ST4SIM-300v2
Security Target

Version: C

Date: 2026-09-11

STMicroelectronics

Document history

Version	Date	Comment	Author
A	2026-05-13	First release based on ST4SIM-300 Security Target version I, with the addition of GBA	STMicroelectronics
B	2026-06-23	OS and IC versions updated to the latest release	STMicroelectronics
C	2026-09-11	IC version reverted from B04 to B03	STMicroelectronics

Contents

1 Introduction 9

1.1 Scope 9

1.2 Definitions 9

1.3 Abbreviations 9

1.4 References 9

2 ST Introduction 13

2.1 ST Reference 13

2.2 TOE Reference 13

2.2.1 Other certifications 13

3 TOE Overview 14

3.1 TOE description 14

3.1.1 Application Layer 15

3.1.1.1 ISD-P 15

3.1.1.2 ISD-R 16

3.1.1.3 MNO-SD 16

3.1.1.4 ECASD 16

3.1.2 Platform Layer 17

3.1.2.1 Telco 17

3.1.2.2 IC+OS 17

3.1.2.3 Java card system 18

3.1.2.4 GlobalPlatform 18

3.2 TOE type and usage 18

3.3 TOE Life Cycle 18

3.4 Non-TOE Hardware/Software/Firmware 20

3.5 TOE scope 21

3.5.1 Physical scope 22

3.5.2 Logical scope 22

3.5.2.1 Remote SIM provisioning 23

3.5.2.2 Test profile support 23

3.5.2.3 Algorithms and cryptography 23

3.5.2.4 Over the air (OTA) functionality 24

3.5.2.5 Java Card 24
3.5.2.6 Memory management 24
3.5.2.7 OS Update 25
3.5.2.8 Local Profile Management (optional) 25

4 Conformance claims 26
4.1 CC Conformance Claims 26
4.2 Package Claims 26
4.3 PP Claims 26
4.4 Conformance Rationale 26
4.4.1 Conformity of the TOE Type 26
4.4.2 SPD Consistency 27
4.4.2.1 Assets consistency 27
4.4.2.2 Users and Subjects consistency 28
4.4.2.3 Threats consistency 29
4.4.2.4 Organizational Security Policies consistency 29
4.4.2.5 Assumptions consistency 29
4.4.3 Security Objectives Consistency 30
4.4.3.1 Objective for the TOE consistency 30
4.4.3.2 Objective for Environment consistency 30
4.4.4 Conformity of the Requirement (SFR/SAR) 31
4.4.4.1 SFR consistency 31
4.4.4.2 SAR consistency 34

5 Security Problem Definition 35
5.1 Assets 35
5.2 Security Aspects 35
5.3 Users and Subjects 35
5.4 Threats 35
5.5 Organizational Security Policies 36

6 Security Objectives 37
6.1 Security Objectives for the TOE 37
6.2 Security Objectives for the Operational Environment 38
6.3 Security Objectives Rationale 38

6.3.1 Threats 38
6.3.1.1 Unauthorized profile and platform management 38
6.3.1.2 Identity Tampering 39
6.3.1.3 eUICC cloning 40
6.3.1.4 LPAd impersonation 40
6.3.1.5 Unauthorized access to the mobile network 40
6.3.1.6 Second Level Threats 40
6.3.1.7 OS Update 41
6.3.2 Organizational Security Policies 42
6.3.3 Assumptions 42
6.3.4 Rationale Tables 42
6.3.4.1 Threats Rationale 42
6.3.4.2 Organizational Security Policies Rationale 43
6.3.4.3 Assumptions Rationale 43

7 Extended Component Definition 44

8 Security Functional Requirements 45
8.1 Java Card 45
8.1.1 COREG_LC SECURITY FUNCTIONAL REQUIREMENTS 45
8.1.1.1 Firewall policy 46
8.1.1.2 Application Programming Interface 47
8.1.1.3 Card Security Management 49
8.1.1.4 AID Management 51
8.1.2 InstG Security Functional Requirements 52
8.1.2.1 FPT_RCV.3/Installer Automated recovery without undue loss 52
8.1.3 ADELG Security Functional Requirements 53
8.1.4 ODELG Security Functional Requirements 53
8.1.5 CarG Security Functional Requirements 54
8.1.5.1 FCO_NRO.2/CM Enforced proof of origin 54
8.1.5.2 FDP_IFF.1/CM Simple security attributes 55
8.1.5.3 FDP_UIT.1/CM Data exchange integrity 56
8.1.5.4 FIA_UID.1/CM Timing of identification 56
8.1.5.5 FMT_MSA.1/CM Management of security attributes 56

8.1.5.6 FMT_MSA.3/CM Static attribute initialisation 57
8.1.5.7 FMT_SMF.1/CM Specification of Management Functions 57
8.1.5.8 FMT_SMR.1/CM Security roles 57
8.2 eUICC 58
8.2.1 Identification and authentication 59
8.2.1.1 FIA_USB.1/EXT User-subject binding 59
8.2.1.2 FIA_UAU.4/EXT Single-use authentication mechanisms 60
8.2.1.3 FIA_UID.1/EXT Timing of identification 60
8.2.1.4 FIA_UAU.1/EXT Timing of authentication 61
8.2.1.5 FIA_UID.1/MNO-SD Timing of identification 61
8.2.1.6 FIA_ATD.1/Base User attribute definition 62
8.2.2 Communication 62
8.2.2.1 FDP_IFF.1/SCP Simple security attributes 62
8.2.2.2 FTP_ITC.1/SCP Inter-TSF trusted channel 63
8.2.2.3 FDP_ITC.2/SCP Import of user data with security attributes 65
8.2.2.4 FPT_TDC.1/SCP Inter-TSF basic TSF data consistency 65
8.2.2.5 FCS_CKM.1/SCP-SM Cryptographic key generation 67
8.2.2.6 FCS_CKM.2/SCP-MNO Cryptographic key distribution 67
8.2.2.7 FCS_CKM.6/SCP-MNO Cryptographic key destruction 68
8.2.2.8 FCS_CKM.6/SCP-SM Cryptographic key destruction 68
8.2.3 Security Domains 69
8.2.3.1 FDP_ACF.1/ISDR Security attribute based access control 69
8.2.3.2 FDP_ACC.1/ECASD Subset access control 70
8.2.3.3 FDP_ACF.1/ECASD Security attribute based access control 70
8.2.4 Platform Services 71
8.2.4.1 FDP_IFC.1/Platform_services Subset information flow control 71
8.2.4.2 FDP_IFF.1/Platform_services Simple security attributes 72
8.2.4.3 FPT_FLS.1/Platform_Services Failure with preservation of secure state 73
8.2.5 Security management 73
8.2.5.1 FCS_RNG.1 Random number generation 73
8.2.5.2 FPT_EMS.1/Base TOE Emanation 75
8.2.5.3 FCS_COP.1/DRBG Cryptographic Operation 75
8.2.5.4 FMT_SMF.1/Base Specification of Management Functions 75

8.2.5.5 FMT_MSA.1/RULES Management of security attributes 76
8.2.5.6 FMT_MSA.1/CERT_KEYS Management of security attributes 76
8.2.6 Mobile Network authentication 76
8.2.6.1 FCS_COP.1/Mobile_network Cryptographic operation 76
8.2.6.2 FCS_CKM.2/Mobile_network Cryptographic key distribution 77
8.2.6.3 FCS_CKM.6/Mobile_network Cryptographic key destruction 78
8.2.7 OS Update functionality 78
8.3 Global Platform 79
8.3.1 Identification and authentication 79
8.3.1.1 FIA_AFL.1/GP Authentication failure handling 79
8.3.2 User data protection 79
8.3.2.1 FDP_UIT.1/GP Basic data exchange integrity 79
8.3.2.2 FDP_UCT.1/GP Basic data exchange confidentiality 80
8.4 Security Functional Requirements Rationale 81
8.4.1 SFRs for eUICC rationale 81
8.4.2 SFRs for Runtime Environment rationale 81
8.4.3 SFRs for Underlying platform IC rationale 82
8.5 SFR Dependencies 82

9 Security Assurance Requirements 87
9.1 SARs 87
9.2 SARs Dependency Rationale 88
9.3 Rationale for the Security Assurance Requirements 89
9.3.1 ALC_DVS.2 Sufficiency of security measures 89
9.3.2 AVA_VAN.5 Advanced methodical vulnerability analysis 89
9.3.3 ALC_FLR.2 Flaw Reporting Procedures 89

10 TOE Summary Specification 90
10.1 Security Functionality 90
10.1.1 Runtime environment SFR coverage 90
10.1.2 eUICC SFR coverage 92

11 Rationales 95
11.1 IC Composition rationale 95
11.1.1 Common Criteria rationale 95

11.1.2 Compatibility between threats (TOE and IC) 95
11.1.3 Compatibility between assumptions (TOE and IC) 96
11.1.4 Compatibility between security objectives for the environment (TOE and IC) 96
11.1.5 Compatibility between Security Objectives (TOE and IC) 96
11.1.6 Compatibility between Organisational Security Policies (TOE and IC) 97
11.1.7 Compatibility between SFRs (TOE and IC) 97

12 Abbreviations and glossary 99

1 Introduction

1.1 Scope

1.2 Definitions

Term	Description
Device	IoT Device

1.3 Abbreviations

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

1.4 References

Ref	DocNumber	Title	Version
[1]	[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model	CC:2022 Rev. 1
[2]	[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components	CC:2022 Rev. 1
[3]	[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components	CC:2022 Rev. 1
[4]	[CC-4]	Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities	CC:2022 Rev. 1
[5]	[CC-5]	Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements	CC:2022 Rev. 1
[6]	[SGP.25]	eUICC for Consumer and IoT Devices Protection Profile, SGP.25	v2.1, 3 February 2025
[7]	[PP-IC]	Security IC Platform Protection Profile with Augmentation Packages - BSI-CC-PP-0084-2014	V1.0
[8]	[CERT-IC]	ST33K1M5A and ST33K1M5M B03 Certification Report, NSCIB-CC-2300112-02-CR	v2.0, 26 September 2024
[9]	[PP-JC]	Java Card System - Open Configuration Protection Profile	v3.0.5
[10]	[PP-GP]	Global Platform – Secure Element Protection Profile	v1.0
[11]	[JCVM]	Java Card Platform - Classic Edition, Virtual Machine (Java Card VM) Specification.	v3.0.5
[12]	[JCAPI]	Java Card Platform - Classic Edition, Application Programming Interface.	v3.0.5
[13]	[JCRE]	Java Card Platform - Classic Edition, Runtime Environment (Java Card RE) Specification.	v3.0.5
[14]	[SOGIS-COMP]	Composite product evaluation for Smart Cards and similar devices	v1.5.1, 05/2018

Ref	DocNumber	Title	Version
[15]	[JIL-LOAD]	Security requirements for post-delivery code loading, Joint Interpretation Library	v1.0, Feb. 2016
[16]	[SGP.32]	eSIM IoT Technical Specification	v1.2, June 2024
[17]	[SGP.21]	Remote SIM Provisioning (RSP) Architecture, GSMA Association	v3.1, December 2023
[18]	[SGP.22]	Remote SIM Provisioning (RSP) Technical Specification, GSMA Association	v3.1, December 2023
[19]	[ANSI X9.31]	Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, American Bankers Association	September 9, 1998
[20]	[AIS20/31]	AIS20: Functionality classes and evaluation methodology for deterministic random number generators AIS31: Functionality classes and evaluation methodology for physical random number generators.	v3.0, May 2013
[21]	[FIPS 46-3]	FIPS 46-3, Data Encryption Standard (ANSI X3.92), National Institute of Standards and Technology	25/10/1999
[22]	[FIPS 81]	FIPS 81, DES Modes of Operation, National Institute of Standards and Technology	2 December 1980
[23]	[FIPS 140-2]	FIPS 140-2, Security requirements for cryptographic modules, National Institute of Standards and Technology	3 December 2002
[24]	[FIPS 180-2]	FIPS 180-2 Secure Hash Standard with Change Notice 1, National Institute of Standards and Technology, U.S.A	25/02/2004
[25]	[FIPS 197]	FIPS 197 Advanced Encryption Standard (AES), National Institute of Standards and Technology	26/11/2001
[26]	[GP]	Global Platform Inc., Global Platform Card Specification 2.3. Reference: GPC_SPE_034	v2.3 12/2015
[27]	[GP-A]	GlobalPlatform Inc., GlobalPlatform Technology, Confidential Card Content Management, Card Specification v2.3 – Amendment A	v1.1.1, Sep. 2018
[28]	[GP-B]	GlobalPlatform Inc., GlobalPlatform Card, Remote Application Management over HTTP, Card Specification v2.2 – Amendment B	v1.1.3, 05/2015
[29]	[GP-C]	GlobalPlatform Inc., GlobalPlatform Technology, Contactless Services, Card Specification 2.3 – Amendment C	v1.2.1, 07/2018
[30]	[GP-D]	GlobalPlatform Inc., GlobalPlatform Card Technology, Secure Channel Protocol '03', Card Specification v2.2 – Amendment D	v1.1.1, 07/2014
[31]	[GP-E]	GlobalPlatform Inc., GlobalPlatform Card Technology, Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E	v1.1, 10/2016
[32]	[GSMA SAS]	GSMA SAS Guidelines for Subscription Manager Roles GSMA SAS Methodology for Subscription Manager Roles GSMA SAS Standard for Subscription Manager Roles	v2.0, 13/05/2015
[33]	[GP-SGBA]	GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications - ref. GPC_GUI_050	v1.0, June 2012
[34]	[IEEE 1363a-2004]	IEEE Standard Specifications for Public-Key Cryptography – Amendment 1: Additional Techniques	2 September 2004
[35]	[KS2011]	W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators", Version 2.0, September 18, 2011	v2.0, 18/09/2011
[36]	[ST-IC]	ST33K1M5A and ST33K1M5M B03 Security Target for composition, SMD_ST33K1M5AM_ST_21_002	Rev B03. 1, Aug. 24

Ref	DocNumber	Title	Version
[37]	[NISTSP800-90A]	NIST Special Publication 800-90A, Recommendation for random number generation using deterministic random bit generators (Revision 1), National Institute of Standards and Technology	June 2015
[38]	[MILENAGE]	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General Document 2: Algorithm Specification Document 3: Implementers Test Data Document 4: Design Conformance Test Data Document 5: Summary and results of design and evaluation	
[39]	[TUAK]	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, “Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification Document 2: Implementers’ test data Document 3: Design conformance test data.”	
[40]	[TS 33 102]	3GPP TS 33.102 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture	Release 17
[41]	[TS 102 221]	ETSI, TS 102 221, UICC-Terminal interface; Physical and logical characteristics	v17.2.0, August 2022
[42]	[TS 102 222]	ETSI, TS 102 222, Administrative commands for telecommunications applications	v17.0.0, July 2022
[43]	[TS 102 223]	ETSI, TS 102 223, Card Application Toolkit (CAT)	v17.2.0, March 2023
[44]	[TS 102 224]	ETSI, TS 102 224, Security mechanisms for UICC based Applications, Functional requirements	v17.0.0, April 2024
[45]	[TS 102 225]	ETSI, TS 102 225, Secured packet structure for UICC based applications	v17.0.0, October 2022
[46]	[TS 102 226]	ETSI, TS 102 226, Remote APDU structure for UICC based application	v17.2.0, October 2022
[47]	[IPP]	eUICC Profile Package: Interoperable Format Technical Specification	v3.3.1, July 2023
[48]	[CEM2022]	Common Methodology for Information Technology Security Evaluation, Revision 1	November 2022
[49]	[ANSI X9.62]	American National Standards Institute (ANSI) ANS X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA)	16 November 2005
[50]	[FIPS 180-4]	FIPS 180-4 Secure Hash Standard (SHS), National Institute of Standards and Technology	4 August 2015
[51]	[FIPS 202]	FIPS 202 SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, National Institute of Standards and Technology	4 August 2015
[52]	[FIPS 198-1]	FIPS 198-1 The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology	16 July 2008

Ref	DocNumber	Title	Version
[53]	[NISTSP800-38B]	Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, National Institute of Standards and Technology	May 2005
[54]	[ISO/IEC 9797]	Information technology – Security techniques – Data Integrity mechanism using a cryptographic check function employing a block cipher algorithm	April 1994
[55]	[NISTSP800-56A, Rev.3]	Recommendation for Pair-Wise Key – Establishment Schemes Using Discrete Logarithm Cryptography	16 April 2018
[56]	[ISO/IEC 14888-3]	IT Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms	November 2018
[57]	[FIPS 186-4]	FIPS 186-4 Digital Signature Standard (DSS), National Institute of Standards and Technology	19 July 2013
[58]	[NISTSP800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, National Institute of Standards and Technology	21 October 2010
[59]	[CC-ERRATA]	Errata and Interpretation for CC 2022 (Release 1) and CEM 2022 (Release 1)	version 1.1, July 2024
[60]	[TS 31 102]	3GPP TS 31.102, “3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application”	Release 17
[61]	[TS 31 103]	3GPP TS 31.103, “3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application”	Release 17

2 ST Introduction

This section provides information about the TOE, which enables a potential user of the TOE to determine, whether the TOE implements the functionality required by the user.

2.1 ST Reference

ST4SIM-300v2 Security Target, Version C, 2026-09-11, STMicroelectronics.

2.2 TOE Reference

TOE Name	ST4SIM-300v2	
TOE Version	2.1.7	
TOE Identification	**IC**	IC Name: ST33K1M5M IC Maskset name: K4A0 Version: B03 Master product identification number: 0x024B Firmware version: 3.1.4 Neslib crypto library version: 6.10.2 Storekeeper library version: v4.1.2
	Java Card OS and eUICC functionality	OS_IDENTIFIER: 0x0000 OS_RELEASE_DATE: 0x6167 OS_RELEASE_LEVEL: 0x0008 OS_VERSION: 0x00020107
TOE Type	eUICC 5G compliant to SGP.32	

Table 1 TOE reference

2.2.1 Other certifications

The ST33K1M5M Secure IC has been already certified:

- IC name: ST33K1M5A and ST33K1M5M B03
- CC certificate reference [CERT-IC].

3 TOE Overview

The ST4SIM-300v2 TOE is based on the ST4SIM-300 TOE version 1.10.1, with the addition of the Generic Bootstrapping Architecture (GBA) USIM/ISIM functionality supported in accordance with 3GPP [TS 31 102] and 3GPP [TS 31 103].

The TOE consists of the following components:

- Secure IC kernel with memory management, ISO7816 communication protocol, memory manager, Storekeeper, Firmware upgrade enabler and Cryptographic operation based on the NesLib security library.
- Storekeeper, NesLib security library.
- Java Card runtime environment supporting multiple profiles.
- The Platform Layer: a set of functions providing support to the Application Layer:
  - A Telecom Framework providing network authentication algorithms;
  - A Profile Package Interpreter translating Profile Package data into an installed Profile;
  - And a Profile Rules Enforcer which comprises the Profile Policy Enabler (Profile Policy verification and enforcement functions) and the enforcement of Enterprise Rules (optional).
- The Application Layer: privileged applications, such as Security Domains, providing the remote provisioning and administration functionality:
  - An ISD-R, including LPA/IPA Services, providing life-cycle management of profiles;
  - An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication;
  - ISD-P security domains, each one hosting a unique profile.

3.1 TOE description

The TOE scope is shown in Figure 1.

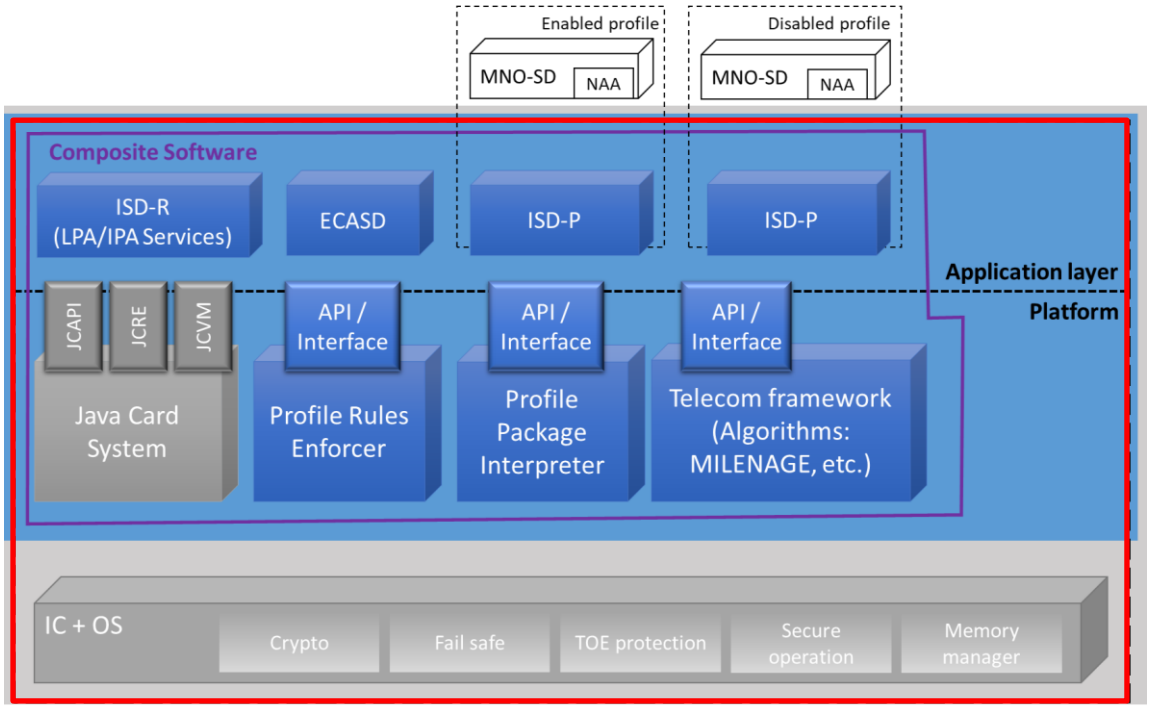


Figure 1 Scope of the TOE

3.1.1 Application Layer

The goal of the Application layer is to implement the eUICC functionalities described in [SGP.21] and [SGP.22], which rely on the notion of a Profile. A Profile is the combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC. Each Profile, combined with the functionality of the eUICC, behaves basically as a SIM card. An eUICC may contain more than one Profile.If an eUICC supports SEP (Single Enabled Profile), then only one Profile can be activated at a time. Each Profile is controlled by a unique ISD-P.

A Profile can have several forms:

- A Provisioning Profile: A Profile that allows connectivity to a mobile network solely to provide the provisioning of Profiles;
- An Operational Profile: A Profile that allows connectivity to a mobile network;
- A Test Profile: A Profile that can only be used in Device Test Mode and cannot be used to connect to any MNO. The support of this kind of profile is not mandatory for an eUICC implementation.

All Profiles include Network Access Applications and associated Parameters, but these applications rely on the algorithms stored in the platform layer of the eUICC.

In the same manner, the Profile includes policy rules (PPR) and may include Enterprise Rules (optional), but relies on the Platform Layer to have them enforced on the eUICC. The Profile structure, composed of a set of Profile Components, is specified by, and under the full control of, the MNO. The full Profile structure shall be contained in a unique ISD-P. The Profile structure shall contain a Profile Component, called MNO-SD, which performs an identical Role as the ISD for a UICC. The Profile structure shall include:

- The MNO-SD;
- Supplementary Security Domains (SSD) and a CASD;
- Applets;
- Applications, e.g. NFC applications;
- NAAs;
- Other elements of the File System;
- Profile metadata, including Profile Policy Rules (PPR) and optionally, Enterprise Rules.

More details on the Profile can be found in [SGP.21] and [SGP.22].

In addition to Profile data, the eUICC itself has a Rules Authorisation Table (RAT) that is used by the Profile Policy Enabler (PPE) and the Local Profile Assistant (non-TOE element LPAd) to determine whether or not a Profile containing PPRs is authorised and can be installed on the eUICC.

The RAT is initialised at eUICC manufacturing time, or during the initial Device setup provided that there is no installed Operational Profile. In particular, it cannot be affected by the Memory Reset function.

3.1.1.1 ISD-P

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

As defined in [SGP.22], the ISD-P shall ensure that:

- It hosts a unique Profile;
- Only the following Application Layer components shall have access to the profiles:
  - ISD-P;
  - ISD-R, which shall only have access to the metadata of the profiles;
- A Profile component shall not have any visibility of, or access to, components outside its ISD-P. An ISD-P shall not have any visibility of, or access to, any other ISD-P;
- Deletion of a Profile shall remove the containing ISD-P and all Profile components of the Profile.

3.1.1.2 ISD-R

The ISD-R is responsible for the creation of new ISD-Ps and life-cycle management of all ISD- Ps. An ISD-R shall be created within an eUICC at the time of manufacture.

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

As defined in [SGP.22]:

- There shall be only one ISD-R on an eUICC;
- The ISD-R shall be installed and personalized by the EUM during eUICC manufacturing. The ISD-R shall be associated with itself;
- The ISD-R cannot be deleted or disabled.

LPA/IPA Services

The LPA/IPA Services is the subset of ISD-R functionalities that provide the necessary access to the services and data required by LPA (the non-TOE element LPAd) or IPA (the non-TOE element IPAd). These services are:

- Transfer Bound Profile Package from the LPAd to the ISD-P;
- Provide list of installed Profiles;
- Retrieve EID;
- Provide Local/Remote Profile Management Operations [SGP.22];
- Transfer eUICC Package from the IPAd to the ISD-R [SGP.32].

LPA Services are mandatory. LPA/IPA Services code is located in the ISD-R.

3.1.1.3 MNO-SD

The MNO-SD is the on-card representative of the MNO Platform. It contains the MNO Over- The-Air (OTA) keys and provides a secure OTA channel.

3.1.1.4 ECASD

The Embedded UICC Controlling Authority Security Domain (ECASD) is responsible for the secure storage of credentials used to enforce trust in the identities of Actors (eUICC, remote Actors such as SM-DS or SM-DP+) and provides security functions used during key establishment and eUICC authentication.

As defined in [SGP.21], the ECASD has the following properties:

There can only be one ECASD on an eUICC;

- It is installed and personalised by the EUM during the eUICC manufacturing as described in [GP][PP-GP][PP-GP];
- It has eUICC private key(s) for creating signatures;
- It has associated certificate(s) for eUICC authentication;
- It has the eSIM CA public key(s) for verifying SM-DP+ and SM-DS certificates;
- It has the certificate of the EUM;
- It MAY have the eIM public key(s) or certificate(s) for verifying eIM messages [SGP.32].

3.1.2 Platform Layer

3.1.2.1 Telco

The Platform capabilities include:

- The Telecom Framework, which includes algorithms used by Network Access Applications (NAA) to access mobile networks. The NAAs are part of the Profiles, but the algorithms, as part of the Telecom Framework, are provisioned onto the eUICC during manufacturing.
- The Profile Package Interpreter, an eUICC Operating System service that translates the Profile Package data as defined in eUICC Profile Package Specification [IPP] into an installed Profile using the specific internal format of the target eUICC.
- The Profile Rules Enforcer, which implements the enforcement of Enterprise Rules (optional), and 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.

3.1.2.2 IC+OS

The hardware is ST33K1M5M, secure chip based on Arm Cortex-M35P CPU.

On the IC the Kernel manages physical / communication protocol (ISO7816), memory manager and Cryptographic operation.

Crypto operations are mainly based on security library (Neslib v6.10.2).

The memory manager has been enhanced to support multiple profiles; in particular:

- the RAM memory is allocated only to the Profile 0, to the currently enabled profile and to the profile in the download.
- The NVM memory is split in segments of 4kb that are assigned to profiles (so a segment can belong to only one profile); objects in a segment are all belonging to the same profile.

In the basic OS is also supported a specific “secure object” container (OM_secure) that is widely used in the platform to protect cryptographic secrets. The “OM_secure” allows masking of the sensitive data with a mask stored in a different memory area. Demasking is done at the last possible moment, e.g. for keys when it’s possible the operation is done with the key still masked, with PINs the comparison is done on the masked value, etc. The mask is stored in a NVM area that is distant by the objects, so if part of the NVM is successful dumped, the content of the sensitive object is not disclosed.

Masks of personalized data are differentiated chip by chip (i.e. it is randomized during production).

In addition, an anti-tear mechanism is present that allows integrity of operation and transactions also in case of power loss.

3.1.2.3 Java card system

The Java Card contains the registry of the profiles and the profile status (like which is the fallback profile, which is the currently enabled profile, etc.).

Applications architecture is based on Java Card, also for Security Domains and network access applications (like USIM); such system applications access to the product OS resources by using specific “native” methods, i.e. methods that allow the execution directly in “C” code.

Most of the RSP cryptographic operations (like SCP03t decryption, Key agreement for eCASD, etc.) are done through the standard Java Card cryptographic APIs.

The virtual machine keeps track of the current profile that can be seen as the profile of the applet currently in execution; so e.g. if a method of the ISD-R is in execution, the profile in execution is the profile 0 and memory allocation and visibility of file system is related to profile 0.

3.1.2.4 GlobalPlatform

The GlobalPlatform manages all the card content management operations and it has been extended to support the multi-profile operation.

In particular:

- The ISD-R is in charge of profile downloading operations.
- The Profile Manager module is in charge of Refresh command issuing after a profile change occurred.
- The ISD-P is the container of the profile, it is installed as first step of a Profile Download. The ISD-P contains a SCP03t keyset (typically but not necessarily established through the eCASD) and receives, encrypted via the SCP03t, the profile package. A sub module of the ISD-P is the profile package interpreter, that executes the ASN.1 format.
- Profile download in SCP03t may occur only over the SCP81 protocol.
- The MNO-SD belongs to a profile and it represents the “Issuer security domain” of the currently enabled profile; it does not have all the privileges of the ISD as it cannot lock the card or perform other operations that have impact beyond the operator profile.

3.2 TOE type and usage

The TOE is a composite of secure software implemented on a secure IC.

The TOE an eUICC for IoT devices.

The eUICC will contain several MNO Profiles, each of them being associated with a given International Mobile Subscriber Identity (IMSI).

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

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

3.3 TOE Life Cycle

This Security Target is conformant to [SGP.25]. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer to [SGP.25].

The composite product life cycle is decomposed into 5 phases. Each of these phases has the very same boundaries as those defined in the claimed protection profile.

The TOE is delivered at the end of the Phase c (see Table 2).

The life cycle phases are summarized in Table 2.

Phase	Name	Description
a	eUICC platform development Development of IC and embedded software	This phase corresponds to the first two stages of the IC development. In this phase the ST4SIM-300v2 OS and related applications are developed according to the Phase 1 of the ST Life cycle model as reported in Operational User Guidance.
b	eUICC platform storage, pre-perso, test Security IC manufacturing and packaging	This phase corresponds to the phases 3 and 4 of the IC development. The TOE hardware is delivered at the end of Phase 4 in packaged form. In addition, an encrypted image containing ST4SIM-300v2 OS and applications is delivered.
c	eUICC platform storage, pre-perso, test integration of Platform Software (JCS, GP, policy enforcement module, telecom framework) and Applications (ECASD / ISD-R)	This phase corresponds to phase 5 of the IC development. In this phase the encrypted image is downloaded on the hardware by using the Flash Loader according to [ST-IC]. Product configuration is performed, including all the applications integration, the system applications configurations and the profile loading and configuration, according to Phase 5 of ST life cycle model reported in Operational User Guidance. Such a phase is done in a STMicroelectronics Software design Center. In this phase, typically: The Issuer Security Domain of profile 0 is installed. Applications of the profile 0 are installed (ISD-R, eCASD, Fallback). A profile is loaded, but not personalized (e.g. the IMSI has a fixed value, like FF…FF). Optionally, other profiles (such as test profiles or emergency profiles) are pre-loaded. An image of the product (including OS + basic configuration) is obtained from a device (golden sample). Phase c and Phase d (GSMA SAS) are performed at the same secure site in which case the eUICC Manufacturer is considered as trusted administrator to enable the TOE self-protection before the end of phase d.
d	eUICC Platform personalization Personalization of (ECASD/ISD-R Keys). Addition of applications (profiles / ISD-P)	This phase corresponds to phase 6 of the IC development, that is equivalent to “Phase D” of [SGP.25]. In this phase, the ST4SIM-300v2 devices are personalized with diversified credentials, according to Phase 6 of ST life cycle model reported in Operational User Guidance. Such a phase is done in a STMicroelectronics Production site (SAS certified). In this phase, typically: The image obtained at configuration time is dumped in every device. The personalization mask is randomized. Personalization data are stored by using administrative file system commands and GlobalPlatform commands without security. The device is finally “secured” by disabling administrative commands and requiring GP security at GP commands.
e	Operational usage	This phase corresponds to phase 7 of the IC development. Such a phase represents the life cycle state of the product on the field, according to Phase 7 of ST life cycle model reported in Operational User Guidance. In this phase:

		The EIM and SM-DP+ through the ISD-R can perform SGP.32 operations over the air. The MNO of the enabled profile can perform content management of its profile through the security domains and remote file management applications in the profile.

Table 2 TOE life cycle phases

3.4 Non-TOE Hardware/Software/Firmware

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

Component	Required	Description
Device	Mandatory	The eUICC is intended to be used in a IoT Device. The IoT Device is expected to include a user interface, at least related to the eUICC functionality. In this case, the eUICC includes the Local User Interface (LUI) part of the LPA. The IoT Device can be either a Network Constrained Device or a User Interface Constrained Device. No security certification is expected to be performed on the Device itself, and the eUICC does not rely on the Device security to protect its assets.
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.
MNO-SD and applications	Mandatory	The Profile controlled by each ISD-P consists in a MNO-SD security domain, which itself may manage several applications. *Basic applications* Basic applications stand for applications that do not require any particular security for their own. Basic applications must be compliant with the security rules as defined in [GP-SGBA]. *Secure Applications* Secure applications are applications requiring a high level of security for their own assets. It is indeed necessary to protect application assets in confidentiality, integrity or availability at different security levels depending on the AP Security Policy. As such, secure applications follow a Common Criteria evaluation and certification in composition with the previously certified underlying Platform.
LPAd/IPAd	Mandatory	The TOE for IoT eUICC relies on a Local Profile Assistant (LPA) or IoT Profile Assistant (IPA) component [SGP.32]. Although LPAd/IPAd is a non-TOE component it uses the LPA/IPAd Services already mentioned in section 3.1.1.2.
Remote provisioning infrastructure for IoT Devices	Mandatory	The eUICC interfaces with the following remote provisioning entities that are responsible for the management of Profiles on the eUICC. Next figure describes the communication channels of the architecture when the IPA is located in the IoT Device (IPAd).

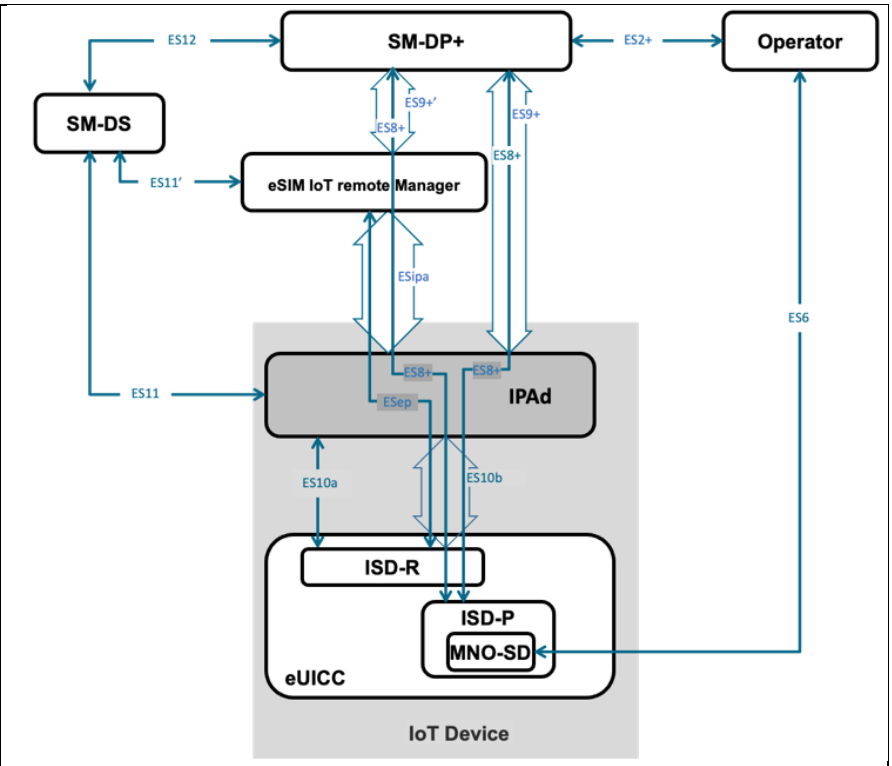
		 The TOE communicates with remote servers of: • SM-DP+, which provides Platform and Profile State Management commands as well as Profiles. • eIM which provides Profile State Management Operations and eIM Configuration Operations. The TOE shall require the use of secure channels for these interfaces. The keys and certificates required for these operations on the TOE are exchanged/generated during operational use of the TOE. Identities (in terms of certificates) rely on a single root of trust called the CA, whose public key is stored pre-issuance on the eUICC. The remote servers and, if any, the security components (such as an HSM) from which the keys are obtained are referred as Trusted IT products.

Table 3 Components of the environment

3.5 TOE scope

The TOE is a composite TOE comprising hardware and software. The physical scope is defined as:

- The STMicroelectronics IC ST33K1M5M Security Integrated Circuit with dedicated software. CC certified by NSCIB with assurance level EAL6+ [CERT-IC].
- An encrypted image of the ST4SIM-300v2 Operating system, including:
  - the Java Card Operating System version 3.0.5.
  - the embedded UICC implementation that supports the USIM applications providing access to Universal Mobile Telecommunications System (UMTS) networks and the IP Multimedia Services Identity Module (ISIM) to access IP Multimedia Subsystem (IMS) networks.

3.5.1 *Physical scope*

Category	Component	Version	Delivery form
HW	ST33K1M5M	B03	See supported form below
FW	ST4SIM-300v2 OS	2.1.7	Encrypted image is transferred to STMicroelectronics engineering department encrypted via PGP by using shared repositories.
DOC	Operational User Guidance	Rev C	PDF file delivered encrypted by e-mail
DOC	Preparative Procedure	Rev C	PDF file delivered encrypted by e-mail

The following form factors shall be supported:

- VFDFPN 8-pin very thin fine pitch dual flat package no lead - 5 mm × 6 mm, 1.27 mm pitch, with wettable flank. (for ETSI MFF2)
- UFQFPN-32 wettable flank (5x5mm)
- TSSOP 20-lead thin shrink small outline package - body 4.4 mm pitch 0.65 mm.
- D16 micromodule (for ETSI 2FF/3FF/4FF)
- WLCSP11, 24-ball wafer-level chip-scale package available for the ST33K1M5 only.

3.5.2 *Logical scope*

The ST4SIM-300v2 is a STMicroelectronics top-class GSMA embedded SIM (eSIM or eUICC) product designed for IoT devices. Figure 2 shows the high-level architecture of the TOE.

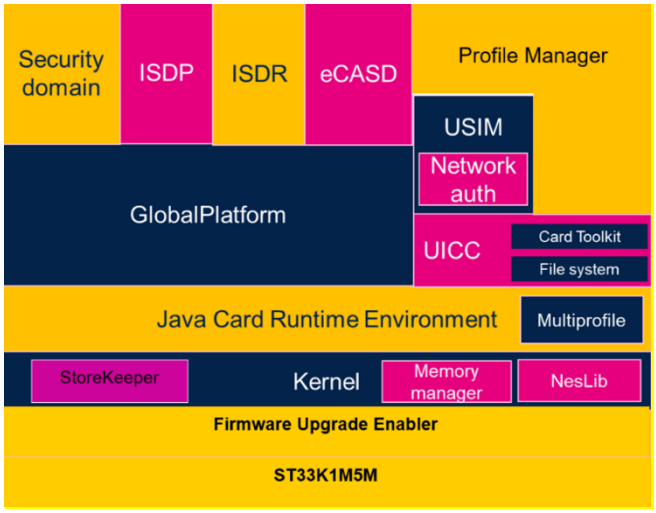


Figure 2 TOE Architecture

It is compliant with the GSM Association (GSMA) specification SGP.32 v1.1.

The ST4SIM-300v2 can remotely manage profiles of different MNOs while ensuring the appropriate security level to all eUICC stakeholders (user, MNO, OEM, hardware integrator, service provider, and so on).

The device can include an embedded secure element to store credentials and/or independent applications directly managed by the MCU (or by another OEM element).

The device provides a secure and interoperable Java Card environment compliant with Java Card v. 3.0.5 Classic. Moreover, the device integrates the most advanced UICC features compliant with GlobalPlatform, ETSI, 3GPP, 3GPP2 specifications.

The ST4SIM-300v2 integrates a dynamic memory management with Java Card garbage collection mechanism optimizing the usage of the memory.

The ST4SIM-300v2 is based on the ST33K1M5M, an industrial grade hardware solution (JEDEC) supporting

severe conditions. This solution is a tamper-resistant secure element certified by Common Criteria EAL6+, with a powerful 32-bit Arm Cortex-M35P CPU

3.5.2.1 Remote SIM provisioning

The ST4SIM-300v2 platform supports all the mechanisms defined by the GSMA SGP.32 specifications to perform ISD-R, ISD-P and profile management.

The ST4SIM-300v2 platform fully supports Trusted Connectivity Alliance interoperable profile package v3.3.1. No proprietary features are introduced. Profiles are coded according to ASN.1/DER coding.

The card may host up to 7 profiles; every profile may have a specific memory quota coded according to GlobalPlatform Amendment C [GP-C] for non-volatile memory or use up to the card available memory for its purpose. Each profile contains a full file system structure (MF, ADFs, …) with is own PINs/PUKs, NAA authentication information, etc. plus an MNO-SD and additional Security Domains.

Each profile is independent from the other profiles, i.e. it is possible to have in two profiles an application with the same AID, TAR or global service.

In addition, on the card there is a basic profile (defined as profile 0) that contains ISD-R, ISD and eCASD, that are visible whatever is the selected profile. It is possible to store in the profile 0 other applications; in this case, such applications shall be visible whatever the selected profile is. Also, java card library packages can be stored in profile 0; all the card provided library packages (java card, sim toolkit, etc.) belong to the profile 0.

3.5.2.2 Test profile support

In addition to Remote SIM provisioning, test profiles can be loaded before issuance. Such profiles shall be available for local and remote profile switch to allow device integrator to test with network simulator equipment.

The local profile switch can be configured to be executed over the ISO interface.

The test profile feature can be disabled before issuance or after issuance with proper credentials.

3.5.2.3 Algorithms and cryptography

The ST4SIM-300v2 supports the following standard authentication algorithms:

- 3GPP Test algorithm
- MILENAGE
- TUAK

The MILENAGE algorithm enables authorized access to UMTS/LTE networks with an easy and flexible parameter customization, according to specific MNO requirements.

The TUAK authentication algorithm is supported with both 128-bit key length and 256-bit key length.

The ST4SIM-300v2 also supports the "3GPP test algorithm" for test profiles.

Besides standard symmetric cryptography and hashing algorithms (DES, Triple DES, AES, and so on), the ST4SIM-300v2 provides a cryptographic co-processor with asymmetric cryptography capabilities.

For applications requiring the strongest level of cryptography, the ST4SIM-300v2 supports:

- elliptic curve cryptography (ECC) with a key length of up to 521 bits.

In addition, the ST4SIM-300v2 offers a rule-based access control mechanism such as digital signature/certificates for data/applications requiring a strong level of cryptography.

The security algorithm implementation adheres to the chip security guidelines of the ST33K1M5M to guarantee the best security level (for more information, contact the local STMicroelectronics sales office).

3.5.2.4 Over the air (OTA) functionality

The ST4SIM-300v2 supports over the air protocol for remote application management (RAM) and remote file management (RFM) compliant with ETSI standard (ETSI TS 102 225 and ETSI TS 102 226 specifications Release 17, API Release 16.

The RAM application is also fully supported by GlobalPlatform® v2.3 and the related amendment B (which enables remote applet management and remote file management over HTTP/TLS).

TLS v1.0, 1.1 and 1.2 are available in the ST4SIM-300v2. In addition, the ST4SIM-300v2 integrates a DNS mechanism allowing the card to request the HTTPS server address from a DNS server.

The ST4SIM-300v2 is able to remotely control the execution of APDU commands over the air, to administrate the card content. It also allows proactive commands to interact with the host device.

The ST4SIM-300v2 supports the secured packet structure and the remote APDU structure for (U)SIM toolkit applications, conforming to 3GPP TS 31.115, and TS 31.116 specifications.

The CAT-TP protocol defined by ETSI release 13 is supported.

As it is compliant with the ETSI, 3GPP, and 3GPP2, the ST4SIM-300v2 can easily be integrated into any OTA platform compliant with the relevant standards. STMicroelectronics cards are field-proven to be interoperable with the mainstream OTA platforms commonly chosen by mobile network operators.

3.5.2.5 Java Card

ST4SIM-300v2 supports Java Card v3.0.5 classic edition; all the mandatory features are included, plus in addition support of int type and of object deletion.

3.5.2.6 Memory management

The OTA mechanism includes the support of administrative commands as specified by ETSI [TS 102 222].

These commands are integrated by a powerful dynamic memory management that allows complete smart

memory defragmentation.

Dynamic memory management provides:

- Common space for files, packages, applets, and objects
- Memory recovery on deletion operations

- Total free memory available in the select MF response.

The OTA mechanism is designed to allow a very fast and silent memory recovery, absolutely safe for the end user data.

The ST4SIM-300v2 is capable of enhancing intrinsic flash memory cells for files requiring intense update and high reliability.

A memory quota mechanism based on the GlobalPlatform Amendment C [GP-C] (CGM) is supported. The mechanism can be disabled at card configuration.

Volatile memory management is based on a STMicroelectronics patented mechanism that optimizes the available resources for the enabled profile while allowing resources for the downloading profile and the disabled profiles.

3.5.2.7 OS Update

ST4SIM-300v2 supports OS update capability to correct existing features as required by the GSMA specifications.The specific mechanisms to upgrade the Operating System functionality are based on the V3 Loader usage, provided by chip, and a java application, i.e. Firmware Upgrade Applet able to enable V3 Loader mode. A script is delivered (sequence of APDUs) to the Customer, with a first part containing the set-up of a secure channel towards the firmware Upgrade Applet, to enable the V3 loader mode, and a second part encrypted with keys of V3 Loader (sequence of APDUs) to the Customer, carrying the new OS version. The confidentiality and integrity of the script are enforced by the Secure channel protocol as supported by Firmware Upgrade Applet and by encryption applied by V3 Loader. This procedure is performed during Phase 7 - TOE Usage (SC normal use) of ST life cycle (described in AGD_OPE section 5.7).

3.5.2.8 Local Profile Management (optional)

ST4SIM-300v2 provides the optional functionality of Local Profile Management which allows Enable/Disable/Delete commands to be issued by IPAd/LPAd and executed by TOE as specified in [18] over ES10c interface. This functionality is enabled in pre-personalization phase, if requested by customer. It is assumed that the entity executing it (IPAd/LPAd) shall have a means to verifying that the originator of the request is authenticated, similarly as it is specified in [SGP.25].

4 Conformance claims

4.1 CC Conformance Claims

The TOE and ST conforms to the Common Criteria 2022 release 1.

The ST is:

- CC Part 1 [CC-1] conformant,
- CC Part 2 [CC-2] extended,
- CC Part 3 [CC-3] conformant,
- CC Part 4 [CC-4] conformant,
- CC Part 5 [CC-5] conformant.

4.2 Package Claims

The assurance requirement of this Protection Profile is EAL4 augmented. Augmentation results from the selection of:

- ALC_DVS.2 Sufficiency of security measures.
- AVA_VAN.5 Advanced methodical vulnerability analysis.
- ALC_FLR.2 Flaw Reporting Procedures.

Completed with ASE_COMP.1, ADV_COMP.1, ATE_COMP.1, ALC_COMP.1, and AVA_COMP.1.

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

4.3 PP Claims

ST claims demonstrable conformance to:

- eUICC for Consumer and IoT Devices Protection Profile [SGP.25]

The PP module for OS update is in scope, as defined in [SGP.25] Appendix A.

4.4 Conformance Rationale

Conformance rationale of the ST against [SGP.25] 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 [SGP.25].
- Refinement (R): The element in the ST refines the corresponding [SGP.25] 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 [SGP.25] and does not affect it.
- X: The element is present in [SGP.25].

4.4.1 Conformity of the TOE Type

The TOE type for this ST is the same as defined in the [SGP.25].

The TOE follows the third scenario from the definition in [SGP.25] 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 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.

The composite evaluation includes the additional composition tasks defined in the [CEM2022] sections 12.10, 13.9, 15.10, 16.7, 17.3.

4.4.2 SPD Consistency

4.4.2.1 Assets consistency

All assets defined in [SGP.25] are relevant for the TOE of this Security Target. The table below indicates the assets' consistency and the additions from [PP-JC].

Assets	SGP.25	Security Target
D.MNO_KEYS	X	(E)
D.PROFILE_NAA_PARAMS	X	(E)
D.PROFILE_IDENTITY	X	(E)
D.PROFILE_RULES	X	(E)
D.PROFILE_USER_CODES (SGP.22)	X	(E)
D.PROFILE_CODE	X	(E)
D.TSF_CODE	X	(E)
D.PLATFORM_DATA	X	(E)
D.DEVICE_INFO	X	(E)
D.PLATFORM_RAT	X	(E)
D.SK.EUICC.ECDSA	X	(E)
D.CERT.EUICC.ECDSA	X	(E)
D.PK.CI.ECDSA	X	(E)
D.PK.EIM.ECDSA (SGP.32)	X	(E)
D.EID	X	(E)
D.SECRETS	X	(E)
D.CERT.EUM.ECDSA	X	(E)
D.CRLs	X	(E)
D.APP_CODE		(A): Added from [PP-JC]
D.APP_C_DATA		(A): Added from [PP-JC]
D.APP_I_DATA		(A): Added from [PP-JC]
D.APP_KEYs		(A): Added from [PP-JC]
D.PIN		(A): Added from [PP-JC]
D.API_DATA		(A): Added from [PP-JC]
D.CRYPTO		(A): Added from [PP-JC]
D.JCS_CODE		(A): Added from [PP-JC]
D.JCS_DATA		(A): Added from [PP-JC]
D.SEC_DATA		(A): Added from [PP-JC]
D.UPDATE_IMAGE	X	(E): Added from Appendix A to cover the OS update
D.TOE_IDENTIFIER	X	(E): Added from Appendix A to cover the OS update
D.OS-UPDATE_KEY(S)	X	(E): Added from Appendix A to cover the OS update

Table 4 Assets Consistency table

4.4.2.2 Users and Subjects consistency

All Users defined in [SGP.25] are relevant for the TOE of this Security Target. The table below indicates the Users' consistency

User	SGP.25	Security Target
U.SM-DP+	X	(E)
U.SM-DS	X	(E)
U.MNO-OTA	X	(E)
U.MNO-SD	X	(E)
U.EIM (SGP.32)	X	(E)
U.End-User (SGP.22)	x	(E)

Table 5 User consistency table

All Subjects defined in [SGP.25] are relevant for the TOE of this Security Target. The table below indicates the Subjects' consistency and the additions from [PP-JC].

Subjects	SGP.25	Security Target
S.ISD-R	X	(E)
S.ISD-P	X	(E)
S.ECASD	X	(E)
S.PPI	X	(E)
S.PRE	X	(E)
S.TELECOM	X	(E)
S.ADEL		(A): Added from [PP-JC]
S.APPLET		(A): Added from [PP-JC]
S.BCV		(A): Added from [PP-JC]
S.CAD		(A): Added from [PP-JC]
S.INSTALLER		(A): Added from [PP-JC]
S.JCRE		(A): Added from [PP-JC]
S.JCVM		(A): Added from [PP-JC]
S.LOCAL		(A): Added from [PP-JC]
S.MEMBER		(A): Added from [PP-JC]
S.CAP_FILE		(A): Added from [PP-JC]
S.OSU	X	(E): Added from Appendix A to cover the OS update
S.UpdateImageCreator	X	(E): Added from Appendix A to cover the OS update

Table 6 Subject consistency table

4.4.2.3 Threats consistency

All Threats defined in [SGP.25] are relevant for the TOE of this Security Target. The table below indicates the Threats' consistency.

Threats	SGP.25	Security Target
T.UNAUTHORIZED-PROFILE-MNG	X	(R): Assets added from [PP-JC] are mapped as threatened assets.
T.UNAUTHORIZED-PLATFORM-MNG	X	(R): Assets added from [PP-JC] are mapped as threatened assets.
T.PROFILE-MNG-INTERCEPTION	X	(R): Assets added from [PP-JC] are mapped as threatened assets.
T.PROFILE-MNG-ELIGIBILITY	X	(R): Assets added from [PP-JC] are mapped as threatened assets.
T.UNAUTHORIZED-IDENTITY-MNG	X	(R): Assets added from [PP-JC] are mapped as threatened assets.
T.IDENTITY-INTERCEPTION	X	(R): Assets added from [PP-JC] 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-JC] are mapped as threatened assets.
T.PHYSICAL-ATTACK	X	(E)
T.CONFID-UPDATE-IMAGE.LOAD	X	(E): Added from Appendix A to cover the OS update
T.INTEG-UPDATE-IMAGE.LOAD	X	(E): Added from Appendix A to cover the OS update
T.UNAUTH-UPDATE-IMAGE.LOAD	X	(E): Added from Appendix A to cover the OS update
T.INTERRUPT_OSU	X	(E): Added from Appendix A to cover the OS update

Table 7 Threats Consistency table

4.4.2.4 Organizational Security Policies consistency

All Organizational Security Policies defined in [SGP.25] are relevant for the TOE of this Security Target. The table below indicates the OSPs consistency.

OSPs	SGP.25	Security Target
OSP.LIFE-CYCLE	X	(E)

Table 8 OSPs Consistency table

4.4.2.5 Assumptions consistency

All Assumptions defined in [SGP.25] are relevant for the TOE of this Security Target. The table below indicates the Assumptions consistency.

Assumptions	SGP.25	Security Target
A.TRUSTED-PATHS-LPAd-IPAd	X	(E)
A.ACTORS	X	(E)
A.APPLICATIONS	X	(E)
A.CONFID_UPDATE_IMAGE.CREATE		(A): Added by the ST for completeness.

Table 9 Assumptions Consistency table

4.4.3 Security Objectives Consistency

4.4.3.1 Objective for the TOE consistency

All Security Objectives defined in [SGP.25] 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 [SGP.25] become security objectives from the TOE in the present security target. The [SGP.25] already provides the conversion of OE.RE* to objectives from the [PP-JC] protection profile.

O.TOE	SGP.25	Security Target
O.PRE-PPI	X	(E)
O.eUICC-DOMAIN-RIGHTS	X	(E)
O.SECURE-CHANNELS	X	(E)
O.INTERNAL-SECURE-CHANNELS	X	(E)
O.PROOF_OF_IDENTITY	X	(E)
O.OPERATE	X	(E)
O.API	X	(E)
O.DATA-CONFIDENTIALITY	X	(E)
O.DATA-INTEGRITY	X	(E)
O.ALGORITHMS	X	(E)
O.SECURE_LOAD_ACODE	X	(E): Added from Appendix A to cover the OS update
O.SECURE_AC_ACTIVATION	X	(E): Added from Appendix A to cover the OS update
O.TOE_IDENTIFICATION	X	(E): Added from Appendix A to cover the OS update
O.CONFID-UPDATE-IMAGE.LOAD	X	(E): Added from Appendix A to cover the OS update
O.AUTH-LOAD-UPDATE-IMAGE	X	(E): Added from Appendix A to cover the OS update

Table 10 Security objectives for the TOE consistency table

4.4.3.2 Objective for Environment consistency

O.ENV	SGP.25	Security Target
OE.CI	X	(E)
OE.SM-DP+	X	(E)
OE.SM-DS	X	(E)
OE.MNO	X	(E)
OE.EIM (SGP.32)	X	(E)
OE.TRUSTED-PATHS-LPAd-IPAd	X	(E)
OE.APPLICATIONS	X	(E)
OE.MNO-SD	X	(E)
OE.CODE-EVIDENCE		(A): Added from [PP-JC]
OE.IC.PROOF_OF_IDENTITY	X	Removed and replaced by O.IC.PROOF_OF IDENTITY.
OE.IC.SUPPORT	X	Removed and replaced by O.IC.SUPPORT.
OE.IC.RECOVERY	X	Removed and replaced by O.IC.RECOVERY.
OE.RE.PRE-PPI	X	Removed and replaced by O.RE.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.CONFID_UPDATE_IMAGE.CREATE	X	(E): Added from Appendix A to cover the OS update

Table 11 Security objectives for the Operational Environment consistency table

4.4.4 Conformity of the Requirement (SFR/SAR)

4.4.4.1 SFR consistency

SFR	SGP.25	Security Target
FIA_UID.1/EXT	X	(E)
FIA_UAU.1/EXT	X	(E)
FIA_USB.1/EXT	X	(E)
FIA_UAU.4/EXT	X	(E)
FIA_UID.1/MNO-SD	X	(E)
FIA_USB.1/MNO-SD	X	(E)
FIA_ATD.1/Base	X	(E)
FIA_API.1	X	(E)
FDP_IFC.1/SCP	X	(E)
FDP_IFF.1/SCP	X	(E)
FTP_ITC.1/SCP	X	(E)
FDP_ITC.2/SCP	X	(E)
FPT_TDC.1/SCP	X	(E)
FDP_UCT.1/SCP	X	(E)
FDP_UIT.1/SCP	X	(E)
FCS_CKM.1/SCP-SM	X	(E)
FCS_CKM.2/SCP-MNO	X	(E)
FCS_CKM.6/SCP-SM	X	(E)
FCS_CKM.6/SCP-MNO	X	(E)
FDP_ACC.1/ISDR	X	(E)
FDP_ACF.1/ISDR	X	(E)
FDP_ACC.1/ECASD	X	(E)
FDP_ACF.1/ECASD	X	(E)
FDP_IFC.1/Platform_services	X	(E)
FDP_IFF.1/Platform_services	X	(E)
FPT_FLS.1/Platform_services	X	(E)
FCS_RNG.1	X	(E)

FPT_EMS.1/Base	X	(E)
FDP_SDI.1/Base	X	(E)
FDP_RIP.1/Base	X	(E)
FPT_FLS.1/Base	X	(E)
FMT_MSA.1/PLATFORM_DATA	X	(E)
FMT_MSA.1/RULES	X	(E)
FMT_MSA.1/CERT_KEYS	X	(E)
FMT_SMF.1/Base	X	(E)
FMT_SMR.1/Base	X	(E)
FMT_MSA.1/RAT	X	(E)
FMT_MSA.3	X	(E)
FCS_COP.1/Mobile_network	X	(E)
FCS_CKM.2/Mobile_network	X	(E)
FCS_CKM.6/Mobile_network	X	(E)
FDP_ACC.2/FIREWALL		(A): Added from [PP-JC]
FDP_ACF.1/FIREWALL		(A): Added from [PP-JC]
FDP_IFC.1/JCVM		(A): Added from [PP-JC]
FDP_IFF.1/JCVM		(A): Added from [PP-JC]
FDP_RIP.1/OBJECTS		(A): Added from [PP-JC]
FMT_MSA.1/JCRE		(A): Added from [PP-JC]
FMT_MSA.1/JCVM		(A): Added from [PP-JC]
FMT_MSA.2/FIREWALL_JCVM		(A): Added from [PP-JC]
FMT_MSA.3/FIREWALL		(A): Added from [PP-JC]
FMT_MSA.3/JCVM		(A): Added from [PP-JC]
FCS_CKM.1		(A): Added from [PP-JC]
FCS_CKM.6		(A): Added from [PP-JC] Note: Since FCS_CKM.4 is deprecated in CC 2022, this SFR is replaced with FCS_CKM.6
FCS_COP.1		(A): Added from [PP-JC]
FCS_COP.1/DRBG		(A): Added in the current ST
FDP_RIP.1/ABORT		(A): Added from [PP-JC]
FDP_RIP.1/APDU		(A): Added from [PP-JC]
FDP_RIP.1/bArray		(A): Added from [PP-JC]
FDP_RIP.1/GlobalArray		(A): Added from [PP-JC]
FDP_RIP.1/KEYS		(A): Added from [PP-JC]
FDP_RIP.1/TRANSIENT		(A): Added from [PP-JC]
FDP_ROL.1/FIREWALL		(A): Added from [PP-JC]
FAU_ARP.1		(A): Added from [PP-JC]
FDP_SDI.2/DATA		(A): Added from [PP-JC]
FPR_UNO.1		(A): Added from [PP-JC]
FPT_FLS.1		(A): Added from [PP-JC]
FPT_TDC.1		(A): Added from [PP-JC]
FIA_ATD.1/AID		(A): Added from [PP-JC]

FIA_UID.2/AID		(A): Added from [PP-JC]
FIA_USB.1/AID		(A): Added from [PP-JC]
FMT_MTD.1/JCRE		(A): Added from [PP-JC]
FMT_MTD.3/JCRE		(A): Added from [PP-JC]
FDP_ITC.2/Installer		(A): Added from [PP-JC]
FMT_SMR.1/Installer		(A): Added from [PP-JC]
FPT_FLS.1/Installer		(A): Added from [PP-JC]
FPT_RCV.3/Installer		(A): Added from [PP-JC]
FDP_ACC.2/ADEL		(A): Added from [PP-JC]
FDP_ACF.1/ADEL		(A): Added from [PP-JC]
FDP_RIP.1/ADEL		(A): Added from [PP-JC]
FMT_MSA.1/ADEL		(A): Added from [PP-JC]
FMT_MSA.3/ADEL		(A): Added from [PP-JC]
FMT_SMF.1/ADEL		(A): Added from [PP-JC]
FMT_SMR.1/ADEL		(A): Added from [PP-JC]
FPT_FLS.1/ADEL		(A): Added from [PP-JC]
FDP_RIP.1/ODEL		(A): Added from [PP-JC]
FPT_FLS.1/ODEL		(A): Added from [PP-JC]
FCO_NRO.2/CM		(A): Added from [PP-JC]
FDP_IFC.2/CM		(A): Added from [PP-JC]
FDP_IFF.1/CM		(A): Added from [PP-JC]
FDP_UIT.1/CM		(A): Added from [PP-JC]
FIA_UID.1/CM		(A): Added from [PP-JC]
FMT_MSA.1/CM		(A): Added from [PP-JC]
FMT_MSA.3/CM		(A): Added from [PP-JC]
FMT_SMF.1/CM		(A): Added from [PP-JC]
FTP_ITC.1/CM		(A): Added from [PP-JC]
FIA_AFL.1/GP		(A): Added from [PP-GP].
FIA_UAU.1/GP		(A): Added from [PP-GP].
FIA_UAU.4/GP		(A): Added from [PP-GP].
FDP_UIT.1/GP		(A): Added from [PP-GP].
FDP_UCT.1/GP		(A): Added from [PP-GP].
FAU_SAS.1		(A): Added from [PP-IC] to cover O.IC.PROOF_OF_IDENTITY.
FPT_RCV.3/OS		(A): Added in the current ST to cover O.IC.RECOVERY.
FPT_RCV.4/OS		(A): Added in the current ST to cover O.IC.SUPPORT.
FTP_ITC.1/Loader		(A): Added from [ST-IC].
FDP_UCT.1/Loader		(A): Added from [ST-IC].
FDP_UIT.1/Loader		(A): Added from [ST-IC].
FDP_ACC.1/Loader		(A): Added from [ST-IC].
FDP_ACF.1/Loader		(A): Added from [ST-IC].
FMT_MSA.3/Loader		(A): Added from [ST-IC].
FMT_MSA.1/Loader		(A): Added from [ST-IC].

FMT_SMR.1/Loader		(A): Added from [ST-IC].
FIA_UID.1/Loader		(A): Added from [ST-IC].
FIA_UAU.1/Loader		(A): Added from [ST-IC].
FMT_SMF.1/Loader		(A): Added from [ST-IC].
FPT_FLS.1/Loader		(A): Added from [ST-IC].
FAU_SAR.1/Loader		(A): Added from [ST-IC].
FAU_SAS.1/Loader		(A): Added from [ST-IC].

Table 12 Security Functional Requirement consistency table

4.4.4.2 SAR consistency

This ST claims the same evaluation assurance level as [SGP.25] which is an EAL4 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2, completed with ASE_COMP.1, ADV_COMP.1, ATE_COMP.1, ALC_COMP.1, and AVA_COMP.1.

5 Security Problem Definition

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

5.1 Assets

The definition of the assets from [SGP.25] and [PP-JC] is not repeated here. See section 4.4.2.1 for complete list is assets.

5.2 Security Aspects

The definition of the assets from [SGP.25] Section A.2.2 is not repeated here.

5.3 Users and Subjects

The definition of users and subjects from [SGP.25] and [PP-JC] is not repeated here. This includes the subjects defined in [SGP.25] Annex A.2.4 for the OS update functionality. See section 4.4.2.2 for complete list is users and subjects.

5.4 Threats

The definition of threats from [SGP.25] where no refinements are made is not repeated here. This includes the threats defined in [SGP.25] Annex A.2.3 for the OS update functionality. See section 4.4.2.3 for complete list is threats.

Refined threats description is detailed below:

T.UNAUTHORIZED-PROFILE-MNG

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

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

T.UNAUTHORIZED-PLATFORM-MNG

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

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

T.PROFILE-MNG-INTERCEPTION

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

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

T.PROFILE-MNG-ELIGIBILITY

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

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

T.UNAUTHORIZED-IDENTITY-MNG

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, D.PK.EIM.ECDSA (SGP.32), D.APP_CODE, D.APP_I_DATA, D.PIN, D.APP_KEYs, D.APP_C_DATA and D.SEC_DATA.

T.IDENTITY-INTERCEPTION

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

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

T.LOGICAL-ATTACK

The definition of this threat is present in [SGP.25]. The mapping against assets has been refined as detailed below.

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

5.5 Organizational Security Policies

The definition of organizational security policies from [SGP.25] and [PP-JC] is not repeated here. See section 4.4.2.4 for complete list is organizational security policies.

6 Security Objectives

6.1 Security Objectives for the TOE

The list and definitions of the Security Objectives for the TOE from [SGP.25] and [PP-JC] are not repeated here, including the SOs for the TOE defined in [SGP.25] Annex A.3.1 for the OS update functionality. See section 4.4.3 for complete list is Security Objectives for the TOE.

Some objectives from the environment have been converted to objectives of the TOE, specifically the ones from [SGP.25] related to OE.RE* and OE.IC*. The replaced objectives from 4.4.3.2 and their description are listed next:

Security Objectives for the TOE	Description
O.IC.PROOF_OF_IDENTITY	The underlying IC used by the TOE is uniquely identified.
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: 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). It provides secure low-level cryptographic processing to Profile Policy Enabler, Profile Package Interpreter, and Telecom Framework (S.PPE, S.PPI, and S.TELECOM). 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). It provides a means to perform memory operations atomically for S.PPE, S.PPI, and S.TELECOM.
O.IC.RECOVERY	If there is a loss of power while an operation is in progress, the underlying IC must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.
O.RE.PPE-PPI	The Runtime Environment shall provide secure means for card management activities, including: • load of a package file, o installation of a package file, • extradition of a package file or an application, • personalization of an application or a Security Domain, • deletion of a package file or an application, • privileges update of an application or a Security Domain, • 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.

6.2 Security Objectives for the Operational Environment

The list and definitions of the Security Objectives for the Operational Environment from [SGP.25] are not repeated here. See section 4.4.3.2 for complete list is Security Objectives for the Operational Environment.

6.3 Security Objectives Rationale

6.3.1 Threats

6.3.1.1 Unauthorized profile and platform management

T.UNAUTHORIZED-PROFILE-MNG

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

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

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

The authentication is supported by corresponding secure channels:

- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication with SM-DP+ and a secure channel for communication with MNO OTA Platform. These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (OE.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).

T.UNAUTHORIZED-PLATFORM-MNG

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

- O.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domains functions and content.
- OE.SM-DP+ and OE.EIM (SGP.32) protect the corresponding credentials when used off- card.

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

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).

T.PROFILE-MNG-INTERCEPTION

Commands and profiles are transmitted by the SM-DP+ to its on-card representative (ISD-P), while profile data (including meta-data such as PPRs) is also transmitted by the MNO OTA Platform to its on-card representative (MNO-SD) by means of RPM requests from Profile owner to ISD-R (UpdateMetadataRequest), or by means of PSMO commands from eIM to ISD-R (SGP.32).

Consequently, the TSF ensures:

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

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

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

T.PROFILE-MNG-ELIGIBILITY

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

Consequently, the TSF ensures:

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

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

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

6.3.1.2 Identity Tampering

T.UNAUTHORIZED-IDENTITY-MNG

O.PRE-PPI and O.eUICC-DOMAIN-RIGHTS covers this threat by providing an access control policy for ECASD content and functionality. The on- card access control policy relies upon the underlying Runtime Environment, which ensures confidentiality and integrity of application data (O.RE.DATA-CONFIDENTIALITY and O.RE.DATA-INTEGRITY).

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

T.IDENTITY-INTERCEPTION

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

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

6.3.1.3 eUICC cloning

T.UNAUTHORIZED-eUICC

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

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

6.3.1.4 LPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

OE.TRUSTED-PATHS-LPAd-IPAd ensures that the interfaces ES10a, ES10b and ES10c (SGP.22) are trusted paths to the LPAd/IPA.

6.3.1.5 Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS

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

6.3.1.6 Second Level Threats

T.LOGICAL-ATTACK

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

- by the APIs provided by the Runtime Environment (O.RE.API);
- by the APIs of the TSF (O.API); the APIs of Telecom Framework, PRE 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 (OE.RE.DATA- CONFIDENTIALITY, O.RE.DATA-INTEGRITY). However these sensitive data are also processed by the PPE, PPI and the Telecom Framework, which are not protected by these mechanisms. Consequently,

- the TOE itself must ensure the correct operation of PRE, PPI and Telecom Framework (O.OPERATE), and
- PRE, PPI and Telecom Framework must protect the confidentiality and integrity of the sensitive data they process(O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY),
- prevention of unauthorized code execution by applications (O.RE.CODE-EXE).

The following objectives for the operational environment are also required:

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

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.DATA- CONFIDENTIALITY). For the same reason, the Runtime Environment (to which Java Card System can be an implementation) security architecture must cover side channels (O.RE.DATA-CONFIDENTIALITY).

6.3.1.7 OS Update

T.CONFID-UPDATE-IMAGE.LOAD

O.CONFID-UPDATE-IMAGE.LOAD counters the threat by ensuring the confidentiality of D.UPDATE_IMAGE during installing it on the TOE.

OE.CONFID-UPDATE-IMAGE.CREATE counters the threat by ensuring that the D.UPDATE_IMAGE is not transferred in plain and that the keys are kept secret.

T.INTEG-UPDATE-IMAGE.LOAD

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

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.

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.

6.3.2 Organizational Security Policies

The OSP defined is OSP.LIFE-CYCLE as in [SGP.25] section 4.3.2.

6.3.3 Assumptions

The assumptions A.TRUSTED-PATHS-LPAd-IPAd, A.ACTORS and A.APPLICATIONS are defined as in [SGP.25]. In addition, the following assumption is defined in the ST for completeness:

A.CONFID_UPDATE_IMAGE.CREATE

It is assumed that the off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

6.3.4 Rationale Tables

6.3.4.1 Threats Rationale

Threats	Security Objectives	Rationale
T.UNAUTHORIZEDPROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP+, OE.MNO, O.PRE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.INTERNAL-SECURECHANNELS, O.RE.SECURE-COMM, O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.MNO-SD	Section 6.3.1.1
T.UNAUTHORIZEDPLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, OE.SM-DP+, OE.EIM (SGP.32)	Section 6.3.1.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP+, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.MNO-SD, OE.EIM (SGP.32)	Section 6.3.1.1
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 6.3.1.1
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY	Section 6.3.1.2
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM	Section 6.3.1.2
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY	Section 6.3.1.3
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 6.3.1.4
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	Section 6.3.1.5
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, and OE.CODE-EVIDENCE, O.OPERATE, O.RE.API, O.RE.CODE-EXE, O.IC.SUPPORT, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY	Section 6.3.1.6
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATA-CONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY	Section 6.3.1.6
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATE-IMAGE.LOAD, OE.CONFID-UPDATE-IMAGE.CREATE	Section 6.3.1.7

T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE	Section 6.3.1.7
T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE, O.AUTH-LOAD-UPDATE-IMAGE	Section 6.3.1.7
T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE, O.TOE_IDENTIFICATION, O.SECURE_AC_ACTIVATION	Section 6.3.1.7

Table 13 Threats and Security Objectives-Coverage

6.3.4.2 Organizational Security Policies Rationale

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

Table 14 Organizational Security Policies and Security Objectives-Coverage

6.3.4.3 Assumptions Rationale

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd-IPAd	Section 6.3.3
A.ACTORS	OE.CI, OE.SM-DP+, OE.MNO, OE.SM-DS, OE.EIM (SGP.32)	Section 6.3.3
A.APPLICATIONS	OE.APPLICATIONS, OE.CODE-EVIDENCE	Section 6.3.3
A.CONFID_UPDATE_IMAGE.CREATE	OE.CONFID_UPDATE_IMAGE.CREATE	Section 6.3.3

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

7 Extended Component Definition

The following extended component is defined in the current Security Target:

- Extended Family FAU_SAS – Audit Data Storage

The same for FAU_SAS.1 which definition from [PP-IC], section 5.3 have been taken with no modification.

8 Security Functional Requirements

Reading notes:

- Selections having been made by the PP author are denoted as underlined text.
- Selections filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are *italicised*.
- Assignments having been made by the PP author are denoted by showing as **bold text**.
- Assignments filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are *italicised*.
- Refinements, if applicable, have been identified in bold and italicised text.
- Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

8.1 Java Card

8.1.1 COREG_LC SECURITY FUNCTIONAL REQUIREMENTS

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
Firewall Policy	FDP_ACC.2/FIREWALL Complete access control
	FDP_ACF.1/FIREWALL Security attribute based access control
	FDP_IFC.1/JCVM Subset information flow control
	FDP_RIP.1/OBJECTS Subset residual information protection
	FMT_MSA.1/JCRE Management of security attributes
	FMT_MSA.1/JCVM Management of security attribut
	FMT_MSA.2/FIREWALL_JCVM Secure security attributes
	FMT_MSA.3/FIREWALL Static attribute initialisation
	FMT_MSA.3/JCVM Static attribute initialisation
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Application Programming Interface	FDP_RIP.1/ABORT Subset residual information protection
	FDP_RIP.1/APDU Subset residual information protection
	FDP_RIP.1/GlobalArray Subset residual information protection
	FDP_RIP.1/bArray Subset residual information protection
	FDP_RIP.1/KEYS Subset residual information protection
	FDP_RIP.1/TRANSIENT Subset residual information protection
	FDP_ROL.1/FIREWALL Basic rollback
Card Security Management	FPT_FLS.1 Failure with preservation of secure state
AID Management	FIA_ATD.1/AID User attribute definition
	FIA_UID.2/AID User identification before any action

	FMT_MTD.1/JCRE Management of TSF data
	FMT_MTD.3/JCRE Secure TSF data

8.1.1.1 Firewall policy

8.1.1.1.1 FDP_IFF.1/JCVM Simple security attributes

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

Subjects	**Security attributes**
S.JCVM	Currently Active Context

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

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

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

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

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

Application Note:

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

8.1.1.1.2 FPT_RCV.3/OS Automated recovery without undue loss

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

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

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

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

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

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

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

8.1.1.1.3 FPT_RCV.4/OS Function recovery

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

8.1.1.2 Application Programming Interface

8.1.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *see table below*] and specified cryptographic key sizes [assignment: *see table below*] that meet the following: [assignment: *see table below*].

Application Note:

- The keys are generated and diversified in accordance with [JCAPI] specification in classes KeyBuilder and KeyPair (at least Session key generation).

Cryptographic key generation algorithm	Cryptographic key size (in bits)	List of standards
TDES	112, 168	[FIPS 46-3] [FIPS 81] [26]
ECC: - ECDH key generation - ECDSA key generation	224, 256, 384, 512, 521 bits	[34] [49] [55] [57]
AES	128, 192, 256	[FIPS 197] [GP-B]

8.1.1.2.2 FCS_CKM.6 Cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy [assignment: *cryptographic keys (including keying material)*] when [selection: *no longer needed*, [assignment: *none*]].

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

Application Note:

- Since FCS_CKM.4 is deprecated in CC 2022, this SFR is replaced with FCS_CKM.6
- The keys are reset as specified in [JCAPI] Key class, with the method clearKey(). Any access to a cleared key for ciphering or signing throws an exception.

8.1.1.2.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations in table below] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm in table below] and cryptographic key sizes [assignment: cryptographic key sizes in table below] that meet the following: [assignment: list of standards in table below].

Application Note:

- The TOE shall provide a subset of cryptographic operations defined in [JCAPI] (see javacardx.crypto.Cipher and javacardx.security packages).

- This component shall be instantiated according to the version of the Java Card API applicable to the security target and the implemented algorithms ([JCAPI], [JCAPI221], [JCAPI222] and [JCAPI3]).

Cryptographic operation	Cryptographic algorithm	Supported key size	Standards
Digital signature algorithm (ECDSA) generation and verification)	ECDSA	160, 192, 256, 384, 512 and 521bits	[49]
Hash functions	SHA-1 SHA-256 SHA-384 SHA-512	NA	[24], [50][51]
Signature	HMAC	64 - 1016 bits Based on SHA-256, SHA-384 and SHA-512	[52]
Signature, signature's verification, encryption and decryption	AES with Modes CBC, and CMAC	128 to 256 bits with a step of 64 bits	[25] [53](CMAC) [58] (CBC)
Signature, signature's verification, encryption and decryption	DES – TDES with Modes CBC, and CMAC	56, 112 or 168 bits	[FIPS 46-3], [22], [54] [58] (CBC) [53] (CMAC)
Key agreement	ECDH	160, 192, 256, 384, 512 and 521bits	[55]

Application note:

Hash algorithm SHA-1 is not considered secure and therefore, it cannot be used when handling sensitive data.

8.1.1.3 Card Security Management

8.1.1.3.1 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(), [JCAPI] and ([JCRE], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow,
- [assignment: integrity error caused by a perturbation attack].

8.1.1.3.2 FDP_SDI.2/DATA Stored data integrity monitoring and action

FDP_SDI.2.1/DATA	The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *integrity protected data*].
FDP_SDI.2.2/DATA	Upon detection of a data integrity error, the TSF shall [assignment: *write a security error information persistently and mute the card*].

Application Note:

The following data elements have the user data attribute "integrity protected data":

- cryptographic keys
- PIN, PUK values
- Profile Data
- Control system variables (such as state machine information, cryptographic algorithm input data)

8.1.1.3.3 FPR_UNO.1 Unobservability

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

8.1.1.3.4 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 [JCVM] specification,** • **the API tokens defined in the export files of reference implementation,** • [assignment: *none*] 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.

8.1.1.4 AID Management

8.1.1.4.1 FIA_USB.1/AID User-subject binding

FIA_USB.1.1/AID	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **Package AID**.
FIA_USB.1.2/AID	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *for each loaded package is associated an unique Package AID*].
FIA_USB.1.3/AID	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *the initially assigned Package AID is unchangeable*].

Application Note:

The user is the applet and the subject is the S.PACKAGE. The subject security attribute "Context" shall hold the user security attribute "package AID".

8.1.2 InstG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
InstG SFRs	FDP_ITC.2/Installer Import of user data with security attributes
	FMT_SMR.1/Installer Security roles
	FPT_FLS.1/Installer Failure with preservation of secure state

8.1.2.1 FPT_RCV.3/Installer Automated recovery without undue loss

FPT_RCV.3.1/Installer	When automated recovery from [assignment: *none*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.3.2/Installer	For [assignment: interrupted deletion, interrupted load or interrupted install (except if the register method has already been invoked)], the TSF shall ensure the return of the TOE to a secure state using automated procedures.
FPT_RCV.3.3/Installer	The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: *0%*] for loss of TSF data or objects under the control of the TSF.
FPT_RCV.3.4/Installer	The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

Application Note:

FPT_RCV.3.1/Installer:

- This element is not within the scope of the Java Card specification, which only mandates the behavior of the Java Card System in good working order. Further details on the "maintenance mode" shall be provided in specific implementations. The following is an excerpt from [CC-2], p298: In this maintenance mode normal operation might be impossible or severely restricted, as otherwise insecure situations might occur. Typically, only authorised users should be allowed access to this mode but the real details of who can access this mode is a function of FMT: Security management. If FMT: Security management does not put any controls on who can access this mode, then it may be acceptable to allow any user to restore the system if the TOE enters such a state. However, in practice, this is probably not desirable as the user restoring the system has an opportunity to configure the TOE in such a way as to violate the SFRs.

FPT_RCV.3.2/Installer:

- Should the installer fail during loading/installation of a package/applet, it has to revert to a "consistent and secure state". The Java Card RE has some clean up duties as well; see [JCRE], §11.1.5 for possible scenarios. Precise behavior is left to implementers. This component shall include among the listed failures the deletion of a package/applet. See ([JCRE], 11.3.4) for possible scenarios. Precise behavior is left to implementers.
- Other events such as the unexpected tearing of the card, power loss, and so on, are partially handled by the underlying hardware platform (see [PP-IC]) and, from the TOE's side, by events "that clear transient objects" and transactional features. See FPT_FLS.1.1, FDP_RIP.1/TRANSIENT, FDP_RIP.1/ABORT and FDP_ROL.1/FIREWALL.

FPT_RCV.3.3/Installer:

- The quantification is implementation dependent, but some facts can be recalled here. First, the SCP ensures the atomicity of updates for fields and objects, and a power-failure during a transaction or the normal runtime does not create the loss of otherwise permanent data, in the sense that memory on a smart card is essentially persistent with this respect (EEPROM). Data stored on the RAM and subject to such failure is intended to have a limited lifetime anyway (runtime data on the stack, transient objects' contents).
  According to this, the loss of data within the TSF scope should be limited to the same restrictions of the transaction mechanism.

8.1.3 ADELG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
ADELG SFRs	FDP_ACC.2/ADEL Complete access control
	FDP_ACF.1/ADEL Security attribute based access control
	FDP_RIP.1/ADEL Subset residual information protection
	FMT_MSA.1/ADEL Management of security attributes
	FMT_MSA.3/ADEL Static attribute initialisation
	FMT_SMF.1/ADEL Specification of Management Functions
	FMT_SMR.1/ADEL Security roles
	FPT_FLS.1/ADEL Failure with preservation of secure state

8.1.4 ODELG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. This section does not contain any SFRs with operations still to be performed.

Section	SFR
ODELG SFRs	FDP_RIP.1/ODEL Subset residual information protection
	FPT_FLS.1/ODEL Failure with preservation of secure state

8.1.5 CarG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
CarG SFRs	FDP_IFC.2/CM Complete information flow control
	FTP_ITC.1/CM Inter-TSF trusted channel

8.1.5.1 FCO_NRO.2/CM Enforced proof of origin

FCO_NRO.2.1/CM	The TSF shall enforce the generation of evidence of origin for transmitted **application packages** at all times.
FCO_NRO.2.2/CM [Editorially Refined]	The TSF shall be able to relate the **identity** of the originator of the information, and the **application package contained in** the information to which the evidence applies.
FCO_NRO.2.3/CM	The TSF shall provide a capability to verify the evidence of origin of information to **recipient** given [assignment: *at the time the Executable load files are received as no evidence is kept on the card for future verification*].

Application Note:

FCO_NRO.2.1/CM:

- Upon reception of a new application package for installation, the card manager shall first check that it actually comes from the verification authority. The verification authority is the entity responsible for bytecode verification.

FCO_NRO.2.3/CM:

- The exact limitations on the evidence of origin are implementation dependent. In most of the implementations, the card manager performs an immediate verification of the origin of the package using an electronic signature mechanism, and no evidence is kept on the card for future verifications.

8.1.5.2 FDP_IFF.1/CM Simple security attributes

FDP_IFF.1.1/CM	The TSF shall enforce the **PACKAGE LOADING information flow control SFP** based on the following types of subject and information security attributes: [assignment: *Load file, DAP authenticated, OTA authenticated*].
FDP_IFF.1.2/CM	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *the rules describing the communication protocol used by the CAD and the card for transmitting a new package as detailed in [GP] Section 9.3.9*].
FDP_IFF.1.3/CM	The TSF shall enforce the [assignment: *none*].
FDP_IFF.1.4/CM	The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
FDP_IFF.1.5/CM	The TSF shall explicitly deny an information flow based on the following rules: • **The TOE fails to verify the integrity and authenticity evidences of the application package** • [assignment: *the rules describing the communication protocol used by the CAD and the card for transmitting a new package as detailed in [GP] Section 9.3.9*].

Application Note:

FDP_IFF.1.1/CM:

- The security attributes used to enforce the PACKAGE LOADING SFP are implementation dependent. More precisely, they depend on the communication protocol enforced between the CAD and the card. For instance, some of the attributes that can be used are: (1) the keys used by the subjects to encrypt/decrypt their messages; (2) the number of pieces the application package has been split into in order to be sent to the card; (3) the ordinal of each piece in the decomposition of the package, etc. See for example [GP-D].

FDP_IFF.1.2/CM:

- The precise set of rules to be enforced by the function is implementation dependent. The whole exchange of messages shall verify at least the following two rules: (1) the subject S.INSTALLER shall accept a message only if it comes from the subject S.CAD; (2) the subject S.INSTALLER shall accept an application package only if it has received without modification and in the right order all the APDUs sent by the subject S.CAD.

FDP_IFF.1.5/CM:

- The verification of the integrity and authenticity evidences can be performed either during loading or during the first installation of an application of the package.

8.1.5.3 FDP_UIT.1/CM Data exchange integrity

FDP_UIT.1.1/CM	The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to [selection: *receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.
FDP_UIT.1.2/CM [Editorially Refined]	The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion, replay of some of the pieces of the application sent by the CAD** has occurred.

Application Note:

Modification errors should be understood as modification, substitution, unrecoverable ordering change of data and any other integrity error that may cause the application package to be installed on the card to be different from the one sent by the CAD.

8.1.5.4 FIA_UID.1/CM Timing of identification

FIA_UID.1.1/CM	The TSF shall allow [assignment: • *application selection* • *initializing a secure channel with the card* • *requesting data that identifies the card or the Card Issuer*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/CM	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

The list of TSF-mediated actions is implementation-dependent, but package installation requires the user to be identified. Here by user is meant the one(s) that in the Security Target shall be associated to the role(s) defined in the component FMT_SMR.1/CM.

8.1.5.5 FMT_MSA.1/CM Management of security attributes

FMT_MSA.1.1/CM	The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to restrict the ability to [selection: *modify* [assignment: *no other operations*]] the security attributes

[assignment: *key data, card life cycle state, secure configuration, default SELECTED configuration*] to [assignment: *card manager*].

8.1.5.6 FMT_MSA.3/CM Static attribute initialisation

FMT_MSA.3.1/CM	The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/CM	The TSF shall allow the [assignment: *card manager*] to specify alternative initial values to override the default values when an object or information is created.

8.1.5.7 FMT_SMF.1/CM Specification of Management Functions

FMT_SMF.1.1/CM	The TSF shall be capable of performing the following management functions: [assignment: *modify key data, card life cycle state, secure configuration, default SELECTED configuration*].

8.1.5.8 FMT_SMR.1/CM Security roles

FMT_SMR.1.1/CM	The TSF shall maintain the roles [assignment: *card manager*].
FMT_SMR.1.2/CM	The TSF shall be able to associate users with roles.

8.2 **eUICC**

The following table shows all the SFRs from [SGP.25] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the [SGP.25] are addressed in the following sections.

Section	**SFR**
Identification and authentication	FIA_USB.1/MNO-SD User-subject binding
	FIA_API.1 Authentication Proof of Identity
Communication	FDP_IFC.1/SCP Subset information flow control
	FDP_UCT.1/SCP Basic data exchange confidentiality
	FDP_UIT.1/SCP Data exchange integrity
Security Domain	FDP_ACC.1/ISDR Subset access control
Security Management	FDP_SDI.1/Base Stored data integrity monitoring
	FDP_RIP.1/Base Subset residual information protection
	FPT_FLS.1/Base Failure with preservation of secure state
	FMT_MSA.1/PLATFORM_DATA Management of security attributes
	FMT_MSA.3 Static attribute initialisation
	FMT_SMR.1/Base Security roles
	FMT_MSA.1/RAT Management of security attributes

8.2.1 Identification and authentication

8.2.1.1 FIA_USB.1/EXT User-subject binding

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

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

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

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

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

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

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);
- U.EIM binds to a subject (S.ISD-R).

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.

This SFR is related to the following commands:

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

8.2.1.2 FIA_UAU.4/EXT Single-use authentication mechanisms

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

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

Application Note:

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

- U.SM-DP+;
- U.MNO-OTA;
- U.EIM (SGP.32).

8.2.1.3 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: *no additional TSF mediated actions*]**.**

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

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

Application Note:

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

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

- U.EIM (SGP.32).

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.

8.2.1.4 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: *no additional TSF mediated actions*]**.**

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

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

Application Note:

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

- U.SM-DP+;
- U.MNO-OTA;
- U.EIM (SGP.32).

8.2.1.5 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.

8.2.1.6 FIA_ATD.1/Base User attribute definition

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

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

8.2.2 Communication

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

FDP_IFF.1.4/SCP The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *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

8.2.2.2 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: • *to all the interfaces below, including SGP.22 ES10c (ES10c.EnableProfile, ES10c.DisableProfile, ES10c.DeleteProfile, ES10c.SetNickname, ES10c.eUICCMemoryReset, ES10c.GetProfilesInfo and ES10c.GetEID), but excluding all other SGP.22 interfaces].*

Application Note:

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/IPAd to transmit the following operations:
- ES10a.GetEuiccConfiguredData (SGP.22 v3.1 or higher)
    - ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.x)
    - ES10a.SetDefaultDpAddress (SGP.22)
    - ES10b.SetDefaultDpAddress (SGP.32)
    - ES10b.PrepareDownload
    - ES10b.LoadBoundProfilePackage
    - ES10b.GetEUICCChallenge
    - ES10b.GetEUICCInfo
    - ES10b.ListNotification
    - ES10b.RetrieveNotificationsList
    - ES10b.RemoveNotificationFromList
    - ES10b.AuthenticateServer
    - ES10b.CancelSession
    - ES10b.LoadEuiccPackage (SGP.32)
    - ES10b.AddInitialEim (SGP.32)
    - ES10b.GetCerts (SGP.32)
    - ES10b.ImmediateEnable (SGP.32)
    - ES10b.ProfileRollback (SGP.32)
    - ES10b.ConfigureImmediateProfileEnabling (SGP.32)
    - ES10b.GetEimConfigurationData (SGP.32)
    - ES10b.GetProfilesInfo (SGP.32)
    - ES10c.GetProfilesInfo (SGP.22)
    - ES10c.EnableProfile (SGP.22)
    - ES10c.DisableProfile (SGP.22)
    - ES10c.DeleteProfile (SGP.22)
    - ES10c.eUICCMemoryReset (SGP.22)
    - ES10b.GetEID (SGP.32)
    - ES10c.GetEID (SGP.22)
    - ES10c.SetNickname (SGP.22)
    - ES10b.GetRAT
- The TSF may permit the LPAd/IPAd to transmit the following operations:
    - ES10b.LoadCRL (SGP.22 V2.x)
    - ES10c.LPA alerting (SGP.22 v3.1 or higher)
    - ES10c.VerifySmdsResponse (SGP.22 v3.1 or higher)
    - ES10b.LoadRPMPackage (SGP.22 v3.1 or higher)
    - ES10b.PrepareDeviceChange (SGP.22 v3.1 or higher)
    - ES10b.VerifyDeviceChange (SGP.22 v3.1 or higher)
    - ES10b.eUICCMemoryReset (SGP.32)
    - ES10b.ExecuteFallbackMechanism (SGP.32)
    - ES10b.ReturnFromFallback (SGP.32)
    - ES10b.EnableEmergencyProfile (SGP.32)
    - ES10b.DisableEmergencyProfile (SGP.32)
    - ES10b.GetConnectivityParameters (SGP.32)

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

8.2.2.3 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*].

8.2.2.4 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: rules defined in [SGP.32]]* 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/IPAd commands
    - ES10a.GetEuiccConfiguredData (SGP.22 v3.1 or higher)
    - ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.x)
    - ES10a.SetDefaultDpAddress (SGP.22)
    - ES10b.SetDefaultDpAddress (SGP.32)
    - ES10b.PrepareDownload
    - ES10b.LoadBoundProfilePackage
    - ES10b.GetEUICCChallenge
    - ES10b.GetEUICCInfo
    - ES10b.ListNotification
    - ES10b.RetrieveNotificationsList
    - ES10b.RemoveNotificationFromList
    - ES10b.LoadCRL (SGP.22 V2.x)
    - ES10b.AuthenticateServer
    - ES10b.CancelSession
    - ES10b.LoadEuiccPackage (SGP.32)
    - ES10b.AddInitialEim (SGP.32)
    - ES10b.GetCerts (SGP.32)
    - ES10b.ImmediateEnable (SGP.32)
    - ES10b.ProfileRollback (SGP.32)
    - ES10b.ConfigureAutomaticProfileEnabling (SGP.32)
    - ES10b.GetEimConfigurationData (SGP.32)
    - ES10b.GetProfilesInfo (SGP.32)
    - ES10c.GetProfilesInfo (SGP.22)
    - ES10c.EnableProfile
    - ES10c.DisableProfile
    - ES10c.DeleteProfile
    - ES10b.eUICCMemoryReset (SGP.32)
    - ES10c.eUICCMemoryReset (SGP.22)
    - ES10b.GetEID (SGP.32)
    - ES10c.GetEID (SGP.22)
    - ES10c.SetNickname (SGP.22)
    - ES10b.GetRAT
    - ES10c.LPA alerting (SGP.22 v3.1 or higher)
    - ES10c.VerifySmdsResponse (SGP.22 v3.1 or higher)
    - ES10b.LoadRPMPackage (SGP.22 v3.1 or higher)
    - ES10b.PrepareDeviceChange (SGP.22 v3.1 or higher)
    - ES10b.VerifyDeviceChange (SGP.22 v3.1 or higher)
    - ES10b.ExecuteFallbackMechanism (SGP.32)
    - ES10b.ReturnFromFallback (SGP.32)
    - ES10b.EnableEmergencyProfile (SGP.32)

    - ES10b.DisableEmergencyProfile (SGP.32)
    - ES10b.GetConnectivityParameters (SGP.32)
- 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 and Enterprise Rules (optional).

8.2.2.5 FCS_CKM.1/SCP-SM Cryptographic key generation

FCS_CKM.1.1/SCP-SM	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curves Key agreement (ECKA)** and specified cryptographic key sizes 256 that meet the following: [assignment: *at least one elliptic curve referenced in [SGP.32]*].

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.

8.2.2.6 FCS_CKM.2/SCP-MNO Cryptographic key distribution

FCS_CKM.2.1/SCP-MNO	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method in table below*] that meets the following: [assignment: *list of standards in table below*].

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).

Algorithm	Distribution Method	List of standards
AES	SCP80 SCP81 STORE DATA functionality of security domain	[TS 102 225] [TS 102 226] [GP-B] [SGP.32] [GP][GP][GP]
ECDH/ECDSA	ES8+.InitialiseSecureChannel	[SGP.32]
TDES	STORE DATA functionality of security domain	[GP]
TUAK	[SGP.32]	[SGP.32] [TUAK][GP][GP][GP][GP]
MILENAGE	GSMA, [SGP.32]	[SGP.32] [MILENAGE]

8.2.2.7 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*, [assignment: *none*]].

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: *non-key material*] that meets the following: [assignment: *none*].

8.2.2.8 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*, [assignment: *none*]].

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: *non-key material*] that meets the following: [assignment: *none*].

8.2.3 Security Domains

8.2.3.1 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" "PPR", and [Selection: *no additional attributes*]**
- **operations:**
  - **Create and configure profile**
  - **Store profile metadata**
  - **Enable profile**
  - **Disable profile**
  - **Delete profile**
  - **Perform a Memory reset.**

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

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

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

- 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)
- ES10b.LoadRpmPackage (Enable/Disable/Delete profile) (SGP.22 v3.1 or higher)*].*

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 all operations by ISD-R required by sections 5.x of [SGP.22], that is:

- 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)
- ES10b.LoadRpmPackage (Enable/Disable/Delete profile) (SGP.22 v3.1 or higher)

8.2.3.2 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].**

8.2.3.3 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 an eUICC signature on material provided by an ISD-R**
- **access to output data of these functions.**
- **[assignment: none].**

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

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

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

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

8.2.4 Platform Services

8.2.4.1 FDP_IFC.1/Platform_services Subset information flow control

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

- **users/subjects:**
    - **S.ISD-R, S.ISD-P, U.MNO-SD**
    - **Platform code (S.PRE, S.PPI, S.TELECOM)**
- **information:**
    - **D.PROFILE_NAA_PARAMS**
    - **D.PROFILE_RULES**
    - **D.PLATFORM_RAT**
- **operations**:
    - **installation of a profile**
    - **PPR and RAT enforcement**

- **network authentication**.
- ***[selection: no additional operations]***

8.2.4.2 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 _RULES**
- **D.PLATFORM_RAT**

operations:

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

FDP_IFF.1.2/Platform_services

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

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

FDP_IFF.1.3/Platform_services

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

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *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, Enterprise Rules, Rules Authorisation Table or 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.

8.2.4.3 FPT_FLS.1/Platform_Services Failure with preservation of secure state

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

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

8.2.5 Security management

8.2.5.1 FCS_RNG.1 Random number generation

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

- *(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*
- *(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw*

random numbers that have been generated after the total failure of the entropy source.

- *(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*
- *(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*
- *(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered externally. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*

].

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

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

].

8.2.5.2 FPT_EMS.1/Base TOE Emanation

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

ID	Emission	Attack surface	TSF data	User data
1	[assignment: *information about chip power consumption, electromagnetic emanation or command execution time*]	**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**.

Application Note:

The TOE prevents 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.

8.2.5.3 FCS_COP.1/DRBG Cryptographic Operation

FCS_COP.1.1/DRBG The TSF shall perform the [assignment: *CTR_DRBG (AES)*] in accordance with a specified cryptographic algorithm [assignment: *CTR_DRBG*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *[NISTSP800-90A]*].

8.2.5.4 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: *profile management functions described in [SGP.32]*].

8.2.5.5 FMT_MSA.1/RULES Management of security attributes

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

- **D.PROFILE_RULES**

to

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

]

8.2.5.6 FMT_MSA.1/CERT_KEYS Management of security attributes

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

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

to

- **S.ISD-R for:**
  - **query D.PK.CI.ECDSA**
  - **delete D.MNO_KEYS, via function *[selection: ES10c.DeleteProfile (SGP.22), ESep.Delete (SGP.32)]***
- **no actor for other operations.**

8.2.6 Mobile Network authentication

8.2.6.1 FCS_COP.1/Mobile_network Cryptographic operation

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

- **MILENAGE according to standard [[38]] 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 [[38]]**
- **Tuak according to [[39]] with the following restrictions:**
  - **Allow any value of TOP**
  - **Allow multiple iterations of Keccak**
  - **Support 256-bit K as well as 128-bit**
  - **Restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.**
  - ***[selection: no additional standards]***

Application Note:

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).

8.2.6.2 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: *during to profile download*] that meets the following: [assignment: *list of standards in table below*].

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

Algorithm	Distribution Method	List of standards
AES	SCP80 SCP81 STORE DATA functionality of security domain	[TS 102 225] [TS 102 226] [GP-B] [SGP.32] [GP]
ECDH/ECDSA	ES5.EstablishISDRKeySet ES8.EstablishISDPKeySet	[SGP.32]
TDES	STORE DATA functionality of security domain	[GP]
TUAK	[SGP.32]	[SGP.32] [TUAK]
MILENAGE	GSMA, [SGP.32]	[SGP.32] [MILENAGE]

8.2.6.3 FCS_CKM.6/Mobile_network Cryptographic key destruction

FCS_CKM.6.1/Mobile_network The TSF shall destroy **MILENAGE keys, TUAK keys and and *[selection: no other keys of the cryptographic algorithm]]*** when ***[selection: no longer needed, [assignment: none]]***

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: *non-key material*] 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.

8.2.7 OS Update functionality

The OS functionality is provided by the certified IC [CERT-IC]. Therefore, the following SFRs from the IC Security Target [ST-IC][ST-IC] are in scope of this evaluation.

- FTP_ITC.1/Loader Inter-TSF trusted channel
- FDP_UCT.1/Loader Basic data exchange confidentiality
- FDP_UIT.1/Loader Data exchange integrity
- FDP_ACC.1/Loader Subset access control
- FDP_ACF.1/Loader Security attribute based access control
- FMT_MSA.3/Loader Static attribute initialisation
- FMT_MSA.1/Loader Management of security attributes
- FMT_SMR.1/ Loader Security roles
- FIA_UID.1/Loader Timing of identification
- FIA_UAU.1/Loader Timing of authentication

- FMT_SMF.1/Loader Specification of management functions
- FPT_FLS.1/Loader Failure with preservation of secure state
- FAU_SAR.1/Loader Audit review
- FAU_SAS.1/ Loader Audit storage

The definition of these SFRs from the [ST-IC][ST-IC] [ST-IC]are not repeated here.

8.3 Global Platform

The following table shows all the SFRs from Global Platform – Secure Element Protection Profile [PP-GP] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by Global Platform – Secure Element Protection Profile [PP-GP] are addressed in the following sections.

Section	SFR
Identification and authentication	FIA_UAU.1/GP Timing of authentication
	FIA_UAU.4/GP Single-use authentication mechanisms

8.3.1 Identification and authentication

8.3.1.1 FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *1*]] unsuccessful authentication attempts occur related to the authentication of the origin of a card management operation command.

FIA_AFL.1.2/GP When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall close the Secure Channel.

8.3.2 User data protection

8.3.2.1 FDP_UIT.1/GP Basic data exchange integrity

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

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

Application Note:

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

8.3.2.2 FDP_UCT.1/GP Basic data exchange confidentiality

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

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.

8.4 Security Functional Requirements Rationale

8.4.1 SFRs for eUICC rationale

The security functional requirements rationale is the same than the ones present in section 6.3 from [SGP.25].

8.4.2 SFRs for Runtime Environment rationale

The next table shows the objectives related to [SGP.25] runtime environment and its translation according to [SGP.25] 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-JC] and are not repeated here. In case of O.CARD-MANAGEMENT, the Security Functional Requirements rationale should be extracted from [PP-GP].

RE objectives	**Translation from JavaCard PP**
O.RE.PRE-PPI	O.INSTALL, O.DELETION, O.LOAD, O.CARD-MANAGEMENT
O.RE.SECURE-COMM	O.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, 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.RESOURCES, O.OBJ-DELETION, OE.SCP.IC
O.RE.API	O.CARD-MANAGEMENT, O.NATIVE, OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.SID, O.OPERATE, O.FIREWALL, O.ALARM, O.RESOURCES, O.OBJ-DELETION, OE.SCP.IC
O.RE.DATA-CONFIDENTIALITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_CONFID, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.RESOURCES, O.OBJ-DELETION, OE.SCP.IC
O.RE.DATA-INTEGRITY	OE.SCP.RECOVERY, OE.SCP.SUPPORT, O.CARD-MANAGEMENT, O.SID, O.OPERATE, O.FIREWALL, O.GLOBAL_ARRAYS_INTEG, O.ALARM, O.TRANSACTION, O.CIPHER, O.RNG, O.PIN-MNGT, O.KEY-MNGT, O.REALLOCATION, O.LOAD, O.NATIVE, O.RESOURCES, O.OBJ-DELETION, OE.SCP.IC
O.RE.IDENTITY	OE.SCP.RECOVERY and OE.SCP.SUPPORT, O.FIREWALL, O.SID, O.INSTALL, O.OPERATE, O.GLOBAL_ARRAYS_CONFID, O.GLOBAL_ARRAYS_INTEG, O.CARD-MANAGEMENT, O.RESOURCES, O.OBJ-DELETION, OE.SCP.IC
O.RE.CODE-EXE	O.FIREWALL, O.NATIVE

Table 16 Runtime environment objectives conversion for SFR rationale

Note that OE.SCP.RECOVERY and OE.SCP.SUPPORT from [PP-JCS] are equivalent to O.IC.RECOVERY and O.IC.SUPPORT from [SGP.25] converted to O.IC.RECOVERY and O.IC.SUPPORT in current Security Target. See next section for the rationale.

8.4.3 SFRs for Underlying platform IC rationale

The security functional requirements for the OS functionality are provided by the certified IC [CERT-IC]. Therefore, the rationale is the same for the ones presented in section 5.4.1 of [ST-IC].

Objectives from [SGP.25] Appendix A	**Translation from [ST-IC]**
O.SECURE_LOAD_ACODE	JIL.O.Secure-Load-ACode
O.SECURE_AC_ACTIVATION	JIL.O.Secure-AC-Activation
O.TOE_IDENTIFICATION	JIL.O.TOE-Identification
O.CONFID-UPDATE-IMAGE.LOAD	O.Secure-Load-AMemImage
O.AUTH-LOAD-UPDATE-IMAGE	O.MemImage-Identification

Table 17 OS functionality objectives conversion for SFR rationale

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

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

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

8.5 SFR Dependencies

Requirement	**Dependency**	**Satisfied by**
FDP_ACC.2/FIREWALL	(FDP_ACF.1)	FDP_ACF.1/FIREWALL
FDP_ACF.1/FIREWALL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/FIREWALL, FMT_MSA.3/FIREWALL
FDP_IFC.1/JCVM	(FDP_IFF.1)	FDP_IFF.1/JCVM
FDP_IFF.1/JCVM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/JCVM, FMT_MSA.3/JCVM
FDP_RIP.1/OBJECTS	No Dependencies	
FMT_MSA.1/JCRE	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FMT_SMR.1
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM, FMT_SMR.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2/AID

FCS_CKM.1	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and FCS_CKM.3 and (FCS_RBG.1 or FCS_RNG.1) and FCS_CKM.6	FCS_COP.1, FCS_RNG.1, FCS_CKM.6
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.6)	FCS_CKM.1, FCS_CKM.6
FCS_RNG.1	No Dependencies	
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)	
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPT_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)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ITC.2/Installer	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FTP_ITC.1/CM, FPT_TDC.1
FMT_SMR.1/Installer	(FIA_UID.1)	
FPT_FLS.1/Installer	No Dependencies	
FPT_RCV.3/Installer	(AGD_OPE.1)	AGD_OPE.1
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL, FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No Dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL, FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No Dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	
FPT_FLS.1/ADEL	No Dependencies	
FDP_RIP.1/ODEL	No Dependencies	
FPT_FLS.1/ODEL	No Dependencies	
FCO_NRO.2/CM	(FIA_UID.1)	FIA_UID.1/CM
FDP_IFC.2/CM	(FDP_IFF.1)	FDP_IFF.1/CM
FDP_IFF.1/CM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/CM, FMT_MSA.3/CM

FDP_UIT.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FTP_ITC.1/CM
FIA_UID.1/CM	No Dependencies	
FMT_MSA.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/CM, FMT_SMF.1/CM, FMT_SMR.1/CM
FMT_MSA.3/CM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/CM, FMT_SMR.1/CM
FMT_SMF.1/CM	No Dependencies	
FMT_SMR.1/CM	(FIA_UID.1)	FIA_UID.1/CM
FTP_ITC.1/CM	No Dependencies	
FTP_ITC.1/Loader	No Dependencies	
FDP_UCT.1/Loader	(FTP_ITC.1/Loader or FTP_TRP.1/Loader) and (FDP_ACC.1/Loader or FDP_IFC.1/Loader)	FTP_ITC.1/Loader, FDP_ACC.1/Loader
FDP_UIT.1/Loader	(FTP_ITC.1/Loader or FTP_TRP.1/Loader) and (FDP_ACC.1/Loader or FDP_IFC.1/Loader)	FTP_ITC.1/Loader, FDP_ACC.1/Loader
FDP_ACC.1/Loader	(FDP_ACF.1/Loader)	FDP_ACF.1/Loader
FDP_ACF.1/Loader	(FDP_ACC.1/Loader) and (FMT_MSA.3/Loader)	FDP_ACC.1/Loader, FMT_MSA.3/Loader
FMT_MSA.3/Loader	(FMT_MSA.1/Loader) and (FMT_SMR.1/Loader)	FMT_MSA.1/Loader and FMT_SMR.1/Loader
FMT_MSA.1/Loader	(FDP_ACC.1/Loader or FDP_IFC.1) and (FDP_SMF.1/Loader) and (FDP_SMR.1/Loader)	FDP_ACC.1/Loader, FDP_SMF.1/Loader, FDP_SMR.1/Loader
FMT_SMR.1/Loader	(FIA_UID.1/Loader)	FIA_UID.1/Loader
FIA_UID.1/Loader	No Dependencies	
FIA_UAU.1/Loader	(FIA_UID.1/Loader)	FIA_UID.1/Loader
FMT_SMF.1/Loader	No Dependencies	
FPT_FLS.1/Loader	No Dependencies	
FAU_SAR.1/Loader	(FAU_GEN.1)	No, by FAU_SAS.1/Loader instead, see discussion below
FAU_SAS.1/Loader	No Dependencies	
FIA_UID.1/EXT	No Dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_UAU.4/EXT	No Dependencies	
FIA_UID.1/MNO-SD	No Dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1/Base
FIA_ATD.1/Base	No Dependencies	
FIA_API.1	No Dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP and FMT_MSA.3
FTP_ITC.1/SCP	No Dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1) and (FPT_TDC.1)	FDP_IFC.1/SCP and FTP_ITC.1/SCP and FPT_TDC.1/SCP
FPT_TDC.1/SCP	No Dependencies	

FDP_UCT.1/SCP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/SCP and FDP_IFC.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 and FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1, FCS_RNG.1 and FCS_CKM.6/SCP-SM
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) or FCS_CKM.5)	FDP_ITC.2/SCP
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR and 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 and 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 and FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	
FPT_EMS.1/Base	No Dependencies	
FDP_SDI.1/Base	No Dependencies	
FDP_RIP.1/Base	No Dependencies	
FPT_FLS.1/Base	No Dependencies	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMR.1) and (FMT_SMF.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.1/RULES	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMR.1) and (FMT_SMF.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMR.1) and (FMT_SMF.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_SMF.1/Base	No Dependencies	
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMR.1) and (FMT_SMF.1)	FDP_ACC.1/ISDR, FMT_SMF.1/Base, FMT_SMR.1/Base
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, MT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS, FMT_SMR.1/Base, FMT_MSA.1/RAT
FCS_COP.1/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and FCS_CKM.6	FDP_ITC.2/SCP and FCS_CKM.6/Mobile_network
FCS_CKM.2/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_CKM.6/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) or FCS_CKM.5)	FDP_ITC.2/SCP
FCS_COP.1/DRBG	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5) and FCS_CKM.6	FDP_ITC.2/SCP and FCS_CKM.6/Mobile_network
FIA_AFL.1/GP	(FIA_UAU.1)	FIA_UAU.1/GP
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/CM
FIA_UAU.4/GP	No Dependencies	
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM and FTP_ITC.1/CM

FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FTP_ITC.1/CM, FDP_IFC.2/CM
FAU_SAS.1	No Dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	Operational User Guidance
FPT_RCV.4/OS	No Dependencies	

Table 18 SFR dependencies

Rationale for the exclusion of dependencies:

- The dependency FIA_UID.1 of FMT_SMR.1/Installer is discarded. The Java Card PP [PP-JC] does not require the identification of the "installer" since it can be considered as part of the TSF.
- The dependency FIA_UID.1 of FMT_SMR.1/ADEL is discarded. The Java Card PP [PP-JC] does not require the identification of the "deletion manager" since it can be considered as part of the TSF.
- The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is discarded. The dependency between FMT_MSA.1/JCRE and FMT_SMF.1 is not satisfied because no management functions are required for the Java Card RE.
- The dependency FAU_SAA.1 of FAU_ARP.1 is discarded. 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 the Java Card PP [PP-JC].
- Part 2 of the Common Criteria defines the dependency of "Audit review (FAU_SAR.1)/Loader" on "Audit data generation (FAU_GEN.1)". In this particular TOE, "Audit storage (FAU_SAS.1) / Loader" is used to ensure the storage of audit data, because FAU_GEN.1 is too comprehensive to be used in this context. Therefore, this dependency is fulfilled by "Audit storage (FAU_SAS.1) / Loader" instead.

9 Security Assurance Requirements

9.1 SARs

This Security Target claims conformance to EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2, completed with ASE_COMP.1, ADV_COMP.1, ATE_COMP.1, ALC_COMP.1, and AVA_COMP.1. ADV_ARC is refined. The requirements are summarised in the following table:

Assurance Class	Component	Component Title
ADV Development	ADV_ARC.1	Security architecture NOTE: This component has been refined as follows: *ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.* *Refinement:* *In order to enforce the domain separation, the rules included in A.APPLICATIONS must be sufficient to maintain the security for all applications loaded on the eUICC containing the TOE..*
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
	ADV_COMP.1	Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC_ Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
	ALC_FLR.2	Flaw reporting procedure
	ALC_COMP.1	Integration of composition parts and consistency check of delivery procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_TSS.1	TOE summary specification
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_COMP.1	Consistency of Security Target
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional tests

Assurance Class	Component	Component Title
	ATE_IND.2	Independent testing
	ATE_COMP.1	Composite product functional testing
AVA: Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis
	AVA_COMP.1	Composite product vulnerability assessment

Table 19 EAL4 requirements description extended with augmented with AVA_VAN.5, ALC_FLR.2 and ALC_DVS.2

9.2 SARs Dependency Rationale

This rationale shows that all dependencies of all security requirements have been addressed:

Requirement	Dependency	Satisfied by
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_FLR.2	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1

AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 20 SAR dependencies rationale

9.3 Rationale for the Security Assurance Requirements

EAL4 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks: the evaluators should have access to the low-level design and source code. The lowest for which such access is required is EAL4.

9.3.1 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the nature of the TOE and embedding product, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

9.3.2 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for Java Card technology-based products hosting sensitive applications. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1 and AGD_OPE.1. All of them are satisfied by EAL4.

9.3.3 ALC_FLR.2 Flaw Reporting Procedures

Due to the nature of the TOE, it is necessary to provide flaw reporting procedures to track all reported security flaws in each release of the TOE.

ALC_FLR.2 requires that the developer is able to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes, TOE users need to understand how to submit security flaw reports to the developer. Flaw remediation guidance from the developer to the TOE user is necessary to ensure that TOE users are aware of this important information.. Flaw remediation guidance from the developer to the TOE user ensures that TOE users are aware of this important information. ALC_FLR.2 has no dependencies.

10 TOE Summary Specification

10.1 Security Functionality

10.1.1 Runtime environment SFR coverage

Security Functionality	Description
SF.FIREWALL	The TOE implements an applet firewall according to [JCRE]. Each applet on the TOE must have been passed the Bytecode Verifier in order to ensure correct applet isolation. As an additional defensive security feature also a type check for API array parameters is performed. This TSF enforces the following SFRs: • FDP_ACC.2/FIREWALL Complete access control • FDP_ACF.1/FIREWALL Security attribute based access control • FDP_IFC.1/JCVM Subset information flow control • FDP_IFF.1/JCVM Simple security attributes • FMT_MSA.1/JCRE Management of security attributes • FMT_MSA.2/FIREWALL_JCVM Secure security attributes • FMT_MSA.3/FIREWALL Static attribute initialisation • FMT_MSA.3/JCVM Static attribute initialization • FMT_SMR.1 Security roles • FDP_ROL.1/FIREWALL Basic rollback • FMT_MSA.1/JCVM Management of security attributes • FMT_MTD.1/JCRE Management of TSF data • FMT_MTD.3/JCRE Secure TSF data • FMT_SMF.1 Specification of Management Functions • FAU_SAS.1 • FPT_RCV.3/OS Automated recovery without undue loss • FPT_RCV.4/OS Function recovery
SF.RIP	This TSF ensures that sensitive information is made unavailable after deletion. This will be done by overwriting keys, APDU buffer and transient objects with zeros or random values. Applications and persistent objects will be marked as deleted. If the deleted resource is reused by a new object creation, the previous content will be set to a random value. This TSF enforces the following SFRs: • FDP_RIP.1/bArray Subset residual information protection • FDP_RIP.1/APDU Subset residual information protection • FDP_RIP.1/KEYS Subset residual information protection • FDP_RIP.1/TRANSIENT Subset residual information protection • FDP_RIP.1/ADEL Subset residual information protection • FDP_RIP.1/ODEL Subset residual information protection • FDP_RIP.1/ABORT Subset residual information protection • FDP_RIP.1/OBJECTS Subset residual information protection • FDP_RIP.1/GlobalArray Subset residual information protection
SF.Rollback	The TOE implements atomicity and rollback mechanism for Java Card runtime environment [JCRE] and GlobalPlatform management functions (see [GP]). The TOE also ensures that objects created during an aborted transaction are made unavailable. This TSF enforces the following SFRs: • FPT_RCV.3/Installer Automated recovery without undue loss • FDP_ROL.1/FIREWALL Basic rollback • FDP_RIP.1/ABORT Subset residual information protection
SF.SCP	The TOE implements secure channel protocols according to [GP], chapter 10. The following protocols are supported: • SCP03 according to [GP-D]. • SCP03t according to [SGP.22][GP-D].

	• SCP80 according to [TS 102 225] and [TS 102 226] and supporting secure messaging over SMS and CAT_TP. • SCP81 according to [GP-B]. The SCP uses as the basic cryptographic primitives the security hardened symmetric cryptographic library which is CC certified together with the underlying platform. This TSF enforces the following SFRs: • FDP_UIT.1/CM Data exchange integrity • FTP_ITC.1/CM Inter-TSF trusted channel • FCO_NRO.2/CM Enforced proof of origin • FDP_IFC.2/CM Complete information flow control • FDP_IFF.1/CM Simple security attributes • FMT_MSA.1/CM Management of security attributes • FMT_MSA.3/CM Static attribute initialisation • FMT_SMF.1/CM Specification of Management Functions • FIA_UID.1/CM Timing of identification • FIA_AFL.1/GP • FMT_SMR.1/CM Security roles • FCS_COP.1 Cryptographic operation
SF.CM	The TOE implements an access control policy for GlobalPlatform card management functions according to [GP] and GlobalPlatform Amendments A [GP-A], B [GP-B], C [GP-C], D [GP-D] and E [GP-E]. In addition to the GP specification, the Java Card Runtime Environment specification [JCRE] is followed to support for application loading, installation, and deletion. AID management is provided by SF.CM according to the GlobalPlatform Specification [GP], the Java Card Runtime Environment Specification [JCRE], and the Java Card API Specification [JCAPI]. This TSF enforces the following SFRs: • FMT_MSA.1/CM Management of security attributes • FMT_MSA.3/CM Static attribute initialisation • FMT_SMF.1/CM Specification of Management Functions • FMT_SMR.1/CM Security roles • FPT_TDC.1 Inter-TSF basic TSF data consistency • FIA_ATD.1/AID User attribute definition • FIA_UID.2/AID User identification before any action • FIA_USB.1/AID User-subject binding • FDP_ITC.2/Installer Import of user data with security attributes • FMT_SMR.1/Installer Security roles • FPT_RCV.3/Installer Automated recovery without undue loss • FPT_FLS.1/Installer Failure with preservation of secure state • FDP_ACC.2/ADEL Complete access control • FDP_ACF.1/ADEL Security attribute based access control • FDP_RIP.1/ADEL Subset residual information protection • FMT_MSA.1/ADEL Management of security attributes • FMT_MSA.3/ADEL Static attribute initialisation • FMT_SMR.1/ADEL Security roles • FPT_FLS.1/ADEL Failure with preservation of secure state • FMT_SMF.1/ADEL Specification of Management Functions • FPT_FLS.1/ODEL Failure with preservation of secure state • FDP_SDI.2/DATA Stored data integrity monitoring and action • FIA_UAU.1/GP Timing of authentication • FIA_UAU.4/GP Single-use authentication mechanisms • FDP_UIT.1/GP Data exchange integrity • FDP_UCT.1/GP Basic data exchange confidentiality
SF.Physical	The TOE provides means to protect SFRs against physical tampering and leakage. The TOE uses mainly the physical security measures of the underlying hardware platform. Security mechanisms involved in this protection are: • Memories scrambiling and encryption

	• Protection of NVM sectors • Memory Protection Unit (MPU) • Library Protection Unit (LPU) This TSF enforces the following SFRs: • FAU_ARP.1 Security alarms • FDP_SDI.2 Stored data integrity monitoring and action • FPT_TST.1 TSF testing • FPT_FLS.1 Failure with preservation of secure state
SF.CRYPTO	The TOE provides key creation, key management, key deletion and cryptographic functionality. It provides the API in accordance to the Java Card API Specification [JCAPI]. The cryptographic API uses as the basic cryptographic implementation the security hardened cryptographic library which is CC certified together with the underlying platform. The integrity of the cryptographic assets is monitored. In addition, key destructions and residual information purging is implemented. SF.CRYPTO provides secure random number generation and makes this functionality available through an API according to the Java Card API Specification [JCAPI]. This TSF enforces the following SFRs: • FCS_CKM.1 Cryptographic key generation • FCS_CKM.6 Cryptographic key destruction • FCS_COP.1 Cryptographic operation • FPR_UNO.1 Unobservability • FCS_RNG.1 Random number generation • FCS_COP.1/DRBG Cryptographic operation
SF.PIN	The TOE implements secure PIN compare functions and integrity protection of the PIN. This TSF enforces the following SFRs: • FPR_UNO.1 Unobservability • FDP_SDI.2 Stored data integrity monitoring and action

10.1.2 eUICC SFR coverage

Security Functionality	Description
SF.eUICC_CRYPTO	This TSF provides key creation, key management, key deletion and cryptographic functionality specific to the eUICC component. It provides the API in accordance to eUICC specification [SGP.32]. This TSF also enforces protection of key material during cryptographic functions processing and key Generation, against state-of-the-art attacks, including IC power consumption analysis. The TSF also provides a secure random generator. This number is used to provide functionality to Platform Support Functions, like generation of a random challenge and generation of a shared secret implemented in FDP_ACF.1/ECASD. This TSF enforces the following SFRs: • FPT_EMS.1/Base • FCS_CKM.1/SCP-SM • FCS_CKM.2/SCP-MNO • FCS_CKM.2/Mobile_network • FCS_CKM.6/SCP-SM • FCS_CKM.6/SCP-MNO • FCS_CKM.6/Mobile_network • FCS_COP.1/Mobile_network • FCS_RNG.1 • FCS_COP.1/DRBG
SF.eUICC_ACCESS	This TSF handles the access to eUICC features by external or local users. It based on JavaCard and GlobalPlatform features to implement: • Flow controls.

	• Access control • Identification and authentication of users. • Establishment of trusted channels in accordance to eUICC specifications [SGP.32]. This TSF enforces the following SFRs: • FDP_IFC.1/SCP • FDP_IFF.1/SCP • FDP_IFC.1/Platform_services • FDP_IFF.1/Platform_services • FPT_FLS.1/Platform_services • FDP_ACC.1/ISDR • FDP_ACF.1/ISDR • FDP_ACC.1/ECASD • FDP_ACF.1/ECASD • FMT_MSA.1/CERT_KEYS • FMT_SMF.1/Base • FMT_SMR.1/Base • FMT_MSA.3 • FIA_UID.1/EXT • FIA_UAU.1/EXT • FIA_UAU.4/EXT • FIA_USB.1/EXT • FIA_UID.1/MNO-SD • FIA_USB.1/MNO-SD • FIA_ATD.1/Base • FIA_API.1 • FTP_ITC.1/SCP • FDP_ITC.2/SCP • FPT_TDC.1/SCP • FDP_UCT.1/SCP • FDP_UIT.1/SCP • FMT_MSA.1/RAT • FMT_MSA.1/PLATFORM_DATA • FMT_MSA.1/RULES
SF.eUICC_PROTECTION	This TSF extends the scope of self-protections features provided by the Java Card platform to the eUICC component needs. This TSF enforces the following SFRs: • FDP_SDI.1/Base • FDP_RIP.1/Base • FPT_FLS.1/Base
SF.eUICC_OS-UPDATE	This TSF addresses the security requirements related to the eUICC OS Update capability. It provides confidentiality and integrity of the update image. This TSF enforces the following SFRs: • FTP_ITC.1/Loader Inter-TSF trusted channel • FDP_UCT.1/Loader Basic data exchange confidentiality • FDP_UIT.1/Loader Data exchange integrity • FDP_ACC.1/Loader Subset access control • FDP_ACF.1/Loader Security attribute based access control • FMT_MSA.3/Loader Static attribute initialisation • FMT_MSA.1/Loader Management of security attributes • FMT_SMR.1/ Loader Security roles • FIA_UID.1/Loader Timing of identification • FIA_UAU.1/Loader Timing of authentication • FMT_SMF.1/Loader Specification of management functions • FPT_FLS.1/Loader Failure with preservation of secure state • FAU_SAR.1/Loader Audit review

	• FAU_SAS.1/ Loader Audit storage

11 Rationales

11.1 IC Composition rationale

11.1.1 Common Criteria rationale

Assurance level of the IC evaluation is EAL5 augmented by ALC_DVS.2 and AVA_VAN.5

Assurance level of the TOE is EAL4 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2.

Assurance level of the current evaluation is consistent with the assurance level in

11.1.2 Compatibility between threats (TOE and IC)

IC Threats	IC Threat description	Rationale
BSI.T.Leak-Inherent	Inherent Information Leakage	This threat is related to the information which is leaked from the TOE during usage of the Security IC in order to disclose sensitive data of the TOE. This threat has been considered in the current evaluation.
BSI.T.Phys-Probing	Physical Probing	This threat is related to physical probing of the TOE to disclose relevant information. This threat has been considered in the current evaluation.
BSI.T.Malfunction	Malfunction due to Environmental Stress	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. This threat has been considered in the current evaluation.
BSI.T.Phys-Manipulation	Physical Manipulation	This threat is related to physical manipulation of the Security IC. This is covered by the IC evaluation.
BSI.T.Leak-Forced	Forced Information Leakage	This threat is related to information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the composite TOE. This is covered by the IC evaluation.
BSI.T.Abuse-Func	Abuse of Functionality	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. This threat has been considered in the current evaluation.
BSI.T.RND	Deficiency of Random Numbers	This threat is related to the deficiency of random numbers. This is covered by the IC evaluation.
BSI.T.Masquerade-TOE	Masquerade the TOE	This threat covers the unique identity of the IC. This is covered by the IC evaluation.
AUG4.T.Mem-Access	Memory Access Violation	The TOE implements memory access violation mechanisms based on the IC security policy. Therefore, this threat also covered by the TOE evaluation.
JIL.T.Open-Samples-Diffusion	Diffusion of open samples	Covers the attack path where an attacker may get access to open samples of the IC and use them to gain information about the TSF. This is covered by the IC evaluation.
T.Confid-Applic-Code	Specific application code confidentiality	Application code of the TOE is protected against unauthorized disclosure. Therefore, this threat also covered by the TOE evaluation.
T.Confid-Applic-Data	Specific application data confidentiality	Application data of the TOE is protected against unauthorized disclosure. Therefore, this threat also covered by the TOE evaluation.

T.Integ-Applic-Code	Specific application code integrity	Application code of the TOE is protected against unauthorized modification. Therefore, this threat also covered by the TOE evaluation.
T.Integ-Applic-Data	Specific application data integrity	Application data of the TOE is protected against unauthorized modification. Therefore, this threat also covered by the TOE evaluation.

11.1.3 Compatibility between assumptions (TOE and IC)

IC Assumptions	IC Assumptions description	Rationale
BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	This assumption ensures the security of the delivery and storage of the IC. It is covered by the ALC_DVS.2 activity of the current TOE evaluation.
BSI.A.Resp-Appl	Treatment of User Data	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.

11.1.4 Compatibility between security objectives for the environment (TOE and IC)

IC OEs	IC OEs description	Rationale
BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE	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.
BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	This objective is covered by the IC evaluation.
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader	This objective is covered by the IC evaluation.
BSI.OE.Loader-Usage	Secure communication and usage of the Loader	This objective is covered by the IC evaluation.
BSI.OE.TOE-Auth	External entities authenticating of the TOE	This objective is covered by the IC evaluation.
OE.Composite-TOE-Id	Composite TOE identification	Also covered by the current evaluation.
OE.TOE-Id	TOE identification	This objective is covered by the IC evaluation.
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	Also covered by the current evaluation.
OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	Also covered by the current evaluation.

11.1.5 Compatibility between Security Objectives (TOE and IC)

IC O.TOE	IC O.TOE description	Rationale
BSI.O.Leak-Inherent	Protection against Inherent Information Leakage	Also covered by the current evaluation.
BSI.O.Phys-Probing	Protection against Physical Probing	Also covered by the current evaluation.
BSI.O.Malfunction	Protection against Malfunctions	Also covered by the current evaluation.
BSI.O.Phys-Manipulation	Protection against Physical Manipulation	Covered by the IC evaluation.
BSI.O.Leak-Forced	Protection against Forced Information Leakage	Covered by the IC evaluation.
BSI.O.Abuse-Func	Protection against Abuse of Functionality	Also covered by the current evaluation.
BSI.O.Identification	TOE Identification	Also covered by the current evaluation.

BSI.O.RND	Random Numbers	Also covered by the current evaluation.
BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader	Also covered by the ALC_DVS.2 activity of the current evaluation.
BSI.O.Ctrl_Auth_Loader	Access control and authenticity for the Loader	Covered by the IC evaluation.
JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF	Covered by the IC evaluation.
JIL.O.Secure-Load-ACode	Secure loading of the Additional Code	Covered by the IC evaluation.
JIL.O.Secure-AC-Activation	Secure activation of the Additional Code	Covered by the IC evaluation.
JIL.O.TOE-Identification	Secure identification of the TOE	Covered by the IC evaluation.
O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image	Covered by the IC evaluation.
O.MemImage-Identification	Secure identification of the Memory Image	Covered by the IC evaluation.
BSI.O.Authentication	Authentication to external entities	Covered by the IC evaluation.
AUG1.O.Add-Functions	Additional Specific Security Functionality	Covered by the IC evaluation.
AUG4.O.Mem-Access	Dynamic Area based Memory Access Control	Also covered by the current evaluation.
O.Firewall	Specific application firewall	Also covered by the current evaluation

11.1.6 Compatibility between Organisational Security Policies (TOE and IC)

IC Policies		**Rationale**
BSI.P.Process-TOE	Protection during TOE Development and Production	This policy is related to the accurate unique identification during IC Development and Production. It was covered by the IC evaluation.
BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality	Limiting and blocking the loader functionality for loading of Security IC Embedded Software. It was covered by the ALC_DVS.2 activity of the current TOE evaluation.
BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality	This policy is related to the capability provided by the TOE to load Security IC Embedded Software into the NVM after TOE delivery, in a controlled manner, during composite product manufacturing. It is covered by the ALC_DVS.2 activity of the current TOE evaluation.
AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)	Additional Specific Security Functionality is provided by the IC. It was covered by the IC evaluation.

11.1.7 Compatibility between SFRs (TOE and IC)

IC SFRs are separated in the following groups as defined in [SOGIS-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 its security properties providing protection attacks to the TOE.

IC SFR	**Rationale**
FRU_FLT.2	RP_SFR-MECH
FPT_FLS.1	RP_SFR-MECH
FMT_LIM.1 / Test	RP_SFR-MECH
FMT_LIM.2 / Test	RP_SFR-MECH
FMT_LIM.1 / Loader	RP_SFR-MECH

FMT_LIM.2 / Loader	RP_SFR-MECH
FMT_LIM.1 / Sdiag	RP_SFR-MECH
FMT_LIM.2 / Sdiag	RP_SFR-MECH
FAU_SAS.1	RP_SFR-MECH
FDP_SDC.1	RP_SFR-MECH
FDP_SDI.2	RP_SFR-MECH
FPT_PHP.3	RP_SFR-MECH
FDP_ITT.1	RP_SFR-MECH
FPT_ITT.1	RP_SFR-MECH
FDP_IFC.1	RP_SFR-MECH
FCS_RNG.1/PTG.2	RP_SFR-SERV
FCS_COP.1/DES	RP_SFR-MECH
FCS_COP.1/AES	RP_SFR-MECH
FDP_ACC.2/Memories	RP_SFR-MECH
FDP_ACF.1/Memories	RP_SFR-MECH
FMT_MSA.3/Memories	RP_SFR-MECH
FMT_MSA.1/Memories	RP_SFR-MECH
FMT_SMF.1/Memories	RP_SFR-MECH
FIA_API.1	RP_SFR-SERV
FTP_ITC.1 / Loader	RP_SFR-MECH
FDP_UCT.1/Loader	RP_SFR-MECH
FDP_UIT.1 / Loader	RP_SFR-MECH
FDP_ACC.1/Loader	RP_SFR-MECH
FDP_ACF.1/Loader	RP_SFR-MECH
FMT_MSA.3/Loader	RP_SFR-MECH
FMT_MSA.1/Loader	RP_SFR-MECH
FDP_SMR.1/Loader	RP_SFR-MECH
FIA_UID.1/Loader	RP_SFR-MECH
FIA_UAU.1/Loader	RP_SFR-MECH
FDP_SMF.1/Loader	RP_SFR-MECH
FPT_FLS.1/Loader	RP_SFR-MECH
FAU_SAS.1/Loader	RP_SFR-MECH
FAU_SAR.1/Loader	RP_SFR-MECH
FTP_ITC.1 / Sdiag	RP_SFR-MECH
FAU_SAR.1 / Sdiag	RP_SFR-MECH

12 Abbreviations and glossary

[CC]	Common Criteria
[EAL]	Evaluation Assurance Level
[LPU]	Library Protection Unit
[MPU]	Memory Protection Unit
[NVM]	Non-Volatile Memory
[SO]	Security Objective
[ST]	Security Target
[TOE]	Target of Evaluation
[TSF]	TOE Security Functionality
[PP]	Protection Profile