.3.2
	AES	128 bits	[Amd B] section 3.3.2

Table 40 - GP-SCP Cryptographic key generation List Explanation

[4] [assignment: cryptographic key generation algorithm]
[5] [assignment: cryptographic key sizes]
[6] [assignment: list of standards]

FCS_COP.1/TDES_MAC	Cryptographic operation

FCS_COP.1.1/TDES_MAC The TSF shall perform **MAC computation of applet instance's data** [7] in accordance with a specified cryptographic algorithm **MAC algorithms mentioned in the application note below** [8] and cryptographic key sizes **128 bits for TDES 2 Keys, 192 bits for TDES 3 Keys** [9] that meet the following: **FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5** [10].

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

MAC length	MAC algorithm	Field name in [JCAPI3] Signature class
4 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC4_ISO9797_1_M1_ALG3
4 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC4_ISO9797_1_M2_ALG3
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_ISO9797_M1
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_ISO9797_M2
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_PKCS5
4 bytes	3DES in outer CBC mode	ALG_DES_MAC4_NOPAD
8 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC8_ISO9797_1_M1_ALG3
8 bytes	ISO9797-1 MAC algorithm 3	ALG_DES_MAC8_ISO9797_1_M2_ALG3
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_ISO9797_M1
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_ISO9797_M2
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_PKCS5
8 bytes	3DES in outer CBC mode	ALG_DES_MAC8_NOPAD

Table 41 - TDES_MAC Cryptographic operation List Explanation

FCS_COP.1/AES_MAC	Cryptographic operation

FCS_COP.1.1/AES_MAC The TSF shall perform **MAC computation of applet instance's data** [11] in accordance with a specified cryptographic algorithm **MAC algorithms mentioned in the application note below** [12] and cryptographic key sizes **128, 192 and 256 bits** [13] that meet the following: **FIPS PUB 197, NIST SP800-38A** [14].

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

MAC length	MAC algorithm	Field name in [JCAPI3] Signature class
16 bytes	AES in CBC mode, block size 128 bits	ALG_AES_MAC_128_NOPAD
16 bytes	AES in CBC mode, block size 128 bits	ALG_AES_CMAC_128
24 bytes	AES in CBC mode, block size 192 bits	ALG_AES_MAC_192_NOPAD
32 bytes	AES in CBC mode, block size 256 bits	ALG_AES_MAC_256_NOPAD

Table 42 - AES_MAC Cryptographic operation List Explanation

FCS_COP.1/ECDH	Cryptographic operation

FCS_COP.1.1/ECDH The TSF shall perform **Secret Key Agreement** [15] in accordance with a specified cryptographic algorithm **Elliptic Curve Diffie-Hellman (ECDH)** [16] and cryptographic key sizes **P ranging from 256 to 521 bits** [17] that meet the following: **IEEE P1363** [18].

Application note: the secret keys are derived using the KeyAgreement class (generate.Secret method) of javacard.security. The following [JCAPI3] fields are supported:

[7] [assignment: list of cryptographic operations]
[8] [assignment: cryptographic algorithm]
[9] assignment: cryptographic key sizes]
[10] [assignment: list of standards]
[11] [assignment: list of cryptographic operations]
[12] [assignment: cryptographic algorithm]
[13] [assignment: cryptographic key sizes]
[14] [assignment: list of standards]
[15] [assignment: list of cryptographic operations]
[16] [assignment: cryptographic algorithm]
[17] [assignment: cryptographic key sizes]
[18] [assignment: list of standards]

Field name in [JCAPI3] KeyAgreement class
ALG_EC_SVDP_DH
ALG_EC_SVDP_DH_PLAIN
ALG_EC_SVDP_DHC
ALG_EC_SVDP_DHC_PLAIN
ALG_XDH

Table 43 - ECDH Cryptographic operation List Explanation

FCS_COP.1/ECDSA_SIGN Cryptographic operation

FCS_COP.1.1/ECDSA_SIGN The TSF shall perform **signature generation and signature verification of applet instance's data** [19] in accordance with a specified cryptographic algorithm **ECDSA as mentioned in the application note below** [20] and cryptographic key sizes **256, 384, 521 bits** [21] that meet the following: **FIPS PUB 186-4** [22].

Application note: the following ECDSA signatures from [JCAPI3] are implemented:

Hash algorithm	Field name in [JCAPI3] Signature class
SHA256	ALG_ECDSA_SHA_256
SHA384	ALG_ECDSA_SHA_384
SHA512	ALG_ECDSA_SHA_512

Table 44 - ECDSA_SIGN Cryptographic operation List Explanation

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**].

[JCAPI3] class	Implemented algorithm
KeyAgreement	ALG_EC_SVDP_DH
	ALG_EC_SVDP_DH_PLAIN

Table 45 - ECKA_EG Cryptographic operation List Explanation

FCS_COP.1/GP-SCP Cryptographic operation

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

SCP Protocol	Operation	Algorithm	Key Sizes	Standards
SCP03, SCP11	Symmetric Encryption/Decryption	AES in CBC mode	128, 192, or 256 bits	FIPS 197 NIST 800 38A
SCP03	MAC Generation/ Verification	CMAC AES	128, 192, or 256 bits	NIST 800 38B
SCP03	Key Derivation	CMAC-based KDF using AES	128, 192, or 256 bits	NIST 800 108 NIST 800 38B

[19] [assignment: list of cryptographic operations]
[20] [assignment: cryptographic algorithm]
[21] [assignment: cryptographic key sizes]
[22] [assignment: list of standards]

SCP03, SCP11	Hash Computing	SHA-256, SHA-384, SHA-512	-	ISO 10118-3 FIPS 180 4
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 128 or 192 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_NULL_SHA256 TLS_PSK_WITH_3DES_EDE_CBC_SHA TLS_PSK_WITH_AES_128_GCM_SHA256 TLS_PSK_WITH_AES_128_CBC_SHA256	-	[Amd B] section 3.3.2
SCP-SGP22	**Secure communication channel with the SM-DP+ for mutual authentication**	**ECKA-EG**	**NIST P-256 brainpoolP256r1**	**SGP.22 FIPS PUB 186-3 Digital Signature Standard,BSI TR-0311 Version 1.11 RFC 5639**
SCP-SGP22 (SCP03t)	**Secure communication channel with the SM-DP+ for profile download**	**AES**	**AES: 128 bits**	**SGP.02**

Table 46 - GP-SCP Cryptographic operation List Explanation

FCS_COP.1/TDES_CIPHER Cryptographic operation

FCS_COP.1.1/TDES_CIPHER The TSF shall perform **encryption and decryption of applet instance's data** [23] in accordance with a specified cryptographic algorithm **Triple DES 2 Keys or Triple DES 3 Keys with cipher modes mentioned in the application note below** [24] and cryptographic key sizes **128 bits for TDES 2 Keys, 192 bits for TDES 3 Keys** [25] that meet the following: **FIPS PUB 46-3, FIPS PUB 81, ISO/IEC 9797-1, PKCS#5** [26].

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

Table 47 - TDES_CIPHER Cryptographic operation List Explanation

FCS_COP.1/AES_CIPHER Cryptographic operation

FCS_COP.1.1/AES_CIPHER The TSF shall perform **encryption and decryption of applet instance's data** [27] in accordance with a specified cryptographic algorithm **AES with cipher modes mentioned in the application note below** [28] and cryptographic key sizes **128, 192 and 256 bits** [29] that meet the following: **FIPS PUB 197, NIST SP800-38A, NIST SP800-38D, ISO/IEC 9797-1, PKCS#5** [30].

[23] [assignment: list of cryptographic operations]
[24] [assignment: cryptographic algorithm]
[25] [assignment: cryptographic key sizes]
[26] [assignment: list of standards]
[27] [assignment: list of cryptographic operations]
[28] [assignment: cryptographic algorithm]

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

Mode	Field name in [JCAPI3] Cipher class
CBC	ALG_AES_BLOCK_256_CBC_NOPAD
CBC	ALG_AES_BLOCK_192_CBC_NOPAD
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_256_ECB_NOPAD
ECB	ALG_AES_BLOCK_192_ECB_NOPAD
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
Mode	**Field name in [JCAPI3] AEADCipher class**
Counter with CBC-MAC	ALG_AES_GCM
Counter with CBC-MAC	CIPHER_AES_GCM

Table 48 - AES_CIPHER Cryptographic operation List Explanation

FCS_COP.1/RSA_SIGN Cryptographic operation

FCS_COP.1.1/RSA_SIGN The TSF shall perform **signature generation and signature verification of applet instance's data**[31] in accordance with a specified cryptographic algorithm **RSA Standard and RSA CRT with hash algorithms and padding schemes mentioned in the application note below**[32] and cryptographic key sizes **1024 to 4096 bits by steps of 32 bits**[33] that meet the following: **PKCS#1, PKCS#1-PSS (IEEE 1363-2000), ISO/IEC 9796-2 and RFC2409**[34].

Application note: the following RSA signatures from [JCAPI3] are implemented:

Hash algorithm	Padding scheme	Field name in [JCAPI3] Signature class
SHA256	PKCS#1	ALG_RSA_SHA_256_PKCS1
SHA256	PKCS#1-PSS scheme (IEEE 1363-2000)	ALG_RSA_SHA_256_PKCS1_PSS
SHA384	PKCS#1	ALG_RSA_SHA_384_PKCS1
SHA384	PKCS#1-PSS scheme (IEEE 1363-2000)	ALG_RSA_SHA_384_PKCS1_PSS
SHA512	PKCS#1	ALG_RSA_SHA_512_PKCS1
SHA512	PKCS#1-PSS scheme (IEEE 1363-2000)	ALG_RSA_SHA_512_PKCS1_PSS

Table 49 - RSA_SIGN Cryptographic operation List Explanation

FCS_COP.1/RSA_CIPHER Cryptographic operation

FCS_COP.1.1/RSA_CIPHER The TSF shall perform **encryption and decryption of applet instance's data**[35] in accordance with a specified cryptographic algorithm **RSA Standard and RSA CRT as mentioned in the application note below**[36] and cryptographic key sizes **1024 to 4096 bits by steps of 32 bits**[37] that meet the following: **ISO14888, ISO9796, PKCS#1, PKCS#1-OAEP scheme (IEEE 1363-2000)**[38].

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

---

[29] [assignment: cryptographic key sizes]
[30] [assignment: list of standards]
[31] [assignment: list of cryptographic operations]
[32] [assignment: cryptographic algorithm]
[33] [assignment: cryptographic key sizes]
[34] [assignment: list of standards]
[35] [assignment: list of cryptographic operations]
[36] [assignment: cryptographic algorithm]
[37] [assignment: cryptographic key sizes]
[38] [assignment: list of standards]

[JCAPI3] class	Implemented algorithms
Cipher	ALG_RSA_ISO9796
	ALG_RSA_NOPAD
	ALG_RSA_PKCS1
	ALG_RSA_PKCS1_OAEP

Table 50 - RSA_CIPHER Cryptographic operation List Explanation

FCS_COP.1/Hash Cryptographic operation

FCS_COP.1.1/Hash The TSF shall perform **computation of a hash value for applet instance's data** [39] in accordance with a specified cryptographic algorithm **see application note** [40] and cryptographic key sizes **none** [41] that meets the following: **see application note** [42].

Application note: the following hash algorithms from [JCAPI3] are implemented

Hash algorithm	Field name in [JCAPI3] MessageDigest class	Related Standard
SHA-256	ALG_SHA_256	FIPS 180-4
SHA-384	ALG_SHA_384	FIPS 180-4
SHA-512	ALG_SHA_512	FIPS 180-4

Table 51 - Hash Cryptographic operation List Explanation

FCS_COP.1/HMAC Cryptographic operation

FCS_COP.1.1/HMAC The TSF shall perform **computation of a HMAC value for applet instance's data** [43] in accordance with a specified cryptographic algorithm **HMAC with hash algorithms mentioned in the application note below** [44] and cryptographic key sizes **see application note** [45] that meet the following: **rfc2104** [46].

Application note: the following HMAC algorithms from [JCAPI3] are implemented

Hash algorithm used in HMAC computation	Field name in [JCAPI3] Signature class
SHA256	ALG_HMAC_SHA_256
SHA384	ALG_HMAC_SHA_384
SHA512	ALG_HMAC_SHA_512
-	SIG_CIPHER_HMAC

Table 52 - HMAC Cryptographic operation List Explanation

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**.

[39] [assignment: list of cryptographic operations]
[40] [assignment: cryptographic algorithm]
[41] [assignment: cryptographic key sizes]
[42] [assignment: list of standards]
[43] [assignment: list of cryptographic operations]
[44] [assignment: cryptographic algorithm]
[45] [assignment: cryptographic key sizes]
[46] [assignment: list of standards]

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

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).

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 either is 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).

5.2.1.3. 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,
- **GlobalPlatform card state inconsistency** [47]

Application note: in FAU_ARP.1.1, the [assignment: list of other actions] is set to 'none', meaning that no other actions are defined in this SFR component.

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 **integrity errors** [48] on all objects, based on the following attributes: **integrity check data** [49].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **mute the card and decrease the global fault detection counter. Once the global fault detection counter reaches 0, the card is put in degraded mode.** [50]

Application note: the following data persistently stored by TOE have an integrity check data security attribute:

- Key (i.e. objects instance of classes implemented the interface Key)
- PIN (objects instance of class OwnerPin)
- Package
- GlobalPlatform card state (OP_READY, SECURED, CARD_LOCKED, TERMINATE)

FPR_UNO.1 Unobservability

[47] [assignment: list of other runtime errors]
[48] [assignment: integrity errors]
[49] [assignment: user data attributes]
[50] [assignment: action to be taken]

FPR_UNO.1.1 The TSF shall ensure that **any user** [51] are unable to observe the operation **read, write, cryptographic operations** [52] on **PIN, Key** [53] by **any other user or subject** [54].

FPT_FLS.1/JC	Failure with preservation of secure state

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

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,**
- **None** [55]

When interpreting the TSF data from another trusted IT product.

Application note: concerning the interpretation of data between the TOE and the underlying Java Card platform, it is assumed that the TOE is developed consistently with the SCP functions, including memory management, I/O functions and cryptographic functions.

5.2.1.4. 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.

---

[51] [assignment: list of users and/or subjects]
[52] [assignment: list of operations]
[53] [assignment: list of objects]
[54] [assignment: list of protected users and/or subjects]
[55] [assignment: list of interpretation rules to be applied by the TSF]

- 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: **CAP file AID are defined with associated value during loading and with context identifier**[56].

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: **None**[57].

Application note: the user is the applet and the subject is the S.CAP_FILE. The subject security attribute "Context" shall hold the user security attribute "CAP file AID".

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**.

5.2.2. INSTG Security Functional requirements

Refer the following SFRs from [PP-GP]:

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

5.2.3. 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 by ST implements.

FDP_ACC.2/ADEL	Complete access control

[56] [assignment: rules for the initial association of attributes]
[57] [assignment: rules for the changing of attributes]

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, and 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

Table 53 - ADEL-Security attribute based access control List Explanation

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], §11.3.4.2, 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, Multiple Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon several O.APPLET only if,**
    1) S.ADEL is currently selected,
    2) there is no instance of any of the O.APPLET being deleted that is active in any logical channel and
    3) there is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a CAP file P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.
  - **R.JAVA.16 ([JCRE3], §11.3.4.3, 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, 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 authorize 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 security target.

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 note 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**.

Application note: patch deletion is an extension of applet/package deletion defined in GlobalPlatform as a patch is managed as a JavaCard Package and registered with specific attributes.

FMT_MSA.3/ADEL Static attribute initialization

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.

Application note: patch deletion is an extension of applet/package deletion defined in GlobalPlatform as a patch is managed as a JavaCard Package and registered with specific attributes.

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.)

Application note: patch deletion is an extension of applet/package deletion defined in GP as a patch is managed as a JavaCard Package and registered with specific attributes.

5.2.4. RMIG Security Functional Requirements

The product does not support RMI features.

5.2.5. 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).

5.2.6. CARG Security Functional Requirements

Refer the following SFRs from [PP-GP]:

- **FCO_NRO.2/GP** using FCO_NRO.2.1/CM of [PP-JCS]
- **FDP_IFC.2/GP-ELF** using FDP_IFC.2/CM of [PP-JCS]
- **FDP_IFF.1/GP-ELF** using FDP_IFF.1/CM of [PP-JCS]
- **FDP_UIT.1/GP** using FDP_UIT.1/CM of [PP-JCS]
- **FIA_UID.1/GP** using FIA_UID.1/CM of [PP-JCS]
- **FMT_MSA.1/GP** using FMT_MSA.1/CM of [PP-JCS]
- **FMT_MSA.3/GP** using FMT_MSA.3/CM of [PP-JCS]
- **FMT_SMF.1/GP** using FMT_SMF.1/CM of [PP-JCS]
- **FTP_ITC.1.3/GP** using FTP_ITC.1/CM of [PP-JCS]

5.2.7. Global Platform Security Functional requirements

FPT_FLS.1/GP	Failure with preservation of secure state

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

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

- **None** [58]

Application Note:

- This SFR extends FPT_FLS.1/Installer of [PP-JCS] to include the failures that may occur during the loading of SD/Application keys and data.
- Refer to [JCRE3] section 11.1.5 and [GPCS] sections 11.5, 11.6, 11.8, and 11.11 for additional details.

FDP_ROL.1/GP Basic rollback

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

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

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

FCO_NRO.2/GP Enforced proof of origin

FCO_NRO.2.1/GP The TSF shall enforce the generation of evidence of origin for transmitted **Executable Load Files, SD/Application data and keys** [59] at all times.

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

FCO_NRO.2.2/GP The TSF shall be able to relate the **identity** [60] of the originator of the information, and the **Executable Load Files, SD/Application data and keys** [61] of the information to which the evidence applies.

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

FCO_NRO.2.3/GP The TSF shall provide a capability to verify the evidence of origin of information to **the off card entity (recipient of the evidence of origin) who requested that verification** given **at the time the ELF, SD/Application data and keys are received** [62].

Application Note:

- This SFR extends FCO_NRO.2/CM of [PP-JCS] to cover the SD/Application data and keys transmitted and loaded to the card via STORE DATA and PUT KEY commands.

FMT_SMR.1/GP Security roles

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

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

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

Application Note: this SFR refines and replaces FMT_SMR.1/Installer and FMT_SMR.1/CM of [PP- JCS], applied to roles involved in card content management operations.

---

[58] [assignment: list of additional types of failures]
[59] [assignment: list of information types]
[60] [assignment: list of attributes]
[61] [assignment: list of information fields]
[62] [assignment: limitations on the evidence of origin]

FMT_SMF.1/GP Specification of Management Functions

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

- **Card and Application Security Management as defined in [GPCS]: Life Cycle, Privileges, Application/SD Locking and Unlocking, Card Locking and Unlocking, Card Termination, Application Status interrogation, Card Status Interrogation, command dispatch, Operational Velocity Checking.**
- **Management functions (Secure Channel Initiation/Operation/Termination) related to SCPs as defined in [GPCS].**

Application Note:

- This SFR refines and replaces FMT_SMF.1/CM of [PP-JCS].
- Management functions related to SCPs are defined in [GPCS] Chapter 10.

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

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

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

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

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

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

- **Referring to Java Card rules defined in [JCVM3] and [JCRE3]: ELF loading is allowed only if, for each dependent ELF, its AID attribute is equal to a resident ELF AID attribute, and the major (minor) Version attribute associated with the dependent ELF is less than or equal to the major (minor) Version attribute associated with the resident ELF.**
- **None** [63]

Application Note:

- This SFR corresponds to FDP_ITC.2/Installer of [PP-JCS].
- Java Card rules are defined in [JCVM3] sections 4.4 and 4.5 and [JCRE3] section 11.
- The TSF shall use the INSTALL data format and the LOAD data format when interpreting the user data from outside the TOE.

FDP_IFC.2/GP-KL Complete information flow control

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

- **Subjects: S.SD, S.CAD, S.OPEN, Application**
- **Information: GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys**

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

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

Application Note:

- GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively.
- The subject S.SD can be the ISD, an APSD, or the CASD.

---

[63] [assignment: additional importation control rules]

FPT_RCV.3/GP Automated recovery without undue loss

FPT_RCV.3.1/GP When automated recovery from **none, see application note below**[64] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/GP For **detection of a potential loss of integrity during the transmission of an Executable Load File to the card, abortion of the installation process of an Executable Load File, or any fatal error occurred during the linking of an Executable Load File to the Executable Files already installed on the card**[65] the TSF shall ensure the return of the TOE to a secure state using automated procedures.

FPT_RCV.3.3/GP The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **the loss of the Executable Load File being loaded or installed**[66] for loss of TSF data or objects under the control of the TSF.

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

Application Note:

- This SFR refines and replaces FPT_RCV.3/Installer of [PP-JCS], applied to card content management operations
- There is no maintenance mode implemented within the TOE. Recovery is always enforced automatically as stated in FPT_RCV.3.2/GP

FDP_IFC.2/GP-ELF Complete information flow control

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

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

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

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

Application Note:

- This SFR replaces FDP_IFC.2/CM of [PP-JCS].
- The subject S.SD can be the ISD, an APSD, or the CASD.
- GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively.

FDP_IFF.1/GP-ELF Simple security attributes

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

- **Subjects: S.SD, S.OPEN**
- **Information: APDU commands INSTALL and LOAD, GlobalPlatform APIs for loading and installing ELF**
- **Security attributes: Card Life Cycle state, ELF signature verification status, ELF AID, SD privileges, Secure Channel Security Level**[67].

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

- **S.SD implements one or more Secure Channel Protocols, namely SCP02, SCP03, SCP11, SCP80, SCP81**[68]**, each with a complete Secure Channel Key Set.**

---

[64] [assignment: list of failures/service discontinuities during card content management operations]
[65] [assignment: list of failures/service discontinuities during card content management operations]
[66] [assignment: quantification]
[67] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]
[68] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]

- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **On receipt of INSTALL or LOAD commands, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **S.OPEN accepts an ELF only if its integrity and authenticity has been verified.**
- **S.OPEN accepts an ELF only if its AID is not already registered by the TSF** [69]

FDP_IFF.1.3/GP-ELF The TSF shall enforce the **none** [70].

FDP_IFF.1.4/GP-ELF The TSF shall explicitly authorize an information flow based on the following rules: **none** [71].

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

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- **S.OPEN fails to verify the Card Life Cycle state**
- **S.OPEN fails to verify the SD privileges.**
- **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.SD fails to unwrap INSTALL or LOAD commands.**
- **The ELF AID is already registered within the card** [72]

Application Note:

- This SFR refines and replaces FDP_IFF.1/CM of [PP-JCS].
- APDUs belonging to the policy ELF Loading information flow control SFP are described in the following references:
  - For INSTALL, see [GPCS] section 11.5.
  - For LOAD, see [GPCS] section 11.6.
- The INSTALL and LOAD commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.
- The Minimum Security Level of INSTALL and LOAD is 'AUTHENTICATED' as defined in [GPCS] section 10.6.
- For more details about the rules to be applied to each role of INSTALL command, refer to [GPCS] sections 9.3 and 3.4.

FIA_UID.1/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **SD selection, Application selection, initializing a Secure Channel with the card, requesting data that identifies the card or off-card entities** [73] on behalf of the user to be performed before the user is identified.

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

Application Note:

- This SFR refines and replaces FIA_UID.1/CM of [PP-JCS].

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **1** [74] unsuccessful authentication attempt 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**.

---

[69] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]
[70] [assignment: additional information flow control SFP rules]
[71] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[72] [assignment: rules, based on security attributes, that explicitly deny information flows]
[73] [assignment: list of TSF-mediated actions]
[74] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

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 **receive** [75] 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.

Application Note:

- This SFR extends FDP_UIT.1/CM of [PP-JCS] to cover the integrity protection of SD/Application data and keys.
- This SFR applies where APDU command and response integrity protection is required (e.g. INSTALL, LOAD, STORE DATA and PUT KEY commands).

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 **receive** [76] user data in a manner protected from unauthorized disclosure.
Application Note: this SFR applies where APDU command and response confidentiality protection is required. For example, the sensitive data (e.g. secret keys) shall always be transmitted as confidential data.

FTP_ITC.1/GP Inter-TSF trusted channel

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

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

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

- **APDU commands sent to the card within a Secure Channel Session**
- **When loading/installing a new ELF on the card**
- **When transmitting and loading sensitive data to the card using STORE DATA or PUT KEY commands**
- **When deleting ELFs, Applications, or Keys**
- **None** [77]

Application Note: this SFR corresponds to FTP_ITC.1/CM of [PP-JCS], applied where APDU command and response integrity and/or confidentiality protection through a Secure Channel are required.

FPR_UNO.1/GP Unobservability

---

[75] [selection: transmit, receive]
[76] [selection: transmit, receive]
[77] [assignment: list of functions for which a trusted channel is required]

FPR_UNO.1.1/GP The TSF shall ensure that **SDs and Applications** are unable to observe the operation **keys or data import (PUT KEY or STORE DATA), encryption, decryption, signature generation and verification, none** [78] on **keys and data** by **the OPEN or any otherSD or Application**.

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

FPT_TDC.1.1/GP The TSF shall provide the capability to consistently interpret **ELFs, SD/Application data and keys, data used to implement a Secure Channel, None** [79] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/GP The TSF shall use **the list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card, None**[80] when interpreting the TSF data from another trusted IT product.
Application Note: the list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card are defined in [GPCS] sections 11.5, 11.6, 11.8, and 11.11.

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

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

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

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

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

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

- **The algorithms and key sizes of the imported keys shall be supported by the SE**
- **The Key Identifier (Key ID) of the imported keys shall be in an allowed range as specified in section 4 of [CIC]** [81]

Application Note:

- The algorithms and key sizes of the imported keys shall be supported by the Card as specified in [GPCS] Appendices B and C.

PUT KEY and STORE DATA are described in [GPCS] sections 11.8 and 11.11.

FDP_IFF.1/GP-KL Complete information flow control

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

- **Subjects: S.SD, S.OPEN**
- **GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys**
- **Security attributes: card Life Cycle State, Application and SD Life Cycle states, Secure Channel Security Level, SD and Application privileges** [82].

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

- **S.SD implements one or more Secure Channel Protocols, namely SCP02, SCP03, SCP11** [83]**, each equipped with a complete Secure Channel Key Set.**

---

[78] [assignment: list of operations]
[79] [assignment: list of TSF data types]
[80] [assignment: list of interpretation rules to be applied by the TSF]
[81] [assignment: additional importation control rules]
[82] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, S.OPEN checks that the card Life Cycle State is not CARD_LOCKED or TERMINATED.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the S.OPEN checks that the requesting S.SD has no restrictions for personalization.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and prior to the command forwarding to the targeted Application or SD.**
- **S.OPEN verifies that the targeted application implements a personalization interface** [84]

FDP_IFF.1.3/GP-KL The TSF shall enforce the **none** [85].

FDP_IFF.1.4/GP-KL The TSF shall explicitly authorize an information flow based on the following rules: **none** [86].

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

- **S.OPEN fails to verify the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to unwrap STORE DATA or PUT KEY.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.OPEN fails to verify that the targeted application implements a personalization interface.** [87]

Application Note:

- APDUs belonging to the Data & Key Loading information flow control SFP are described in the following references:
  - For PUT KEY, see [GPCS] section 11.8.
  - For STORE DATA, see [GPCS] section 11.11.
- The PUT KEY and STORE DATA commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.
- The Minimum Security Level of PUT KEY and STORE DATA is 'AUTHENTICATED' as defined in [GPCS] Section 10.6.
- For more details about Key Access Conditions, Data and Key Management, refer to [GPCS] sections 7.5.2 and 7.6.

FMT_MSA.1/GP Management of security attributes

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

Operations(APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorised Identified Roles with Privileges
DELETE Executable Load File	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Executable Load File and related Application(s)	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Application	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD

[83] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]
[84] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]
[85] [assignment: additional information flow control SFP rules]
[86] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[87] [assignment: rules, based on security attributes, that explicitly deny information flows]

DELETE Key	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
INSTALL	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
INSTALL [for personalisation]	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
LOAD	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
PUT KEY	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
SELECT	OP_READY, INITIALIZED, SECURED	ISD, AM SD, DM SD,
SET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, CARD_LOCKED, or TERMINATED	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD

Operations: SCP11 Commands	**Security Attributes: Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorised Identified Roles with Privileges**
GET DATA (ECKA Certificate)	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	None	ISD, AM SD, DM SD, SD
PERFORM SECURITY OPERATION		None	
MUTUAL AUTHENTICATE		AUTHENTICATED or ANY_AUTHENTICATED	
INTERNAL AUTHENTICATE		AUTHENTICATED or ANY_AUTHENTICATED	
STORE DATA (ECKA Certificate)		None	
STORE DATA (Whitelist)		None	
VERIFY PIN		None	
Operations: SCP80 Command	**Security Attributes: Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorised Identified Roles with Privileges**
Remote File Management Commands SELECT, UPDATE BINARY, UPDATE RECORD, SEARCH RECORD, INCREASE, VERIFY PIN, CHANGE PIN, DISABLE PIN, ENABLE PIN, UNBLOCK PIN, DEACTIVATE FILE, ACTIVATE FILE, READ BINARY, READ RECORD, CREATE FILE, DELETE FILE, RESIZE FILE, SET DATA, RETRIEVE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]

Remote Applet Management Commands DELETE, SET STATUS, INSTALL, LOAD, PUT KEY, GET STATUS, GET DATA, STORE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]
Operations: SCP81 Command	**Security Attributes: Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorised Identified Roles with Privileges**
PUT KEY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, ARD_LOCKED, or TERMINATED	None	ISD, AM SD, DM SD, SD

Table 54 - GP Management of security attributes List Explanation

Legend for tables above:

- ISD: Issuer Security Domain
- AM SD: Security Domain with Authorized Management privilege
- DM SD: Security Domain with Delegated Management privilege
- SD: Other Security Domain

Application Note:

- This SFR refines and replaces FMT_MSA.1/CM of [PP-JCS]. It is extended to cover Data and Key loading Policy.
- The authorized identified roles could be off-card or on-card entities as defined in FMT_SMR.1/GP.

FMT_MSA.3/GP Security attribute initialization

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

FMT_MSA.3.2/GP The TSF shall allow the **None**[88] to specify alternative initial values to override the default values when an object or information is created.

Application Note:

- This SFR refines and replaces FMT_MSA.3/CM of [PP-JCS]. It is extended to cover the Data and Key loading Policy.
- The authorized identified roles could be off-card or on-card entities as defined in FMT_SMR.1/GP.

5.2.8. OS Upgrade Security Functional requirements

FDP_IFC.2/OSU Complete information flow control

FDP_IFC.2.1/OSU The TSF shall enforce the **[assignment: OS Upgrade information flow control SFP]** on **[assignment: S.OSU and D.UPDATE_IMAGE]**.

[88] [assignment: authorized identified roles]

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

FDP_IFF.1/OSU Simple security attributes

FDP_IFF.1.1/OSU The TSF shall enforce the **[assignment: OS Upgrade information flow control SFP]** based on the following types of subject and information security attributes **[assignment:**

- **S.OSU: security attributes Current Sequence Number, Verification Key, Package Decryption Key**
- **D.UPDATE_IMAGE: security attributes Received Sequence Number, Image Type].**

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

[assignment:

- **S.OSU shall only accept D.UPDATE_IMAGE which signature can be verified with Verification Key.**
- **S.OSU shall only accept D.UPDATE_IMAGE for the update process that can be decrypted with Package Decryption Key].**

FDP_IFF.1.3/OSU The TSF shall enforce the additional information flow control SFP rules **[assignment: S.OSU shall only authorize D.UPDATE_IMAGE for the update process if the following rules apply:**

- **If Image Type equals Reset then Received Sequence Number shall equal Current Sequence Number.**
- **If Image Type equals Upgrade then Received Sequence Number shall be higher than Current Sequence Number.**
- **If Image Type equals Downgrade then Received Sequence Number shall be lower than Current Sequence Number].**

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

FDP_IFF.1.5/OSU The TSF shall explicitly deny an information flow based on the following rules: **[assignment: D.UPDATE_IMAGE which is not included in the pre-loaded OS Upgrade plan].**

Application note:

- The on-card S.OSU role interacts with the off-card S.UpdateImageCreator via OSU commands. The D.UPDATE_IMAGE is split up into smaller chunks and transmitted as payload within the OSU Commands to the TOE.
- Decrypting the D.UPDATE_IMAGE with the Package Decryption Key prevents the authorization of the D.UPDATE_IMAGE for the update process on a not certified system. The Package Decryption Key is only available on a certified TOE.

FMT_MSA.3/OSU Static attribute initialization

FMT_MSA.3.1/OSU The TSF shall enforce the **[assignment: OS Upgrade information flow control SFP]** to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/OSU The TSF shall allow the **[assignment: S.OSU]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/OSU Management of security attributes

FMT_MSA.3.1/OSU The TSF shall enforce the **[assignment: OS Upgrade information flow control SFP]** to restrict the ability to **[selection: modify]**
the security attributes **[assignment: Current Sequence Number]** to **[assignment: S.OSU].**

FMT_SMR.1/OSU Security roles

FMT_SMR.1.1/OSU The TSF shall maintain the roles **[assignment: S.OSU]**.

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

Application note: The roles of the CONFIGURATION information flow control SFP are defined by the HED Configuration Token generation key and the Customer Configuration Token generation key.

FMT_SMF.1/OSU Specification of Management Functions

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

- **query Current Sequence Number**
- **query Reference Sequence Number].**

Application note: After the atomic activation of the additional code the Final Sequence Number is returned on querying the Current Sequence Number.

FIA_UID.1/OSU Timing of Identification

FIA_UID.1.1/OSU The TSF shall allow **[assignment: OP.TRIGGER_UPDATE]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/OSU 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/OSU Timing of authentication

FIA_UAU.1.1/OSU The TSF shall allow **[assignment: OP.TRIGGER_UPDATE]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/OSU 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/OSU Single-use authentication mechanisms

FIA_UAU.4.1/OSU The TSF shall prevent reuse of authentication data related to **[assignment: the authentication mechanism used to load D.UPDATE_IMAGE]**.

FTP_TRP.1/OSU Trusted Path

FTP_TRP.1.1/OSU The TSF shall provide a communication path between itself and **remote** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**selection:** none].

FTP_TRP.1.2/OSU The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/OSU The TSF shall require the use of the trusted path for **the transfer of the additional code to the TOE**.

Application Note: during the transmission of the additional code to the TOE for loading, the confidentiality is ensured through direct encryption of the additional code, hence the 'none' selection in FTP_TRP.1.1/OSU.

FCS_COP.1/OSU-DEC Cryptographic operation

FCS_COP.1.1/OSU-DEC The TSF shall perform **Decryption of the additional code prior installation** in accordance with a specified cryptographic algorithm [**assignment: AES in CBC mode with null IV**] and cryptographic key sizes [**assignment: 128 bits**] that meet the following: [**assignment: FIPS 197**].

FCS_COP.1/OSU-VER	Cryptographic operation

FCS_COP.1.1/OSU-VER The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm [**assignment: AES-CMAC**] and cryptographic key sizes [**assignment: 128 bits**] that meet the following: [**assignment: FIPS 197 and SP800-38B**].

FPT_FLS.1/OSU	Failure with preservation of secure state

FPT_FLS.1.1/OSU The TSF shall preserve a secure state when the following types of failures occur: **[assignment:**

- **Corrupted D.UPDATE_IMAGE is received.**
- **Unauthorized D.UPDATE_IMAGE is received.**
- **The OS Upgrade Process is interrupted.**
- **The activation of the additional code failed].**

5.2.9. Underlying platform IC Security Functional Requirements

FAU_SAS.1	Audit Storage

FAU_SAS.1.1 The TSF shall provide **[assignment: the test process before TOE Delivery]** with the capability to store **[selection: the Initialisation Data, Pre-personalisation Data, [assignment: none]]** in the **[assignment: C1U98N70 FLASH]**.

FPT_RCV.3/OS	Automated recovery without undue loss

FPT_RCV.3.1/OS When automated recovery from **none, see application note below**[89] 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**[90] 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** [91]

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** [92] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

---

[89] [assignment: list of failures/service discontinuities during card content management operations]
[90] [assignment: list of failures/service discontinuities during card content management operations]
[91] [assignment: quantification]

5.3. Security Functional Requirements Rationale

5.3.1. SFRs for eUICC rationale

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

5.3.2. SFRs for Runtime Environment rationale

The security functional requirements rationale for objectives O.RE*is extracted from [PP-JCS] and adapted depending on the implementation and the included SFRs and its iterations.

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

RE objectives	Translation from JavaCard PP
O.RE.PPE-PPI	O.INSTALL, O.DELETION, O.LOAD
O.RE.SECURE-COMM	O.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION
O.RE.API	O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM
O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG
O.RE.CODE-EXE	O.FIREWALL, O.REMOTE, O.NATIVE, OE.VERIFICATION, OE.CAP_FILE
O.SECURE_LOAD_ACODE	FDP_IFC.2/OSU, FDP_IFF.1/OSU, FMT_MSA.3/OSU, FMT_SMR.1/OSU, FMT_SMF.1/OSU, , FCS_COP.1/OSU-VER, FIA_UAU.4/OSU
O.SECURE_AC_ACTIVATION	FMT_MSA.3/OSU, FMT_SMR.1/OSU, FMT_SMF.1/OSU
O.TOE_IDENTIFICATION	FDP_SDI.2, FMT_MSA.3/OSU, FMT_SMR.1/OSU, FMT_SMF.1/OSU
O.CONFID-UPDATE-IMAGE.LOAD	FPR_UNO.1, FIA_UID.1/OSU, FIA_UAU.1/OSU, FMT_MSA.3/OSU, FMT_SMR.1/OSU, FMT_SMF.1/OSU, FTP_TRP.1/OSU, FCS_COP.1/OSU-DEC, FPT_FLS.1/OSU
O.AUTH-LOAD-UPDATE-IMAGE	FDP_IFC.2/OSU, FDP_IFF.1/OSU, FMT_MSA.3/OSU, FMT_SMR.1/OSU, FMT_SMF.1/OSU, FIA_UID.1/OSU, FIA_UAU.1/OSU, FTP_TRP.1/OSU, FCS_COP.1/OSU-DEC, FPT_FLS.1/OSU

Table 55 - 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.

Note that For O.RE.IDENTITY, this objective is translated from OE.RE.IDENTITY to cover the following threats:T.UNAUTHORIZED-IDENTITY-MNG.

[92] [assignment: list of functions and failure scenarios]

5.3.3. 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.

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

FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/RULES	(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/CERT_KEYS	(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_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/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS, FMT_SMR.1, FMT_MSA.1/RAT
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FDP_ITC.2/SCP, FCS_CKM.6/Mobile_network
FCS_CKM.2/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS, FMT_SMR.1, FMT_MSA.1/RAT
FCS_CKM.6/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5)	FDP_ITC.2/SCP, FCS_CKM.6/Mobile_network
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 **See rationale** FMT_SMR.1/JC
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/GP 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 or FCS_CKM.5)	FCS_COP.1/RSA_SIGN FCS_COP.1/RSA_CIPHER FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECDH FCS_COP.1/GP-SCP

FCS_COP.1/TDES_MAC FCS_COP.1/AES_MAC FCS_COP.1/ECDH FCS_COP.1/ECDSA_SIGN FCS_COP.1/ECKA_EG FCS_COP.1/GP-SCP FCS_COP.1/TDES_CIPHER FCS_COP.1/AES_CIPHER FCS_COP.1/RSA_SIGN FCS_COP.1/RSA_CIPHER FCS_COP.1/Hash FCS_COP.1/HMAC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FCS_CKM.1/ECDSA FCS_CKM.1/GP-SCP **See rationale**
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_SAA.1)	**See rationale**
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPR_FLS.1	No Dependencies	
FPT_TDC.1	No Dependencies	
FIA_ATD.1/AID	No Dependencies	
FIA_UID.2/AID	No Dependencies	
FIA_USB.1/AID	(FIA_ATD.1/Base)	FIA_USB.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/GP FMT_SMR.1/JC
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No Dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL FMT_SMF.1/ADEL FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No Dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	**See rationale**
FPT_FLS.1/ADEL	No Dependencies	
FDP_RIP.1/ODEL	No Dependencies	
FPT_FLS.1/ODEL	No Dependencies	
FPT_FLS.1/GP	No Dependencies	
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMR.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/GP	No Dependencies	
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1/GP FTP_ITC.1/GP
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL FPT_TDC.1/GP FTP_ITC.1/GP
FPT_RCV.3/GP	(AGD_OPE.1)	AGD_OPE.1

FDP_IFC.2/GP-ELF	(FDP_IFF.1)	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FIA_UID.1/GP	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/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FTP_ITC.1/GP	No Dependencies	
FPR_UNO.1/GP	No Dependencies	
FPT_TDC.1/GP	No Dependencies	
FDP_IFC.2/GP-KL	(FDP_IFF.1)	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-KL FMT_MSA.3/GP
FMT_MSA.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FIA_UID.1/OSU	No Dependencies	
FIA_UAU.1/OSU	FIA_UID.1	
FIA_UAU.4/OSU	No Dependencies	
FPT_FLS.1/OSU	No Dependencies	
FDP_IFC.2/OSU	FDP_IFF.1	
FDP_IFF.1/OSU	(FDP_IFC.1) and (FMT_MSA.3)	
FMT_MSA.3/OSU	(FMT_MSA.1) and (FMT_SMR.1)	
FMT_MSA.1/OSU	[FDP_ACC.1 or FDP_IFC.1] and (FMT_SMR.1) and (FMT_SMF.1)	
FMT_SMR.1/OSU	FIA_UID.1	
FMT_SMF.1/OSU	No Dependencies	
FTP_TRP.1/OSU	No Dependencies	
FCS_COP.1/OSU-DEC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FDP_ITC.2/GP-ELF **See rationale**
FCS_COP.1/OSU-VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.6)	FDP_ITC.2/GP-ELF **See rationale**
FAU_SAS.1	No Dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No Dependencies	

Table 56 - SFRs dependencytable

Rationale for the exclusion of dependencies:

- **The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is unsupported.**

The dependency between FMT_MSA.1/JCRE and FMT_SMF.1 is not satisfied because no management functions are required for the Java Card RE.

- **The dependencies of FCS_COP.1/Hash are unsupported**

Hash operation does not require any key.

- **The dependency FAU_SAA.1 of FAU_ARP.1 is unsupported**

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

- **The dependency FIA_UID.1 of FMT_SMR.1/ADEL is unsupported**

This ST does not require the identification of the "deletion manager" since it can be considered as part of the TSF.

6. 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

6.1. eUICC security functions

6.1.1. GSMA.ProfileManagement

This security function implements the controls related to profiles management as defined by **[SGP.22]** and **[EUPP]**, encompassing the following operations:

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

It also supports everything related to profile data isolation.

6.1.2. GSMA.ECASD

This security function handles the Embedded UICC Controlling Authority Security Domain (ECASD) management as defined by **[SGP.22]**. The ECASD is responsible for secure storage of credentials required to support the required Security Domains on the eUICC.

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

6.1.3. GSMA.ISDR

This security function handles the ISD-R management as defined by **[SGP.22]**. The ISD-R is responsible for the creation of new ISD-Ps and lifecycle management of all ISD-Ps.

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

6.1.4. GSMA.ISDP

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

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

6.1.5. GSMA.PPR

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

Secure management and processing of the PPRs are covered.

6.2. Runtime Environment security functions

6.2.1. GP.CardContentManagement

This security function provides the capability and a dedicated flow control for the loading, installation, extradition, registry update, selection and removal of card content and especially executable files and application instances. Such features are offered to the Card Issuer and its business partners, allowing the Card Issuer to delegate card content management to an Application Provider according to privileges assigned to the various security domains on the card. It supports Delegated management (DM), Authorized management (AM) and it can use DAP or Mandated DAP verification and generation of Reception token. It also checks that only the card management commands specified and allowed at each state of the smart card's life cycle are accepted, and ill-formed ones are rejected with an appropriate error response

6.2.2. GP.KeyLoading

This security function provides the capability and a dedicated flow control for the loading of keys and other sensitive data using the GlobalPlatform STORE DATA and PUT KEY APDUs, or by using GlobalPlatform APIs for loading and storing data and keys.

6.2.3. GP.SecurityDomain

This security function provides security domain management, as SD creation, SD selection, SD privileges setting and SD deletion in SD hierarchy. It provides means to associate or extradite an application to a security domain in order to provide services (as secure channel) to the dedicated application without sharing the related keys stored in SD. It also provides Keyset Management in SD, with Key Set creation, Key set deletion, key importation, replacement, or deletion in Key Set.

Security Domains are privileged Applications as defined in [GPCS] § 7, holding cryptographic keys to be used to support Secure Channel Protocol operations and/or to authorize card content management functions. There are different types of security domain with dedicated privileges and associated operations: ISD Security domain, Supplementary Security domains, and Controlling Authority Security domains.

ISD Security domain as defined in [GPCS] §7.1.1, is the mandatory Security Domain, implicitly selected if the Application implicitly selectable on the same logical channel of the same card I/O interface is removed. It inherits of the Final Application privilege if the Application with that privilege is removed.

Supplementary Security Domains are privileged Applications with dedicated privileges:

- Token Verification Privilege as described in [GPCS] §9.1.3.1
- Authorized Management Privilege as described in [GPCS] §9.1.3.2
- Delegated Management Privilege as described in [GPCS] §9.1.3.3
- Global Delete Privilege as described in [GPCS] §9.1.3.4
- Global Lock Privilege as described in [GPCS] §9.1.3.5
- Receipt Generation Privilege as described in [GPCS] §9.1.3.6
- Ciphered Load File Data Block Privilege as described in [GPCS] §9.1.3.7

Controlling Authority Security Domain is a supplementary Security Domain dedicated to the Controlling Authority with dedicated privileges. It contains Security Domains cryptographic keys needed to confidentially personalize an initial set of Secure Channel Keys of an APSD.

6.2.4. GP.SecureChannel

This security function provides a secure communication channel between a card and an off-card entity during an Application Session according to [GPCS], [Amd A], [Amd B], [Amd C], [Amd D], [TS 102.225]

and [TS 102.226]. It provides an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.

A Secure Channel Session is divided into three sequential phases:

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

The Secure Channel provides the following services:

- Entity authentication in which the card or the off-card entity proves its authenticity to the other entity through a cryptographic exchange, based on session key generation and a dedicated flow control; For SCP80, envelope APDU shall contain secured packet structure defined in [TS 102.225] §5 and Anti-replay mechanism is proposed optionally using a counter defined in [TS 102.225] §5.1.4;
- Integrity and authentication in which the receiving entity (the card or off-card entity) ensures that the data being received from the sending entity (respectively the off-card entity or card) actually came from an authenticated entity in the correct sequence and has not been altered;
- Confidentiality in which data being transmitted from the sending entity (the off-card entity or card) to the receiving entity (respectively the card or off-card entity) is not viewable by an unauthenticated entity.

The TOE supports the following Secure Channel Protocols: SCP02, SCP03, SCP11, SCP80 and SCP81.

6.2.5. GP.GPRegistry

This security function provides management and access to the GlobalPlatform Registry used for:

- Store card management information;
- Store relevant application management information (e.g., AID, associated Security Domain and Privileges);
- Support card resource management data;
- Store Application Life Cycle information;
- Store card Life Cycle information;
- Track any counters associated with logs.

The content of the GlobalPlatform Registry may be accessed by administrative commands or by applet using a dedicated GlobalPlatform API.

Only secure values are accepted for the information stored in the GlobalPlatform registry (including Life Cycle states, Security Levels and Privileges).

6.2.6. JCS.APDUBuffer

The security function maintains a byte array buffer accessible from any applet context. This buffer is used to transfer incoming APDU header and data bytes as well as outgoing data according to [JCAPI3]. The APDU class API is designed to be transport protocol independent T=0, T=1, T=CL (as defined in ISO 7816-3).

Application note: ADPU buffer is a JCRE temporary entry point object where no associated reference can be stored in a variable or an array component.

6.2.7. JCS.ByteCodeExecution

This security function handles applet bytecode execution according to the rules defined in [JCVM3].

The JCVM execution may be summarized in JCVM interpreter start-up, bytecode execution and JCVM interpreter loop. The applet bytecode execution consists in:

- fetching the next bytecode to execute according to the applet's code flow control,
- decoding the next bytecode,
- Executing the fetched bytecode.

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

6.2.8. JCS.Firewall

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

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

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

6.2.9. JCS.Package

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

6.2.10. JCS.CryptoAPI

This security function offers the following cryptographic services to applets through the JavaCard API:

- Generation of random numbers as defined in [JCAPI3] to be used for key values or challenges during external exchanges. The Random Number Generator (RNG) is deterministic and conformant to [AIS20] DRG.3, providing enhanced backward secrecy. It passes [AIS20] test procedure A.
- Encryption and decryption using TDES algorithm as defined in [JCAPI3] Cipher class. Both TDES 2-keys (128 bits key length) and TDES 3-keys (192 bits key length) are supported.
- Generation of 4-byte or 8-byte MAC using TDES algorithm as defined in [JCAPI3] Signature class. Both TDES 2-keys (128 bits key length) and TDES 3-keys (192 bits key length) are supported.
- Encryption and decryption using AES (128, 192 or 256 bits key) algorithm as defined in [JCAPI3] Cipher class.
- Generation of 16-byte, 24-byte or 32-byte MAC using AES algorithm (128, 192 or 256 bits key) in CBC mode as defined in [JCAPI3] Signature class.
- Data hash computation as defined in [JCAPI3] MessageDigest class.
- HMAC computation as defined in [JCAPI3] Signature class.
- Encryption and decryption using RSA with Standard or CRT modes, as defined in [JCAPI3] Cipher class. All key lengths from 1024 to 4096 bits (by steps of 32 bits) are supported.
- Generation and verification of RSA signatures in Standard or CRT modes, as defined in [JCAPI3] Signature class. All key lengths from 1024 to 4096 bits (by steps of 32 bits) are supported.
- Generation and verification of ECDSA signatures as defined in [JCAPI3] Signature class. Elliptic curve cryptography over GF(p) is considered here, with P ranging from 192 to 521 bits.
- Secret key agreement according to the ECDH algorithm, as defined in [JCAPI3] KeyAgreement class.

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

6.2.11. JCS.KeyManagement

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

- Key generation implemented through KeyBuilder and/or KeyPair classes : TDES key generation (128 or 192 bits), AES key generation (128, 192 or 256 bits), RSA Standard and RSA CRT Key Pair Generation (1024 to 4096 bits by steps of 32 bits), ECDSA Key Pair Generation (P ranging from 256 to 521 bits) and HMAC Key generation.
- Key importation and exportation is done using method protecting confidentiality and integrity of key.
- Key masking protects the confidentiality of cryptographic keys from being read out from the memory. It ensures the service of accessing and modifying them.
- Key destruction (implemented through the method clearKey() of the Key class) disables the use of a key both logically and physically. Reuse is only possible after erase.

6.2.12. JCS.OwnerPIN

This security function provides to applets a means to perform user identification and authentication with the OwnerPin class conformant to [JCAPI3].

It offers to create a PIN and store it securely in the persistent memory. It allows access to PIN value only to perform a secure comparison between a PIN stored in the persistent memory and a data received as parameter.

A method returns a positive result if a valid Pin has been presented during current session. If the PIN is not blocked and the comparison is successful, the validated flag is set to and the try counter is set to its maximum, otherwise the authentication fails and the associated try counter is decremented.

When the validated flag is set, it is assumed that the user is authenticated.

When the try counter reaches zero, the PIN is blocked and the authentication is no more possible until the PIN is unblocked.

6.2.13. JCS.EraseResidualData

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

- Deletion of package and/or applications,
- Deletion of objects.

They are erased when space needs to be reused for allocation of new objects.

This security function also ensures that the sensitive temporary buffers (transient object, bArray object, Global Array object, APDU buffer, Cryptographic buffer) are securely cleared after their usage with respect to their life-cycle and interface as defined in [JCRE3], transient object at reset or allocation and persistent object are erased at allocation for new object.

6.2.14. JCS.OutOfLifeDataUndisclosure

This security function ensures that sensitive data are locked until postponed erasure on the following operations: Deletion of persistent and transient objects according to [JCRE3].

6.2.15. JCS.RunTimeExecution

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

- Instance registration or deletion,

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

6.2.16. JCS.Exception

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

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

6.2.17. OS.Atomicity

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

6.2.18. OS.MemoryManagement

This security function allocates memory areas and performs access control on them to avoid unauthorized access. It manages circular writing to avoid instable memory state. It enforces memory recovery in case of error detection. It offers (when required) confidentiality services for data storage: Ciphering / Deciphering of Data in RAM or in FLASH, Scrambling / Unscrambling of Data in RAM or in FLASH. Sensitive data (including keys or PINs) is protected using the CRC algorithm to ensure integrity and encrypted via the XOR algorithm to ensure confidentiality.

6.2.19. OS.OS Update

OS.OS Update provides secure functionality to update the COS with an image created by a trusted off-card entity. OS.OS Update allows an authenticated OSU command to upload an integrity and confidentiality protected update image to update to another operating system version. User authentication is based on the verification of signed OSU commands. Integrity protection of OSU commands uses AES CMAC verification. To ensure proper COS startup, HASH 256 is employed to verify the integrity of certain system data. Confidentiality of the update image is ensured by ECDH and AES encryption. SF.OSU ensures that the system stays in a secure state in case of invalid or aborted update procedures and ensures that the information identifying the currently running OS is modified and the updated code is activated only after successfully OS Upgrade procedure.

6.3. 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.

6.3.1. eUICC SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	This SFR is covered by GSMA.ISDR
FIA_UAU.1/EXT	This SFR is covered by GSMA.ECASD and GP.SecureChannel
FIA_USB.1/EXT	This SFR is covered by GSMA.ECASD and

	GP.SecurityDomain
FIA_UAU.4/EXT	This SFR is covered by GSMA.ECASD and GP.SecureChannel
FIA_UID.1/MNO-SD	This SFR is covered by GP.SecurityDomain
FIA_USB.1/MNO-SD	This SFR is covered by GP.SecurityDomain, GSMA.ISDP, GSMA.ECASD
FIA ATD.1	This SFR is covered by GP.SecurityDomain and GSMA.ECASD
FIA API.1	This SFR is covered by GSMA.ECASD
FDP_IFC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_IFF.1/SCP	This SFR is covered by GSMA.ProfileManagement
FTP_ITC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_ITC.2/SCP	This SFR is covered by GSMA.ProfileManagement
FPT_TDC.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_UCT.1/SCP	This SFR is covered by GSMA.ProfileManagement
FDP_UIT.1/SCP	This SFR is covered by GSMA.ProfileManagement
FCS_CKM.1/SCP-SM	This SFR is covered by GSMA.ProfileManagement and JCS.CryptoAPI for ECKA-EG
FCS_CKM.2/SCP-MNO	This SFR is covered by JCS.CryptoAPI
FCS_CKM.6/SCP-SM	This SFR is covered by JCS.KeyManagement
FCS_CKM.6/SCP-MNO	This SFR is covered by JCS.KeyManagement
FDP_ACC.1/ISDR	This SFR is covered by GSMA.ISDR
FDP_ACF.1/ISDR	This SFR is covered by GSMA.ISDR
FDP_ACC.1/ECASD	This SFR is covered by GSMA.ECASD
FDP_ACF.1/ECASD	This SFR is covered by GSMA.ECASD
FDP_IFC.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FDP_IFF.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FPT_FLS.1/Platform_services	This SFR is covered by GSMA.ProfileManagement
FCS_RNG.1	This SFR is covered by JCS.CryptoAPI providing AIS20 DRG.3 random number generation to applets.
FPT_EMS.1	This SFR is covered by JCS.CryptoAPI and JCS.KeyManagement
FDP SDI.1	This SFR is covered by GSMA.ProfileManagement
FDP RIP.1	This SFR is covered by GSMA.ProfileManagement
FPT FLS.1	This SFR is covered by GSMA.ProfileManagement
FMT_MSA.1/PLATFORM_DATA	This SFR is covered by GSMA.ISDR
FMT_MSA.1/RULES	This SFR is covered by GSMA.PPR
FMT_MSA.1/CERT_KEYS	This SFR is covered by GSMA.ProfileManagement
FMT_SMF.1	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR
FMT_SMR.1	This SFR is covered by GSMA.ProfileManagement, GSMA.ISDR, GSMA.ISDP, GSMA.ECASD, and GSMA.PPR
FMT_MSA.1/RAT	This SFR is covered by GSMA.ISDR
FMT MSA.3	This SFR is covered by GSMA.ISDR, GSMA.ISDP, GSMA.ECASD
Security Functional Requirement	**Coverage by TSS Security Function(s)**
FCS_COP.1/Mobile_network	This SFR is covered by JCS.CryptoAPI
FCS_CKM.2/Mobile_network	This SFR is covered by JCS.CryptoAPI
FCS_CKM.6/Mobile_network	This SFR is covered by JCS.KeyManagement

Table 57 - eUICC SFRs Coverage List

6.3.2. Runtime Environment SFRs coverage

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_ACC.2/FIREWALL	This SFR is covered by JCS.Firewall.

FDP_ACF.1/FIREWALL	This SFR is covered by JCS.Firewall.
FDP_IFC.1/JCVM	This SFR is covered by JCS.Firewall and JCS.APDUBuffer controlling unauthorized access or invalid storage of reference.
FDP_IFF.1/JCVM	This SFR is covered by JCS.Firewall.
FDP_RIP.1/OBJECTS	This SFR is covered by JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data).
FMT_MSA.1/JCRE	This SFR is covered by JCS.RunTimeExecution covering context switch and application selection.
FMT_MSA.1/JCVM	This SFR is covered by JCS.ByteCodeExecution requiring context switch for specific code execution and JCS.RunTimeExecution covering context switch and modification of the Currently Active Context according to given rules.
FMT_MSA.2/FIREWALL_JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_SMF.1/JC	This SFR is addressed by JCS.RunTimeExecution covering context management and instance registration.
FMT_SMR.1/JC	This SFR is addressed by JCS.RunTimeExecution covering JCVM and JCRE roles.
FCS_CKM.1/ECDSA	This SFR is addressed by JCS.KeyManagement covering key generation.
FCS_CKM.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FCS CKM.4	This SFR is addressed by JCS.KeyManagement covering key deletion.
FCS_COP.1/TDES_MAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/AES_MAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/ECDH	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/ECDSA_SIGN	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/ECKA_EG	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FCS_COP.1/TDES_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/AES_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/RSA_SIGN	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/RSA_CIPHER	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FCS_COP.1/Hash	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.

FCS_COP.1/HMAC	This SFR is covered by JCS.CryptoAPI dealing with the cryptographic services provided to applets through the Javacard API.
FDP_RIP.1/ABORT	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/APDU	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/bArray	This SFR is addressed by JCS.OutOfLifeDataUndisclosure and JCS.EraseResidualData covering data erasure.
FDP_RIP.1/GlobalArray	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/KEYS	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/TRANSIENT	This SFR is covered by JCS.OutOfLifeDataUndisclosure managing the access control to transient object to be erased prior the erasure of the content in memory.
FDP_ROL.1/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering transaction rollback during specific operations.
FAU ARP.1	This SFR is addressed by JCS.RunTimeExecution, JCS.Exception, JCS.Firewall, and OS.MemoryManagement covering exception handling with different specific operations.
FDP_SDI.2/DATA	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, OS.Atomicity and OS.MemoryManagement covering integrity handling with specific operations.
FPR UNO.1	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, JCS.CryptoAPI and OS.MemoryManagement covering data handling with specific operations avoiding observation.
FPT_FLS.1/JC	This SFR is addressed by JCS.Exception, JCS.ByteCodeExecution, JCS.RunTimeExecution, and OS.Atomicity preserving a secure state when unexpected events occur during specific operations.
FPT TDC.1	This SFR is covered by JCS.Package enforcing export check, CAP file translation and link specific operations.
FIA_ATD.1/AID	This SFR is covered by JCS.RunTimeExecution and GP.GPRegistry controlling applet registration and uninstallation.
FIA_UID.2/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing user identity (package AID) during applet selection and identify associated context provided.
FIA_USB.1/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing registration of each applet and associated package during its installation with its AID.
FMT_MTD.1/JCRE	This SFR is covered by JCS.RunTimeExecution offering services for applet registration and uninstallation managing associated access rights.
FMT_MTD.3/JCRE	This SFR is fully covered by JCS.RunTimeExecution managing presence and legacy of AID with ISO rules.
FDP_ACC.2/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_ACF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.

FDP_RIP.1/ADEL	This SFR is covered by GP.CardContentManagement and JCS.OutOfLifeDataUndisclosure by checking operations to avoid access to freed resources prior to its reuse.
FMT_MSA.1/ADEL	This SFR is covered by GP.GPRegistry, GP.CardContentManagement and JCS.RunTimeExecution responsible of checking rules concerning applet attributes, implicit and explicit selection rules prior to authorize deletion operation.
FMT_MSA.3/ADEL	This SFR is covered by JCS.RunTimeExecution and GP.CardContentManagement dealing with Security Attributes initialization, providing secure, restrictive default values for the security attributes of subject and objects involved in applet deletion.
FMT_SMF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.SecurityDomain and JCS.RunTimeExecution.
FMT_SMR.1/ADEL	This SFR is covered by GP.SecurityDomain maintaining the ISD and SDD roles responsible of applet deletion. This SFR is also covered by JCS.RunTimeExecution maintaining the JCRE role for applet uninstallation
FPT_FLS.1/ADEL	This SFR is covered by GP.GPRegistry, JCS.RunTimeExecution and OS.Atomicity preserving a secure state when unexpected events occur during package or instance deletion, managing the transaction part of the deletion operation by either rolling back, or completing it.
FDP_RIP.1/ODEL	This SFR is covered by JCS.EraseResidualData and OS.MemoryManagement ensuring that the content of deleted objects is erased upon the deletion and by JCS.OutOfLifeDataUndisclosure making unavailable for disclosure upon further reallocation of the freed space.
FPT_FLS.1/ODEL	This SFR is covered by JCS.RunTimeExecution and OS.MemoryManagement performing memory management to release no more used memory on unreferenced objects and preserves a secure state when unexpected events occur during object deletion.
FPT_FLS.1/GP	This SFR is addressed by JCS.Package, JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FDP_ROL.1/GP	This SFR is addressed by GP.CardContentManagement, GP.KeyLoading and OS.Atomicity.
FCO_NRO.2/GP	This SFR is covered by GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading: * mutual authentication between the external entity (Issuer or Application provider) and the selected security Domain, including creation of a session key, * by the verification of a (chained) MAC that the Issuer or Application provider attaches to each file or data block sent, * by the erase of the session key at the end of the session.
FMT_SMR.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain managing the roles: S.OPEN, issuer, application provider, verification authority and controlling authority.
FMT_SMF.1/GP	This SFR is covered by GP.SecurityDomain and GP.SecureChannel.
FDP_ITC.2/GP-ELF	This SFR is covered by JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations.
FDP_ITC.2/GP-KL	This SFR is covered by GP.KeyLoading.
FPT_RCV.3/GP	This SFR is addressed by JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails.

FDP_IFC.2/GP-ELF	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_IFF.1/GP-ELF	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
FIA_UID.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
FIA_AFL.1/GP	This SFR is covered by GP.SecureChannel.
FIA_UAU.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain (as for FIA_UID.1/GP).
FIA_UAU.4/GP	This SFR is covered by GP.SecureChannel.
FDP_UIT.1/GP	This SFR is covered by GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
FDP_UCT.1/GP	This SFR is covered by GP.SecureChannel, which provides confidentiality protection for sensitive data (such as secret keys).
FTP_ITC.1/GP	This SFR is addressed by GP.SecureChannel.
FPR_UNO.1/GP	This SFR is covered by JCS.RunTimeExecution and JCS.CryptoAPI.
FPT_TDC.1/GP	This SFR is addressed by GP.CardContentManagement, GP.SecureChannel and GP.KeyLoading.
FDP_IFC.2/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FDP_IFF.1/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FMT_MSA.1/GP	This SFR is covered by GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.
FMT_MSA.3/GP	This SFR is covered by GP.SecureChannel providing setting of the default value.
FDP_IFC.2/OSU	This SFR is addressed by OS.OS Update.
FDP_IFF.1/OSU	This SFR is addressed by OS.OS Update.
FMT_MSA.3/OSU	This SFR is addressed by OS.OS Update.
FMT_MSA.1/OSU	This SFR is addressed by OS.OS Update.
FMT_SMR.1/OSU	This SFR is addressed by OS.OS Update.
FMT_SMF.1/OSU	This SFR is addressed by OS.OS Update.
FTP_TRP.1/OSU	This SFR is addressed by OS.OS Update.
FCS_COP.1/OSU-DEC	This SFR is addressed by OS.OS Update.
FCS_COP.1/OSU-VER	This SFR is addressed by OS.OS Update.
FIA_UID.1/OSU	This SFR is addressed by OS.OS Update.
FIA_UAU.1/OSU	This SFR is addressed by OS.OS Update.
FIA_UAU.4/OSU	This SFR is addressed by OS.OS Update.
FPT_FLS.1/OSU	This SFR is addressed by OS.OS Update.
FAU_SAS.1	This SFR is covered by OS.MemoryManagement
FPT_RCV.3/OS	This SFR is covered by OS.Atomicity.
FPT_RCV.4/OS	This SFR is covered by OS.MemoryManagement.

Table 58 - Runtime Environment SFRs Coverage List

7. Composition with IC

7.1. Statement of compatibility

This is a statement of compatibility between this Composite Security Target (Composite-ST) and the IC Security Target (IC-ST).

This statement is compliant with the requirement of [SUPP] (Joint Interpretation Library (JIL) for Smart Cards and similar devices, May 2018, version 1.5.1).

The TOE relies on fulfilment of the following implicit assumptions on the IC:

- Certified IC HED CIU98N70.
- Cryptographic and functional library includes the functions of TDES, AES, ECC (with ECDH/ECDSA) and RSA with key length from 1024 bits to 4096 bits.
- Lib file API library includes the functions of a highly reliable true random number generation API interface with FA countermeasures cooperating with hardware which is compliant with PTG.2 class of AIS20/31[2013], a deterministic random number generation API with FA countermeasures which is compliant with DRG.3 class of AIS20/31[2013].

7.1.1. Threats

IC Threats	Rationale
Part of [PP-0084]	
T.Leak-Inherent	This threat is related to the information which is leaked from the TOE during usage of the Security IC to disclose sensitive data of the TOE. It is considered in the TOE evaluation.
T.Phys-Probing	This threat is related to physical probing of the TOE to disclose relevant information. It is considered in the TOE evaluation.
T.Malfunction	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. It is considered in the TOE evaluation.
T.Phys-Manipulation	This threat is related to physical manipulation of the Security IC. It is covered by the IC evaluation.
T.Leak-Forced	This threat is related to information which is leaked from the TOE during usage of the Security IC to disclose confidential user data of the composite TOE.
T.Abuse-Func	This threat is related to the usage of functions of the TOE that are not allowed once the TOE Delivery and can impact the security of the TOE. It is considered in the TOE evaluation
T.RND	This threat is related to the deficiency of random numbers. It is covered by the IC evaluation.
T.Unauthorized-Access	This threat is related with unauthorized access to code or data stored in restricted memory areas or with hardware resources operation that are restricted.

Table 59 - IC Threats compatibility between Composite-ST and IC-ST

7.1.2. Organizational Security Policies

Organizational Security Policies	Rationale
Part of [PP-0084]	

P.Process-TOE	This policy is related to protection during IC Development and Production. It is covered by the IC evaluation.
P.Crypto-Service	This policy is related to cryptographic services of the IC. It is covered by the IC evaluation.

Table 60 - Organizational Security Policies compatibility between Composite-ST and IC-ST

7.1.3. Assumptions

IC Assumptions	Rationale
Part of [PP-0084]	
A.Process-Sec-IC	This assumption ensures the security of the delivery and storage of the IC. It is covered by the ALC_DVS.2 activity of the TOE evaluation.
A.Resp-Appl	This assumption ensures that security relevant data of the current TOE are properly treated according to the IC security needs. It is covered by the ADV_IMP.1 activity of the TOE evaluation.

Table 61 - IC Assumptions compatibility between Composite-ST and IC-ST

7.1.4. Security Objectives for the environment

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

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

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

IC OEs	Rationale
Part of [PP-0084]	
OE.Process-Sec-IC	This objective is covered by the IC evaluation and by the ALC_DVS.2 activity of the TOE evaluation. - During phases b and c: CfPOE - During phase e: SgOE
OE.Resp-Appl	This objective deals with the treatment of TOE user data by the TOE itself. It is covered by the ADV_IMP.1 activity of the TOE evaluation. - CfPOE

Table 62 - IC OEs compatibility between Composite-ST and IC-ST

7.1.5. Security Objectives

IC Security Objectives	Rationale
Part of [PP-0084]	
O.Leak-Inherent	This objective is covered by TOE evaluation.
O.Phys-Probing	This objective is covered by the IC evaluation.
O.Malfunction	This objective is covered by TOE evaluation.
O.Phys-Manipulation	This objective is covered by the IC evaluation.
O.Leak-Forced	This objective is covered by the IC evaluation.
O.Abuse-Func	This objective is covered by TOE evaluation.
O.Identification	This objective is covered by the IC evaluation.

O.RND	This objective is covered by the IC evaluation.
O.TDES	This objective is covered by the IC evaluation.
O.AES	This objective is covered by TOE evaluation.
O.RSA	This objective is covered by TOE evaluation.
O.ECC	This objective is covered by TOE evaluation.
O.X25519	This objective is covered by the IC evaluation.
O.MEM-ACCESS	This objective is covered by the IC evaluation

Table 63 - IC Security Objectives compatibility between Composite-ST and IC-ST

7.1.6. Security Functional Requirements

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

- IP_SFR: Irrelevant IC SFR not being used by the current TOE.

- RP_SFR_SERV: Relevant IC SFR being used by the current TOE to implement a security service with associated TSFI.

- RP_SFR_MECH: Relevant IC SFR being used by the current evaluation because of its security properties providing protection attacks to the TOE as a whole and are addressed in ADV_ARC. The required security properties are a result of the security mechanism and services that are implemented in the IC.

The Composite-ST requires EAL4 according to Common Criteria 2022 Revision 1 augmented by ALC_DVS.2 and AVA_VAN.5.

The IC-ST has been certified to EAL5 augmented with ADV_IMP.2, ADV_INT.3, ADV_TDS.5, ALC_CMC.5, ALC_DVS.2, ALC_TAT.3, ATE_COV.3, ATE_FUN.2, and AVA_VAN.5, ALC_FLR.2 and EAL6 augmented with ALC_FLR.2

The assurance requirements of the Composite-ST represent a subset of the assurance requirements of the IC-ST.

IC Security Functional Requirements	Rationale
Part of [PP-0084]	
From “Hardware random number generators”	
FCS_RNG.1	RP_SFR_SERV
From “Access Control Policy”	
FDP_ACC.1	RP_SFR_SERV
FDP_ACF.1	RP_SFR_SERV
From “Cryptographic services implemented in hardware”	
FCS_COP.1[TDES]	RP_SFR_SERV
FCS_CKM.6[TDES]	RP_SFR_SERV
FCS_COP.1[AES]	RP_SFR_SERV
FCS_CKM.6[AES]	RP_SFR_SERV
FCS_COP.1[RSA]	RP_SFR_SERV
FCS_CKM.6[RSA]	RP_SFR_SERV
FCS_COP.1[ECC]	RP_SFR_SERV
FCS_CKM.6[ECC]	RP_SFR_SERV
FCS_COP.1[X25519]	IP_SFR
FCS_CKM.6[X25519]	IP_SFR
From “Malfunctions”	
FRU_FLT.2	RP_SFR_MECH
FPT_FLS.1	RP_SFR_MECH
From “Abuse of Functionality”	
FMT_LIM.1	RP_SFR_MECH
FMT_LIM.2	RP_SFR_MECH
FAU_SAS.1	RP_SFR_SERV
From “Physical Manipulation and Probing”	

FPT_PHP.3	RP_SFR_MECH
FDP_SDI.2	RP_SFR_MECH
FDP_SDC.1	RP_SFR_MECH
From “Leakage”	
FDP_ITT.1	RP_SFR_MECH
FPT_ITT.1	RP_SFR_MECH
FDP_IFC.1	RP_SFR_MECH

Table 64 - IC Security Functional Requirements compatibility between Composite-ST and IC-ST

8. BIBLIOGRAPHY

8.1. External references

Reference	Title
[ISO7816]	Identification cards – Integrated circuit(s) cards with contacts - Books 1 to 9
[CC-1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022, Revision 1, November 2022 (CCMB-2022-11-001).
[CC-2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC:2022, Revision 1, November 2022, (CCMB-2022-11-002).
[CC-3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC:2022, Revision 1, November 2022, (CCMB-2022-11-003).
[CC-4]	Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC:2022, Revision 1, November 2022, (CCMB-2022-11-004).
[CC-5]	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC:2022, Revision 1, November 2022, (CCMB-2022-11-005).
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CEM:2022, Revision 1, November 2022, (CCMB-2022-11-006).
[CC-E&I]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, 22 July 2024, (CCMB-2024-002).
[CC-COMP]	EUCC SCHEME STATE-OF-THE-ART DOCUMENT, Composite product evaluation for Smart Cards and similar devices for CC 3.1, Version 2, December 2024.
[CIC]	Common Implementation Configuration v2.0 (GPC_GUI_080)
[EUPP]	TCA eUICC Profile Package Interoperable Format Test Specification v3.2, May 2022
[GPCS]	[GPCS] Global Platform Card Specification v2.3.1 (GPC_SPE_034), March 2018 – ref [11] in [PP/0100] and amendments ● [Amd A] Amendment A - Confidential Card Content Management, v1.2 (GPC_SPE_007) ● [Amd B] Amendment B - Remote Application Management over HTTP, v1.2 (GPC_SPE_011) ● [Amd C] Amendment C - Contactless Service, v1.3 (GPC_SPE_025) ● [Amd D] Amendment D - Secure Channel Protocol 03, v1.2 (GPC_SPE_014) ● [Amd F] Amendment F - Secure Channel Protocol '11' (SCP11c), v1.4
[SCP80]	SCP80 ETSI TS 102 225, ETSI TS 102 226 – ref [12] in [PP/0100]
[JC] [JCAPI3] [JCVM3] [JCRE3]	Java Card Specification v3.1.0, November 2019 Java Card 3 Platform - Java Card API, Classic Edition, Version 3.1.0, November 2019 Java Card 3 Platform - Virtual Machine Specification, Classic Edition, Version 3.1.0, November 2019 Java Card 3 Platform - Runtime Environment Specification, Classic Edition, Version 3.1.0, November 2019
[JCBV]	Java Card 3.1.0 - Off-card Verifier and onwards
[PP-84]	Security IC Platform Protection Profile with Augmentation Packages version 1.0, February 2014, BSI-CC- PP-0084-2014
[PP-eUICC]	eUICC for Consumer and IoT Devices Protection Profile Version 2.1, 3 February 2025 (SGP.25 v2.1 by GSMA)

[PP-JCS]	Java Card System – Open Configuration Protection Profile Version 3.2, July 2024
[PP-GP]	Secure Element Protection Profile version 1.0, February 2021, GPC_SPE_174
[SGP.06]	eUICC Security Assurance Principles, version 2.3, 27 May 2025
[SGP.07]	eUICC Security Assurance Methodology, version 2.3, 27 May 2025
[SGP.21]	Architecture Specification, version 3.0, March 2022
[SGP.22]	RSP Technical Specification, version 3.1, 01 December 2023 – ref [24] in [PP/0100]
[SGP.23]	RSP Test Specification for the eUICC SGP.23-1 Version 3.1.3 27 January 2025
[SGP.24]	RSP Compliance Process, Version 3.2, 27 January 2025
[ST/IC]	Security target of HED Secure Chip CIU98N70 V1.0 with IC Dedicated Software V1.0
[GUIDES/IC]	List of documents applicable to the certified IC: ● [AGD_API]HED_secure_chip_CIU98N70 1.0_with_IC_Dedicated_Software_V1.0_Crypto_and_Funcion_Library_User_Guide ● [AGD_OPE]HED_secure_chip_CIU98N70 V1.0_With_IC_Dedicated_Software_V1.0_Operational_User_Guidance ● [AGD_DS]HED_secure_chip_ CIU98N70 V1.0_with_IC_Dedicated_Software_V1.0_Product_Datasheet
[VER]	Global Platform Card Composition Model, Security Guidelines for Basic Applications (GPC_GUI_050, v2.0)

Table 65 - External References List

8.2. Internal references

Reference	Title
[GUIDES]	List of documents applicable to the certified **CIU98N70 eUICC V1.0 :** ● [AGD_OPE] HED_MCOS_V3.8_Operational_User_Guidance ● [AGD_PRE] HED_MCOS_V3.8_Preparative Procedures

Table 66 - Internal References List

8.3. Glossary

Term	Definition
Application	Instance of an Executable Module after it has been installed and made selectable
Controlling Authority	A Controlling Authority is entity independent from the OEM represented on the eUICC and responsible for securing the keys creation and personalization of the Supplementary Security Domains.
DAP Block	Part of the Load File used for ensuring Load File Data Block verification
DAP Verification	A mechanism used by a Security Domain to verify that a Load File Data Block is authentic
Issuer Security Domain	The primary on-card entity providing support for the control, security, and communication requirements of the card administrator
Profile	Security Domains, UICC file system and secure objects (Keys, PIN codes…) formatted as defined by [EUPP]. A Profile can be downloaded from RSP Servers onto a eUICC by end user consent, as defined by [SGP.21] [SGP.22].
RSP Servers	GSMA-defined SM-DP+ and SM-DS servers. Used to distribute a Profile to the end user.
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)
Supplementary Security Domain	A Security Domain other than the Issuer Security Domain dedicated to Application provider.

Verification Authority	The Verification Authority (VA), is a trusted third party represented on the (U)SIM card, acting on behalf of the OEM and responsible for the verification of application signatures (mandated DAP) during the loading process.

Table 67 - Glossary List

8.4. Abbreviations

Term	Definition
CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
PP	Protection Profile
SPE	Secure Processing Environment
NSPE	Non-Secure Processing Environment
COS	Chip Operating System
MCOS	HED Chip Operating System
HW	Hardware
SW	Software
OEM	Original Equipment Manufacturer
REE	Rich Execution Environment (e.g. Android, iOS, Linux, Windows, etc.)
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile (see [SGP.22])
ISD-R	Issuer Security Domain Root (see [SGP.22])
LPAd	Local Profile Assistant on Device (see [SGP.22])
PPE	Profile Policy Enforcer
PPI	Profile Package Interpreter
RAM	Remote Application Management
RFM	Remote File Mangement
OTA	Over-The-Air
OSU	Operating System Update
VA	Verification Authority
COMP	Composite Product Package

Table 68 - Abbreviations List

END OF DOCUMENT