THALES

Building a future we can all trust

MultiSIM M2M 4.3.0 Platform

GSMA eSA Security Target – Public version

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1 Reference documents

1.1 External references [ER]

[GSMA]	**GSMA references**
[SGP01]	SGP01 - Embedded SIM Remote Provisioning Architecture Reference: SGP01, Version 4.3, November 18th 2022
[SGP02]	Remote Provisioning Architecture for Embedded UICC Technical Specification Reference: SGP02, Version 4.3, January 25th 2023
[GSMA-SAS]	GSMA SAS Guidelines for Subscription Manager Roles GSMA SAS Methodology for Subscription Manager Roles GSMA SAS Standard for Subscription Manager Roles Version 2.0 - 13 May 2015
[ISO]	**ISO references**
[ISO7816]	Identification cards – Integrated circuit(s) cards with contacts - Books 1 to 9
[Javacard]	**Javacard references**
[JCRE310]	Java Card 3 Platform - Runtime Environment Specification, Classic Edition Version 3.1.0, November 2019
[JCVM310]	Java Card 3 Platform - Virtual Machine Specification, Classic Edition Version 3.1.0, November 2019
[JCAPI310]	Java Card 3 Platform - Java Card API, Classic Edition Version 3.1.0, November 2019
[GP]	**Global Platform references**
[GPCS]	GlobalPlatform Technology - Card Specification v2.3.1, March 2018 Reference: GPC_SPE_034
[Amd A]	GlobalPlatform Card - Confidential Card Content Management Card Specification v2.3 – Amendment A v1.2 Reference: GPC_SPE_007
[Amd B]	GlobalPlatform Technology - Remote Application Management over HTTP Card Specification v2.3 – Amendment B v1.2 Reference: GPC_SPE_011
[Amd C]	GlobalPlatform Card – Contactless services Card Specification v2.3 – Amendment C v1.3 Reference: GPC_SPE_025
[Amd D]	GlobalPlatform Card Technology - Secure Channel Protocol '03' Card Specification v2.3 – Amendment D v1.2 Reference: GPC_SPE_014
[Amd E]	GlobalPlatform Card Technology - Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E v1.1 Reference: GPC_SPE_042
[Amd F]	GlobalPlatform Card - Secure Channel Protocol '11' Card Specification v2.3 – Amendment F v1.3 Reference: GPC_SPE_093
[Amd H]	GlobalPlatform Card - Executable Load File Upgrade Card Specification v2.3 – Amendment H v1.1 Reference: GPC_SPE_120
[CIC]	Common Implementation Configuration v2.0 Reference: GPC_GUI_080
[UICC_CFG]	GlobalPlatform Card – UICC Configuration v2.0 Reference: GPC_GUI_010
[AGD-DEV-App-Basic]	GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications Reference: GPC_GUI_050, Version 2.0, November 2014

[ETSI]	ETSI references
[TS 102 124]	Transport Protocol for UICC based Applications; Stage 1 Version 7.1.0
[TS 102 127]	Transport protocol for CAT applications; Stage 2 Version 15.0.0
[TS 102 221]	Physical and logical characteristics, Version 16.6.0 (Partial)
[TS 102 222]	Administrative commands and telecommunications applications Version 15.0.0 (Partial)
[TS 102 223]	Card Application Toolkit (CAT), Version 15.3.0
[TS 102 224]	Security mechanisms for UICC based Applications - Functional requirements Version 15.0.0
[TS 102 225]	Secured packet structure for UICC based applications, Version 16.0.1 (Partial)
[TS 102 226]	Remote APDU structure for UICC based applications, Version 16.0.1 (Partial)
[TS 102 240]	UICC API and Loader Requirements; Service description Version 11.0.0
[TS 102 241]	UICC API for Java Card, Version 16.2.0 (Partial)
[TS 102 310]	Extensible Authentication Protocol support in the UICC, Version 7.0.0
[3GPP]	**3GPP references**
[TS 31 101]	UICC-terminal interface; Physical and logical characteristics Version 16.2.0 (Partial)
[TS 31 102]	Characteristics of the USIM application, Version 16.9.0 (Partial)
[TS 31 103]	Characteristics of the IP Multimedia Services Identity Module (ISIM) application, Version 16.1.0 (Partial)
[TS 31 111]	USIM Application Toolkit (USAT), Version 16.5.0
[TS 31 115]	Secured packet structure for USIM Toolkit applications Version 16.0.0 (Partial)
[TS 31 116]	Remote APDU Structure for USIM Toolkit applications Version 16.0.0
[TS 31 130]	USIM API for Java Card, Version 16.0.0 (Partial)
[TS 31 133]	ISIM API for Java Card, Version 16.0.0
[TS 33 102]	3G security; Security architecture Version 16.0.0
[TS 33 105]	Cryptographic algorithm requirements, Version 16.0.0
[TS 33 501]	Security architecture and procedures for 5G system, Version 16.9.1
[TS 35 206]	Specification of the Milenage algorithm, document 2: Algorithm specification Version 16.0.0
[TS 35 231]	Specification of the TUAK algorithm, document 1: Algorithm specification Version 16.0.0
[CC]	**Common Criteria references**
[CC-1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC-2]	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC-3]	Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CCDB]	Common Criteria Supporting Document, Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices Version 1.5.1, May 2018.
[PP-SGP05]	SGP.05 Embedded UICC Protection Profile Ref: GSMA SGP 05, Version 4.1
[PP-GP]	GlobalPlatform Technology - Secure Element Protection Profile Ref: GPC_SPE_174, Version 1.0
[PP-JCS]	Java Card System – Open Configuration Protection Profile Ref: BSI-CC-PP-0099-V2-2020, Version 3.1, April 2020

[PP/0084]	Security IC Platform Protection Profile with augmentation Packages Ref: BSI-CC-PP-0084-2014
[ST_IC]	ST33K1M5A and ST33K1M5M B02 - Security Target for composition Ref: SMD_ST33K1M5AM_ST_21_002, Revision B02.1, May 2023
[OTHERS]	**Other references**
[AIS31]	A proposal for: Functionality classes for random number generators, version 2.0, 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik

1.2 INTERNAL REFERENCES [IR]

[AGD]	**TOE guidance documentation**
[AGD-PRE]	eSA preparative guidance of Thales MultiSIM M2M 4.3.0 Reference: D1606247, Version 1.3, June 2024
[AGD-OPE]	eSA operational guidance of Thales MultiSIM M2M 4.3.0 Reference: D1606362, Version 1.4, August 2024
[AGD-DEV-App-Basic]	GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications Reference: GPC_GUI_050, Version 2.0, November 2014
[AGD-DEV-App-Secure]	Guidance for Secure application development on Thales MultiSIM M2M Products Reference: D1608375, Version 0.2, April 2024
[AGD-PLT-IdentConf]	Platform Identification and Configurability for MultiSIM M2M 4.3.0 Reference: D1607319, Version 2.1, April 18th 2024
[AGD-PLT-USR]	MultiSIM M2M 4.3.0 User's Guide Reference: D1609183A, July 11th 2024
[AGD-PLT-APDU]	M2M Automotive MultiSIM 4.3 APDU Guide Reference: D1609185A, November 27th 2023

2 Acronyms

AES	Advanced Encryption Standard
AID	Application Identifier
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
APSD	Application Provider Security Domain
CA	Controlling Authority
CASD	Controlling Authority Security Domain
CBC	Cipher Block Chaining
CC	Common Criteria
CVM	Cardholder Verification Method
DAP	Data Authentication Pattern
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ELF	Executable Load File
GASD	GemActivate Security Domain
GP	GlobalPlatform
HMAC	Keyed-Hash Message Authentication Code
JCAPI	Javacard API
JCRE	Javacard Runtime Environment
JCVM	Javacard Virtual Machine
M2M	Machine To Machine
MAC	Message Authentication Code
MNO	Mobile Network Operator
NAA	Network Authentication Application
OEM	Original Equipment Manufacturer
OTA	Over-The-Air
PIN	Personal Identification Number
PP	Protection Profile
RAM	Random Access Memory
RSA	Rivest / Shamir / Adleman asymmetric algorithm
SCP	Secure Channel Protocol; or (ETSI) Smart Card Platform
SD	Security Domain
SIM	Subscriber Identity Module
SSD	Supplementary Security Domain
ST	Security Target
TDES (or 3DES)	Triple Data Encryption Standard
TOE	Target Of Evaluation
USIM	Universal Subscriber Identity Module

3 Security Target introduction

3.1 Security Target Identification

Title:	MultiSIM M2M 4.3.0 Platform – GSMA eSA Security Target
Version:	1.2p
Author:	Thales
Reference:	D1599957
Publication date:	01/08/2024

3.2 TOE Identification

Product name:	MultiSIM M2M 4.3.0
TOE name:	MultiSIM M2M 4.3.0 platform
TOE version:	83040
TOE documentation:	Guidance [AGD]
TOE hardware part:	ST33K1M5 security controller
Developer:	Thales

3.3 TOE Overview

TOE type: eUICC opened platform implementing the Javacard and GlobalPlatform standards.

Product description:

The MultiSIM M2M 4.3.0 product is a discrete eUICC with M2M configuration, compliant with the GSMA [SGP01] and [SGP02] specifications. As such, it is a multi-profile product, supporting remote profile management over SMS and over HTTP. Soldered in an M2M device, it provides connectivity to the MNO network corresponding to the currently enabled profile.

The MultiSIM M2M 4.3.0 product is a contact-only product supporting the [ISO7816] T=0 communication protocol. It is built upon an opened [Javacard] / [GP] platform, meaning that additional applications - which may not be known at the time of the present evaluation - can be remotely loaded and installed on the eUICC “post-issuance”, i.e. after the M2M device has been delivered to the end-user. Applications can also be installed “pre-issuance” during the pre-personalization or personalization phases. Whatever the scenario (pre-issuance or post-issuance), applications’ loading and installation are secured by the GP security mechanisms and verification processes.

The MultiSIM M2M 4.3.0 product has an OS Update capability to correct existing features.

For the present evaluation, the **Target of Evaluation (TOE)** is the platform part of the MultiSIM M2M 4.3.0 software. The TOE boundaries encompass:

- **The Telecom environment** implemented according to [GSMA], [ETSI] and [3GPP], which implements the GSMA Remote SIM Provisioning (RSP) Architecture and supports network authentication and Telecom communication protocols.
- **The Javacard System (JCS)** implemented according to the [Javacard] standard, which manages and executes applications called applets.

- **The GlobalPlatform (GP) functionalities** implemented according to the [GP] standard, which provide a common and widely used interface to communicate with a smartcard and manage applications in a secure way
- **The GemActivate application**, which is the Thales proprietary solution to activate services and/or load software patches post-issuance, under the M2M device owner and Thales administration
- **The ST33K1M5 Integrated Circuit (either ST33K1M5A or ST33K1M5M[1])**
- **The guidance documentation [AGD]**

[1] ST33K1M5A is the ‘Auto-grade’ flavor of ST33K1M5, whereas ST33K1M5M is the ‘Indus-grade’ flavor. Both IC flavors are identical in terms of security and are covered by the same IC security certificate. In the next sections of the present ST, the IC will be designated as “ST33K1M5” without further distinction.

4 TOE Description

4.1 ARCHITECTURE OF MULTISIM M2M 4.3.0

The high-level architecture of MultiSIM M2M 4.3.0 can be represented by Figure 1. In this figure, the elements in blue are configurable.

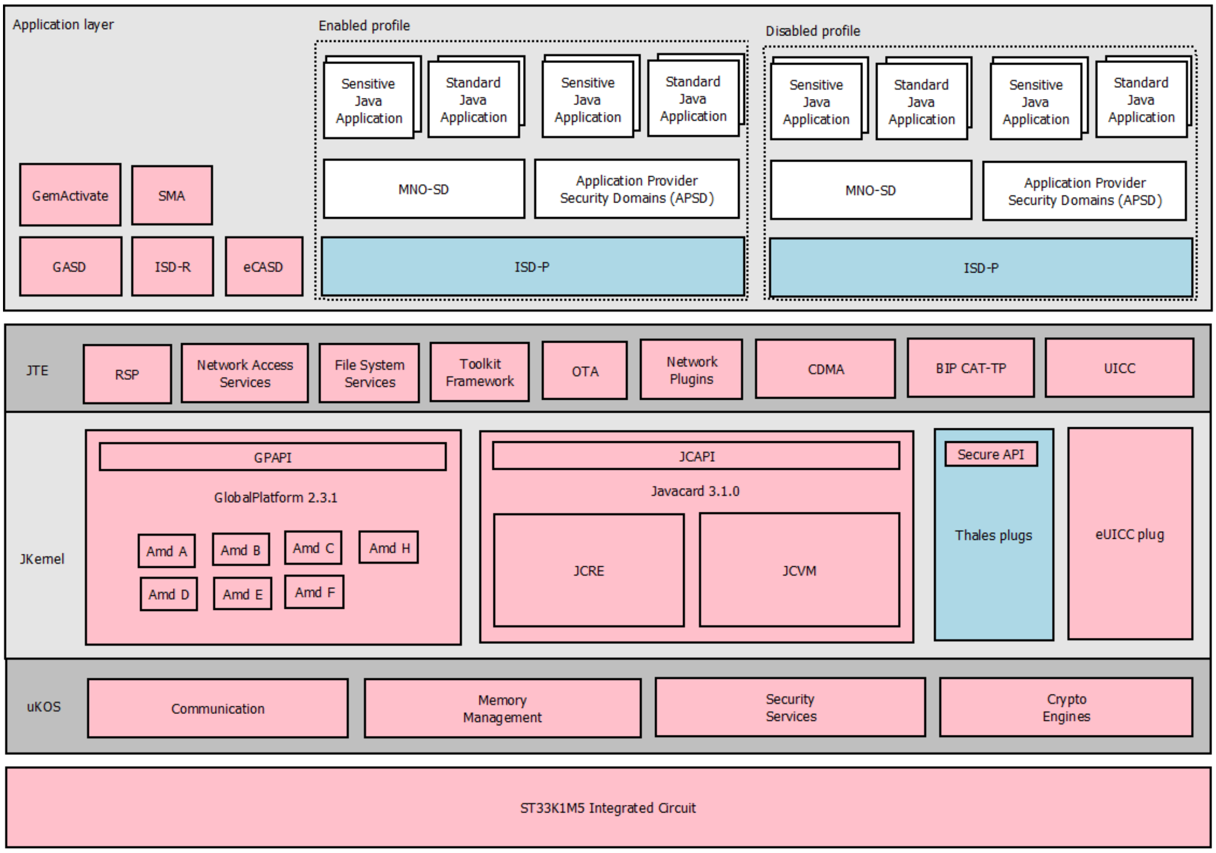


Figure 1: MultiSIM M2M 4.3.0 architecture

The architecture can be decomposed in three layers:

- The hardware layer composed of the ST33K1M5 integrated circuit
- The MultiSIM M2M 4.3.0 platform, which is the operating system of the product
- The application layer, encompassing the eUICC security domains (ISD-R, eCASD, ISD-P), the OS Update security domain (GASD) and the applications / profiles loaded on top of them.

4.2 TOE BOUNDARIES

4.2.1 TOE physical boundaries

The ST33K1M5 IC is a tamper-proof chip available in MFF2 or SIM 2FF formats[2], which can be embedded in any M2M device.

[2] The “Auto-Grade” flavor of the IC (ST33K1M5A) is available in MFF2 format, whereas the “Indus-Grade” flavor (ST33K1M5M) is available in either MFF2 or SIM 2FF formats. Both IC flavors are identical in terms of security and are covered by the same IC security certificate.

For the present evaluation, the TOE physical boundaries encompass the ST33K1M5 IC with the Thales MultiSIM M2M 4.3.0 embedded software. Any other item is outside the scope of the evaluation.

TOE component	Developer	Item	Identifier	Form of delivery
IC	STM	ST33K1M5A/M IC (Hardware and IC Dedicated Software)	ST33K1M5A and ST33K1M5M B01	IC packaged in MFF2 or SIM 2FF formats
eUICC Platform	Thales	MultiSIM M2M 4.3.0 Embedded Software	83040	▪ Thales life-cycle: Software embedded within the IC ▪ Alternative life-cycle: Software embedded in secure loading script
eUICC Guidance	Thales	MultiSIM M2M 4.3.0 guidance documentation	References and versions listed in [AGD]	Electronic document (PDF) via secure email

4.2.2 TOE logical boundaries

The present Security Target claims conformance to the [PP-SGP05] protection profile; the TOE logical boundaries are delimited (dash line in red) in Figure 2.

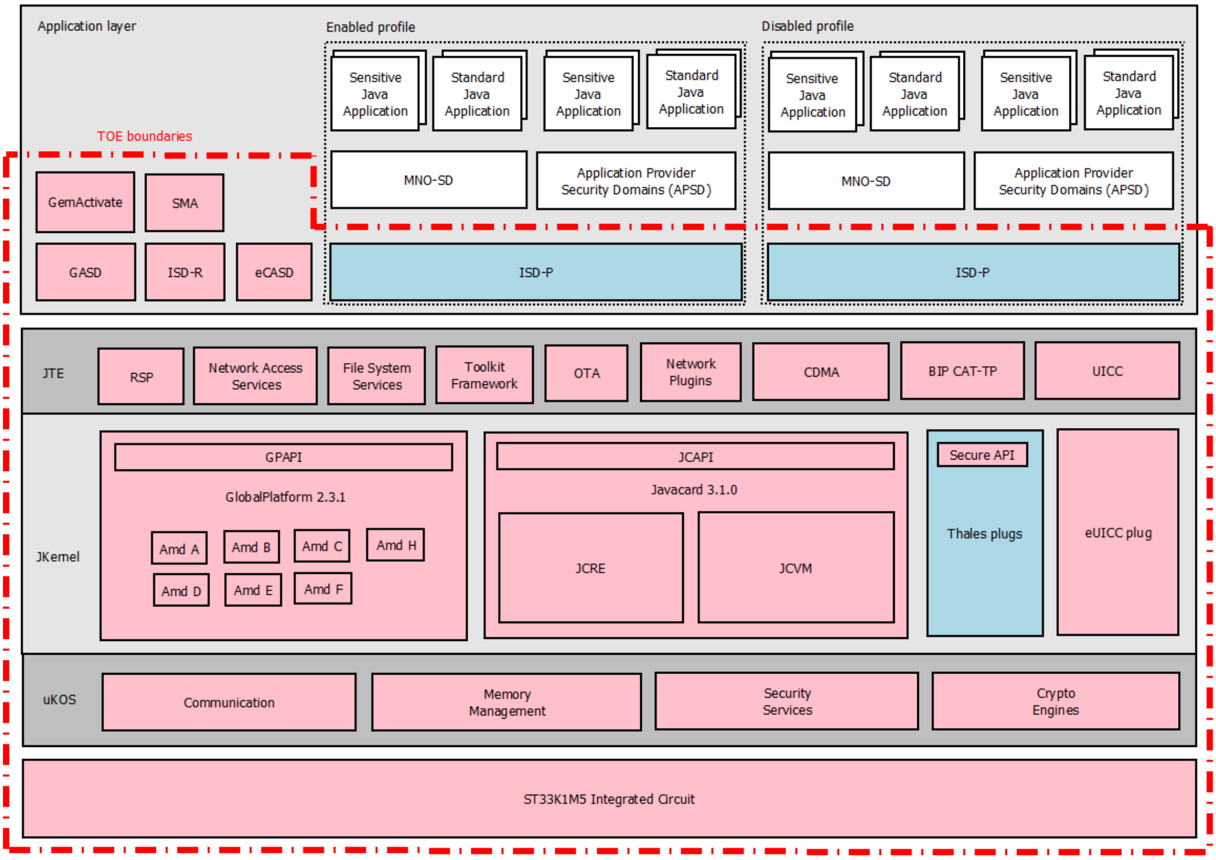


Figure 2: TOE logical boundaries

4.3 Application Layer

4.3.1 Profiles

The goal of the application layer is to implement the eUICC functionalities described in [SGP02], which rely on the notion of Profile. A Profile is the combination of a file structure, data and applications to be provisioned onto, or present on, a eUICC. Each Profile, combined with the functionality of the eUICC, behaves basically as a SIM card. A eUICC may contain more than one Profile, but one and only one is activated at a time. Each Profile is controlled by a unique ISD-P; consequently, there is one and only one enabled ISD-P at a time on the eUICC.

A Profile can have several forms:

- A Provisioning Profile: A Profile containing Network Authentication Parameters. When installed on a eUICC, it enables access to communication network(s), only to provide transport capability for eUICC management and Profile management between the eUICC and an SM-SR.
- An Operational Profile: A Profile containing Network Authentication Parameters as well as MNO's applications and 3rd party applications.
- A Test Profile: A Profile that is used to provide connectivity to test equipment and cannot be used to connect to any MNO.
- Additionally, an operational profile can be set with the Emergency Profile attribute which can be only used to make/receive Emergency calls.

The present document will use the term “Profile” to describe either Provisioning Profiles, operational Profiles or Test Profiles.

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 (POL1 data), but rely 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
- At least one NAA
- POL1, even if not used
- The file system
- Connectivity parameters of the Profile

More details on the Profile can be found in [SGP02].

4.3.2 ISD-P

The ISD-P is the on-card representative of the MNO, or SM-DP if delegated by the MNO.

An ISD-P controls the content of a single MNO Profile. The ISD-P may be created during the operational life of the eUICC. In order to create a new Profile, a SM-DP will use the secure routing functionalities of the SM-SR to:

- Require the creation of a new ISD-P
- Perform a confidential key establishment with the ISD-P
- Download and install the Profile.

The Profile is then managed by SM-SR Platform management commands. It should be noted that the SM-SR shall not have access to the content of a Profile, including the ISD-P.

As defined in [SGP01], the ISD-P shall:

- Be a separate and independent entity on the eUICC
- Contain a Profile including file system, NAAs and Policy Rules
- Contain a state machine related to creating, enabling and disabling the Profile
- Contain keys for Profile management for the loading and installation phase
- Implement a key establishment protocol to generate a keyset for personalisation of the ISD-P
- Be able to receive and decrypt, load and install the Profile created by the SM-DP
- Be able to set its own state to disabled once the Profile is installed
- Provide SCP03(t) capabilities to secure its communication with the SM-DP
- Be able to contain a CASD. This CASD is optional within the Profile and provides services only to security domains of the Profile and only when the Profile is in Enabled state.

4.3.3 ISD-R

The ISD-R is the on-card representative of the SM-SR that executes the Platform Management commands. An ISD-R shall be created within a eUICC at the time of manufacture.

During operational life of the eUICC, the ISD-R is associated with a single SM-SR, which routes securely the Profiles transmitted by a SM-DP, and triggers the Platform management operations (enabling/disabling a Profile, and so on).

As defined in [SGP01], the ISD-R shall:

- Be created within an eUICC at time of manufacture
- Be associated to an SM-SR
- Not be deleted or disabled
- Provide a secure OTA channel using Platform Management Credentials (SCP80 or
- SCP81) to the SM-SR
- Implement a key establishment protocol for the support of the change of SM-SR
- Offer wrapping and unwrapping service of the transport part during Profile download
- Be able to create new ISD-Ps with the Cumulative Granted Non Volatile Memory
- Not be able to create any SD except an ISD-P
- Execute Platform Management functions in accordance to the Policy Rules
- Not be able to perform any operation inside an ISD-P.

The ISD-R may change its associated SM-SR during the life of the eUICC.

The Subscription Manager Applet (SMA) complies with the GSMA Remote Provisioning Architecture and is located under the ISD-R. It is used e.g. to notify the SM-SR platform whenever there is a change of subscription, to manage the swap to the emergency profile or the fallback procedure. It cannot be installed post-issuance.

4.3.4 MNO-SD

The MNO-SD is the on-card representative of the MNO Platform. It is, according to [SGP02], the Security domain part of the Profile, owned by the MNO, providing the Secured Channel to the MNO's OTA Platform. It is used to manage the content of a Profile once the Profile is enabled. The MNO-SD is used to perform two operations on the eUICC:

- Modifying the POL1 policy data, which defines how, and if, the Profile can be disabled or deleted
- Modifying the connectivity parameters of the MNO OTA Platform. The connectivity parameters are a set of data (for example SMSC address) required by the eUICC to open a communication channel (for example SMS, HTTPS).

As defined in [SGP01], the MNO-SD shall:

- Be associated to itself
- Contain the MNO OTA Keys
- Provide a secure OTA channel (SCP80 or SCP81)
- Have the capability to host Supplementary Security Domains.

4.3.5 ECASD

The ECASD is the representative of the off-card entity CI root. It contains the data used to enforce trust in the identities of Actors (eUICC, remote Actors such as SM-SR or SM-DP).

The ECASD provides services to the ISD-P and ISD-R, in order to perform confidential key establishments.

As defined in [SGP01], the ECASD:

- Is created within an eUICC at time of manufacture
- Cannot be deleted or disabled after delivery
- Is based on the concept of CASD from Global Platform
- Is configured by the eUICC Manufacturer at pre-issuance
- Contains a non-modifiable eUICC private key, the associated Certificate, the CI's root public keys and the EUM keyset for key/certificate renewal
- Is associated to the ISD-R, which provides the underlying secure OTA channel
- Is required for, and is not limited to, establishment of new keysets in the ISD-P(s) and ISD-R
- Does not support the Mandated DAP verification feature

4.3.6 GASD and GemActivate

The GASD (GemActivate Security Domain) is the Security Domain representing a Thales administrator on the card. This entity can authorize the activation of optional services and the loading of additional code (i.e. patch) post issuance.

The GemActivate application, located under the GASD, is the Thales application supporting this OS Update capability.

4.3.7 Secure and Standard Applications

The applications loaded on top of the MultiSIM M2M 4.3.0 Platform can be split in two categories:

- Secure applications: these are sensitive applications, such as e.g. banking applets, whose security is assessed and certified through international schemes (Common Criteria, EMVco etc.)
- Standard applications, also called “basic” applications: these are the other applications. Although they do not face a formal security evaluation, assurance has to be provided that they do not threaten the sensitive applications and their assets. This assurance is provided through a verification process. Security mechanisms are in place at platform level to ensure that applications which are loaded post issuance have been verified.

4.4 PLATFORM LAYER

The MultiSIM M2M 4.3.0 platform implements two major industry standards:

- Oracle's Java Card 3.1.0 [Javacard], which consists of the Java Card 3.1.0 Virtual Machine, Java Card 3.1.0 Runtime Environment and the Java Card 3.1.0 Application Programming Interface.
- GlobalPlatform 2.3.1 [GP], UICC Configuration.

It is an opened platform, meaning that additional applications - which may not be known at the time of the present evaluation - can be remotely loaded and installed on the eUICC “post issuance”, i.e. after the M2M device has been integrated into the end-usage system or equipment. Applications can also be installed “pre-issuance” during the pre-personalization or personalization phases. Whatever the scenario (pre-issuance or post-issuance), applications’ loading and installation are secured by the GlobalPlatform security mechanisms and verification processes.

The platform implements (at least) the following services:

- Management and control of the communication between the eUICC and external entities
- Basic security services as follows:
  - Checking environmental operating conditions using information provided by the IC
  - Checking life cycle consistency
  - Providing secure cryptography primitives and algorithms
  - Ensuring the security of the PIN and cryptographic key objects
  - Generating random numbers
  - Handling secure data object and backup mechanisms
  - Managing memory content
- Enforcement of the Javacard firewall mechanism
- Standard Application Programming Interfaces (APIs) such as the Javacard API (JCAPI) and the Global Platform API (GPAPI)
- Proprietary Thales API: Secure API which provides security services to applications
- Creation and management of Security Domains (SSD)
- Management of lifecycle information (for the eUICC, Security Domains and Applications)
- SCP02, SCP03(t), SCP11, SCP80 and SCP81 support
- Secure loading, installation and deletion of applications within each SD
- Secure loading of software patches (OS Update feature, called GemActivate)
- DAP and Mandated DAP verification
- GlobalPlatform ‘Authorized Management’ and ‘Delegated Management’
- GlobalPlatform CLFDB
- PIN verification (GP CVM)
- Global Services (GS) according to GP
- ELF Upgrade according to GP [Amd H]
- Confidential Card Content Management (CCCM) according to GP [Amd A][3]

Note that the following optional features are not supported by the platform:

- Javacard Remote Method Invocation (JCRMI)
- Contactless features of GP [Amd C] (only the non-contactless features of [Amd C] are supported).

The MultiSIM M2M 4.3.0 platform also implements a Java Telecom Environment (JTE) compliant with the [GSMA], [ETSI] and [3GPP] specifications. The JTE implements the GSMA Remote SIM Provisioning (RSP) Architecture and supports network authentication and Telecom communication protocols. The following capabilities are supported, according to [GSMA]:

- Extended GlobalPlatform OPEN functions. The extension of the GP capabilities is typically needed to enforce additional states of the SDs (ENABLED and DISABLED) or the restrictions of privileges granted to SDs (see Annex C of [SGP02])
- Policy Enforcement functions, which are in charge of the verification and application of POL1 rules during eUICC Management activities.

[3] Note that the GP [Amd A] features are technically supported by the TOE, but are not in the scope of the present security evaluation.

- 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.

Application Note:

- Authentication to a Public Mobile Network (PMN) is done in accordance with the 3GPP standards TS 33.102 and TS 33.401. According to these standards (especially TS 33.102) the 3G and 4G authentication mechanisms allow the response values RES to have a length that is any multiple of 8 bits between 32 and 128 bits inclusive. In practice, either 32-bit or 64-bit RES is used. The [PP-SGP05] protection profile (and hence, the present ST) covers products only when used to create 64-bit RES. Operators choosing to use 32-bit RES will therefore be using the product outside the scope of [PP-SGP05] (and therefore, outside the scope of the present ST).
- [PP-SGP05] (and hence, the present ST) includes origin authentication of the PMN that owns the customer subscription to the Profile. It also includes entity authentication of the Profile to the PMN in which a customer subscriber is roaming on. It does not include entity authentication of this visited PMN to the Profile, except in 4G authentication.

4.5 TOE USAGE

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 the MNO’s property, and stores MNO specific information.

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

4.6 TOE LIFE-CYCLE

In accordance with [PP-SGP05], the product and TOE life cycle is composed of 5 phases which are described in the following subsections. Two possible life cycle options are considered in the present ST:

- In the ‘Thales life-cycle’, the integration of the MultiSIM M2M 4.3.0 Embedded Software into the ST33K1M5 IC is done by Thales. The TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of phase c, as illustrated in figure 3.
- In the ‘alternative life-cycle’, the integration of the MultiSIM M2M 4.3.0 Embedded Software into the ST33K1M5 IC is done by an accredited manufacturing actor. The TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of phase b, as illustrated in figure 4.

Note related to patch development (applicable to both life cycles)

No patch is present within the TOE for the present evaluation. Indeed, should a patch be needed in the future, it would require at least a maintenance of the eSA certificate, as required by the eSA scheme rules. However, the patch mechanism (called OS Update, or GemActivate in the present ST) is part of the TOE and as such its security is assessed within the present evaluation.

Note related to TOE delivery

The format of the TOE components at the TOE delivery point depends on the considered life cycle scenario (Thales life cycle or alternative life cycle). See the corresponding subsections (§4.6.1 and §4.6.2) for further details.

Whatever the considered life cycle, the guides [AGD] are delivered by the Thales Technical representative:

- in form of electronic documents (*.PDF)
- via secure email (PGP ciphered)
- on a Need-To-Know basis.

4.6.1 Thales life cycle

In the Thales life-cycle, the integration of the MultiSIM M2M 4.3.0 Embedded Software into the ST33K1M5 IC is done by Thales. The life cycle is composed of 5 phases which are described in table 1. The table also mentions the actor(s) involved in each phase, as well as the associated location(s).

The loading of the MultiSIM M2M 4.3.0 Embedded Software occurs during phase c, after which the IC loading service is locked and no more available. The TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of phase c, as illustrated in figure 3. At this stage, the TOE is entirely built and protects itself through the security mechanisms implemented in the operating system and the underlying IC.

Note: as mentioned in section 4.4, the TOE has an OS Update capability. Should a patch be needed once the TOE is on the field, its development and validation will be done by Thales during phase a, and patch deployment will be performed by the OEM during phase e. The corresponding steps are highlighted in grey color in table 1.

<table>
<tr><th>Phase</th><th>Designation</th><th colspan="2">Description / comments</th><th>Actor</th><th>Location</th></tr>
<tr><td rowspan="5">a</td><td rowspan="5">eUICC platform development</td><td colspan="2">IC development: Development of the ST33K1M5 IC and associated tools.</td><td><b>STMicroelectronics</b>
- Secure environment -</td><td>Development site(s) stated in the ST33K1M5 CC certificate</td></tr>
<tr><td colspan="2" rowspan="2">MultiSIM M2M 4.3.0 Embedded Software development and validation.
[OS UPDATE] Patch development and validation</td><td><b>Thales</b> R&D team
- secure environment -</td><td><b>Thales La Ciotat</b> site
<b>Thales Singapore</b> site</td></tr>
<tr><td><b>Thales</b> Crypto team
- secure environment -</td><td><b>Thales Singapore</b> site</td></tr>
<tr><td rowspan="2">Industrialization</td><td>Test scripts development for phase b (step b2)</td><td><b>Thales</b> Product Engineering Team
- secure environment -</td><td><b>Thales Gémenos</b> site
<b>Thales Singapore</b> site</td></tr>
<tr><td>Loading and pre-perso scripts development for phase c</td><td><b>Thales</b> CPC team
- secure environment -</td><td><b>Thales Tczew</b> site</td></tr>
<tr><td rowspan="2">b</td><td rowspan="2">eUICC platform storage, pre-perso, test</td><td colspan="2">Step b1: Manufacturing of ST33K1M5 integrated circuits
MFF2 packaging (for “Auto-grade” and optionally “Indus-grade” TOE)</td><td><b>STMicroelectronics</b>
- Secure environment -</td><td>Manufacturing site(s) stated in the ST33K1M5 CC certificate</td></tr>
<tr><td colspan="2">Step b2: SIM 2FF packaging (optionally for “Indus-grade” TOE)
Testing (whatever the format, either MFF2 or SIM 2FF)</td><td><b>Thales</b>
- Secure environment -</td><td><b>Thales Pont-Audemer</b> site
<b>Thales Curitiba</b> site</td></tr>
<tr><td>c</td><td>eUICC platform storage, pre-perso, test</td><td colspan="2">Loading of the MultiSIM M2M 4.3.0 Embedded Software into the ST33K1M5 IC, Pre-personalization and Testing.</td><td><b>Thales</b>
- Secure environment -</td><td><b>Thales Pont-Audemer</b> site
<b>Thales Cuernavaca</b> site
<b>Thales Shanghai</b> site</td></tr>
<tr><td>d</td><td>eUICC personalization</td><td colspan="2">Personalization, addition of applications (profiles / ISD-P)
Final tests</td><td><b>eUICC Personalizer:</b> Thales or any other accredited company
- Secure environment -</td><td>eUICC Personalizer site</td></tr>
<tr><td rowspan="3">e</td><td rowspan="3">eUICC operational usage</td><td colspan="2">eUICC device integration and registration</td><td><b>Original Equipment Manufacturer (OEM)</b></td><td>OEM site(s) which manufacture the targeted M2M device</td></tr>
<tr><td colspan="2">eUICC usage and eUICC remote provisioning</td><td><b>Owner of the M2M device</b></td><td>Field</td></tr>
<tr><td colspan="2">[OS UPDATE] Remote loading of patch on deployed eUICC</td><td><b>Original Equipment Manufacturer (OEM)</b></td><td>Field</td></tr>
</table>

Table 1: ‘Thales life-cycle’ phases

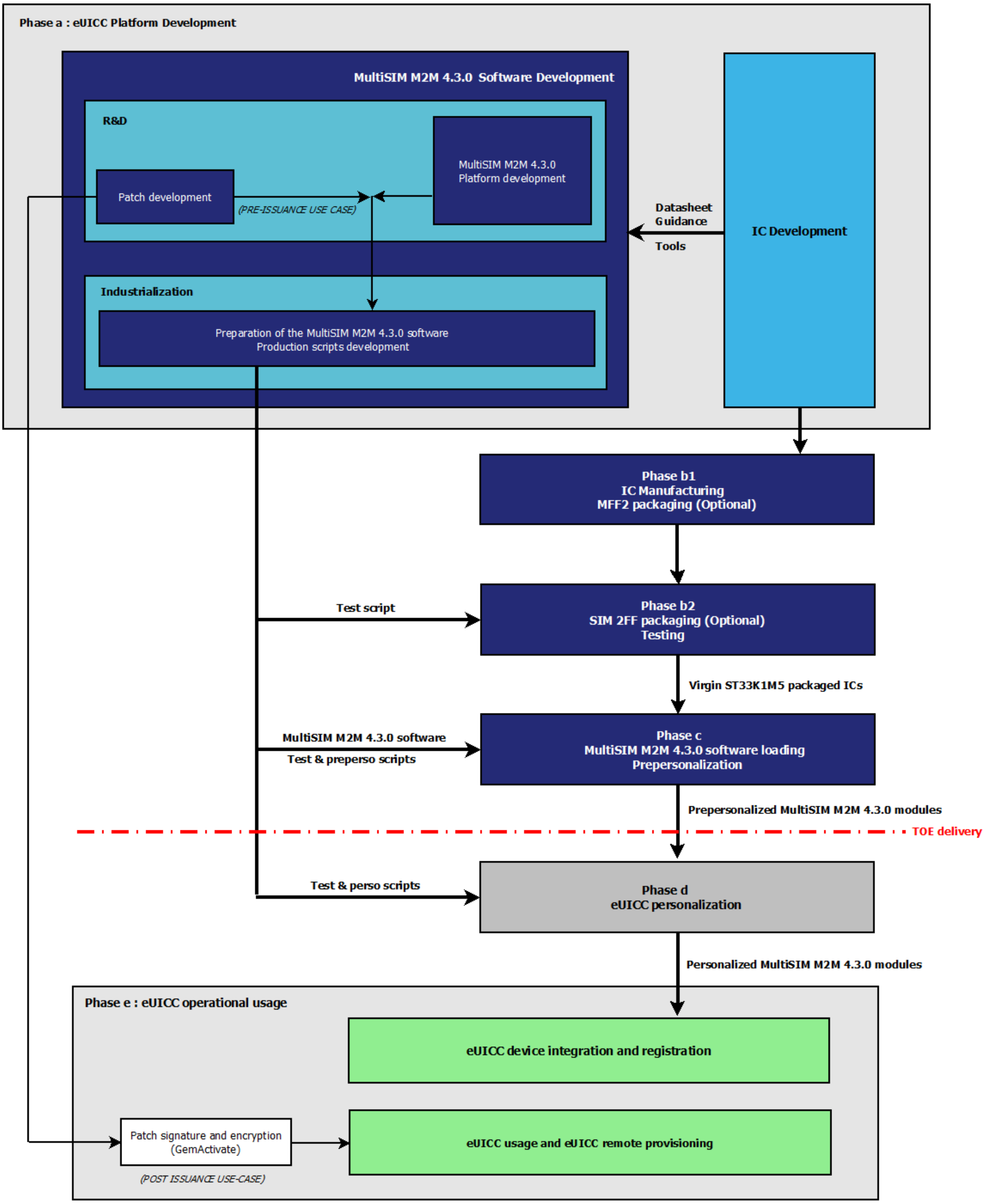

Phase a : eUICC Platform Development
MultiSIM M2M 4.3.0 Software Development
R&D
Patch development
MultiSIM M2M 4.3.0 Platform development
(PRE-ISSUANCE USE CASE)
Industrialization
Preparation of the MultiSIM M2M 4.3.0 software Production scripts development
Datasheet Guidance
Tools
IC Development
Phase b1 IC Manufacturing MFF2 packaging (Optional)
Test script
Phase b2 SIM 2FF packaging (Optional) Testing
Virgin ST33K1M5 packaged ICs
MultiSIM M2M 4.3.0 software
Test & preperso scripts
Phase c MultiSIM M2M 4.3.0 software loading Prepersonalization
Prepersonalized MultiSIM M2M 4.3.0 modules
TOE delivery
Test & perso scripts
Phase d eUICC personalization
Personalized MultiSIM M2M 4.3.0 modules
Phase e : eUICC operational usage
eUICC device integration and registration
Patch signature and encryption (GemActivate)
(POST ISSUANCE USE-CASE)
eUICC usage and eUICC remote provisioning

Figure 3: ‘Thales life-cycle’

4.6.2 *Alternative life cycle*

In the alternative life-cycle, the integration of the MultiSIM M2M 4.3.0 Embedded Software into the ST33K1M5 IC is done by an accredited manufacturing actor. The life cycle is composed of 5 phases which are described in table 2. The table also mentions the actor(s) involved in each phase, as well as the associated location(s).

The loading of the MultiSIM M2M 4.3.0 Embedded Software occurs during phase c, after which the IC loading service is locked and no more available. In this life cycle, the TOE delivery point - which determines the boundary between the ALC and AGD Common Criteria assurance classes - is put at the end of phase b, as illustrated in figure 4.

Therefore, at the TOE delivery point, the accredited manufacturing actor receives the TOE in two separate parts:

- The ST33K1M5 IC, already initialized with a dedicated Embedded Software loading key.
- The MultiSIM M2M 4.3.0 Embedded Software (ES), already encrypted with a dedicated encryption key.

The accredited manufacturing actor has no access to the MultiSIM M2M 4.3.0 Embedded Software in plaintext. The encrypted ES is sent directly to the ST33K1M5 IC which decrypts it “on-the-fly” inside the component and performs the loading process. As such, the TOE protects itself at (and after) the TOE delivery point and the integration step is performed by the accredited manufacturing actor through a “black box” process.

Note: as mentioned in section 4.4, the TOE has an OS Update capability. Should a patch be needed once the TOE is on the field, its development and validation will be done by Thales during phase a, and patch deployment will be performed by the OEM during phase e. The corresponding steps are highlighted in grey color in table 2.

Phase	Designation	Description / comments		Actor	Location
a	eUICC platform development	IC development: Development of the ST33K1M5 IC and associated tools.		**STMicroelectronics** - Secure environment -	Development site(s) stated in the ST33K1M5 CC certificate
		MultiSIM M2M 4.3.0 Embedded Software development and validation. [OS UPDATE] Patch development and validation		**Thales** R&D team - secure environment -	**Thales La Ciotat** site **Thales Singapore** site
				Thales Crypto team - secure environment -	**Thales Singapore** site
		Industrialization	Test scripts development for phase b (step b2)	**Thales** Product Engineering Team - secure environment -	**Thales Gémenos** site **Thales Singapore** site
			Loading and pre-perso scripts development for phase c	**Thales** CPC team - secure environment -	**Thales Tczew** site
b	eUICC platform storage, pre-perso, test	Step b1: Manufacturing of ST33K1M5 integrated circuits MFF2 packaging (for “Auto-grade” and optionally “Indus-grade” TOE)		**STMicroelectronics** - Secure environment -	Manufacturing site(s) stated in the ST33K1M5 CC certificate
		Step b2: SIM 2FF packaging (optionally for “Indus-grade” TOE) Testing (whatever the format, either MFF2 or SIM 2FF)		**Thales** - Secure environment -	**Thales Pont-Audemer** site **Thales Curitiba** site
c	eUICC platform storage, pre-perso, test	Loading of the MultiSIM M2M 4.3.0 Embedded Software into the ST33K1M5 IC, Pre-personalization and Testing.		**Accredited manufacturing actor** - Secure environment -	Accredited manufacturing actor site
d	eUICC personalization	Personalization, addition of applications (profiles / ISD-P) Final tests		**eUICC Personalizer:** Thales or any other accredited company - Secure environment -	eUICC Personalizer site
e	eUICC operational usage	eUICC device integration and registration		**Original Equipment Manufacturer (OEM)**	OEM site(s) which manufacture the targeted M2M device
		eUICC usage and eUICC remote provisioning		**Owner of the M2M device**	Field
		[OS UPDATE] Remote loading of patch on deployed eUICC		**Original Equipment Manufacturer (OEM)**	Field

Table 2: ‘Alternative life-cycle’ phases

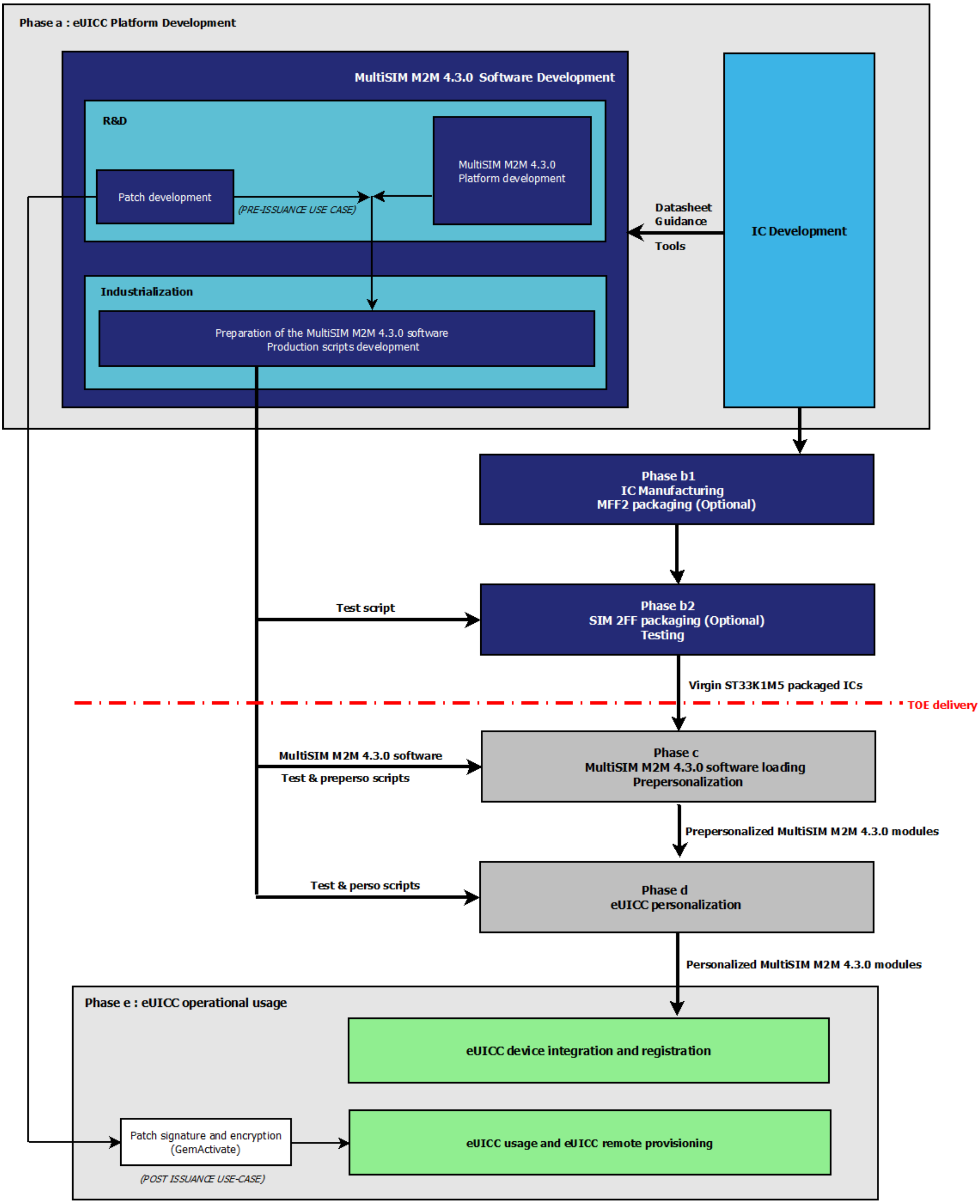

Phase a : eUICC Platform Development
MultiSIM M2M 4.3.0 Software Development
R&D
Patch development
(PRE-ISSUANCE USE CASE)
MultiSIM M2M 4.3.0 Platform development
Industrialization
Preparation of the MultiSIM M2M 4.3.0 software Production scripts development
Datasheet Guidance
Tools
IC Development
Phase b1 IC Manufacturing MFF2 packaging (Optional)
Test script
Phase b2 SIM 2FF packaging (Optional) Testing
Virgin ST33K1M5 packaged ICs
TOE delivery
MultiSIM M2M 4.3.0 software
Test & preperso scripts
Phase c MultiSIM M2M 4.3.0 software loading Prepersonalization
Prepersonalized MultiSIM M2M 4.3.0 modules
Test & perso scripts
Phase d eUICC personalization
Personalized MultiSIM M2M 4.3.0 modules
Phase e : eUICC operational usage
eUICC device integration and registration
Patch signature and encryption (GemActivate)
(POST ISSUANCE USE-CASE)
eUICC usage and eUICC remote provisioning

Figure 4: ‘Alternative life-cycle’

4.6.3 Actors of the TOE

The eUICC delivered to the end-user is embedded onto the M2M device. For this reason, the end user does not have a direct interface to the eUICC.

The MNO-SD not being part of the TOE, [PP-SGP05] (and hence, the present ST) also considers that the MNO is not an Actor of the TOE.

The only Actors having an interface to the TOE are:

- The M2M Device Manufacturer, when integrating the eUICC onto the M2M Device
- The remote provisioning Actors, during the final usage of the eUICC
- The application developers, during the final usage of the eUICC (since their applications, within the Profiles, will have interfaces with the applications of the eUICC).

4.7 AVAILABLE NON-TOE HARDWARE/SOFTWARE/FIRMWARE

The TOE of the present ST includes the complete eUICC except:

- The loaded Profiles consisting in a MNO-SD and associated applications.
- Any other Javacard application loaded on the eUICC and not belonging to a profile.

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

- M2M device: the eUICC is intended to be plugged in a M2M Device. This equipment can be a module within a car, medical equipment, camera, utility meter or any other connecting Device.
- Remote provisioning infrastructure: the eUICC interfaces with remote provisioning entities, that are responsible for the management of Profiles on the eUICC. For that purpose, the TOE communicates with remote servers of:
  - SM-SR, which provides Platform management commands and secure routing for SMDP
  - SM-DP, which provides Profile management commands and Profiles
  - MNO OTA Platforms

  The TOE requires the use of secure channels for these interfaces. The keys and/or certificates required for these operations on the TOE are either provisioned onto the eUICC prior issuance, or generated post issuance, or provisioned over-the-air post issuance, depending on the interface. Identities (in terms of certificates) rely on a single root of trust called the CI (Certificate Issuer), whose public key is stored pre-issuance on the eUICC. The remote servers and, if any, the Devices (such as a HSM) from which the keys are obtained are referred as Trusted IT products.

5 Conformance claims

Common criteria Version: This ST conforms to CC Version 3.1 [CC-1] [CC-2] [CC-3]

Conformance to CC part 2 and 3:

- This ST is CC part 2 extended with the FCS_RNG.1, FPT_EMS.1 and FIA_API.1 families. All the other SFRs have been drawn from the catalogue of requirements in CC part 2 [CC-2].
- This ST is CC part 3 conformant. It means that all SARs in that ST are based only upon assurance components in CC part 3 [CC-3].

Assurance package conformance: EAL4 augmented (EAL4+)
This ST conforms to the assurance package EAL4 augmented by ALC_DVS.2 and AVA_VAN.5.

Evaluation type
This is a composite evaluation, which relies on the ST33K1M5 chip certificate and evaluation results:

- Certification done under the NSCIB scheme
- Certification report NSCIB-CC-2300112-01-CR
- Security Target [ST_IC] strictly conformant to IC Protection Profile [PP/0084]
- Common criteria version: 3.1
- Assurance level: EAL6+ (ALC_FLR.1 augmentation)

Consequently, the composite product evaluation (i.e. the present evaluation) includes the additional composition tasks defined in the CC supporting document “Composite product evaluation for smart cards and similar devices” [CCDB].

Protection Profile (PP) conformance claims:
This Security Target claims conformance to the [PP-SGP05] protection profile. As the TOE has an OS Update capability, the PP Module ‘OS Update’ defined in Annex A of [PP-SGP05] is taken into account for the present evaluation.
The conformance type is demonstrable.

PP rationale:

- As required, the TOE of the present ST includes the lower layers of the eUICC down to the IC (i.e. the underlying GP/JCS runtime environment, the low-level operating system and the IC).
- Assets are those listed in [PP-SGP05]. As required, the [PP-JCS] assets are also considered.
- Threats, OSPs and Assumptions are those listed in [PP-SGP05].
- TOE security objectives are those listed in [PP-SGP05]. As required, OE.IC* and OE.RE* objectives in [PP-SGP05] have been turned into security objectives for the TOE.
- All the SFRs from [PP-SGP05] have been taken into account. Moreover, as required, O.IC* and O.RE* security objectives have been covered by related SFRs, mostly from [PP-GP] and [PP-JCS]. The security objectives related to the OS Update functionality have also been covered by [PP-GP] SFRs. The corresponding mapping and rationales are available in sections 9.3.1 and 9.3.2.

6 Security problem definition

6.1 ASSETS

6.1.1 [PP-SGP05] Protection Profile

The following assets are listed in [PP-SGP05] and shall be considered for the present evaluation.

User data	
D.MNO_KEYS	Keys used by MNO OTA Platform to request management operations from the ISD-P. The keys are loaded during provisioning and stored under the control of the MNO SD. To be protected from unauthorized disclosure and modification.
D.ISDR_KEYS	This Platform Management keyset is used by SM-SR to perform Platform Management functions, via its on-card representative (ISD-R). To be protected from unauthorized disclosure and modification.
D.ISDP_KEYS	This Profile Management keyset is used by SM-DP to perform Profile Management functions via its on-card representative (ISD-P). To be protected from unauthorized disclosure and modification.
D.PROFILE_NAA_PARAMS	Parameters used for network authentication, including keys. Such parameters may include for example Opc, Ri, Ci, and so on. Parameters are loaded during provisioning and stored under the control of the ISD-P. They may be transmitted to the Telecom Framework, which contains the authentication algorithms. To be protected from unauthorized disclosure and modification.
D.PROFILE_IDENTITY	The International Mobile Subscriber Identity is the user credential when authenticating on a MNO's network via an Authentication algorithm. The IMSI is a representation of the subscriber's identity and will be used by the MNO as an index for the subscriber in its HLR. Each IMSI is stored under the control of the ISD-P during provisioning. To be protected from unauthorized modification.
D.PROFILE_POL1	Data describing the Policy Control Functions in a profile. These rules are loaded during provisioning and stored under the control of the ISD-P. They are managed by the MNO OTA Platform. To be protected from unauthorized modification.
D.PROFILE_CODE	The profile applications include first and second level applications ([TS 102 221]), in particular: ▪ The MNO-SD and the Security Domains under the control of the MNO-SD (CASD, SSD) ▪ The other applications that may be provisioned within the MNO-SD (network access applications, and so on) This asset also includes, by convention, the file system of the Profile. All these applications are under the control of the MNO SD. To be protected from unauthorized modification.
TSF data	
D.TSF_CODE	The TSF Code distinguishes between: ▪ the ISD-R, ISD-Ps and ECASD ▪ the Platform code Knowledge of this code may allow bypassing the TSF. This concerns logical attacks at runtime in order to gain a read access to executable code, typically by executing an application that tries to read the memory area where a piece of code is stored. To be protected from unauthorized disclosure and modification. Application Note: this does not include applications within the MNO-SD, which are part of the user data (see D.PROFILE_CODE).
D.PSF_DATA	The data of the PSF environment, like for instance: ▪ the identifiers and privileges including smsr-id, mno-id and smdp-id, ▪ the eUICC life cycle states ▪ the provisioning status, or "ISD-P state", of the eUICC (INSTALLED, SELECTABLE, PERSONALIZED, DISABLED, ENABLED)

	- the fallback attribute (which must be "true" for one and only one Profile) The "provisioning status" is the set of data defining the provisioning lifecycle of the ISD-P, which is completely distinct from the eUICC lifecycle. The different states and authorized transitions are described in section 2.2.1.3 ISD-P of [SGP02]. This data may be partially implemented in the logic of ISD-R and the PSF code, instead of being "data" properly speaking. As a consequence, this asset is strongly linked with D.TSF_CODE. To be protected from unauthorized modification.
D.eUICC_PRIVKEY	The eUICC private key is used by the eUICC to prove its identity and generate shared secrets with remote actors. It is stored in ECASD. To be protected from unauthorized disclosure and modification
D.eUICC_CERT	A certificate issued by the EUM for a specific, individual, eUICC. This certificate can be verified using the EUM Certificate. It is stored in ECASD. To be protected from unauthorized modification.
D.CI_ROOT_PUBKEY	The CI's root public key is used to verify the certification chain of eUICC and remote actors. It is stored in ECASD. To be protected from unauthorized modification.
D.EID	The EID (eUICC-ID) uniquely identifies the eUICC. This identifier is set by the eUICC manufacturer and does not change during operational life of the eUICC. It is stored in ECASD. The EID is used as a key by SM-SRs to identify eUICCs in its database. To be protected from unauthorized modification.
D.SECRETS	This asset includes: - the shared secret used to protect the Profile download - the shared secret used to protect the new SM-SR credentials during a handover The shared secrets are generated by the ECASD when required by the ISD-R or ISD-P, then transmitted to the security domain that required the key. To be protected from unauthorized disclosure and modification.
From PP Module ‘OS Update’	
D.UPDATE_IMAGE	Also referred to as Additional Code, it is an update for the OS, as a patch. It is sent to the TOE, and possibly includes executable code, configuration data and/or image type information. To be protected from unauthorized disclosure and modification. Security aspects: - SA.CONFID-UPDATE-IMAGE (Confidentiality of Update Image): the update image must be kept confidential. This concerns the non-disclosure of the update image in the transit to the eUICC. - SA.INTEG-UPDATE-IMAGE (Integrity of Update Image): the update image must be protected against unauthorized modification. This concerns the modification of the image in transit to the eUICC.
D.TOE_IDENTIFIER	Identification data to identify the TOE. To be protected from unauthorized modification.
D.OS-UPDATE_KEY(S)	Key(s) used for OS Update. To be protected from unauthorized disclosure and modification.

6.1.2 [PP-JCS] Protection Profile

The following assets are listed in [PP-JCS]. According to [PP-SGP05] they shall also be considered for the present evaluation.

From core part	
D.APP_CODE	The code of the applets and libraries loaded on the card. To be protected from unauthorized modification.

D.APP_C_DATA	Confidentiality - sensitive data of the applications, like the data contained in an object, an array view, a static field, a local variable of the currently executed method, or a position of the operand stack. To be protected from unauthorized disclosure.
D.APP_I_DATA	Integrity sensitive data of the applications, like the data contained in an object, an array view and the PIN security attributes (PIN Try limit, PIN Try counter and State). To be protected from unauthorized modification.
D.APP_KEYS	Cryptographic keys owned by the applets. To be protected from unauthorized disclosure and modification.
D.PIN	Any end-user's PIN. To be protected from unauthorized disclosure and modification.
D.API_DATA	Private data of the API, like the contents of its private fields. To be protected from unauthorized disclosure and modification.
D.CRYPTO	Cryptographic data used in runtime cryptographic computations, like a seed used to generate a key. To be protected from unauthorized disclosure and modification.
D.JCS_CODE	The code of the Java Card System. To be protected from unauthorized disclosure and modification.
D.JCS_DATA	The internal runtime data areas necessary for the execution of the Java Card VM, such as, for instance, the frame stack, the program counter, the class of an object, the length allocated for an array, any pointer used to chain data-structures. To be protected from unauthorized disclosure or modification.
D.SEC_DATA	The runtime security data of the Java Card RE, like, for instance, the AIDs used to identify the installed applets, the currently selected applet, the current context of execution and the owner of each object. To be protected from unauthorized disclosure and modification.

6.2 USERS / SUBJECTS

6.2.1 [PP-SGP05] Protection Profile

This section distinguishes between:

- users, which are entities external to the TOE that may access its services or interfaces
- subjects, which are specific parts of the TOE performing specific operations. The subjects are subparts of the asset D.TSF_CODE.

All users and subjects are roles for the remainder of this Security Target.

Users	
U.SM-SR	Role that securely performs functions of Platform Management commands and the transport of Profile Management commands.
U.SM-DP	Role that prepares the Profiles and manages the secure download and installation of these Profiles onto the eUICC.
U.MNO-OTA	An MNO platform for remote management of UICCs and the content of Enabled MNO Profiles on eUICCs.
U.MNO-SD	A MNO-SD is a Security Domain part of the Profile, owned by the MNO, providing the Secured Channel to the MNO's OTA Platform (U.MNO-OTA). It is used to manage the content of a Profile once the Profile is enabled. A eUICC can contain more than one MNO-SD.
U.DEVICE	An equipment into which an Embedded UICC and a communication module are inserted during assembly or test equipment which is used to test the eUICC.

Subjects	
S.ISD-R	The ISD-R is the representative of the off-card entity U.SM-SR.
S.ISD-P	An ISD-P is the representative of an off-card entity U.SM-DP.
S.ECASD	The ECASD is the representative of the off-card entity CI.
S.PSF	The PSF is the (set of) application(s) with specific rights responsible for the administration of the eUICC, described in D.TSF_CODE
S.TELECOM	Set of algorithms used by Network Access Applications to authenticate the eUICC on the mobile network. The Telecom Framework is described in D.TSF_CODE.
S.OSU	OS Update provides secure functionality to update the TOE operating system with an image created by a trusted off-card entity (S.UpdateImageCreator).
S.UpdateImageCreator	The off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

6.2.2 *[PP-GP] and [PP-JCS] Protection Profiles*

Subjects are active components of the TOE that (essentially) act on the behalf of users. Relevant subjects are those mentioned in [PP-JCS] (i.e. S.ADEL, S.APPLET, S.BCV, S.CAD, S.INSTALLER, S.JCRE, S.JCVM, S.LOCAL, S.MEMBER and S.CAP_FILE)[4] plus the following ones:

S.SD	A GlobalPlatform SD representing an off-card entity on the card.
S.OPEN	It represents the GlobalPlatform Environment (OPEN) on the card. The main responsibility of the S.OPEN is to provide an API to applications, command dispatch, Application selection, (optional) logical channel management, Card Content management, memory management, and Life Cycle management. Note: S.ADEL and S.INSTALLER from [PP-JCS] are parts of S.OPEN.
S.GEMACTIVATE	GemActivate Security Domain representing a Thales administrator on the card. This entity can authorize the activation of optional services and the loading of additional code (i.e. patch) post issuance. Note: this subject corresponds to 'S.OS-DEVELOPER' in the PP-Module 'OS Update' of [PP-GP]. S.GEMACTIVATE and S.OS-DEVELOPER are aliases of the same subject. Another alias of this subject is S.UpdateImageCreator described above.

6.3 THREATS

The following threats are listed in [PP-SGP05] and shall be considered for the present evaluation.

Unauthorized Profile and Platform Management

An off-card actor or on-card application may try to compromise the eUICC by trying to perform:

- Either unauthorized Profile Management (typically accessing or modifying the content of a profile, for example altering a downloaded profile before installation, or leaking the network authentication parameters stored in the profile)
- Or unauthorized Platform Management (typically trying to disable an enabled profile).

These two generic categories break down into four specific threats:

- T.UNAUTHORIZED-PROFILE-MNG: trying to disclose/modify the content of functionality of the ISD-P or MNO-SD without authorization
- T.UNAUTHORIZED-PLATFORM-MNG: trying to disclose/modify the content or functionality of the ISD-R without authorization

[4] For the description of these [PP-JCS] subjects, see the table at the beginning of section 9.1.3.3

- T.PROFILE-MNG-INTERCEPTION: trying to forge/intercept/modify/replay commands or profiles transmitted by SM-DP or MNO-SD (either during transmission or during the loading on the eUICC)
- T.PLATFORM-MNG-INTERCEPTION: trying to forge / intercept / modify / replay commands or credentials transmitted by SM-SR (either during transmission or during the loading on the eUICC).

T.UNAUTHORIZED-PROFILE-MNG	A malicious on-card application: ▪ modifies or discloses profile data belonging to ISD-P or MNO-SD ▪ executes or modifies operations from profile applications (ISD-P, MNO-SD and applications controlled by MNO-SD) ▪ modifies or discloses the ISD-P or MNO-SD application. Such threat typically includes for example: ▪ direct access to fields or methods of the Java objects ▪ exploitation of the APDU buffer and global byte array The PP (and hence, the present ST) does not address the following cases: ▪ An application within a ISD-P tries to compromise its own MNO-SD ▪ An application within a ISD-P tries to compromise another application under the control of its own MNO-SD or ISD-P. These cases are considered the responsibility of the MNO, since they only compromise their own profile, without any side-effect on other MNO profiles. The PP (and hence, the present ST) addresses the following cases: ▪ An application within a ISD-P tries to compromise another MNO-SD or ISD-P ▪ An application within a ISD-P tries to compromise application under the control of another MNO-SD or ISD-P ▪ An application within a ISD-P tries to compromise its own ISD-P The first two cases have an impact on other MNO profiles for trivial reasons. The last case would consist, for example, in modifying the fallback attribute of the ISD-P, thus having an impact on the whole Platform Management behavior. Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*, D.PIN
T.UNAUTHORIZED-PLATFORM-MNG	An on-card application: ▪ modifies or discloses ISD-R data ▪ executes or modifies operations from ISD-R. Such a threat typically includes for example: ▪ direct access to fields or methods of the Java objects ▪ exploitation of the APDU buffer and global byte array Directly threatens the assets: D.ISDR_KEYS, D.TSF_CODE (ISD-R) NB: by altering the behavior of ISD-R, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens D.PSF_DATA and the same assets as T.UNAUTHORIZED-PROFILE-MNG.

T.PROFILE-MNG-INTERCEPTION	An actor alters or eavesdrops the transmission between eUICC and SM-DP or MNO OTA Platform, in order to: ▪ disclose, replace or modify the content of a profile during its download to the eUICC ▪ download a Profile on the eUICC without authorization ▪ replace or modify the content of a command from SM-DP or MNO OTA Platform ▪ replace or modify the content of POL1 data when updated by the MNO OTA Platform. NB: the attacker may be an on-card application intercepting transmissions to the Security Domains, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device. Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*
T.PLATFORM-MNG-INTERCEPTION	An attacker alters or eavesdrops the transmission between eUICC and SM-SR, in order to: ▪ disclose, replace or modify the SM-SR credentials transmitted during SM-SR handover ▪ replace or modify the content of a command from SM-SR. NB: the attacker may be an on-card application intercepting transmissions to the Security Domains, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device. Directly threatens the assets: D.ISDR_KEYS, D.TSF_CODE (ISD-R) NB: by altering the behavior of ISD-R, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens D.PSF_DATA and the same assets as T.UNAUTHORIZED-PROFILE-MNG.

Identity tampering

T.UNAUTHORIZED-IDENTITY-MNG	A malicious on-card application: ▪ discloses or modifies data under the control of ECASD: - discloses or modifies D.eUICC_PRIVKEY - modifies D.EID, D.eUICC_PUBKEY or D.CI_ROOT_PUBKEY - modifies the shared secrets generation methods ▪ discloses or modifies functionalities of the ECASD Such a threat typically includes for example: ▪ direct access to fields or methods of the Java objects ▪ exploitation of the APDU buffer and global byte array ▪ impersonation of an application, of the Runtime Environment, or modification of privileges of an application Directly threatens the assets: D.TSF_CODE (ECASD), D.eUICC_PRIVKEY, D.eUICC_CERT, D.CI_ROOT_PUBKEY, D.EID, D.SECRETS
T.IDENTITY-INTERCEPTION	An attacker may try to intercept credentials, either on-card or off-card, in order to: ▪ use them on another eUICC or on a simulator ▪ modify them / replace them with other credentials. This includes:

	▪ on-card interception of the shared secrets used in either SM-SR handover or profile download This does not include: ▪ off-card or on-card interception of SM-DP credentials during profile download (taken into account by T.PROFILE-MNG-INTERCEPTION) ▪ off-card or on-card interception of SM-SR credentials during SM-SR handover (taken into account by T.PLATFORM-MNG-INTERCEPTION) Directly threatens the assets: D.SECRETS

Profile cloning

T.UNAUTHORIZED-eUICC	The attacker uses a legitimate profile on an unauthorized eUICC, or on any other unauthorized support (for example a simulator or soft SIM). Directly threatens the assets: D.TSF_CODE (ECASD), D.eUICC_PRIVKEY, D.eUICC_CERT, D.CI_ROOT_PUBKEY, D.EID, D.SECRETS

Unauthorized access to the mobile network

T.UNAUTHORIZED-MOBILE-ACCESS	An on-card or off-card actor tries to authenticate on the mobile network of a MNO in place of the legitimate profile. Directly threatens the assets: D.PROFILE_NAA_PARAMS

Second level threats

T.LOGICAL-ATTACK	An on-card malicious application bypasses the PSF measures by logical means, in order to disclose or modify sensitive data when they are processed by the Platform: ▪ IC and OS software ▪ Runtime Environment (for example provided by JCS) ▪ the Platform Support Functions: o the extended GP OPEN o the Policy enforcement functions(accessing POL1) ▪ the Telecom Framework (accessing Network Authentication Parameters). An example of such a threat would consist of using buffer overflows to access confidential data manipulated by native libraries. This threat also includes cases of unauthorized code execution by applications. Directly threatens the assets: D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_POL1, D.PSF_DATA
T.PHYSICAL-ATTACK	The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (as opposed to logical) tampering means. This threat includes environmental stress, IC failure analysis, electrical probing, unexpected tearing, and side channels. That also includes the modification of the TOE runtime execution through alteration of the intended execution order of (set of) instructions through physical tampering techniques.

	Directly threatens: all assets.

Threats from PP Module 'OS Update'

T.CONFID-UPDATE-IMAGE.LOAD	**Confidentiality of Update Image – Load** The attacker discloses (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the eUICC for installation. See SA.CONFID-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, TSF data.
T.INTEG-UPDATE-IMAGE.LOAD	**Integrity of update Image - Load** The attacker modifies (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the card for installation. See SA.INTEG-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, TSF data.
T.UNAUTH-UPDATE-IMAGE.LOAD	**Load an unauthorized update** The attacker tries to upload an unauthorized update image. See SA.INTEG-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, TSF data.
T.INTERRUPT_OSU	**OS Update procedure interrupted** The attacker tries to interrupt the OS update procedure (Load Phase through activation of Additional Code) leaving the TOE in a partially functional state. Directly threatened asset(s): D.TOE_IDENTIFIER, D.UPDATE_IMAGE, TSF data.

6.4 ORGANISATIONAL SECURITY POLICIES

The following OSP is listed in [PP-SGP05] and shall be considered for the present evaluation.

OSP.LIFECYCLE	The TOE must enforce the eUICC lifecycle defined in [SGP02]. In particular: ▪ There is only one ISD-P enabled at a time ▪ The eUICC must enforce the POL1 rules in case of disabling or deletion of profile, except during the master delete: in this case, the eUICC may disable and delete the currently enabled profile, even if POL1 states that the profile cannot be disabled or deleted. Application Note: [SGP02] also includes a fallback functionality ensuring that the eUICC is able to detect a loss of connectivity, then fallback to a secure provisioning profile and notify the SM-SR. This function is not addressed by this PP (and hence is not addressed by the present ST).

6.5 SECURE USAGE ASSUMPTIONS

The following assumptions are listed in [PP-SGP05] and shall be considered for the present evaluation.

A.ACTORS	Actors of the infrastructure (CI, SM-DP, SM-SR and MNO) securely manage their own credentials and otherwise sensitive data. In particular for the overall mobile authentication mechanism defined in 3GPP TS 33.102 [23] to be secure, certain properties need to hold that are outside the scope of

	the eUICC. In particular, subscriber keys need to be strongly generated and securely managed. The following assumptions are therefore stated: ▪ The key K is randomly generated during profile preparation and is securely transported to the Authentication Centre belonging to the MNO ▪ The random challenge RAND is generated with sufficient entropy in the Authentication Centre belonging to the MNO ▪ The Authentication Centre belonging to the MNO generates unique sequence numbers SQN, so that each quintuplet can only be used once ▪ Triplets / quintuplets are communicated securely between MNOs for roaming
A.APPLICATIONS	The applications comply with [AGD-DEV-App-Basic].

6.6 Composition tasks – Security Problem Definition Part

6.6.1 *Statement of Compatibility – Threats part*

The following table (see next page) lists the relevant threats of the security target [ST_IC], and provides the link to the threats on the composite-product, showing that there is no contradiction between the two.

IC relevant threat label	IC relevant threat title	IC relevant threat content	Link to the composite-product threats
BSI.T.Leak-Inherent	Inherent Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets.	T.PHYSICAL-ATTACK
BSI.T.Phys-Probing	Physical Probing	An attacker may perform physical probing of the TOE in order (i) to disclose user data while stored in protected memory areas, (ii) to disclose/reconstruct the user data while processed or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.	T.PHYSICAL-ATTACK
BSI.T.Malfunction	Malfunction due to Environmental Stress	An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions.	T.PHYSICAL-ATTACK
BSI.T.Phys-Manipulation	Physical Manipulation	An attacker may physically modify the Security IC in order to (i) modify user data of the Composite TOE, (ii) modify the Security IC Embedded Software, (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.	T.PHYSICAL-ATTACK
BSI.T.Leak-Forced	Forced Information Leakage	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the Composite TOE as part of the assets even if the information leakage is not inherent but caused by the attacker.	T.PHYSICAL-ATTACK
BSI.T.Abuse-Func	Abuse of Functionality	An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate user data of the Composite TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the user data of the Composite TOE or the Security IC Embedded Software.	Analysis of the composite-product threats does not reveal any contradiction with this IC threat.
BSI.T.RND	Deficiency of Random Numbers	An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.	Analysis of the composite-product threats does not reveal any contradiction with this IC threat.
BSI.T.Masquerade-TOE	Masquerade the TOE	An attacker may threaten the property being a genuine TOE by producing an IC which is not a genuine TOE but wrongly identifying itself as genuine TOE sample.	T.UNAUTHORIZED-eUICC
AUG4.T.Mem-Access	Memory Access Violation	Parts of the Security IC Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by	T.LOGICAL-ATTACK

IC relevant threat label	IC relevant threat title	IC relevant threat content	Link to the composite-product threats
		the security policy of the specific application context and must be implemented by the Security IC Embedded Software.	
JIL.T.Open-Samples-Diffusion	Diffusion of open samples	An attacker may get access to open samples of the TOE and use them to gain information about the TSF (loader, memory management unit, ROM code…). He may also use the open samples to characterize the behavior of the IC and its security functionalities (for example: characterization of side channel profiles, perturbation cartography…). The execution of a dedicated security features (for example: execution of a DES computation without countermeasures or by de-activating countermeasures) through the loading of an adequate code would allow this kind of characterization and the execution of enhanced attacks on the IC.	T.PHYSICAL-ATTACK
T.Confid-Applic-Code	Specific application code confidentiality	A specific application code may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the specific application executable code is stored. The attacker executes another application to disclose code belonging to the specific application.	T.LOGICAL-ATTACK
T.Confid-Applic-Data	Specific application data confidentiality	A specific application data may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the specific application by another application. For example, the attacker executes an application that tries to read data belonging to the specific application.	T.LOGICAL-ATTACK
T.Integ-Applic-Code	Specific application code integrity	A specific application code may need to be protected against unauthorized modification. This relates to attacks at runtime to gain write access to memory area where the specific application executable code is stored and executed. The attacker executes another application that tries to alter (part of) the specific application code.	T.LOGICAL-ATTACK
T.Integ-Applic-Data	Specific application data integrity	A specific application product data may need to be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the specific application data by another application. The attacker executes an application that tries to alter (part of) the specific application data.	T.LOGICAL-ATTACK

6.6.2 *Statement of compatibility – OSPs part*

The following table lists the relevant OSPs of the security target [ST_IC], and provides the link to the OSPs related to the composite-product, showing that there is no contradiction between the two.

IC OSP label	IC OSP content	Link to the composite product
BSI.P.Process-TOE	Identification during TOE Development and Production: an accurate identification is established for the TOE. This requires that each instantiation of the TOE carries this unique identification.	No contradiction with the present evaluation; the chip traceability information participates to the composite TOE identification.
BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality: the composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation. Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.	As mentioned in section 4.6, the MultiSIM M2M 4.3.0 software is loaded during phase c of the composite TOE life cycle, after which the IC loading service is locked and no more available.
BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality: authorized user controls the usage of the loader functionality in order to protect stored and loaded user data from disclosure and manipulation.	As mentioned in section 4.6, the MultiSIM M2M 4.3.0 software is loaded during phase c of the composite TOE life cycle. Access to the Loader can only be done by an authorized actor, and is conditioned by a successful authentication.
AUG1.P.Add-Functions	Additional Specific Security Functionality: the TOE shall provide the following specific security functionality to the Security IC Embedded Software: - Triple Data Encryption Standard (TDES) - Advanced Encryption Standard (AES)	The TDES and AES hardware accelerators are used by the composite TOE cryptographic library, to provide respectively TDES and AES encryption and decryption.

6.6.3 *Statement of compatibility – Assumptions part*

The following table (see next page) lists the relevant assumptions of the security target [ST_IC], and provides the link to the assumptions related to the composite-product, showing that there is no contradiction between the two.

IC assumption label	IC assumption title	IC assumption content	IrPA	CfPA	SgPA	Link to the composite product
BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization	It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).		X	X	• 'Thales life-cycle': During phases b2 and c: CfPA (Fulfilled by the ALC composite-SARs) During phases d and e: SgPA (A.ACTORS) • 'Alternative life-cycle': During phase b2: CfPA (Fulfilled by the ALC composite-SARs) During phases c, d and e: SgPA (A.ACTORS)
BSI.A.Resp-Appl	Treatment of User Data of the Composite TOE	All user data of the Composite TOE are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.		X		O.DATA-CONFIDENTIALITY O.DATA-INTEGRITY O.RE.DATA-CONFIDENTIALITY O.RE.DATA-INTEGRITY

7 Security objectives

7.1 SECURITY OBJECTIVES FOR THE TOE

The following TOE security objectives are listed in [PP-SGP05] and shall be considered for the present evaluation.

Platform Support Functions	
O.PSF	The TOE shall provide the functionalities of the PSF (loading, installation, enabling, disabling, deletion of applications and GP registry updates) in charge of the life cycle of the whole eUICC and installed applications, as well as the corresponding authorization control. In particular, the PSF ensures that: ▪ There is only one ISD-P enabled at a time ▪ The eUICC must enforce the POL1 rules in case of disabling or deletion of a profile, except during the master delete and during ESx commands enabling and disabling Test/Emergency profiles: in this case of master delete, the eUICC may disable and delete the currently enabled profile, even if POL1 states that the profile cannot be disabled or deleted. This functionality shall rely on the Runtime Environment secure services for package loading, application installation and deletion. Application Note: The PSF will be tightly connected in practice with the rest of the TOE, which in return shall very likely rely on the PSF for the effective enforcement of some of its security functions. The Platform guarantees that only the ISD-R or the Service Providers (SM-DP, MNO) owning a Security Domain with the appropriate privilege can manage the applications on the card associated with its Security Domain. This is done accordingly with the policy POL1. The actor performing the operation must beforehand authenticate with the Security Domain.
O.eUICC-DOMAIN-RIGHTS	The TOE shall ensure that unauthorized actors shall not get access or change personalized ISD-R, ISD-P or MNO-SD keys. Modification of these Security Domains keysets is restricted to their corresponding owner (SM-SR, SM-DP, MNO OTA Platform). The TOE shall not permit the change of ECASD keyset after personalization. In the same manner, the TOE shall ensure that only the legitimate owner of each Security Domain can access or change its confidential or integrity-sensitive data, such as for instance identity data (for ECASD) or D.PROFILE_NAA_PARAMS (for ISD-P). This domain separation capability relies upon the Runtime Environment protection of applications.
O.SECURE-CHANNELS	The eUICC shall maintain secure channels between: ▪ ISD-P and SM-DP ▪ ISD-R and SM-SR ▪ MNO-SD and MNO OTA Platform. The TOE shall ensure at any time: ▪ that incoming messages are properly provided unaltered to the corresponding Security Domain ▪ that any response messages are properly returned to the off-card entity. Communications shall be protected from unauthorized disclosure, modification and replay.

	This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment and PSF (see O.PSF).
O.INTERNAL-SECURE-CHANNELS	The TOE ensures that the communication shared secrets transmitted from the ECASD to the ISD-R or ISD-P are protected from unauthorized disclosure or modification. This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment.
eUICC proof of identity	
O.PROOF_OF_IDENTITY	The TOE ensures that the eUICC is identified by a unique EID, based on the hardware identification of the eUICC. The eUICC must provide a cryptographic means to prove its identity to off-card actors, based on this EID.
Platform services	
O.OPERATE	The PSF and Telecom framework belonging to the TOE shall ensure the correct operation of their security functions.
O.API	The Platform code belonging to the TOE shall provide an API to ▪ provide atomic transaction to its services, and ▪ control the access to its services. The TOE must prevent the unauthorized use of commands.
Data protection	
O.DATA-CONFIDENTIALITY	The TOE shall avoid unauthorized disclosure of the following data when stored and manipulated by the TOE: ▪ D.SECRETS ▪ D.eUICC_PRIVKEY ▪ The secret keys which are part of the following keysets: - D.MNO_KEYS - D.ISDR_KEYS - D.ISDP_KEYS - D.PROFILE_NAA_PARAMS Application Note: amongst the components of the TOE, ▪ Platform Support Functions and Telecom Framework must protect the confidentiality of the sensitive data they process, while ▪ applications must use the protection mechanisms provided by the Runtime Environment. This objective includes resistance to side channel attacks.
O.DATA-INTEGRITY	The TOE shall avoid unauthorized modification of the following data when managed or manipulated by the TOE: ▪ Identity management data: - D.eUICC_PRIVKEY - D.eUICC_CERT - D.CI_ROOT_PUBKEY - D.EID - D.SECRETS ▪ The following keysets: - D.MNO_KEYS - D.ISDR_KEYS - D.ISDP_KEYS ▪ Profile data: - D.PROFILE_NAA_PARAMS - D.PROFILE_IDENTITY - D.PROFILE_POL1

	Application Note: amongst the components of the TOE, ▪ Platform Support Functions and Telecom Framework must protect the integrity of the sensitive data they process, while ▪ applications must use the integrity protection mechanisms provided by the Runtime Environment.
Connectivity	
O.ALGORITHMS	The eUICC shall provide a mechanism for the authentication to the mobile networks.

As the MultiSIM M2M 4.3.0 Platform is not separately certified according to [PP-JCS] or [PP-GP], the following TOE security objectives must also be considered for the present evaluation:

Underlying GP/Javacard OS and runtime environment	
O.IC.PROOF_OF_IDENTITY	The underlying IC used by the TOE is uniquely identified
O.IC.SUPPORT	The IC embedded software shall support the following functionalities: ▪ (1) It does not allow the TSFs to be bypassed or altered and does not allow access to low-level functions other than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification). ▪ (2) It provides secure low-level cryptographic processing to Platform Support Functions and Telecom Framework (S.PSF and S.TELECOM). ▪ (3) It allows the S.PSF and S.TELECOM to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection). ▪ (4) It provides a means to perform memory operations atomically for S.PSF 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.PSF	The Runtime Environment shall provide secure means for card management activities, including: ▪ load of a package file ▪ installation of a package file ▪ extradition of a package file or an application ▪ personalization of an application or a Security Domain ▪ deletion of a package file or an application ▪ privileges update of an application or a Security Domain ▪ access to an application outside of its expected availability
O.RE.SECURE-COMM	The Runtime Environment shall provide means to protect the confidentiality and integrity of applications communication. Application Note: this objective requires in particular that the runtime environment provide: ▪ an Application Firewall ▪ Cryptographic functions that applications may use to actually protect the exchanged information.
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.

Finally, the following TOE Security Objectives shall be considered (as mentioned in the PP Module 'OS Update'):

From PP Module 'OS Update'	
O.SECURE_LOAD_ACODE	**Secure loading of the Additional Code** ▪ The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. ▪ The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. ▪ During the Load Phase of an Additional Code, the TOE shall remain secure.
O.SECURE_AC_ACTIVATION	**Secure activation of the Additional Code** ▪ Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. ▪ If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE such as tearing, integrity violation, error case…), the Initial TOE shall remain in its initial state or fail secure.
O.TOE_IDENTIFICATION	**Secure identification of the TOE by the user** ▪ The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. ▪ After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.
O.CONFID-UPDATE-IMAGE.LOAD	The TOE shall ensure that the D.UPDATE_IMAGE transferred to the device is not disclosed during the installation.
O.AUTH-LOAD-UPDATE-IMAGE	The TOE shall ensure that it is only possible to load an authorized image.

7.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following security objectives for the operational environment are listed in [PP-SGP05] and shall be considered for the present evaluation.

Actors	
OE.CI	The Certificate Issuer is a trusted third-party for the purpose of authentication of the entities of the system. The CI provides certificates for the EUM, SM-SR and SM-DP. The CI must ensure the security of its own credentials.
OE.SM-SR	The SM-SR shall be a trusted actor responsible for the secure routing and the associated OTA servers. The SM-SR site must be accredited following GSMA SAS [GSMA-SAS]. The SM-SR has secure communication channels with MNOs and SM-DP. The SM-SR must ensure the security of the Platform Management Credentials received from the EUM or another SM-SR.
OE.SM-DP	The SM-DP shall be a trusted actor responsible for the data preparation and the associated OTA servers. The SM-DP site must be accredited following GSMA SAS [GSMA-SAS]. It must ensure the security of the profiles it manages and loads into the eUICC, including but not limited to: ▪ MNO keys including OTA keys (telecom keys either generated by the SM-DP or by the MNO) ▪ ISD-P keys ▪ Application Provider Security Domain keys (APSD keys) ▪ Controlling Authority Security Domain keys (CASD keys). The SM-DP must ensure that any key used in ISD-P are securely generated before they are transmitted to the eUICC. The SM-DP must ensure that any key used in ISD-P are not compromised before they are transmitted to the eUICC. The security of the ISD-P token verification keys must be ensured by a well-defined security policy that covers generation, storage, distribution, destruction and recovery. This policy is enforced by the SM-DP in collaboration with the personalizer.
OE.MNO	The MNO must be a trusted actor responsible for the mobile network and associated OTA servers (interface ES6).
Profile	
OE.APPLICATIONS	The applications shall comply with [AGD-DEV-App-Basic].
OE.MNOSD	The Security Domain U.MNO-SD must use the secure channel SCP80/81 provided by the TOE according to [SGP02].
From PP Module 'OS Update'	
OE.CONFID_UPDATE_IMAGE.CREATE	Confidentiality of Update Image – CREATE: the off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

7.3 SECURITY OBJECTIVES RATIONALE

7.3.1 *Threats, OSPs and Assumptions coverage – Mapping tables*

Threat	Security objectives
T.UNAUTHORIZED-PROFILE-MNG	O.PSF, O.eUICC-DOMAIN-RIGHTS, OE.SM-DP, OE.MNO, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURECOMM, OE.MNOSD, OE.APPLICATIONS
T.UNAUTHORIZED-PLATFORM-MNG	O.PSF, O.eUICC-DOMAIN-RIGHTS, OE.SM-SR, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM, OE.APPLICATIONS
T.PROFILE-MNG-INTERCEPTION	O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, O.RE.SECURECOMM, OE.APPLICATIONS, OE.MNOSD, OE.SM-DP, OE.MNO
T.PLATFORM-MNG-INTERCEPTION	O.SECURE-CHANNELS, O.INTERNALSECURE-CHANNELS, O.RE.SECURE-COMM, OE.APPLICATIONS, OE.SM-SR

T.UNAUTHORIZED-IDENTITY-MNG	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.IDENTITY
T.IDENTITY-INTERCEPTION	O.INTERNAL-SECURE-CHANNELS, O.RE.SECURE-COMM
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, O.IC.PROOF_OF_IDENTITY
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS
T.LOGICAL-ATTACK	O.RE.API, O.API, O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.OPERATE, O.DATACONFIDENTIALITY, O.DATA-INTEGRITY, O.RE.CODE-EXE, OE.APPLICATIONS, O.IC.SUPPORT
T.PHYSICAL-ATTACK	O.IC.SUPPORT, O.IC.RECOVERY, O.DATACONFIDENTIALITY, O.RE.DATA-CONFIDENTIALITY, O.OPERATE
T.CONFID-UPDATE-IMAGE.LOAD	O.CONFID-UPDATEIMAGE.LOAD, OE.CONFID_UPDATE_IMAGE.CREATE
T.INTEG-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE
T.UNAUTH-UPDATE-IMAGE.LOAD	O.SECURE_LOAD_ACODE, O.AUTH-LOAD-UPDATE-IMAGE
T.INTERRUPT_OSU	O.SECURE_LOAD_ACODE, O.TOE_IDENTIFICATION, O.SECURE_AC_ACTIVATION

Table 3: Threats coverage by security objectives – Mapping table

OSP	Security objectives
OSP.LIFECYCLE	O.PSF, O.RE.PSF, O.OPERATE

Table 4: OSP coverage by security objectives – Mapping table

Assumption	Security objectives
A.ACTORS	OE.CI, OE.SM-SR, OE.SM-DP, OE.MNO
A.APPLICATIONS	OE.APPLICATIONS

Table 5: Assumptions coverage by security objectives – Mapping table

7.3.2 Threats coverage – Rationale

T.UNAUTHORIZED-PROFILE-MNG

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

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

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

The authentication is supported by corresponding secure channels:

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

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.MNOSD).

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.PSF and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-SR) will access the Security Domains functions and content.
- OE.SM-SR 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 a corresponding secure channel:

- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication with SM-SR.
- These secure channels rely upon the underlying Runtime Environment, which protects the applications communications (O.RE.SECURE-COMM).

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 POL1 is transmitted by the MNO OTA Platform to its on-card representative (MNO-SD). Consequently, the TSF ensures:

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

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).

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.MNOSD).

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

T.PLATFORM-MNG-INTERCEPTION

Commands and profiles are transmitted by the SM-SR to its on-card representative (ISD-R). Consequently, the TSF ensures:

- Security of the transmission to the ISD-R (O.SECURE-CHANNELS and O.INTERNALSECURE-CHANNELS) by requiring authentication from SM-SR, 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).

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

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

T.UNAUTHORIZED-IDENTITY-MNG

O.PSF 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.

NB: No secure channel can be established to the ECASD in this version of the [PP-SGP05] Protection Profile, since the eUICC keyset renewal is not yet taken into account. Consequently, no remote actor is authorized to access ECASD content of functionality.

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).

NB: No secure channel can be established to the ECASD in this version of the [PP-SGP05] Protection Profile, since the eUICC keyset renewal is not yet taken into account. Consequently, no remote actor is authorized to access ECASD content of functionality. OE.CI ensures that the CI root will manage securely its credentials off-card.

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

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.

T.LOGICAL-ATTACK

This threat is covered by controlling the information flow between Security Domains and the Platform Support Functions, 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 and Platform Support Functions shall ensure atomic transactions.

Whenever sensitive data of the TOE are processed by applications, confidentiality and integrity must be protected at all times by the Runtime Environment (O.RE.DATACONFIDENTIALITY, O.RE.DATA-INTEGRITY).

However, these sensitive data are also be processed by the Platform Support Functions and the Telecom Framework, which are not protected by these mechanisms. Consequently:

- the TOE itself must ensure the correct operation of Platform Support Functions and Telecom Framework (O.OPERATE)
- Platform Support Functions and Telecom Framework must protect the confidentiality and integrity of the sensitive data they process, while applications must use the protection

mechanisms provided by the Runtime Environment (O.DATACONFIDENTIALITY, O.DATA-INTEGRITY)

The following objectives for the operational environment are also required:

- Prevention of unauthorized code execution by applications (O.RE.CODE-EXE)
- compliance to security guidelines for applications (OE.APPLICATIONS)

The IC embedded software supports these objectives via the objective O.IC.SUPPORT. In particular, the IC embedded software:

- provides secure low-level cryptographic processing to Platform Support Functions and Telecom Framework (S.PSF and S.TELECOM).
- allows the S.PSF 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)
- provides a means to perform memory operations atomically for S.PSF and S.TELECOM.

T.PHYSICAL-ATTACK

This threat is countered mainly by physical protections which rely on the underlying Platform.

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

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

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

O.OPERATE contributes covering this threat by ensuring that these security functions are always enforced.

T.CONFID-UPDATE-IMAGE.LOAD

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

OE.CONFID_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.

7.3.3 *OSP coverage – Rationale*

OSP.LIFECYCLE

O.PSF ensures that a blocking orphaned profile can be deleted by the SM-SR, and only by the SM-SR. This deletion capability relies on the secure application deletion mechanisms provided by O.RE.PSF.

O.PSF ensures that there is a single ISD-P enabled at every moment.

O.OPERATE contributes to this OSP by ensuring that the PSF security functions are always enforced.

7.3.4 *Assumptions coverage – Rationale*

A.ACTORS
This assumption is upheld by objectives OE.CI, OE.SM-SR, OE.SM-DP and OE.MNO, which ensure that credentials and otherwise sensitive data will be managed correctly by each actor of the infrastructure.

A.APPLICATIONS
This assumption is directly upheld by objective OE.APPLICATIONS.

7.4 COMPOSITION TASKS – OBJECTIVES PART

7.4.1 *Statement of compatibility – TOE Objectives part*

The following table (see next page) lists the relevant TOE security objectives of the security target [ST_IC], and provides the link to the composite-product TOE security objectives, showing that there is no contradiction between the two sets of objectives.

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
BSI.O.Leak-Inherent	Protection against Inherent Information Leakage	The TOE must provide protection against disclosure of confidential data stored and/or processed in the Security IC - By measurement and analysis of the shape and amplitude of signals (for example on the power, clock, or I/O lines) and - By measurement and analysis of the time between events found by measuring signals (for instance on the power, clock, or I/O lines).	O.IC.SUPPORT
BSI.O.Phys-Probing	Protection against Physical Probing	The TOE must provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the TOE. This includes protection against - measuring through galvanic contacts which is direct physical probing on the chips surface except on pads being bonded (using standard tools for measuring voltage and current) or - measuring not using galvanic contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis) with a prior reverse-engineering to understand the design and its properties and functions.	O.IC.SUPPORT
BSI.O.Malfunction	Protection against Malfunctions	The TOE must ensure its correct operation. The TOE must indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested. This is to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields.	O.IC.SUPPORT
BSI.O.Phys-Manipulation	Protection against Physical Manipulation	The TOE must provide protection against manipulation of the TOE (including its software and TSF data), the Security IC Embedded Software and the user data of the Composite TOE. This includes protection against - Reverse-engineering (understanding the design and its properties and functions), - Manipulation of the hardware and any data, as well as - Undetected manipulation of memory contents.	O.IC.SUPPORT
BSI.O.Leak-Forced	Protection against Forced Information Leakage	The Security IC must be protected against disclosure of confidential data processed in the Security IC (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker - By forcing a malfunction (refer to “Protection against Malfunction due to Environmental Stress (O.Malfunction)” and/or - By a physical manipulation (refer to “Protection against Physical Manipulation (O.Phys-Manipulation)”. If this is not the case, signals which normally do not contain significant information about secrets could become an information channel for a leakage attack.	O.IC.SUPPORT
BSI.O.Abuse-Func	Protection against Abuse of Functionality	The TOE must prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical user data of the Composite TOE, (ii) manipulate critical user data of the Composite TOE, (iii) manipulate Security IC Embedded Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.	O.IC.SUPPORT
BSI.O.Identification	TOE Identification	The TOE must provide means to store Initialization Data and Pre-personalization Data in its non-volatile memory. The Initialization Data (or parts of them) are used for TOE identification.	O.IC.PROOF_OF_IDENTITY

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
BSI.O.RND	Random Numbers	The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.	Used by the composite TOE, although there is no direct link to the composite TOE security objectives. No contradiction.
BSI.O.Cap-Avail-Loader	Capability and availability of the Loader	The TSF provides limited capability of the Loader functionality and irreversible termination of the Loader in order to protect stored user data from disclosure and manipulation.	Used by the composite TOE, although there is no direct link to the composite TOE security objectives. No contradiction.
BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the loader	The TSF provides trusted communication channel with authorized user, supports authentication of the user data to be loaded and access control for usage of the Loader functionality.	This IC security objective supports the loading of the MultiSIM M2M 4.3.0 software during phase c.
BSI.O.Authentication	Authentication to external entities	The TOE shall be able to authenticate itself to external entities. The Initialization Data (or parts of them) are used for TOE authentication verification data.	This IC security objective supports the loading of the MultiSIM M2M 4.3.0 software during phase c.
JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF	The TOE must provide protection against disclosure of confidential operations of the Security IC (loader, memory management unit…) through the use of a dedicated code loaded on open samples.	No direct link to the composite TOE security objectives, nevertheless it supports the IC global robustness and thus participates to the composite TOE resistance to attacks.
JIL.O.Secure-Load-ACode	Secure loading of the Additional Code	The Loader of the TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure. Note: concretely, the TOE manages the Additional Code as a Memory Image.	This IC security objective may be relevant in phase b1 in case the IC Manufacturer needs to patch the IC Dedicated Software.
JIL.O.Secure-AC-Activation	Secure activation of the Additional Code	Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE such as tearing, integrity violation, error case…), the Initial TOE shall remain in its initial state or fail secure.	This IC security objective may be relevant in phase b1 in case the IC Manufacturer needs to patch the IC Dedicated Software.
JIL.O.TOE-Identification	Secure identification of the TOE	The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data.	This IC security objective may be relevant in phase b1 in case the IC Manufacturer needs to

Label of the chip TOE security objective	Title of the chip TOE security objective	Content of the chip TOE security objective	Linked Composite-product TOE security objectives
		After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.	patch the IC Dedicated Software.
O.Secure-Load-AMemImage	Secure Loading of the Additional Memory Image	The Loader of the TOE shall check an evidence of authenticity and integrity of the loaded Memory Image. The Loader enforces that only the allowed version of the Additional Memory Image can be loaded after the Initial Memory Image. The Loader shall forbid the loading of an Additional Memory Image not intended to be assembled with the Initial Memory Image. Note: this objective is similar to JIL.O.Secure-Load-ACode, applied to user data (e.g. embedded software).	Not used by the composite TOE, as the loading of any patch on the MultiSIM M2M 4.3.0 Embedded Software would be managed by the GemActivate OS Update feature (and not by the ST33K1M5 Loader).
O.MemImage-Identification	Secure identification of the Memory Image	The Identification Data identifies the Initial Memory Image and Additional Memory Image. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. Storage of the Additional Memory Image and update of the Identification Data shall be performed at the same time in an Atomic way, otherwise (in case of interruption or incident which prevents this alignment), the Memory Image shall remain in its initial state or the TOE shall fail secure. The Identification Data of the Final Memory Image allows identifications of Initial Memory Image and Additional Memory Image. Note: this objective is similar to JIL.O.Secure-AC-Activation and JIL.O.TOE-Identification, applied to user data (e.g. embedded software).	Not used by the composite TOE, as the loading of any patch on the MultiSIM M2M 4.3.0 Embedded Software would be managed by the GemActivate OS Update feature (and not by the ST33K1M5 Loader).
AUG1.O.Add-Functions	Additional Specific Security Functionality	The TOE must provide the following specific security functionality to the Security IC Embedded Software: - Triple Data Encryption Standard (TDES) - Advanced Encryption Standard (AES)	Used by several composite TOE security objectives, such as e.g. O.RE.SECURE-COMM, O.SECURE_LOAD_ACODE, O.CONFID-UPDATE-IMAGE.LOAD, O.AUTH-LOAD-UPDATE-IMAGE
AUG4.O.Mem-Access	Dynamic area based Memory Access Control	The TOE must provide the Security IC Embedded Software with the capability to define dynamic memory segmentation and protection. The TOE must then enforce the defined access rules so that access of software to memory areas is controlled as required, for example, in a multi-application environment.	O.RE.SECURE-COMM, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY, O.RE.CODE-EXE
O.Firewall	Specific application firewall	The TOE shall ensure isolation of data and code between a specific application and the other applications. An application shall not read, write, compare any piece of data or code belonging to the specific application.	Analysis of the composite TOE objectives does not reveal any contradiction with this IC TOE objective.

7.4.2 *Statement of compatibility – ENV Objectives part*

The following table lists the relevant ENV security objectives of the security target [ST_IC], and provides the link to the composite-product, showing that they have been taken into account and that no contradiction has been introduced.

IC ENV security objective label	IC ENV security objective title	IC ENV security objective content	Link to the composite-product
BSI.OE.Resp-Appl	Treatment of user data of the Composite TOE	Security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant user data of the Composite TOE to unauthorized users or processes when communicating with a terminal.	Covered by TOE Security Objectives, e.g. O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.RE.DATA-CONFIDENTIALITY, O.RE.DATA-INTEGRITY
BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.	• 'Thales life-cycle': During phases b2 and c: covered by the ALC composite-SARs During phase d and e: covered by OE.CI, OE.SM-SR, OE.SM-DP, OE.MNO. • 'Alternative life-cycle': During phase b2: covered by the ALC composite-SARs During phase c, d and e: covered by OE.CI, OE.SM-SR, OE.SM-DP, OE.MNO.
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the loader	The Composite Product Manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and, if desired, terminate irreversibly the Loader after intended usage of the Loader. Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.	No contradiction with the composite TOE objectives. Note that the Loader is deactivated at the end of phase c.
BSI.OE.Loader-Usage	Secure communication and usage of the loader	The authorized user must support the trusted communication channel with the TOE by confidentiality protection and authenticity proof of the data to be loaded and fulfilling the access conditions required by the Loader.	No contradiction with composite TOE objectives.

		The authorized user must organize the maintenance transactions to ensure that the additional code (loaded as data) is able to operate as in the Final Composite TOE. The authorized user must manage and associate unique Identification to the loaded data.	
BSI.OE.TOE-Auth	External entities authenticating of the TOE	The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.	No contradiction with composite TOE objectives. Note that the Loader is deactivated at the end of phase c.
OE.Composite-TOE-Id	Composite TOE identification	The composite manufacturer must maintain a unique identification of a composite TOE under maintenance.	O.TOE_IDENTIFICATION
OE.TOE-Id	TOE identification	The IC manufacturer must maintain a unique identification of the TOE under maintenance.	O.IC.PROOF_OF_IDENTITY
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	If desired, the Composite Product Manufacturer will enable (or disable) irreversibly the Secure Diagnostic capability, thus enabling the IC manufacturer (or disabling everyone) to exercise the Secure Diagnostic capability.	The Secure Diagnostic capability is enabled. No contradiction with composite TOE objectives as this feature and associated security controls are in the scope of the IC certificate.
OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	The IC manufacturer must support the trusted communication channel with the TOE by fulfilling the access conditions required by the Secure Diagnostic. The IC manufacturer must manage the Secure Diagnostic transactions so that they cannot be used to disclose critical user data of the Composite TOE, manipulate critical user data of the Composite TOE, manipulate Security IC Embedded Software or bypass, deactivate, change or explore security features or security services of the TOE.	Fulfilled by STMicroelectronics. No contradiction with composite TOE objectives.

8 Extended components definition

8.1 EXTENDED FAMILY FCS_RNG – RANDOM NUMBER GENERATION

8.1.1 Description

Generation of random numbers requires that random numbers meet a defined quality metric.

Family behavior: this family defines requirements for random number generation where the random numbers are intended to be used for cryptographic purposes. The requirements address the type of the random number generator as defined in AIS 20/31 and quality of the random numbers. The classes of random number generators used in this family (DRG and PTG) are described in document [AIS31].

FCS_RNG.1 does not include a dependency to FPT_TST.1, since the ST writer might select a RNG that does not require self-test (typically, a deterministic RNG).

8.1.2 Definition

Hierarchical to: No other components.
Dependencies: No dependencies.
Management: No management activities are foreseen.
Audit: No actions are defined to be auditable.

FCS_RNG.1 Random Number Generation

FCS_RNG.1.1 The TSF shall provide a [selection: deterministic, hybrid deterministic, physical, hybrid physical] random number generator [selection: DRG.2, DRG.3, DRG.4, PTG.2, PTG.3] that implements: [assignment: list of security capabilities of the selected RNG class].

FCS_RNG.1.2 The TSF shall provide random numbers that meet [assignment: a defined quality metric of the selected RNG class].

8.2 EXTENDED FAMILY FPT_EMS – TOE EMANATION

8.2.1 Description

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations.

The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation.

Family behavior: this family defines requirements to mitigate intelligible emanations.

Component leveling: FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

8.2.2 Definition

Hierarchical to: No other components.
Dependencies: No dependencies.
Management: No management activities are foreseen.
Audit: No actions are defined to be auditable.

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

8.3 Extended Family FIA_API – Authentication Proof of Identity

8.3.1 Description

To describe the IT security functional requirements of the TOE a functional family FIA_API (Authentication Proof of Identity) of the Class FIA (Identification and authentication) is defined here. This family describes the functional requirements for the proof of the claimed identity by the TOE and enables the authentication verification by an external entity. The other families of the class FIA address the verification of the identity of an external entity by the TOE.

The other families of the Class FIA describe only the authentication verification of users' identity performed by the TOE and do not describe the functionality of the user to prove their identity. The following paragraph defines the family FIA_API in the style of the Common Criteria part 2 from a TOE point of view.

Family Behavior: this family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component leveling: FIA_API.1 Authentication Proof of Identity, provides proof of the identity of the TOE, an object or an authorized user or role to an external entity.

8.3.2 Definition

Hierarchical to: No other components.
Dependencies: No dependencies.
Management: The following actions could be considered for the management functions in FMT:

a) Management of authentication information used to prove the claimed identity.

Audit: There are no auditable events foreseen.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a [assignment: authentication mechanism] to prove the identity of the [selection: TOE, [assignment: object, authorized user or role]] to an external entity.

9 Security requirements

9.1 SECURITY FUNCTIONAL REQUIREMENTS

9.1.1 *Typographical conventions*

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

- Selections, assignments and refinements that have already been made in the [PP-SGP05], [PP-GP] and [PP-JCS] Protection Profiles are **in bold**, and the original text on which the selection, assignment or refinement has been made is not reminded.
- Selections, assignments and refinements made in this ST are **<u>in bold and underlined</u>**, and the PP original text on which the selection or assignment has been made is indicated in a footnote.
- Iteration operations on SFR components are denoted by showing a slash "/" and the iteration indicator after the SFR component identifier.

9.1.2 *[PP-SGP05] Protection Profile*

9.1.2.1 *Introduction*

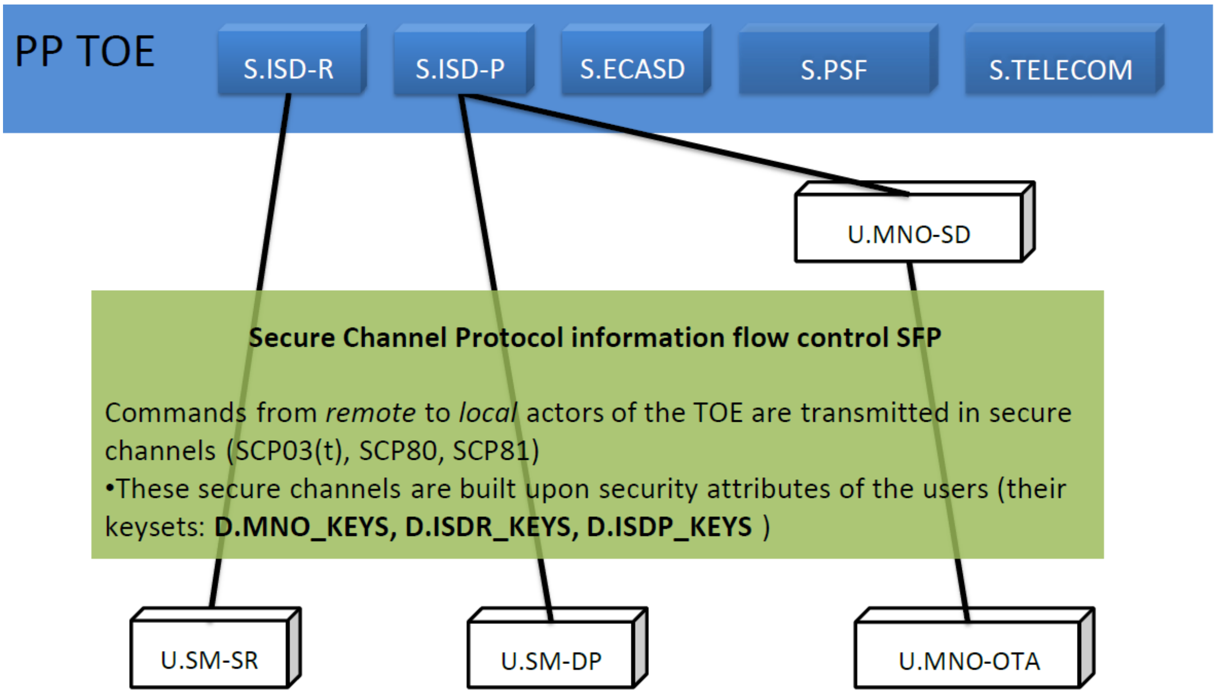
The following security policies are defined:

- Secure Channel Protocol information flow control SFP
- Platform services information flow control SFP
- ISD-R access control SFP
- ISD-P access control SFP
- ECASD content access control SFP

All roles used in security policies are defined either as users or subjects in section 6.2.1. A role is defined as a user if it does not belong to the TOE, or as a subject if it is a part of the TOE.

Users can be remote (U.SM-SR, U.SM-DP, U.MNO OTA Platform) or local (U.MNO-SD, which is an application on the eUICC).

Secure Channel Protocol information flow control SFP



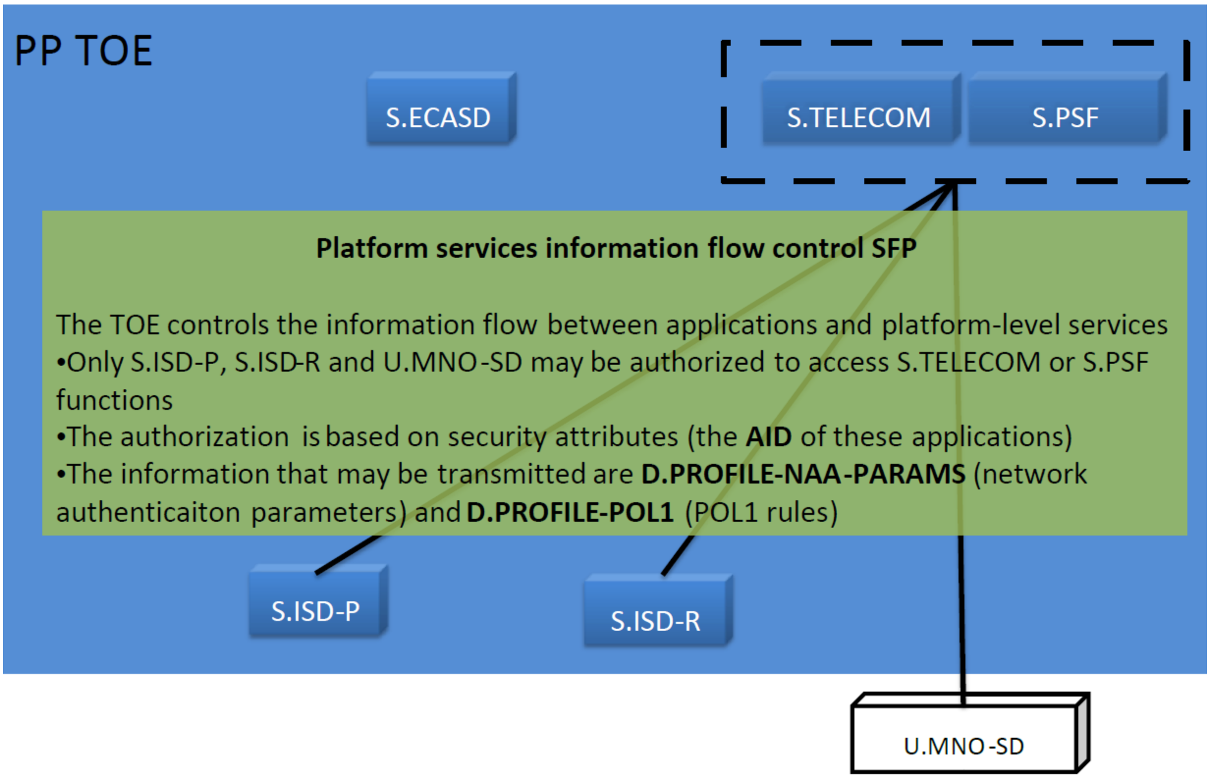
Secure Channel Protocol information flow control SFP

Commands from *remote* to *local* actors of the TOE are transmitted in secure channels (SCP03(t), SCP80, SCP81)

•These secure channels are built upon security attributes of the users (their keysets: **D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS**)

The eUICC shall support SCP03(t), SCP80, SCP81.

Platform services information flow control SFP



Platform services information flow control SFP

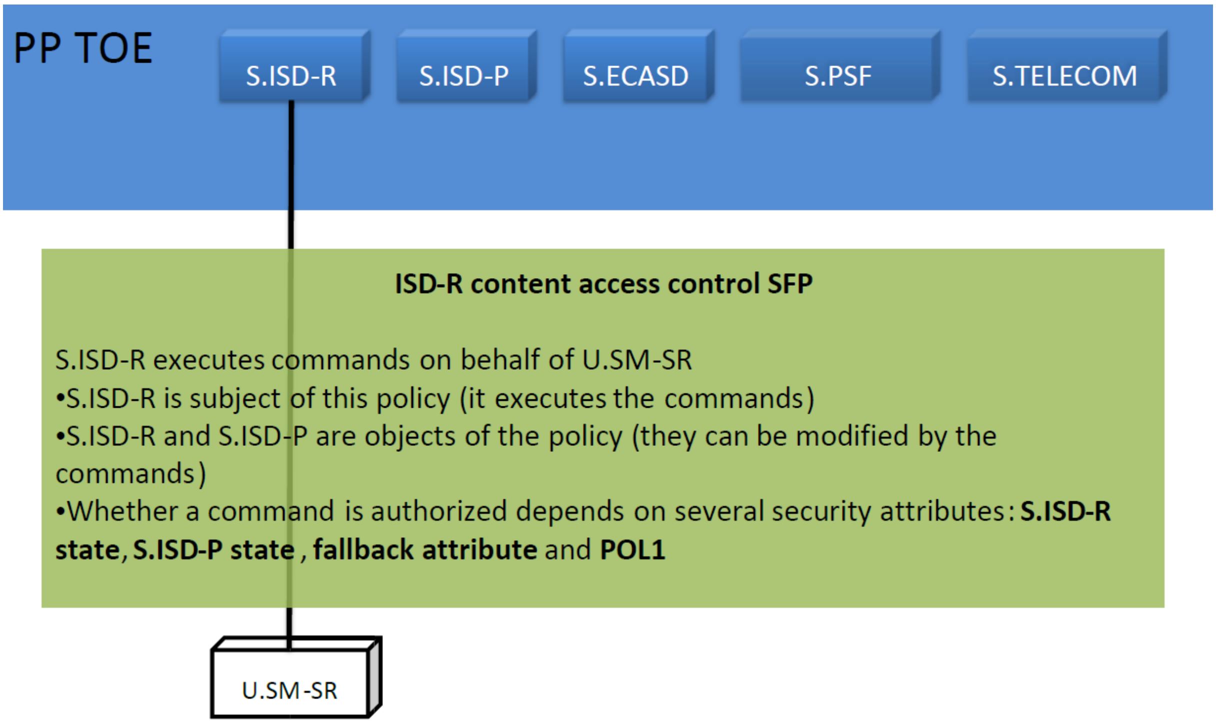
The TOE controls the information flow between applications and platform-level services

•Only S.ISD-P, S.ISD-R and U.MNO-SD may be authorized to access S.TELECOM or S.PSF functions

•The authorization is based on security attributes (the **AID** of these applications)

•The information that may be transmitted are **D.PROFILE-NAA-PARAMS** (network authenticaiton parameters) and **D.PROFILE-POL1** (POL1 rules)

ISD-R access control SFP

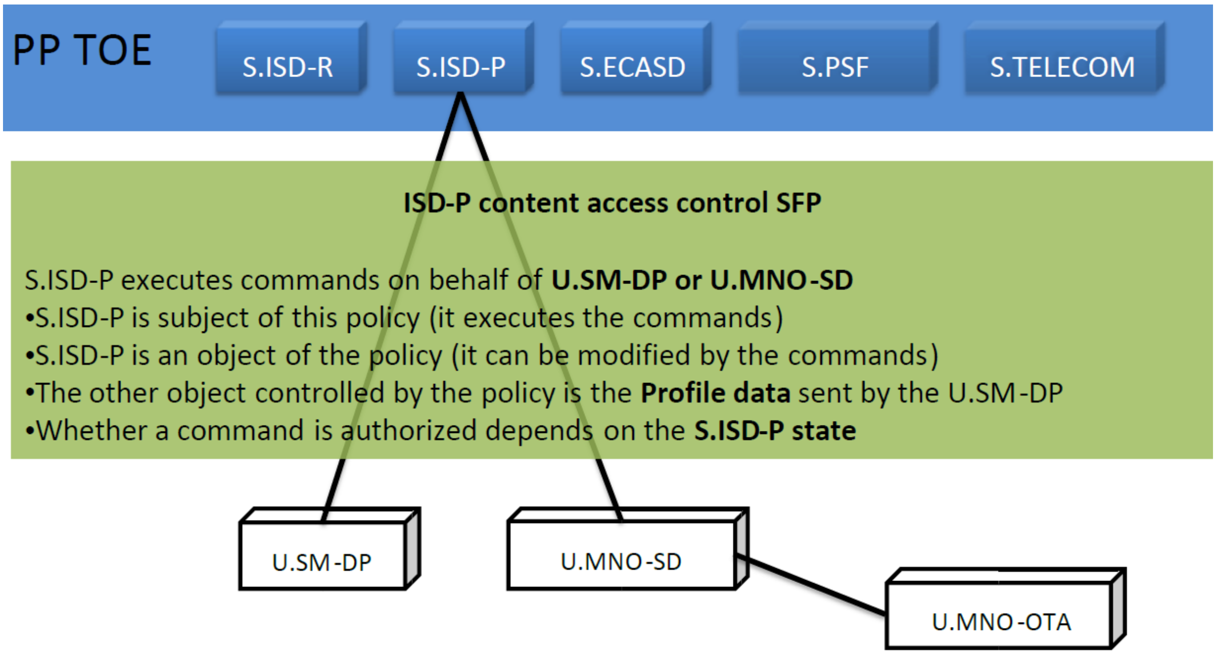


ISD-R content access control SFP

S.ISD-R executes commands on behalf of U.SM-SR

- S.ISD-R is subject of this policy (it executes the commands)
- S.ISD-R and S.ISD-P are objects of the policy (they can be modified by the commands)
- Whether a command is authorized depends on several security attributes: **S.ISD-R state**, **S.ISD-P state**, **fallback attribute** and **POL1**

ISD-P access control SFP

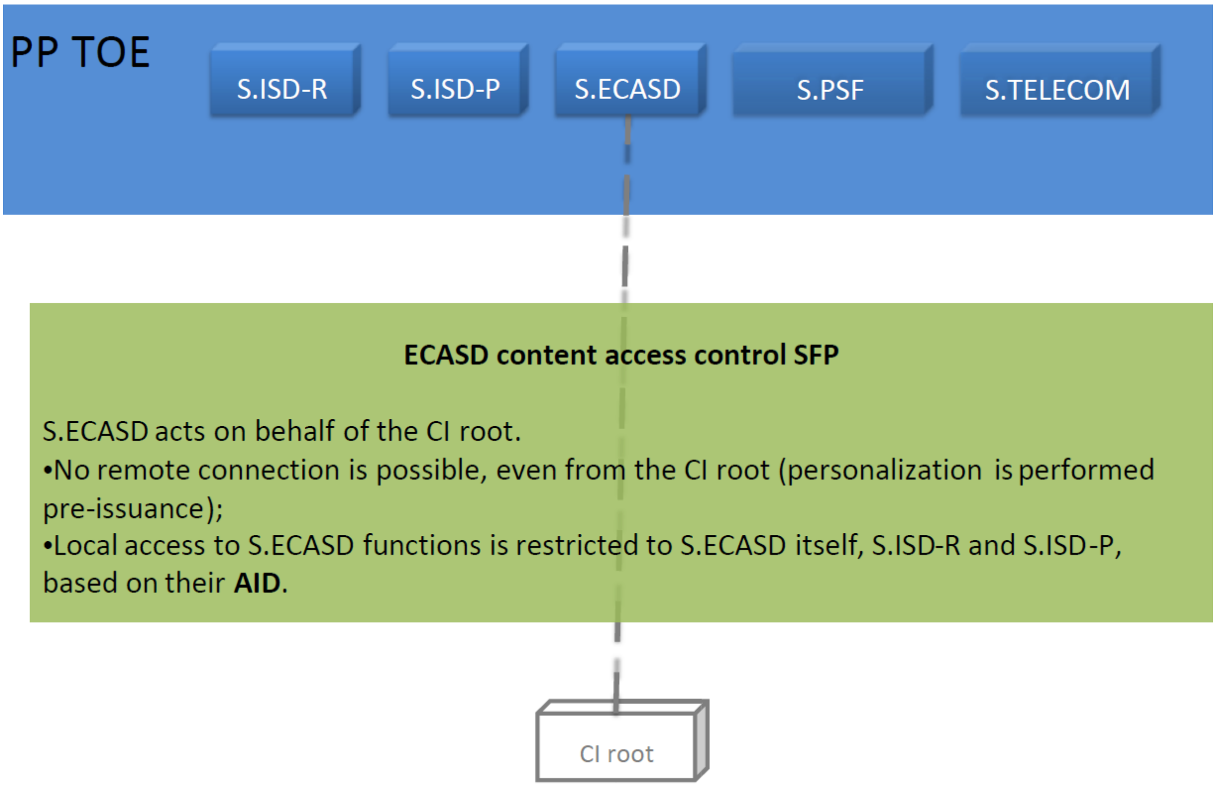


ISD-P content access control SFP

S.ISD-P executes commands on behalf of **U.SM-DP or U.MNO-SD**

- S.ISD-P is subject of this policy (it executes the commands)
- S.ISD-P is an object of the policy (it can be modified by the commands)
- The other object controlled by the policy is the **Profile data** sent by the U.SM-DP
- Whether a command is authorized depends on the **S.ISD-P state**

ECASD content access control SFP



ECASD content access control SFP

S.ECASD acts on behalf of the CI root.

•No remote connection is possible, even from the CI root (personalization is performed pre-issuance);

•Local access to S.ECASD functions is restricted to S.ECASD itself, S.ISD-R and S.ISD-P, based on their **AID**.

Security attributes used in SFRs

Security attribute	Details	Relationship to assets
AID	The AID is an identifier for the applications in the JCS runtime environment.	The AID belongs to the runtime environment. It is a part of D.SEC_DATA described in section 6.1
S.ISD-R state	The state of the subject S.ISD-R. The possible value for this state are: CREATED, SELECTABLE, PERSONALIZED.	This attribute is a part of D.PSF_DATA described in section 6.1
S.ISD-P state	The state of the subject S.ISD-R. The possible value for this state are: CREATED, SELECTABLE, PERSONALIZED, ENABLED, DISABLED	This attribute is a part of D.PSF_DATA described in section 6.1
fallback attribute	The fallback attribute is “true” for one and only one S.ISD-P. It means that, if the TOE performs a fallback operation, this specific S.ISD-P must be enabled, while the other ones must be disabled.	This attribute is a part of D.PSF_DATA described in section 6.1
POL1	The POL1 rules are associated to a given S.ISD-P and are used by the TOE to assess whether an ISD-P disabling or deletion is authorized. POL1 may include one or several of the following rules: ▪ Disabling of this Profile is not allowed ▪ Deletion of this Profile is not allowed ▪ Profile deletion is mandatory when its state is changed to disabled	This attribute is described as D.PROFILE_POL1 in section 6.1
Keysets (D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS)	Keysets are used by the TOE to build secure channels between remote actors and their local counterparts on the eUICC.	These attributes (D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS) are defined in section 6.1

Security attribute	Details	Relationship to assets
CERT.DP.ECDSA CERT.SR.ECDSA	Certificates of the U.SM-SR and U.SM-DP that are used by the TOE to authenticate these users. These certificates are signed by the CI root. The TOE can verify this signature using the CI root public key.	These attributes are not assets of this ST. The CI root public key is described as the asset D.CI_ROOT_PUBKEY in section 6.1
smsr-id smdp-id mno-id	smsr-id is the identification of the SM-SR currently in charge of eUICC management. smsr-id may change during the eUICC's lifetime. smdp-id is the identification of the SM-DP that has initially downloaded and installed the Profile. This value can be empty in case the Profile has been loaded during issuance of the eUICC, else the value is mandatory. Once this information is associated to the Profile, it remains unchanged during the Profile's lifetime. mno-id is the identification of the MNO owner of the Profile. Once this information is associated to the Profile, it remains unchanged during the Profile's lifetime.	These attributes are included in D.PSF_DATA described in section 6.1
EID	The EID is the identifier of the physical eUICC on which the TOE is implemented.	This attribute is described as D.EID in section 6.1
Connectivity Parameters	A set of data (for example SMSC address) required by the eUICC to open a communication channel (for example SMS, HTTPS) on a dedicated network.	It is part of the file system (user data) controlled by the ISD-P. Note that Connectivity Parameters could contain User and Password associated to HTTP and CAT_TP Protocols that should be restricted accordingly.

9.1.2.2 Identification and authentication

This package describes the identification and authentication measures of the TOE.

The TOE must:

- identify the remote user U.SM-SR by its smsr-id
- identify the remote user U.SM-DP by its smdp-id
- identify the remote user U.MNO-OTA by its mno-id
- identify the on-card user U.MNO-SD by its AID

The TOE must:

- authenticate U.SM-SR:
  - using CERT.SR.ECDSA (for U.SM-SR first connection, in order to create a shared SCP80/81 keyset)
  - via SCP80/81 once the keyset is initialized
- authenticate U.SM-DP:

    - using CERT.DP.ECDSA (for U.SM-DP first connection, in order to create a shared SCP03(t) keyset)
    - via SCP03(t) once the keyset is initialized
- authenticate U.MNO-OTA via SCP80/81 using the keyset loaded in the MNO profile.

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

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

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

Finally, the TOE shall provide a means to prove its identity to off-card users.

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow:

- **application selection**
- **requesting data that identifies the eUICC**
- **requesting non-sensitive configuration data (e.g. available memory size) through GET DATA command**[5].

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 external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA

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

FIA_UAU.1/EXT Timing of authentication

FIA_UAU.1.1/EXT The TSF shall allow:

- **application selection**
- **requesting data that identifies the eUICC**
- **user identification**
- **requesting non-sensitive configuration data (e.g. available memory size) through GET DATA command**[6]

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

[5] [assignment: list of additional TSF mediated actions]
[6] [assignment: list of additional TSF mediated actions]

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-SR
- U.SM-DP
- U.MNO-OTA

FCS_COP.1/AUTH_SMSR Cryptographic operation

FCS_COP.1.1/AUTH_SMSR The TSF shall perform **U.SM-SR authentication by verifying its ECDSA signature**[7] in accordance with a specified cryptographic algorithm **ECDSA**[8] and cryptographic key sizes **256 bits**[9] that meet the following:

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard), or**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639), or**
- **FRP256V1 (ANSSI ECC FRP256V1)**[10].

Application note:

- This SFR deals with the first authentication of a new SM-SR, using the public key included in its CERT.SR.ECDSA certificate (this enables the new SM-SR to create a D.ISDR_KEYS keyset to build SCP80 or SCP81 secure channels, according to FCS_CKM.1/SCP-SM).
- Once the D.ISDR_KEYS keyset is created, U.SM-SR must be authenticated according to SCP80 secure or optionally SCP81. The corresponding cryptographic operation is addressed through FCS_COP.1/GP-SCP.

FCS_COP.1/AUTH_SMDP Cryptographic operation

FCS_COP.1.1/AUTH_SMDP The TSF shall perform **U.SM-DP authentication by verifying its ECDSA signature**[11] in accordance with a specified cryptographic algorithm **ECDSA**[12] and cryptographic key sizes **256 bits**[13] that meet the following:

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard), or**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639), or**
- **FRP256V1 (ANSSI ECC FRP256V1)**[14].

Application note:

- This SFR deals with the first authentication of a new SM-DP, using the public key included in its CERT.DP.ECDSA certificate (this enables the new SM-DP to create a D.ISDP_KEYS keyset to build SCP03(t) secure channels, according to FCS_CKM.1/SCP-SM. For profile download, notice that two different session keys can be used: either SCP03t session keys or PPK (random keys) according to [SGP02] section 4.1.3.3).
- Once the D.ISDP_KEYS keyset is created, U.SM-DP must be authenticated using a SCP03(t) secure channel. The corresponding cryptographic operation is addressed through FCS_COP.1/GP-SCP.

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:

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

- **smsr-id is associated to S.ISD-R, acting on behalf of U.SM-SR**
- **smdp-id is associated to S.ISD-P, acting on behalf of U.SM-DP**
- **mno-id is associated to U.MNO-SD, acting on behalf of U.MNO-OTA.**

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

- **Initial association of smsr-id requires U.SM-SR to be authenticated via "CERT.SR.ECDSA"**
- **Initial association of smdp-id and mno-id requires U.SM-DP to be authenticated via "CERT.DP.ECDSA".**

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

- **change of smsr-id requires U.SM-SR to be authenticated via "CERT.SR.ECDSA"**
- **change of smdp-id and mno-id is not allowed.**

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

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

This SFR is related to the following commands:

- Initial association and change of the D.ISDP_KEYS keyset is performed by the ES8.EstablishISDPKeySet command
- Initial association and change of the D.ISDR_KEYS keyset is performed by the ES5.EstablishISDRKeySet command
- Initial association of the D.MNO_KEYS keyset is performed by the ES8.DownloadAndInstallation command

FIA_UAU.4/EXT Single-use authentication mechanisms

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

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

Application Note: this SFR is related to the authentication of external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow **application selection** 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.MNOSD is installed on the TOE by the U.SM-DP via the subject S.ISD-P (see "Download and install" in FDP_ACF.1/ISDP), and the binding between U.SM-DP and S.ISD-P requires authentication of U.SM-DP, as described in FIA_USB.1/EXT.
- Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user.

FIA_USB.1/MNO-SD User-subject binding

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

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

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

Application Note:

- This SFR is related to the identification of the local user U.MNO-SD.
- Being a local but external user of the TOE, the U.MNO-SD is bound to the S.ISD-P which is responsible for its installation during the "Profile download and install". This profile installation is controlled by the FDP_ACC.1/ISDP SFP. Being performed by the S.ISD-P, it requires authentication of the U.SM-DP.
- In order to perform operations such as POL1 update and connectivity parameters update, U.MNO-OTA authenticates, then sends a command to U.MNO-SD, which transmits it to S.ISDP; the operation is eventually executed by the S.ISD-P according to the FDP_ACC.1/ISDP SFP.
- The identification does not depend on direct authentication of the MNO OTA Platform, but on the authentication of the S.ISD-P: The S.ISD-P installs a profile which includes a U.MNO-SD and associated keyset.

FIA_ATD.1 User attribute definition

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

- **CERT.SR.ECDSA and smsr-id belonging to U.SM-SR**
- **CERT.DP.ECDSA and smdp-id belonging to U.SM-DP**
- **mno-id belonging to U.MNO-OTA**
- **AID belonging to U.MNO-SD**.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **cryptographic authentication mechanism based on the EID of the eUICC** to prove the identity of the **TOE** to an external entity.

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

9.1.2.3 Communication

This package describes how the TSF shall protect communications with external users.

The TSF shall enforce secure channels (FTP_ITC.1/SCP and FTP_ITC.2/SCP):

- between U.SM-SR and S.ISD-R
- between U.SM-DP and S.ISD-P
- between U.MNO-OTA and U.MNO-SD

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

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

The TSF must use cryptographic means to enforce this protection, and securely manage the associated keysets:

- generation and deletion of D.ISDP_KEYS and D.ISDR_KEYS (FCS_CKM.1/SCP-SM and FCS_CKM.4/SCP-SM)
- distribution and deletion of D.MNO_KEYS (FCS_CKM.2/SCP-MNO and FCS_CKM.4/SCPMNO)

FDP_IFC.1/SCP Subset information flow control

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

- **users/subjects:**
  - **U.SM-SR and S.ISD-R**
  - **U.SM-DP and S.ISD-P**
  - **U.MNO_OTA and U.MNO-SD**
- **information: transmission of commands**.

FDP_IFF.1/SCP Simple security attributes

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

- **users/subjects:**
  - **U.SM-SR and S.ISD-R, with security attribute D.ISDR_KEYS**
  - **U.SM-DP and S.ISD-P, with security attribute D.ISDP_KEYS**
  - **U.MNO_OTA and U.MNO-SD, with security attribute D.MNO_KEYS**
- **information: transmission of commands.**

FDP_IFF.1.2/SCP The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **The TOE shall permit communication between U.MNO_OTA and U.MNOSD in a SCP80 or SCP81 secure channel**.

FDP_IFF.1.3/SCP The TSF shall enforce **no additional information flow control SFP rules**[15].

[15] [assignment: additional information flow control SFP rules]

FDP_IFF.1.4/SCP The TSF shall explicitly authorize an information flow based on the following rules: **No additional rules**[16].

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-SR and S.ISD-R if it is not performed in a SCP80 or SCP81 secure channel through SMS, CAT_TP or HTTPS**
- **The TOE shall reject communication between U.SM-DP and S.ISD-P if it is not performed in a SCP03(t) secure channel, through the tunnel previously created between U.SM-SR and S.ISD-R.**

Application Note: More details on the secure channels can be found in [SGP02]

- For SM-SR: section 2.2.5.1 and section 2.4
- For SM-DP: section 2.2.5.2 and section 2.5
- For MNO-SD: section 2.2.5.3 and section 2.7

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 **sending notifications through ES5.HandleDefaultNotification**[17].

Application Note:

Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP_KEYS, D.ISDR_KEYS); 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-SR to open a SCP80 or SCP81 secure channel to perform Profile Download and Installation, divided in the following steps:
  - The TSF shall permit the SM-SR to transmit a ES5.CreateISDP command
  - The TSF shall then permit the SM-DP to open a SCP03(t) secure channel to transmit
    - a ES8.EstablishISDPKeySet command, followed by
    - a ES8.DownloadAndInstallation command
  - The TSF shall permit the SM-SR to transmit a ES5.EnableProfile command (optional)
- The TSF shall permit the SM-SR to open a SCP80 or SCP81 secure channel to transmit the following Platform Management commands:
  - ES5.EnableProfile
  - ES5.DisableProfile
  - ES5.DeleteProfile
  - ES5.eUICCCapabilityAudit
  - ES5.MasterDelete

[16] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[17] [assignment: list of functions for which a trusted channel is required]

    - ES5.SetFallbackAttribute
    - ES5.HandleNotificationConfirmation
- The TSF shall permit the SM-SR to open a SCP80 or SCP81 secure channel to transmit the following eUICC management commands:
    - ES5.EstablishISDRKeySet
    - ES5.FinaliseISDRhandover
    - ES5.UpdateSMSRAddressingParameters
- The TSF shall permit the SM-SR to open a SCP80 or SCP81 secure channel to modify the connectivity parameters of the SM-DP:
    - The TSF shall then permit the SM-DP to open a SCP03(t) secure channel to transmit a ES8.UpdateConnectivityParameters SCP03 command
- The TSF shall permit the remote OTA Platform to open a SCP80 secure channel to transmit the following Profile management operations:
    - ES6.UpdatePOL1byMNO
    - ES6.UpdateConnectivityParametersByMNO
- In terms of commands, the TSF shall initiate communication via the trusted channel for:
    - ES5.HandleDefaultNotification

The cryptographic operations taking place to enforce the SCP03(t), SCP80 and SCP81 secure channel are addressed through FCS_COP.1/GP-SCP.

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: **No additional rules**[18].

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-SR, U.SM-DP and U.MNO-OTA**
- **Downloaded objects from U.SM-SR, 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 **the interpretation rules specified in [SGP02] chapter 4** [19] 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:

[18] [assignment: additional importation control rules]

[19] [assignment: list of interpretation rules to be applied by the TSF]

- SM-SR commands: ES5.CreateISDP, ES5.EnableProfile, ES5.DisableProfile, ES5.DeleteProfile, ES5.eUICCCapabilityAudit, ES5.MasterDelete, ES5.SetFallbackAttribute, ES5.EstablishISDRKeySet, ES5.FinaliseISDRhandover, ES5.UpdateSMSRAddressingParameters, ES5.SetEmergencyProfileAttribute
- Downloaded objects from SM-SR: Platform management keysets
- SM-DP commands: ES8.EstablishISDPKeySet, ES8.DownloadAndInstallation, ES8.UpdateConnectivityParameters SCP03
- Downloaded objects from SM-DP: Profile management keysets, MNO profiles
- MNO commands: ES6.UpdatePOL1byMNO, ES6.UpdateConnectivityParametersByMNO
- Downloaded objects from MNO OTA Platform: POL1 data, Connectivity parameters

FDP_UCT.1/SCP Basic data exchange confidentiality

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

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

- Profiles downloaded from SM-DP
- SM-SR credentials received from SM-SR during handover

Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP_KEYS, D.ISDR_KEYS); 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

The cryptographic operations taking place to enforce confidentiality within the SCP03(t), SCP80 and SCP81 secure channel are addressed through FCS_COP.1/GP-SCP.

FDP_UIT.1/SCP Data exchange integrity

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

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

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

- Profiles downloaded from SM-DP
- SM-SR credentials received from SM-SR during handover
- Commands received from the SM-SR, SM-DP, and MNO OTA Platform
- POL1 received from the MNO OTA Platform.

Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP_KEYS, D.ISDR_KEYS); 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.

The cryptographic operations taking place to enforce integrity within the SCP03(t), SCP80 and SCP81 secure channel are addressed through FCS_COP.1/GP-SCP.

FCS_CKM.1/SCP-SM Cryptographic key generation

FCS_CKM.1.1/SCP-SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **ElGamal Elliptic Curves key agreement** and specified cryptographic key sizes **256** that meet the following: **ECKA-EG using one of the following standards:**

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

Application Note:
This key generation mechanism is used to generate:

- D.ISDP_KEYS keyset via the ES8.EstablishISDPKeySet command, using the U.SM-DP public key included in CERT.DP.ECDSA
- D.ISDR_KEYS keyset via the ES5.EstablishISDRKeySet command, using the U.SM-SR public key included in CERT.SR.ECDSA

FCS_COP.1/ECKA-EG Cryptographic operation

FCS_COP.1.1/ECKA-EG The TSF shall perform **key agreement**[20] in accordance with a specified cryptographic algorithm **ECKA-EG**[21] and cryptographic key sizes **256 bits**[22] that meet the following:

- **NIST P-256 (FIPS PUB 186-3 Digital Signature Standard), or**
- **brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639), or**
- **FRP256V1 (ANSSI ECC FRP256V1)**[23].

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 **distribution method from SCP-SGP22 (SCP03t)**[24] that meets the following: [**SGP02**][25].

Application Note:
This SFR is related to the distribution of

- D.MNO_KEYS during profile download
- Public keys distributed in the user certificates (CERT.SR.ECDSA and CERT.DP.ECDSA) or loaded pre-issuance of the TOE (D.eUICC_CERT, D.CI_ROOT_PUBKEY)

This SFR does not apply to the private keys loaded pre-issuance of the TOE (D.eUICC_PRIVKEY)

FCS_CKM.4/SCP-SM Cryptographic key destruction

FCS_CKM.4.1/SCP-SM The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key value with random bytes**[26] that meets the following: **None**[27].

Application Note: this SFR is related to the destruction of the following keys:

- D.ISDP_KEYS

[20] [assignment: list of cryptographic operations]
[21] [assignment: cryptographic algorithm]
[22] [assignment: cryptographic key sizes]
[23] [assignment: list of standards]
[24] [assignment: cryptographic key distribution method]
[25] [assignment: list of standards]
[26] [assignment: cryptographic key destruction method]
[27] [assignment: list of standards]

- D.ISDR_KEYS
- CERT.SR.ECDSA
- CERT.DP.ECDSA
- D.eUICC_CERT,
- D.eUICC_PRIVKEY,
- D.CI_ROOT_PUBKEY

FCS_CKM.4/SCP-MNO Cryptographic key destruction

FCS_CKM.4.1/SCP-MNO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key value with random bytes**[28] that meets the following: **None**[29].

Application Note: this SFR is related to the destruction of the following keys: D.MNO_KEYS

9.1.2.4 Security Domains

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

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

FDP_ACC.1/ISDR Subset access control

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

- **subjects: S.ISD-R**
- **objects: S.ISD-R and S.ISD-P**
- **operations:**
  - **Create (S.ISD-P)**
  - **Enable (S.ISD-P)**
  - **Disable (S.ISD-P)**
  - **Delete (S.ISD-P)**
  - **Set the fallback attribute (S.ISD-P)**
  - **Set the Emergency profile attribute (S.ISD-P)**
  - **Perform a capability audit (S.ISD-P)**
  - **Perform a Master Delete (S.ISD-P)**
  - **Updating the SM-SR addressing parameters (S.ISD-R)**
  - **Finalizing the SM-SR handover (S.ISD-R)**.

Application Note:
This policy describes the rules to be applied to access Platform Management operations. It covers the access to all operations by ISD-R required by sections 3.x of [SGP02].

[28] [assignment: cryptographic key destruction method]
[29] [assignment: list of standards]

It should be noted that ISD-R is subject and object of this SFP, since the SFP controls the modification of S.ISD-P and S.ISD-R by S.ISD-R.

FDP_ACF.1/ISDR Security attribute based access control

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

- **subjects: S.ISD-R**
- **objects:**
  - **S.ISD-R with security attribute "state"**
  - **S.ISD-P with security attributes "state", "fallback" and "POL1"**
- **operations:**
  - **Create (S.ISD-P)**
  - **Enable (S.ISD-P)**
  - **Disable (S.ISD-P)**
  - **Delete (S.ISD-P)**
  - **Set the fallback attribute (S.ISD-P)**
  - **Set the Emergency profile attribute (S.ISD-P)**
  - **Perform a capability audit (S.ISD-P)**
  - **Perform a Master Delete (S.ISD-P)**
  - **Updating the SM-SR addressing parameters (S.ISD-R)**
  - **Finalizing the SM-SR handover (S.ISD-R).**

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

Authorized states:

- **Enabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "DISABLED" and**
  - **the previously enabled S.ISD-P is in the state "DISABLED"**
- **Enabling a Test/Emergency Profile triggered by U.DEVICE is authorized only if**
  - **The corresponding S.ISD-P is a Test Profile and is in state “DISABLED” and Emergency profile is not already enabled or**
  - **The corresponding S.ISD-P is an Emergency Profile and is in state “DISABLED”.**
- **Disabling a S.ISD-P is authorized only if**
  - **the corresponding S.ISD-P is in the state "ENABLED" or "PERSONALIZED" and**
  - **the corresponding S.ISD-P's POL1 data allows its disabling and**
  - **the corresponding S.ISD-P's fallback attribute is not set.**
- **Disabling a Test/Emergency Profile triggered by U.DEVICE is authorized only if**
  - **The corresponding S.ISD-P is a Test or Emergency Profile and is in state “ENABLED”**
- **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 POL1 data allows its deletion and**
  - **the corresponding S.ISD-P's fallback attribute is not set or**
  - **the corresponding S.ISD-P is not a Test Profile**
- **Performing a S.ISD-P Master Delete is authorized only if**
  - **the corresponding S.ISD-P is in the state "DISABLED" and**
  - **the corresponding S.ISD-P's fallback attribute is not set and**
  - **the corresponding S.ISD-P has successfully verified the U.SM-DP token transmitted with the command.**

FDP_ACF.1.3/ISDR The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **No additional rules**[30].

FDP_ACF.1.4/ISDR The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any of the following operations is rejected if S.ISD-R is not in the state "PERSONALIZED":**

- **Creating an ISD-P**
- **Performing a capability audit on a S.ISD-P**
- **Setting the fallback attribute of a S.ISD-P**
- **Updating the SM-SR addressing parameters on the S.ISD-R**
- **Finalizing the SM-SR handover on the S.ISD-R o Any operation on S.ISD-R is forbidden to other subjects than S.ISD-R.**

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 3.x of [SGP02], that is:

- CreateISDP (Creating an ISD-P)
- EnableProfile (Enabling a profile)
- DisableProfile (Disabling a profile)
- DeleteProfile (Deleting a profile)
- eUICCCapabilityAudit (Performing a capability audit)
- MasterDelete (Performing a Master Delete)
- SetFallbackAttribute (Setting the fallback attribute)
- UpdateSMSRAddressingParameters (Updating the SM-SR addressing parameters)
- FinaliseISDRhandover (Finalizing the SM-SR handover)

Identification and authentication SFRs (FIA_*/EXT) require that these operations are only available for the legitimate user U.SM-SR after being authenticated.

FDP_ACC.1/ISDP Subset access control

FDP_ACC.1.1/ISDP The TSF shall enforce the **ISD-P access control SFP** on:

- **subjects: S.ISD-P**
- **objects:**
  - **Profile (received from U.SM-DP)**
  - **S.ISD-P**
- **operations:**
  - **Download and install (Profile)**
  - **Establish keyset (S.ISD-P)**
  - **Update the POL1 data (S.ISD-P)**
  - **Update the ISD-P connectivity parameters using a secure channel SCP03(t) as defined in FDP_IFF.1.1/SCP (S.ISD-P)**
  - **Update the ISD-P connectivity parameters by MNO (S.ISD-P)**.

Application Note: this policy describes the rules to be applied during Platform Management operations. It covers all operations by ISD-P required by sections 3.x of [SGP02]. NB: this includes Profile installation.

FDP_ACF.1/ISDP Security attribute based access control

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

- **subjects: S.ISD-P**

[30] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

- **objects:**
  - **Profile data (received from U.SM-DP)**
  - **S.ISD-P with security attribute "state"**
- **operations:**
  - **Download and install (Profile data)**
  - **Establish keyset (S.ISD-P)**
  - **Update the POL1 data (S.ISD-P)**
  - **Update the ISD-P connectivity parameters using SCP03(t) (S.ISD-P)**
  - **Update the ISD-P connectivity parameters by MNO (S.ISD-P)**.

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

- **Downloading and installing profile data is authorized only if S.ISD-P's attribute "state" is "PERSONALIZED"**
- **Establishing a D.ISDP_KEYS keyset is authorized if S.ISD-P's attribute "state" is at least "SELECTABLE"**
- **Updating POL1 is authorized only if S.ISD-P's attribute "state" is "ENABLED"**
- **Updating the ISD-P connectivity parameters by SCP03(t) is authorized only if S.ISD-P's attribute "state" is "DISABLED", "ENABLED"**
- **Updating the ISD-P connectivity parameters by MNO is authorized only if S.ISD-P's attribute "state" is "PERSONALIZED".**

FDP_ACF.1.3/ISDP The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **No additional rules**[31].

FDP_ACF.1.4/ISDP The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Any operation on Profile data or S.ISD-P is forbidden to other subjects than S.ISD-P**.

Application Note:
This policy describes the rules to be applied during profile management operations. It covers SM-DP operations described in [SGP02]:

- DownloadAndInstallation (Downloading and installing a profile)
- EstablishISDPKeySet (Establishing a D.ISDP_KEYS keyset)
- UpdateConnectivityParameters SCP03 (Updating the ISD-P connectivity parameters using SCP03(t))

Identification and authentication SFRs (FIA_*/EXT) require that these operations are only available for the legitimate user U.SM-DP after being authenticated.
It also covers the MNO operations described in [SGP02]:

- POL1 update (updating the POL1 data)
- UpdateConnectivityParametersByMNO (Connectivity Parameters Update by MNO)

Identification and authentication SFRs (FIA_*/EXT and FIA_*/MNO-SD) require that these operations are only available for the legitimate user U.MNO-OTA, via the local user U.MNOSD, after being authenticated.

FDP_ACC.1/ECASD Subset access control

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

- **subjects: S.ISD-R and S.ISD-P**
- **objects: S.ECASD**
- **operations:**
  - **execution of a ECASD function**

[31] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

  - **access to output data of these functions.**

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 and S.ISD-P, with security attribute "AID"**
- **objects: S.ECASD**
- **operations:**
  - **execution of a ECASD function:**
    - **Verification of a certificate**
    - **Generation of a random challenge (and access to the generated random challenge)**
    - **Verification of a signed random challenge using a public key**
    - **Generation of a shared secret (and access to the generated shared secret)**
  - **access to output data of these functions.**

Application Note: The length of the random challenge is 16 or 32 bytes.

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-P (resp. S.ISD-R), identified by its AID, shall be authorized to execute the following S.ECASD functions:

- **Verification of a certificate CERT.DP.ECDSA (resp. CERT.SR.ECDSA)**
- **Generation of a random challenge (and access to the generated random challenge)**
- **Verification of a signed random challenge using PK.DP.ECDSA (resp. PK.SR.ECDSA)**
- **Generation of shared secret (and access to the generated shared secret)**.

FDP_ACF.1.3/ECASD The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **The value of EID, PK.CI.ECDSA and CERT.ECASD.ECKA may be retrieved by any on-card subject without authentication**.

FDP_ACF.1.4/ECASD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **Other data controlled by S.ECASD cannot be accessed by any other subject than S.ECASD**.

9.1.2.5 Platform Services

This package describes the specific requirements applicable to the Platform Support Functions and the Telecom Framework. In particular it defines:

- FDP_IFC.1/Platform_services and FDP_IFF.1/Platform_services: the measures taken to control the flow of information between the Security Domains and Platform Support Functions (or Telecom Framework)
- FPT_FLS.1/Platform_Services: the measures to enforce a secure state in case of failures of Platform Support Functions (or Telecom Framework).

FDP_IFC.1/Platform_services Subset information flow control

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

- **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD**

  - **Platform code (S.PSF, S.TELECOM)**
- **information:**
  - **D.PROFILE-NAA-PARAMS**
  - **D.PROFILE-POL1**
- **operations:**
  - **installation of a profile**
  - **POL1 enforcement**
  - **network authentication**.

FDP_IFF.1/Platform_services Simple security attributes

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

- **users/subjects: S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)"**
- **information:**
  - **D.PROFILE-NAA-PARAMS**
  - **D.PROFILE-POL1**
- **operations:**
  - **installation of a profile**
  - **POL1 enforcement**
  - **network authentication**.

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

- **D.PROFILE-NAA-PARAMS shall be transmitted only:**
  - **by U.MNO-SD to S.TELECOM in order to execute the "Network authentication" API function**
  - **by S.ISD-P to S.PSF using the "Installation" API function**
- **D.PROFILE-POL1 shall be transmitted only by S.ISD-P to S.PSF in order to execute the "POL1 enforcement" function**.

FDP_IFF.1.3/Platform_services The TSF shall enforce **no additional information flow control SFP rules**[32].

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorize an information flow based on the following rules: **no additional rules**[33].

FDP_IFF.1.5/Platform_services The TSF shall explicitly deny an information flow based on the following rules: **no additional rules**[34].

Application Note: This SFR aims to control which subject is able to transmit POL1 or network authentication keys to the PSF and Telecom Framework.

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.PSF or S.TELECOM API specific functions:**

[32] [assignment: additional information flow control SFP rules]
[33] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[34] [assignment: rules, based on security attributes, that explicitly deny information flows]

  - **Installation of a profile**
  - **POL1 enforcement**
  - **Network authentication**
- **None**[35].

9.1.2.6 *Security management*

This package includes several supporting security functions:

- Random number generation that will be used by the ECASD (FCS_RNG.1)
- User data and TSF self-protection measures:
  - TOE emanation (FPT_EMS.1)
  - protection from integrity errors (FDP_SDI.1)
  - residual data protection (FDP_RIP.1)
  - preservation of a secure state (FPT_FLS.1)
- Security management measures:
  - Management of security attributes such as PSF data (FMT_MSA.1/PSF_DATA), POL1 and connectivity parameters (FMT_MSA.1/POL1) and keys (FMT_MSA.1/CERT_KEYS) with restrictive default values (FMT_MSA.3)
  - Management of roles and security functions (FMT_SMR.1 and FMT_SMF.1)

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **hybrid deterministic**[36] random number generator **DRG.4**[37] that implements:

(DRG.4.1) **The internal state of the RNG shall use PTRNG of class PTG.2 as random source.**

(DRG.4.2) **The RNG provides forward secrecy.**

(DRG.4.3) **The RNG provides backward secrecy even if the current internal state is known.**

(DRG.4.4) **The RNG provides enhanced forward secrecy on condition the ALG_KEYGENERATION or ALG_TRNG algorithms from [JCAPI310] RandomData class are used.**

(DRG.4.5) **The internal state of the RNG is seeded by a PTRNG of class PTG.2.**[38]

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

(DRG.4.6) **The RNG generates output for which 2^35 strings of bit length 128 are mutually different with probability greater than or equal to 1-1/(2^58).**

(DRG.4.7) **Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A.**[39]

[35] [assignment: other type of failure]
[36] [selection: deterministic, hybrid deterministic, physical, hybrid physical]
[37] [selection: DRG.2, DRG.3, DRG.4, PTG.2, PTG.3]
[38] [assignment: list of security capabilities of the selected RNG class]
[39] [assignment: a defined quality metric of the selected RNG class]

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **Side-channel information (through power consumption, electromagnetic emanations and processing timings)**[40] in excess of **IC limits**[41] enabling access to:

- **D.SECRETS**
- **D.eUICC_PRIVKEY**
- **the secret keys which are part of the following keysets:**
  - **D.MNO_KEYS**
  - **D.ISDR_KEYS**
  - **D.ISDP_KEYS**
  - **D.PROFILE_NAA_PARAMS**.

FPT_EMS.1.2 The TSF shall ensure **users**[42] are unable to use the following interface **ISO7816 Power and IO lines, IC surface**[43] to gain access to:

- **D.SECRETS**
- **D.eUICC_PRIVKEY**
- **the secret keys which are part of the following keysets:**
  - **D.MNO_KEYS**
  - **D.ISDR_KEYS**
  - **D.ISDP_KEYS**
  - **D.PROFILE_NAA_PARAMS**.

FDP_SDI.1 Stored data integrity monitoring

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

Refinement: The notion of integrity-sensitive data covers the assets of the TOE that require to be protected against unauthorized modification, including:

- **D.MNO_KEYS**
- **D.ISDR_KEYS**
- **D.ISDP_KEYS**
- **Profile data**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE_IDENTITY**
  - **D.PROFILE_POL1**
- **Identity management data:**
  - **D.eUICC_PRIVKEY**
  - **D.eUICC_CERT**
  - **D.CI_ROOT_PUBKEY**
  - **D.EID**
  - **D.SECRETS**

FDP_RIP.1 Subset residual information protection

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

[40] [assignment: types of emissions]
[41] [assignment: specified limits]
[42] [assignment: type of users]
[43] [assignment: type of connection]

- **D.SECRETS**
- **D.eUICC_PRIVKEY**
- **The secret keys which are part of the following keysets:**
    - **D.MNO_KEYS**
    - **D.ISDR_KEYS**
    - **D.ISDP_KEYS**
    - **D.PROFILE_NAA_PARAMS.**

FPT_FLS.1 Failure with preservation of secure state

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

- **failure of creation of a new ISD-P by ISD-R**
- **failure of creation of a profile by ISD-P**
- **failure of installation due to the presence of an orphaned profile**.

FMT_MSA.1/PSF_DATA Management of security attributes

FMT_MSA.1.1/PSF_DATA The TSF shall enforce the **ISD-R access control policy and ISD-P access control policy** to restrict the ability to **modify** the security attributes **mentioned in the table below** to the subjects **mentioned in the table below**:

Security attribute	Subject
ISD-P state ▪ from "INSTALLED" to "SELECTABLE" (during ISD-P creation) ▪ from "DISABLED" to "ENABLED" (during profile enabling) ▪ from "ENABLED" to "DISABLED" (during profile disabling)	S.ISD-R
ISD-P state ▪ from "SELECTABLE" to "PERSONALIZED" (during profile personalization) ▪ from "PERSONALIZED" to "DISABLED" (during profile personalization)	S.ISD-P
ISD-P state ▪ from "ENABLED" to "DISABLED" (during fall-back)	S.PSF
Fallback attribute (when setting the fallback attribute)	S.ISD-R

Refinement: the usage of a table to instantiate this SFR has been done to express the requirement in a more readable manner. The requirement itself is strictly equivalent to the [PP-SGP05] wording.

Application Note: [SGP02] includes a fallback functionality ensuring that the eUICC is able to detect a loss of connectivity, then fallback to a secure provisioning profile and notify the SM-SR. This function is not addressed by [PP-SGP05] (and hence not addressed by the present ST). However, the fallback attribute is still included, since it has an impact on the lifecycle policy and capacity to disable/delete a given profile (see FDP_ACF.1/ISDR).

FMT_MSA.1/POL1 Management of security attributes

FMT_MSA.1.1/POL1 The TSF shall enforce the **Secure Channel Protocol information flow SFP, ISD-P access control SFP and ISD-R access control SFP** to restrict the ability to **perform the operations mentioned in the table below** on **the security attributes mentioned in the table below** to **the subjects mentioned in the table below**:

Security attribute	Operation	Subject
D.PROFILE_POL1	change_default	S.ISD-P, upon request of U.SM-DP via "ES8.DownloadAndInstallation"

Security attribute	Operation	Subject
D.PROFILE_POL1	query	S.ISD-R, S.ISD-P
D.PROFILE_POL1	modify	S.ISD-P, upon request of U.MNO-SD via "ES6.UpdatePOL1byMNO"
D.PROFILE_POL1	delete	S.ISD-R, upon request of U.SM-SR by "ES5.DeleteProfile"
Connectivity parameters	query	S.ISD-R, S.ISD-P

Refinement: the usage of a table to instantiate this SFR has been done to express the requirement in a more readable manner. The requirement itself is strictly equivalent to the [PP-SGP05] wording.

FMT_MSA.1/CERT_KEYS Management of security attributes

FMT_MSA.1.1/CERT_KEYS The TSF shall enforce the **Secure Channel Protocol information flow SFP, ISD-P access control SFP, ISD-R access control SFP and ECASD content access control SFP** to restrict the ability to **perform the operations mentioned in the table below** on **the security attributes mentioned in the table below** to **the subjects mentioned in the table below**:

Security attribute	Operation	Subject
CERT.DP.ECDSA	query	S.ISD-P
D.ISDP_KEYS	change_default	S.ISD-P, upon request of U.SM-DP via "ES8.EstablishISDPKeySet"
D.MNO_KEYS	change_default	S.ISD-P, upon request of U.SM-DP via "ES8.DownloadAndInstallation"
D.ISDP_KEYS	query	S.ISD-P
CERT.SR.ECDSA	query	S.ISD-R
D.ISDR_KEYS	change_default	S.ISD-R, upon request of U.SM-SR via "ES5.EstablishISDRKeySet"
D.ISDR_KEYS	query	S.ISD-R
D.ISDR_KEYS	delete	S.ISD-R, upon request of U.SM-SR via "ES5.FinaliseISDRhandover"
D.ISDP_KEYS and D.MNO_KEYS	delete	S.ISD-R, upon request of U.SM-SR by "ES5.DeleteProfile"
CERT.DP.ECDSA, CERT.SR.ECDSA, D.ISDP_KEYS, D.ISDR_KEYS, D.MNO_KEYS	Any other operation	No actor

Refinement: the usage of a table to instantiate this SFR has been done to express the requirement in a more readable manner. The requirement itself is strictly equivalent to the [PP-SGP05] wording.

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

FMT_MSA.3 Static attribute initialization

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

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

FMT_SMF.1 Specification of Management Functions

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

- **Secure Channel Protocol information flow control**
- **Platform services information flow control**
- **ISD-R access control**
- **ISD-P access control**
- **ECASD content access control**[44].

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles:

- **External users:**
  - **U.SM-DP**
  - **U.SM-SR**
  - **U.MNO-SD**
  - **U.MNO-OTA**
- **Subjects:**
  - **S.ISD-R**
  - **S.ISD-P**
  - **S.ECASD**
  - **S.PSF**
  - **S.TELECOM**.

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

Application Note: The roles defined here correspond to the users and subjects defined in section 6.2.1.

9.1.2.7 Mobile Network authentication

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

The TSF must implement cryptographic mechanisms for the authentication on the MNO network (FCS_COP.1/Mobile_network) and manage the keys securely (FDP_ITC.2/SCP and FCS_CKM.4/Mobile_network).

FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE, TUAK, CAVE**[45] and cryptographic key sizes **according to the corresponding standard** that meet the following:

- **MILENAGE according to standard [TS 35 206] with the following restrictions:**
  - **Only use 128-bit AES as the kernel function – do not support other choices**
  - **Allow any value for the constant OP**
  - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [TS 35 206]**
- **TUAK according to [TS 35 231] with the following restrictions:**
  - **Allow any value of TOP**
  - **Allow multiple iterations of Keccak**

[44] [assignment: list of management functions to be provided by the TSF]
[45] [selection: TUAK, other algorithm, no other algorithm]

  - **Support 256-bit K as well as 128-bit**
  - **To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.**
- **CAVE according to standard TIA TR-45.AHAG Common Cryptographic Algorithms**

Application Note: The keys used by these algorithms are distributed within the profiles during provisioning (FDP_ITC.2/SCP) and must be securely deleted (FCS_CKM.4/Mobile_network).

FCS_CKM.2/Mobile_network	Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **distribution method from SCP-SGP22 (SCP03t)**[46] that meets the following: **[SGP02]**[47].

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

FCS_CKM.4/Mobile_network	Cryptographic key destruction

FCS_CKM.4.1/Mobile_network The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key value with random bytes**[48] that meets the following: **None**[49].

9.1.3 [PP-GP] and [PP-JCS] Protection Profiles

9.1.3.1 Introduction

The SFRs in the present section have been selected from [PP-GP] and [PP-JCS], and deal with the security properties of the Javacard and GlobalPlatform TOE implementation. As such these SFRs cover the following TOE security objectives mentioned in section 7.1.1:

- O.IC.SUPPORT
- O.IC.RECOVERY
- O.RE.PSF
- O.RE.SECURE-COMM
- O.RE.API
- O.RE.DATA-CONFIDENTIALITY
- O.RE.DATA-INTEGRITY
- O.RE.IDENTITY
- O.RE.CODE-EXE

[46] [assignment: cryptographic key distribution method]
[47] [assignment: list of standards]
[48] [assignment: cryptographic key destruction method]
[49] [assignment: list of standards]

9.1.3.2 [PP-GP] Protection Profile

GlobalPlatform Card Management - Security Functional Requirements

Application note: patch management is an extension of the card management defined in GlobalPlatform since a patch is managed as a JavaCard Package, loaded as a standard executable load file and registered with specific attributes handled with GemActivate.

ELF loading

FDP_IFC.2/GP-ELF Complete information flow control

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

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

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

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

Application Note:

- This SFR replaces FDP_IFC.2/CM of [PP-JCS].
- GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively.

FDP_IFF.1/GP-ELF Complete information flow control

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

- **Subjects: S.SD, S.OPEN**
- **Information: APDU commands INSTALL and LOAD, GlobalPlatform APIs for loading and installing ELF**
- **Security attributes: ELF signature verification status, ELF AID, SD privileges, Secure Channel Security Level**[50].

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

- **S.SD implements one or more Secure Channel Protocols, namely SCP02, SCP03, SCP11, SCP80, SCP81**[51]**, each with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **S.OPEN accepts an ELF only if its integrity and authenticity has been verified.**
- **S.OPEN accepts an ELF only if its AID is not already registered by the TSF**[52]

FDP_IFF.1.3/GP-ELF The TSF shall enforce the **none**[53].

[50] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]
[51] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]
[52] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]
[53] [assignment: additional information flow control SFP rules]

FDP_IFF.1.4/GP-ELF The TSF shall explicitly authorize an information flow based on the following rules: **none**[54].

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

- **S.OPEN fails to verify the integrity and request verification of the authenticity for ELFs**
- **S.OPEN fails to verify the SD privileges.**
- **S.SD fails to verify the security level applied to protect INSTALL or LOAD commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.SD fails to unwrap INSTALL or LOAD commands.**
- **The ELF AID is already registered within the card**[55]

Application Note:

- This SFR refines and replaces FDP_IFF.1/CM of [PP-JCS].
- On receipt of INSTALL or LOAD commands, the verification by S.OPEN that the card Life Cycle State is not CARD_LOCKED or TERMINATED has been removed from this SFR. Indeed these states cannot be reached in eUICC product.
- APDUs belonging to the policy ELF Loading information flow control SFP are described in the following references:
  - For INSTALL, see [GPCS] section 11.5.
  - For LOAD, see [GPCS] section 11.6.
- The INSTALL and LOAD commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.
- The Minimum Security Level of INSTALL and LOAD is ‘AUTHENTICATED’ as defined in [GPCS] section 10.6.
- For more details about the rules to be applied to each role of INSTALL command, refer to [GPCS] sections 9.3 and 3.4.

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

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

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

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

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

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

- **Referring to Java Card rules defined in [JCVM310] and [JCRE310]: ELF loading is allowed only if, for each dependent ELF, its AID attribute is equal to a resident ELF AID attribute, and the major (minor) Version attribute associated with the dependent ELF is less than or equal to the major (minor) Version attribute associated with the resident ELF.**
- **None**[56]

Application Note:

- This SFR corresponds to FDP_ITC.2/Installer of [PP-JCS].

[54] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[55] [assignment: rules, based on security attributes, that explicitly deny information flows]
[56] [assignment: additional importation control rules]

- Java Card rules are defined in [JCVM310] sections 4.4 and 4.5 and [JCRE310] section 11.
- The TSF shall use the INSTALL data format and the LOAD data format when interpreting the user data from outside the TOE.

Data & Key Loading

FDP_IFC.2/GP-KL Complete information flow control

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

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

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

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

Application Note: GlobalPlatform's card content management APDU commands and API methods are described in [GPCS] Chapter 11 and Appendix A.1, respectively.

FDP_IFF.1/GP-KL Complete information flow control

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

- **Subjects: S.SD, S.OPEN**
- **GlobalPlatform APDU commands STORE DATA and PUT KEY, GlobalPlatform APIs for loading and storing data and keys**
- **Security attributes: Application and SD Life Cycle states, Secure Channel Security Level, SD and Application privileges**[57].

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

- **S.SD implements one or more Secure Channel Protocols, namely SCP02, SCP03, SCP11, SCP80, SCP81[58], each equipped with a complete Secure Channel Key Set.**
- **S.SD has all of the cryptographic keys required by its privileges (e.g. CLFDB, DAP, DM).**
- **An Application accepts a message only if it comes from the S.SD it belongs to.**
- **On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the S.OPEN checks that the requesting S.SD has no restrictions for personalization.**
- **S.SD unwraps STORE DATA or PUT KEY according to the Current Security Level of the current Secure Channel Session and prior to the command forwarding to the targeted Application or SD.**
- **S.OPEN verifies that the targeted application implements a personalization interface**[59]

FDP_IFF.1.3/GP-KL The TSF shall enforce the **none**[60].

[57] [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

[58] [selection: SCP02, SCP03, SCP10, SCP11, SCP21, SCP22, SCP80, SCP81]

[59] [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]

[60] [assignment: additional information flow control SFP rules]

FDP_IFF.1.4/GP-KL The TSF shall explicitly authorize an information flow based on the following rules: **none**[61].

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

- **S.OPEN fails to verify the Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to unwrap STORE DATA or PUT KEY.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **S.SD fails to set the security level (integrity and/or confidentiality), to apply to the next incoming command and/or next outgoing response.**
- **S.OPEN fails to verify that the targeted application implements a personalization interface.**[62]

Application Note:

- On receipt of a request to forward STORE DATA or PUT KEY commands to an Application, the verification by S.OPEN that the card Life Cycle State is not CARD_LOCKED or TERMINATED has been removed from this SFR. Indeed these states cannot be reached in eUICC product.
- APDUs belonging to the Data & Key Loading information flow control SFP are described in the following references:
  - For PUT KEY, see [GPCS] section 11.8.
  - For STORE DATA, see [GPCS] section 11.11.
- The PUT KEY and STORE DATA commands must only be issued within a Secure Channel Session; the levels of security for these commands depend on the security level defined in the EXTERNAL AUTHENTICATE command.
- The Minimum Security Level of PUT KEY and STORE DATA is 'AUTHENTICATED' as defined in [GPCS] section 10.6.
- For more details about Key Access Conditions, Data and Key Management, refer to [GPCS] sections 7.5.2 and 7.6.

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

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

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

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

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

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

- **The algorithms and key sizes of the imported keys shall be supported by the eUICC**
- **The Key Identifier (Key ID) of the imported keys shall be in an allowed range as specified in section 4 of [CIC]**[63]

Application Note:

- The algorithms and key sizes of the imported keys shall be supported by the Card as specified in [GPCS] Appendices B and C.
- PUT KEY and STORE DATA are described in [GPCS] sections 11.8 and 11.11.

[61] [assignment: rules, based on security attributes, that explicitly authorize information flows]
[62] [assignment: rules, based on security attributes, that explicitly deny information flows]
[63] [assignment: additional importation control rules]

Secure Communication

The purpose of an SCP is to authenticate the on-card and off-card entities and to protect the data exchanged between them with regard to Authenticity, Integrity, and/or Confidentiality.

The Secure Communication requirements cover all the SCPs defined by GlobalPlatform which are supported by the TOE:

- The symmetric key Secure Channel Protocol '02' defined in [GPCS], using 3DES cryptography
- The symmetric key Secure Channel Protocol '03' defined in [Amd D] includes services similar to SCP02; however, it uses AES rather than DES cryptography.
- The asymmetric key Secure Channel Protocol '11' defined in [Amd F] offers authentication services using an ECC-based Public Key Infrastructure (PKI) and secure messaging protection of commands and responses based on SCP03.
- The Secure Channel Protocol '80' supports the Over-The-Air security scheme defined in [TS 102 225], [TS 102 226].
- The Secure Channel Protocol '81' defined in [Amd B] supports an Over-The-Air security scheme based on the usage of both HTTP and Pre Shared Key TLS protocols.

APDU commands belonging to SCPs are defined in the following references:

- SCP02: [GPCS] Annex E
- SCP03: [Amd D] section 7
- SCP11: [Amd F] section 6
- SCP80: [TS 102 225] and [TS 102 226]
- SCP81: [Amd B]

The following references give details about the rules to be applied to SCPs:

- Rules that apply to all Secure Channel Protocols as defined in [GPCS] Chapter 10.
- Rules for handling Security Levels in [GPCS] section 10.6
- SCP02 protocol rules as defined in [GPCS] section E.1.6
- SCP03 protocol rules as defined in [Amd D] section 5.6
- SCP11 protocol rules as defined in [Amd F] section 4.8
- SCP80 protocol rules as defined in [TS 102 225] and [TS 102 226]
- SCP81 protocol rules as defined in [Amd B] section 3.

FCS_CKM.1/GP-SCP Cryptographic key generation

FCS_CKM.1.1/GP-SCP The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **as listed in table 6**[64] and specified cryptographic key sizes **as listed in table 6**[65] that meet the following: **the standards listed in table 6**[66].

SCP protocol	Cryptographic algorithm	Cryptographic key sizes	Standard
SCP02	TDES 2-keys	112 bits	[GPCS] section E.4.1
SCP03	AES	128, 192, 256 bits	[Amd D] section 6.2.1
SCP11	AES	128, 192, 256 bits	[Amd F] section 5.2
SCP81	TDES 3-keys	168 bits	[Amd B] section 3.3.2
SCP81	AES	128 bits	[Amd B] section 3.3.2

Table 6: Session key generation covering the supported SCPs

Application note: this SFR deals with the generation of the session keys which are used by the SCPs supported by the TOE.

[64] [assignment: cryptographic key generation algorithm]
[65] [assignment: cryptographic key sizes]
[66] [assignment: list of standards]

FCS_COP.1/GP-SCP Cryptographic operation

FCS_COP.1.1/GP-SCP The TSF shall perform **the cryptographic operations listed in table 7**[67] in accordance with a specified cryptographic algorithm **as listed in table 7**[68] and cryptographic key sizes **as listed in table 7**[69] that meet the following: **the standards listed in table 7**[70].

SCP Protocol	Operation	Algorithm	Key Sizes	Standards
SCP02	MAC Generation/ Verification	CMAC using TDES	112 bits	FIPS 198
SCP02	Symmetric Encryption/ Decryption	TDES in CBC mode	112 bits	NIST 800 67 NIST 800 38A
SCP02	Key Derivation	HMAC-based KDF, CMAC-based KDF using TDES	112 bits	NIST 800 108 FIPS 198
SCP03, SCP11	Symmetric Encryption/ Decryption	AES in CBC mode	128, 192, or 256 bits	FIPS 197 NIST 800 38A
SCP03	MAC Generation/ Verification	CMAC AES	128, 192, or 256 bits	NIST 800 38B
SCP03	Key Derivation	CMAC-based KDF using AES	128, 192, or 256 bits	NIST 800 108 NIST 800 38B
SCP11	Hash Computing	SHA-256, SHA-384, SHA-512	-	ISO 10118 3 FIPS 180 4
SCP80	Secure communication channel with OTA Server	TDES or AES	TDES: 112 bits AES: 128, 192, or 256 bits	TS 102 225 TS 102 226
SCP81	Secure communication channel with the Remote Administration Server	TLS_PSK_WITH_AES_128_CBC_SHA256		[Amd B] section 3.3.2

Table 7: Cryptographic Operations covering the supported SCPs

Application note:

[67] [assignment: list of cryptographic operations]
[68] [assignment: cryptographic algorithm]
[69] [assignment: cryptographic key sizes]
[70] [assignment: list of standards]

The table above lists the secure channels which are available to any application on the product (provided that their parent SD is configured to support the SCP and personalized with the corresponding keyset). The following requirements are added when considering the communication to SM-DP, SM-SR and MNO-OTA according to [SGP02]:

- The secure channels to SM-DP must be SCP03(t) secure channels. Identification of endpoints is addressed by the use of AES according to [Amd D] using the parameters defined in [SGP02] Chapter 2.5. For profile download, notice that two different session keys can be used: either SCP03t session keys or PPK (random keys) according to [SGP02] section 4.1.3.3.

- SCP80 must be provided to build secure channels to SM-SR and MNO OTA Platform. The TSF may also permit to use a SCP81 secure channel to build non-parallel secure channels and perform the same functions than the SCP80 secure channel. The identification of endpoints is addressed by:
  - For SCP80: the use of AES according to [TS 102 225] using the parameters defined in [SGP02] Chapter 2.4.3.
  - For SCP81: the use of TLS V1.2 (RFC 5246) according to [TS 102 226] using the parameters defined in [SGP02] Chapter 2.4.4 and excluding the support of session resumption extension based on RFC 4507 or its superseded RFC 5077.

GlobalPlatform Card Management: Common SFRs

FMT_MSA.1/GP Management of security attributes

FMT_MSA.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to restrict the ability to **perform the operations listed in tables 8 to 12 acting on**[71] the security attributes **mentioned in tables 8 to 12**[72] to **the authorized identified roles mentioned in tables 8 to 12**[73].

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorised Identified Roles with Privileges
DELETE Executable Load File	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Executable Load File and related Application(s)	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Application	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
DELETE Key	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
INSTALL	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
INSTALL [for personalisation]	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
LOAD	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD
PUT KEY	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
SELECT	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED (If an SD does have the Final Application privilege)	ISD, AM SD, DM SD, SD with Final Application privilege
SET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD

[71] [selection: change_default, query, modify, delete, [assignment: other operations]]
[72] [assignment: list of security attributes]
[73] [assignment: the authorized identified roles]

Operations (APDUs or APIs)	Security Attributes: Card Life Cycle State	Authorised Identified Roles with Privileges
STORE DATA	OP_READY, INITIALIZED, or SECURED	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, CARD_LOCKED, or TERMINATED	ISD, AM SD, DM SD, SD
GET STATUS	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	ISD, AM SD, DM SD, SD

Table 8: GlobalPlatform Common Operations, Security Attributes, and Roles

Operations: SCP11 Commands	Used by	Security Attributes: Card Life Cycle State	Security Attributes: Minimum Security Level	Authorised Identified Roles with Privileges
GET DATA (ECKA Certificate)	SCP11a SCP11b SCP11c	OP_READY, INITIALIZED, SECURED, or CARD_LOCKED	None	ISD, AM SD, DM SD, SD
PERFORM SECURITY OPERATION	SCP11a SCP11c		None	
MUTUAL AUTHENTICATE	SCP11a SCP11c		AUTHENTICATED or ANY_AUTHENTICATED	
INTERNAL AUTHENTICATE	SCP11b		AUTHENTICATED or ANY_AUTHENTICATED	
STORE DATA (ECKA Certificate)	SCP11a SCP11b SCP11c		None	
STORE DATA (Whitelist)	SCP11a SCP11c		None	
VERIFY PIN	SCP11b		None	

Table 9: SCP11 Operations, Security Attributes, and Roles

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

Table 10: SCP02 / SCP03 Operations, Security Attributes, and Roles

Operations: **SCP80 Command**	**Security Attributes:** **Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorised Identified Roles with Privileges**
Remote File Management Commands SELECT, UPDATE BINARY, UPDATE RECORD, SEARCH RECORD, INCREASE, VERIFY PIN, CHANGE PIN, DISABLE PIN, ENABLE PIN, UNBLOCK PIN, DEACTIVATE FILE, ACTIVATE FILE, READ BINARY, READ RECORD, CREATE FILE, DELETE FILE, RESIZE FILE, SET DATA, RETRIEVE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]
Remote Applet Management Commands DELETE, SET STATUS, INSTALL, LOAD, PUT KEY, GET STATUS, GET DATA, STORE DATA	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]	See [TS 102 225] and [TS 102 226]

Table 11: SCP80 Operations, Security Attributes, and Roles

Operations: **SCP81 Command**	**Security Attributes:** **Card Life Cycle State**	**Security Attributes: Minimum Security Level**	**Authorised Identified Roles with Privileges**
PUT KEY	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
STORE DATA	OP_READY, INITIALIZED, SECURED	None	ISD, AM SD, DM SD, SD
GET DATA	OP_READY, INITIALIZED, SECURED, CARD_LOCKED, or TERMINATED	None	ISD, AM SD, DM SD, SD

Table 12: SCP81 Operations, Security Attributes, and Roles

Application Note:

- This SFR refines and replaces FMT_MSA.1/CM of [PP-JCS]. It is extended to cover Data and Key loading Policy.
- The authorized identified roles could be off-card or on-card entities as defined in FMT_SMR.1/GP.
- The generic “ISD” term has been kept as in [PP-GP]. It has to be read as the privileged SD which is the administrator of a given SD hierarchy (such as for example, the MNO-SD within a given profile).

FMT_MSA.3/GP Security attribute initialization

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

FMT_MSA.3.2/GP The TSF shall allow the **None**[74] to specify alternative initial values to override the default values when an object or information is created.

Application Note:

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

FMT_SMR.1/GP Security roles

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

- **On-card: S.OPEN, S.SD, Application**
- **Off-card: Users owning SDs**

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

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

FMT_SMF.1/GP Specification of Management Functions

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

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

Application Note:

- This SFR refines and replaces FMT_SMF.1/CM of [PP-JCS].
- Management functions related to SCPs are defined in [GPCS] Chapter 10.
- Card Locking, Card Unlocking and Card Termination have been removed from this SFR. Indeed, these states cannot be reached in eUICC product.

FPT_RCV.3/GP Automated recovery without undue loss

FPT_RCV.3.1/GP When automated recovery from **none, see application note below**[75] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/GP For **detection of a potential loss of integrity during the transmission of an Executable Load File to the card, abortion of the installation process of an Executable Load File, or any fatal error occurred during the linking of an Executable Load File to the Executable Files already installed on the card**[76] the TSF shall ensure the return of the TOE to a secure state using automated procedures.

[74] [assignment: authorized identified roles]

[75] [assignment: list of failures/service discontinuities during card content management operations]

[76] [assignment: list of failures/service discontinuities during card content management operations]

FPT_RCV.3.3/GP The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding **the loss of the Executable Load File being loaded or installed**[77] for loss of TSF data or objects under the control of the TSF.

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

Application Note:

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

FPT_FLS.1/GP Failure with preservation of secure state

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

- **S.OPEN fails to load/install an Executable Load File / Application instance.**
- **S.SD fails to load SD/Application data and keys.**
- **S.OPEN fails to verify/change the Card Life Cycle, Application and SD Life Cycle states.**
- **S.OPEN fails to verify the privileges belonging to an SD or an Application.**
- **S.SD fails to verify the security level applied to protect APDU commands.**
- **None**[78]

Application Note:

- This SFR extends FPT_FLS.1/Installer of [PP-JCS] to include the failures that may occur during the loading of SD/Application keys and data.
- Refer to [JCRE310] section 11.1.5 and [GPCS] sections 11.5, 11.6, 11.8, and 11.11 for additional details.

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

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

FPT_TDC.1.2/GP The TSF shall use **the list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card, None**[80] when interpreting the TSF data from another trusted IT product.

Application Note: the list of interpretation rules to be applied by the TSF when processing the INSTALL, LOAD, PUT KEY, and STORE DATA commands sent to the card are defined in [GPCS] sections 11.5, 11.6, 11.8, and 11.11.

FTP_ITC.1/GP Inter-TSF trusted channel

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

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

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

[77] [assignment: quantification]

[78] [assignment: list of additional types of failures]

[79] [assignment: list of TSF data types]

[80] [assignment: list of interpretation rules to be applied by the TSF]

- **APDU commands sent to the card within a Secure Channel Session**
- **When loading/installing a new ELF on the card**
- **When transmitting and loading sensitive data to the card using STORE DATA or PUT KEY commands**
- **When deleting ELFs, Applications, or Keys**
- **None**[81]

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

FCO_NRO.2/GP Enforced proof of origin

FCO_NRO.2.1/GP The TSF shall enforce the generation of evidence of origin for transmitted **Executable Load Files, SD/Application data and keys** [82] at all times.

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

FCO_NRO.2.2/GP The TSF shall be able to relate the **identity**[83] of the originator of the information, and the **Executable Load Files, SD/Application data and keys**[84] of the information to which the evidence applies.

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

FCO_NRO.2.3/GP The TSF shall provide a capability to verify the evidence of origin of information to **the off card entity (recipient of the evidence of origin) who requested that verification** given **at the time the ELF, SD/Application data and keys are received**[85].
Application Note:

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

FIA_UID.1/GP Timing of identification

FIA_UID.1.1/GP The TSF shall allow **SD selection, Application selection, initializing a Secure Channel with the card, requesting data that identifies the card or off-card entities**[86] on behalf of the user to be performed before the user is identified.

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

Application Note:

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

FDP_UIT.1/GP Basic data exchange integrity

FDP_UIT.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to **receive**[87] user data in a manner protected from **modification, deletion, insertion, replay** errors.

[81] [assignment: list of functions for which a trusted channel is required]
[82] [assignment: list of information types]
[83] [assignment: list of attributes]
[84] [assignment: list of information fields]
[85] [assignment: limitations on the evidence of origin]
[86] [assignment: list of TSF-mediated actions]
[87] [selection: transmit, receive]

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

Application Note:

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

FDP_ROL.1/GP Basic rollback

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

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

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

FDP_UCT.1/GP Basic data exchange confidentiality

FDP_UCT.1.1/GP The TSF shall enforce the **ELF Loading information flow control SFP and Data & Key Loading information flow control SFP** to **receive**[88] user data in a manner protected from unauthorized disclosure.

Application Note: this SFR applies where APDU command and response confidentiality protection is required. For example, the sensitive data (e.g. secret keys) shall always be transmitted as confidential data.

FPR_UNO.1/GP Unobservability

FPR_UNO.1.1/GP The TSF shall ensure that **SDs and Applications** are unable to observe the operation: **keys or data import (PUT KEY or STORE DATA), encryption, decryption, signature generation and verification, none**[89] on **keys and data** by **the OPEN or any other SD or Application**.

FIA_UAU.1/GP Timing of authentication

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

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

FIA_UAU.4/GP Single-use authentication mechanisms

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

FIA_AFL.1/GP Authentication failure handling

FIA_AFL.1.1/GP The TSF shall detect when **1**[90] unsuccessful authentication attempt occur related to **the authentication of the origin of a card management operation command**.

[88] [selection: transmit, receive]

[89] [assignment: list of operations]

[90] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]

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**.

FCS_CKM.4/GP Cryptographic key destruction

FCS_CKM.4.1/GP The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting the key value with random bytes**[91] that meets the following: **None**[92].

Application note: this SFR applies to the destruction of keys used in GP mechanisms, such as keys involved in:

- Secure Channel Protocols (SCPs)
- DAP verification
- OS Update (additional code decryption and signature verification)

ETSI PIN verification - Security Functional Requirements

FIA_AFL.1/ETSI-PIN Authentication failure handling

FIA_AFL.1.1/ETSI-PIN The TSF shall detect when **3** [93] unsuccessful authentication attempts occur related to **user authentication using ETSI PIN**[94].

FIA_AFL.1.2/ETSI-PIN When the defined number of unsuccessful authentication attempts has been **met**[95], the TSF shall **block the usage of the ETSI PIN**[96].

Application note: this SFR refines FIA_AFL.1/GP-CVM from [PP-GP] in order to focus on the ETSI PIN objects defined in [TS 102 221].

FPR_UNO.1/ETSI-PIN Unobservability

FPR_UNO.1.1/ETSI-PIN The TSF shall ensure that **all users and subjects**[97] are unable to observe the operation **comparison** on **ETSI PIN**[98] by **S.OPEN**[99].

Application note: this SFR refines FPR_UNO.1/GP-CVM from [PP-GP] in order to focus on the ETSI PIN objects defined in [TS 102 221].

[91] [assignment: cryptographic key destruction method]
[92] [assignment: list of standards]
[93] [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]
[94] Refines "user authentication using CVM" from [PP-GP]
[95] [selection: met, surpassed]
[96] [assignment: list of actions]
[97] [assignment: list of users and/or subjects]
[98] Refines "Global PIN" from [PP-GP]
[99] [assignment: list of protected users and/or subjects]

GlobalPlatform 'DAP Verification' & 'Mandated DAP Verification' - Security Functional Requirements

FCS_COP.1/GP-DAP_SHA Cryptographic operation

FCS_COP.1.1/GP-DAP_SHA The TSF shall perform **computation of a hash value for DAP Verification** in accordance with a specified cryptographic algorithm **SHA-256, SHA-384, or SHA-512**[100] and cryptographic key sizes **SHA-256, SHA-384, or SHA-512 hash lengths**[101] that meet the following: **[NIST 800 57]**[102].

Application Note: refer to the description in [GPCS] section C.3 for more details.

FCS_COP.1/GP-DAP_VER Cryptographic operation

FCS_COP.1.1/GP-DAP_VER The TSF shall perform **verification of the DAP signature attached to Load Files** in accordance with a specified cryptographic algorithm **as mentioned in table 13**[103] and cryptographic key sizes **as mentioned in table 13**[104] that meet the following: **standards mentioned in table 13**[105].

Algorithm	Key sizes	Recommended Standards
TDES	112 bits, 168 bits	[ISO 9797-1]
AES	128, 192, or 256 bits	[NIST 800-38B]
RSA	1024 or 2048 bits	[PKCS#1]
ECC	256, 384, 512 or 521 bits	[ANSI X9.62]

Table 13: Algorithms Used to Verify the DAP Signature

Application Note: refer to the description in [GPCS] section C.3 for more details.

FCO_NRO.2/GP-DAP Enforced proof of origin

FCO_NRO.2.1/GP-DAP The TSF shall enforce the generation of evidence of origin for transmitted **'ELF with DAP', as mentioned in the refinement below**[106] at all times.

Refinement: the TSF shall be able to generate an evidence of origin at all times for 'ELF with DAP' received from the off-card entity (originator of transmitted data) that communicates with the card.

[100] [assignment: cryptographic algorithm]
[101] [assignment: cryptographic key sizes]
[102] [assignment: list of standards]
[103] [assignment: cryptographic algorithm]
[104] [assignment: cryptographic key sizes]
[105] [assignment: list of standards]
[106] [assignment: list of information types]

FCO_NRO.2.2/GP-DAP The TSF shall be able to relate the **Load File Data Block Signature, as mentioned in the refinement below**[107] of the originator of the information, and the **'ELF with DAP', as mentioned in the refinement below**[108] of the information to which the evidence applies.

Refinement: the TSF shall be able to load 'ELF with DAP' to the card with associated security attributes (Load File Data Block Signature) such that the integrity and authenticity of transmitted data can be verified.

FCO_NRO.2.3/GP-DAP The TSF shall provide a capability to verify the evidence of origin of information to **the off-card entity (recipient of the evidence of origin) who requested that verification** given **at the time the ELF with DAP is received**.

Application Note: this SFR addresses the DAP verification as defined in [GPCS] sections 9.2.1, 11.6.2.3, and C.3.

GlobalPlatform 'Amendment H: Executable Load File Upgrade (ELFU)' - Security Functional Requirements

FDP_ACC.1/GP-ELFU Subset access control

FDP_ACC.1.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** on **the following list of subjects, objects and operations**:

- **Subjects: S.OPEN, ELF Provider, S.SD**
- **Objects: Application instance data, ELF, ELF Registry data, ELF session data**
- **Operation controlled by the policy: APDUs 'MANAGE ELF UPGRADE', INSTALL [for load] and LOAD, and Upgrade API methods.**

Application Note:

- The APDU 'MANAGE ELF UPGRADE' is defined in [Amd H] section 4.1.
- The INSTALL [for load], LOAD commands, and Upgrade API methods are defined in [Amd H] Annex A.

FDP_ACF.1/GP-ELFU Security attribute based access control

FDP_ACF.1.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** to objects based on the following **Security Attributes: AIDs, ELF session status, ELF versions (old or new).**

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

- **Only a single ELF Upgrade Session is processed at a time. No new ELF Upgrade Session may be started until the previous one (if any) has been completed or aborted.**
- **The MANAGE ELF UPGRADE [start] command is rejected with an error and the ELF Upgrade Process is aborted if any of the conditions defined in [Amd H] are satisfied.**
- **S.OPEN allows an ELF upgrade session to be initiated if no other ELF upgrade session is running.**
- **S.OPEN allows an ELF upgrade session to be initiated if processing S.SD has authorized management privilege or delegate management privilege**[109]

[107] [assignment: list of attributes]
[108] [assignment: list of information fields]
[109] [assignment: rules governing access among controlled subjects and controlled objects using

FDP_ACF.1.3/GP-ELFU The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**[110].

FDP_ACF.1.4/GP-ELFU The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**[111].

Application Note:

- AIDs, ELF session status are given in [Amd H] Table 4-8.
- Rules to be applied when starting the Upgrade session are described in [Amd H] section 3.2.1.
- Rules to be applied during the Saving phase are described in [Amd H] section 3.2.2.
- Rules to be applied during the Loading phase are described in [Amd H] section 3.2.3.
- Rules to be applied during the Restore phase are described in [Amd H] section 3.2.4.
- Card Content Management Operations described in [Amd H] section 3.4 shall always be rejected during an ELF Upgrade Session.

FDP_ROL.1/GP-ELFU Basic rollback

FDP_ROL.1.1/GP-ELFU The TSF shall enforce **ELF Upgrade Access Control Policy** to permit the rollback of the **deletion** on the **Application instances and ELF(s).**

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

- **If the deletion of the application instances and ELF(s) (atomic and irreversible operation) was started and then interrupted and/or disturbed by for example unexpected power-down, it shall automatically restart and complete at next power-up.**
- **If the interruption occurred during the Deletion Sequence and the latter did not complete automatically (i.e. the irreversible deletion operation did not start already), the Deletion Sequence shall restart.**

FMT_MSA.1/GP-ELFU Management of security attributes

FMT_MSA.1.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** to restrict the ability to **set and maintain** the security attributes **defined in FDP_ACF.1.1/GP-ELFU** to the **S.OPEN**.

FMT_MSA.3/GP-ELFU Security attribute initialization

FMT_MSA.3.1/GP-ELFU The TSF shall enforce the **ELF Upgrade Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/GP-ELFU The TSF shall allow the **S.OPEN** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/GP-ELFU Specification of Management Functions

FMT_SMF.1.1/GP-ELFU The TSF shall be capable of performing the following management functions:

controlled operations on controlled objects]

[110] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

[111] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

- **The Saving, Loading, Restore phases of the Executable Load File Process**
- **Management of the ELF upgrade session status**
- **Card management during the ELF upgrade session**
- **None**[112]

FPT_FLS.1/GP-ELFU Failure with preservation of secure state

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

- **The required minimum amount of memory is not available at the time the command MANAGE ELF UPGRADE is received,**
- **A fatal error occurs using the new ELF version during the Restore Phase**
- **The ELF Upgrade Recovery Procedure fails,**
- **The installation of an Application instance fails,**
- **An interruption occurred during the Installation, Saving, Restore, or Consolidation Sequences,**
- **none**[113]**.**

'OS Update' functionality - Security Functional Requirements

FDP_ACC.1/OS-UPDATE Subset access control

FDP_ACC.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** on **the following list of subjects, objects, and operations**:

- **Subjects: S.OS-DEVELOPER is the representative of the OS Developer within the TOE, being responsible for signature verification and decryption of the additional code, before Loading, Installation and Activation are authorized.**
- **Objects: additional code and associated cryptographic signature**
- **Operations: loading, installation, and activation of additional code**

FDP_ACF.1/OS-UPDATE Security attribute based access control

FDP_ACF.1.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to objects based on the following Security Attributes:

- **The additional code cryptographic signature verification status**
- **The Identification Data verification status (between the Initial TOE and the additional code)**

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

- **The verification of the additional code cryptographic signature by S.OS-DEVELOPER is successful.**
- **The decryption of the additional code prior installation by S.OS-DEVELOPER is successful.**
- **The comparison between the identification data of both the Initial TOE and the additional code demonstrates that the OS Update operation can be performed.**
- **none**[114]

[112] [assignment: list of management functions to be provided by the TSF]
[113] [assignment: list of types of failures in the TSF]
[114] [assignment: rules governing access among controlled subjects and controlled objects using

FDP_ACF.1.3/OS-UPDATE The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **none**[115].

FDP_ACF.1.4/OS-UPDATE The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**[116].

Application Note:

- Identification data verification is necessary to ensure that the received additional code is actually targeting the TOE and that its version is compatible with the TOE version.
- Confidentiality protection must be enforced when the additional code is transmitted to the TOE for loading. Confidentiality protection is achieved through direct encryption of the additional code.

FMT_MSA.3/OS-UPDATE Security attribute initialization

FMT_MSA.3.1/OS-UPDATE The TSF shall enforce the **OS Update Access Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/OS-UPDATE The TSF shall allow the **OS Developer** to specify alternative initial values to override the default values when an object or information is created.

Application Note: the additional code signature verification status must be set to “Fail” by default. This prevents installation of any additional code until the additional code signature is successfully verified by the TOE.

FMT_SMR.1/OS-UPDATE Security roles

FMT_SMR.1.1/OS-UPDATE The TSF shall maintain the roles **OS Developer**.

FMT_SMR.1.2/OS-UPDATE The TSF shall be able to associate users with roles.

FMT_SMF.1/OS-UPDATE Specification of Management Functions

FMT_SMF.1.1/OS-UPDATE The TSF shall be capable of performing the following management functions: **activation of additional code**.

Application Note: once verified and installed, additional code needs to be activated to become effective.

FIA_ATD.1/OS-UPDATE User attribute definition

FIA_ATD.1.1/OS-UPDATE The TSF shall maintain the following list of security attributes belonging to individual users: **additional code ID for each activated additional code**.

Refinement: "Individual users" stands for additional code.

controlled operations on controlled objects]

[115] [assignment: rules, based on security attributes, that explicitly authorize access of subjects to objects]

[116] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

FTP_TRP.1/OS-UPDATE Trusted Path

FTP_TRP.1.1/OS-UPDATE The TSF shall provide a communication path between itself and **remote** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **none**[117].

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

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

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

FCS_COP.1/OS-UPDATE-DEC Cryptographic operation

FCS_COP.1.1/OS-UPDATE-DEC The TSF shall perform **Decryption of the additional code prior installation** in accordance with a specified cryptographic algorithm **AES in CBC mode with null IV**[118] and cryptographic key sizes **128 bits**[119] that meet the following: **FIPS 197**[120].

FCS_COP.1/OS-UPDATE-VER Cryptographic operation

FCS_COP.1.1/OS-UPDATE-VER The TSF shall perform **digital signature verification of the additional code to be loaded** in accordance with a specified cryptographic algorithm **AES-CMAC**[121] and cryptographic key sizes **128 bits**[122] that meet the following: **FIPS 197 and SP800-38B**[123].

FPT_FLS.1/OS-UPDATE Failure with preservation of secure state

FPT_FLS.1.1/OS-UPDATE The TSF shall preserve a secure state when the following types of failures occur: **interruption or incident which prevents the forming of the Updated TOE**.

Application Note:

- The OS Update operation must either be successful or fail securely. There are 3 steps in an OS Update operation:
  - step 1: loading
  - step 2: activation
  - step 3: update of TOE identification data

  Steps 2 and 3 are performed atomically, so that the TOE active code and identification data always remain consistent.
- If a failure (interruption or incident) occurs during step 1 (loading), then the TOE remains in its initial state (no update, neither of code nor of the TOE identification data).

[117] [selection: disclosure, none]
[118] [assignment: cryptographic algorithm]
[119] [assignment: cryptographic key sizes]
[120] [assignment: list of standards]
[121] [assignment: cryptographic algorithm]
[122] [assignment: cryptographic key sizes]
[123] [assignment: list of standards]

- If a failure (interruption or incident) occurs during the atomic sequence step 2 / step 3 (activation / update of TOE identification data), then the enforced behavior depends on the nature of the update:
    - For java code updates, the TOE remains in its initial state and the OS Update operation is aborted.
    - For native code updates, the TOE does some retries to complete the atomic sequence step 2 / step 3 (activation / update of TOE identification data) until it is successful.
    - In any case, only two possible secure states are possible at any given time:
        - Either activation is not done and the TOE identification data is not updated (i.e. initial state)
        - Or the atomic sequence completes successfully, i.e. the OS update is activated and the TOE identification data is updated accordingly.

9.1.3.3 [PP-JCS] Protection Profile

This section states the security functional requirements for the Java Card System - Open configuration. For readability, requirements are arranged into groups. All the groups defined in the table below come from [PP-JCS].

Group	Name	Description
CoreG_LC	Core with Logical Channels	The CoreG_LC contains the requirements concerning the runtime environment of the Java Card System implementing logical channels. This includes the firewall policy and the requirements related to the Java Card API. Logical channels are a Java Card specification version 2.2 feature.
ADELG	Applet deletion	The ADELG contains the security requirements for erasing installed applets from the card, a feature introduced in Java Card specification version 2.2.
ODELG	Object deletion	The ODELG contains the security requirements for the object deletion capability. This provides a safe memory recovering mechanism. This is a Java Card specification version 2.2 feature.

Subjects are active components of the TOE that (essentially) act on the behalf of users. The users of the TOE include people or institutions (like the applet developer, the card issuer, the verification authority), hardware (like the CAD where the card is inserted or the PCD) and software components (like the application packages installed on the card). Some of the users may just be aliases for other users. For instance, the verification authority in charge of the bytecode verification of the applications may be just an alias for the card issuer.

Subjects (prefixed with an "S") are described in the following table:

Subject	Description
S.ADEL	The applet deletion manager which also acts on behalf of the card issuer. It may be an applet ([JCRE310], §11), but its role asks anyway for a specific treatment from the security viewpoint.
S.APPLET	Any applet instance.
S.BCV	The bytecode verifier (BCV), which acts on behalf of the verification authority who is in charge of the bytecode verification of the CAP files.
S.CAD	The CAD represents off-card entity that communicates with the S.INSTALLER. If the TOE provides JCRMI functionality, CAD can request RMI services by issuing commands to the card.
S.INSTALLER	The installer is the on-card entity which acts on behalf of the card issuer. This subject is involved in the loading of CAP files and installation of applets.
S.JCRE	The runtime environment under which Java programs in a smart card are executed.
S.JCVM	The bytecode interpreter that enforces the firewall at runtime.
S.LOCAL	Operand stack of a JCVM frame, or local variable of a JCVM frame containing an object or an array of references.
S.MEMBER	Any object's field, static field or array position.
S.CAP_FILE	A CAP file may contain multiple Java language packages. A package is a namespace within the Java programming language that may contain classes and interfaces. A CAP file may contain packages that define either user library, or one or several applets. A COMPACT CAP file as specified in Java Card Specifications version 3.1 or CAP files compliant to previous

	versions of Java Card Specification, MUST contain only a single package representing a library or one or more applets.

Objects (prefixed with an "O") are described in the following table:

Object	Description
O.APPLET	Any installed applet, its code and data.
O.CODE_CAP_FILE	The code of a CAP file, including all linking information. On the Java Card platform, a CAP file is the installation unit.
O.JAVAOBJECT	Java class instance or array. It should be noticed that KEYS, PIN, arrays and applet instances are specific objects in the Java programming language.

Information (prefixed with an "I") is described in the following table:

Information	Description
I.APDU	Any APDU sent to or from the card through the communication channel.
I.DATA	JCVM Reference Data: objectref addresses of APDU buffer, JCRE-owned instances of APDU class and byte array for install method.

Security attributes linked to these subjects, objects and information are described in the following table with their values:

Security attribute	Description / Value
Active Applets	The set of the active applets' AIDs. An active applet is an applet that is selected on at least one of the logical channels.
Applet Selection Status	"Selected" or "Deselected".
Applet's version number	The version number of an applet indicated in the export file.
CAP File AID	The AID of a CAP file.
Context	CAP file AID or "Java Card RE".
Currently Active Context	CAP file AID or "Java Card RE".
Dependent package AID	Allows the retrieval of the package AID and Applet's version number ([JCVM310], §4.5.2).
LC Selection Status	Multiselectable, Non-multiselectable or "None".
LifeTime	CLEAR_ON_DESELECT or PERSISTENT (*).
Owner	The Owner of an object is either the applet instance that created the object or the CAP file (library) where it has been defined (these latter objects can only be arrays that initialize static fields of the CAP file). The owner of a remote object is the applet instance that created the object.
Package AID	The AID of each package indicated in the export file.
Registered Applets	The set of AID of the applet instances registered on the card.
Resident CAP files	The set of AIDs of the CAP files already loaded on the card.
Resident packages	The set of AIDs of the packages already loaded on the card.
Selected Applet Context	CAP file AID or "None".
Sharing	Standard, SIO, Array View, Java Card RE entry point or global array.
Static References	Static fields of a CAP file may contain references to objects. The Static References attribute records those references.

(*) Transient objects of type CLEAR_ON_RESET behave like persistent objects in that they can be accessed only when the Currently Active Context is the object's context.

Operations (prefixed with "OP") are described in the following table. Each operation has parameters given between brackets, among which there is the "accessed object", the first one, when applicable. Parameters may be seen as security attributes that are under the control of the subject performing the operation.

Operation	Description
OP.ARRAY_ACCESS (O.JAVAOBJECT, field)	Read/Write an array component.
OP.ARRAY_LENGTH (O.JAVAOBJECT, field)	Get length of an array component.
OP.ARRAY_T_ALOAD(O.JAVAOBJECT, field)	Read from an array component.

OP.ARRAY_T_ASTORE(O.JAVAOBJECT, field)	Write to an array component.
OP.ARRAY_AASTORE(O.JAVAOBJECT, field)	Store into reference array component.
OP.CREATE(Sharing, LifeTime) (*)	Creation of an object (new, makeTransient or createArrayView call).
OP.DELETE_APPLET(O.APPLET,...)	Delete an installed applet and its objects, either logically or physically.
OP.DELETE_CAP_FILE(O.CODE_CAP_FILE,...)	Delete a CAP file, either logically or physically.
OP.DELETE_CAP_FILE_APPLET(O.CODE_CAP_FILE,...)	Delete a CAP file and its installed applets, either logically or physically.
OP.INSTANCE_FIELD(O.JAVAOBJECT, field)	Read/Write a field of an instance of a class in the Java programming language.
OP.INVK_VIRTUAL(O.JAVAOBJECT, method, arg1,...)	Invoke a virtual method (either on a class instance or an array object).
OP.INVK_INTERFACE(O.JAVAOBJECT, method, arg1,...)	Invoke an interface method.
OP.JAVA(...)	Any access in the sense of [JCRE310], §6.2.8. It stands for one of the operations OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW, OP.TYPE_ACCESS, OP.ARRAY_LENGTH
OP.PUT(S1,S2,I)	Transfer a piece of information I from S1 to S2.
OP.THROW(O.JAVAOBJECT)	Throwing of an object (athrow, see [JCRE310], §6.2.8.7).
OP.TYPE_ACCESS (O.JAVAOBJECT, class)	Invoke checkcast or instance of on an object in order to access to classes (standard or shareable interfaces objects).

(*) For this operation, there is no accessed object. This rule enforces that shareable transient objects are not allowed. For instance, during the creation of an object, the JavaCardClass attribute's value is chosen by the creator.

CoreG_LC Security Functional Requirements

This group is focused on the main security policy of the Java Card System, known as the firewall.

Firewall Policy

FDP_ACC.2/FIREWALL Complete access control

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

Refinement: the operations involved in the policy are: OP.CREATE, OP.INVK_INTERFACE, OP.INVK_VIRTUAL, OP.JAVA, OP.THROW, OP.TYPE_ACCESS, OP.ARRAY_LENGTH, OP.ARRAY_T_ALOAD, OP.ARRAY_T_ASTORE, OP.ARRAY_AASTORE.

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

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

FDP_ACF.1/FIREWALL Security attribute based access control

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

Subject / Object	Security attributes
S.CAP_FILE	LC Selection Status
S.JCVM	Active Applets, Currently Active Context

S.JCRE	Selected Applet Context
O.JAVAOBJECT	Sharing, Context, LifeTime

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

- **R.JAVA.1 ([JCRE310], §6.2.8): S.CAP_FILE may freely perform OP.INVK_VIRTUAL, OP.INVK_INTERFACE, OP.THROW or OP.TYPE_ACCESS upon any O.JAVAOBJECT whose Sharing attribute has value "JCRE entry point" or "global array".**
- **R.JAVA.2 ([JCRE310], §6.2.8): S.CAP_FILE may freely perform OP.ARRAY_ACCESS, OP.INSTANCE_FIELD, OP.INVK_VIRTUAL, OP.INVK_INTERFACE or OP.THROW upon any O.JAVAOBJECT whose Sharing attribute has value "Standard" and whose Lifetime attribute has value "PERSISTENT" only if O.JAVAOBJECT's Context attribute has the same value as the active context.**
- **R.JAVA.3 ([JCRE310], §6.2.8.10): S.CAP_FILE may perform OP.TYPE_ACCESS upon an O.JAVAOBJECT with Context attribute different from the currently active context, whose Sharing attribute has value "SIO" only if O.JAVAOBJECT is being cast into (checkcast) or is being verified as being an instance of (instanceof) an interface that extends the Shareable interface.**
- **R.JAVA.4 ([JCRE310], §6.2.8.6): S.CAP_FILE may perform OP.INVK_INTERFACE upon an O.JAVAOBJECT with Context attribute different from the currently active context, whose Sharing attribute has the value "SIO", and whose Context attribute has the value "CAP File AID ", only if the invoked interface method extends the Shareable interface and one of the following conditions applies:**
  a) **The value of the attribute Selection Status of the CAP file whose AID is "CAP File AID" is "Multiselectable",**
  b) **The value of the attribute Selection Status of the CAP file whose AID is "CAP File AID " is "Non-multiselectable", and either "CAP File AID" is the value of the currently selected applet or otherwise "CAP File AID" does not occur in the attribute Active Applets.**
- **R.JAVA.5: S.CAP_FILE may perform OP.CREATE upon O.JAVAOBJECT only if the value of the Sharing parameter is "Standard" or “SIO”.**
- **R.JAVA.6 ([JCRE310], §6.2.8): S.CAP_FILE may freely perform OP.ARRAY_ACCESS or OP.ARRAY_LENGTH upon any O.JAVAOBJECT whose Sharing attribute has value "global array".**

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

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

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

1) **Any subject with OP.JAVA upon an O.JAVAOBJECT whose LifeTime attribute has value "CLEAR_ON_DESELECT" if O.JAVAOBJECT's Context attribute is not the same as the Selected Applet Context.**
2) **Any subject attempting to create an object by the means of OP.CREATE and a "CLEAR_ON_DESELECT" LifeTime parameter if the active context is not the same as the Selected Applet Context.**
3) **S.CAP_FILE performing OP.ARRAY_AASTORE of the reference of an O.JAVAOBJECT whose sharing attribute has value “global array” or “Temporary”.**
4) **S.CAP_FILE performing OP.PUTFIELD or OP.PUTSTATIC of the reference of an O.JAVAOBJECT whose sharing attribute has value “global array” or “Temporary”.**
5) **R.JAVA.7 ([JCRE310], §6.2.8.2): S.CAP_FILE performing OP.ARRAY_T_ASTORE into an array view without ATTR_WRITABLE_VIEW access attribute.**
6) **R.JAVA.8 ([JCRE310], §6.2.8.2):S.CAP_FILE performing OP.ARRAY_T_ALOAD into an array view without ATTR_READABLE_VIEW access attribute.**

Application note, FDP_ACF.1.4/FIREWALL:

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

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

The Sharing attribute defines five categories of objects:

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

When a new object is created, it is associated with the Currently Active Context. But the object is owned by the applet instance within the Currently Active Context when the object is instantiated ([JCRE310], §6.1.3). An object is owned by an applet instance, by the JCRE or by the library where it has been defined (these latter objects can only be arrays that initialize static fields of CAP files).

([JCRE310], Glossary) Selected Applet Context. The Java Card RE keeps track of the currently selected Java Card applet. Upon receiving a SELECT command with this applet's AID, the Java Card RE makes this applet the Selected Applet Context. The Java Card RE sends all APDU commands to the Selected Applet Context.

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

([JCRE310], §6.1.2.1) At any point in time, there is only one active context within the Java Card VM (this is called the Currently Active Context).

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

It should be noticed that the Java Card platform, version 2.2.x and version 3.x.x Classic Edition, introduces the possibility for an applet instance to be selected on multiple logical channels at the same time, or accepting other applets belonging to the same CAP file being selected simultaneously. These applets are referred to as multiselectable applets. Applets that belong to a same CAP file are either all multiselectable or not ([JCVM310], §2.2.5). Therefore, the selection mode can be regarded as an attribute of CAP files. No selection mode is defined for a library CAP file.

An applet instance will be considered an active applet instance if it is currently selected in at least one logical channel. An applet instance is the currently selected applet instance only if it is processing the current command. There can only be one currently selected applet instance at a given time. ([JCRE310], §4).

FDP_IFC.1/JCVM Subset information flow control

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

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

FDP_IFF.1/JCVM Simple security attributes

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

Subjects	Security attributes
S.JCVM	Currently Active Context

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

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

FDP_IFF.1.3/JCVM The TSF shall enforce the **No additional rules**[124].

FDP_IFF.1.4/JCVM The TSF shall explicitly authorize an information flow based on the following rules: **No additional rules**[125].

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: **No additional rules**[126].

Application note:

The storage of temporary Java Card RE-owned objects references is runtime-enforced ([JCRE310], §6.2.8.1-3).

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

FDP_RIP.1/OBJECTS Subset residual information protection

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

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

[124] [assignment: additional information flow control SFP rules]

[125] [assignment: rules, based on security attributes, that explicitly authorize information flows]

[126] [assignment: rules, based on security attributes, that explicitly deny information flows]

FMT_MSA.1/JCRE Management of security attributes

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

Application note: the modification of the Selected Applet Context should be performed in accordance with the rules given in [JCRE310], §4 and [JCVM310], §3.4.

FMT_MSA.1/JCVM Management of security attributes

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

Application note: the modification of the Currently Active Context should be performed in accordance with the rules given in [JCRE310], §4 and [JCVM310], §3.4.

FMT_MSA.2/FIREWALL_JCVM Secure security attributes

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

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

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

FMT_MSA.3/FIREWALL Static attribute initialization

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

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

Application note, FMT_MSA.3.1/FIREWALL:

Objects' security attributes of the access control policy are created and initialized at the creation of the object or the subject. Afterwards, these attributes are no longer mutable (FMT_MSA.1/JCRE). At the creation of an object (OP.CREATE), the newly created object, assuming that the FIREWALL access control SFP permits the operation, gets its Lifetime and Sharing attributes from the parameters of the operation; on the contrary, its Context attribute has a default value, which is its creator's Context attribute and AID respectively ([JCRE310], §6.1.3). There is one default value for the Selected Applet Context that is the default applet identifier's Context, and one default value for the Currently Active Context that is "Java Card RE".
The knowledge of which reference corresponds to a temporary entry point object or a global array and which does not is solely available to the Java Card RE (and the Java Card virtual machine).

Application note, FMT_MSA.3.2/FIREWALL:

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

FMT_MSA.3/JCVM Static attribute initialization

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

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

FMT_SMF.1/JCS Specification of Management Functions

FMT_SMF.1.1/JCS The TSF shall be capable of performing the following management functions: **modify the Currently Active Context, the Selected Applet Context and the Active Applets**.

FMT_SMR.1/JCS Security roles

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

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

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

Application Programming Interface

The following SFRs are related to the Java Card API.

It should be noticed that the execution of the additional native code is not within the TSF. Nevertheless, access to API native methods from the Java Card System is controlled by TSF because there is no difference between native and interpreted methods in their interface or invocation mechanism.

FDP_RIP.1/ABORT Subset residual information protection

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

Application note: the events that provoke the de-allocation of a transient object are described in [JCRE310], §5.1.

FDP_RIP.1/APDU Subset residual information protection

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

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

FDP_RIP.1/GlobalArray Subset residual information protection

FDP_RIP.1.1/GlobalArray (refined) The TSF shall ensure that any previous information content of a resource is made unavailable upon **deallocation of the resource from** *the applet as a result of returning from the process method to* the following objects: **a user Global Array**.

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

FDP_RIP.1/bArray Subset residual information protection

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

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

FDP_RIP.1/KEYS Subset residual information protection

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

Application note: the javacard.security & javacardx.crypto packages do provide secure interfaces to the cryptographic buffer in a transparent way. See javacard.security.KeyBuilder and Key interface of [JCAPI310].

FDP_RIP.1/TRANSIENT Subset residual information protection

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

Application note:

- The events that provoke the de-allocation of any transient object are described in [JCRE310], §5.1.
- The clearing of CLEAR_ON_DESELECT objects is not necessarily performed when the owner of the objects is deselected. In the presence of multiselectable applet instances, CLEAR_ON_DESELECT memory segments may be attached to applets that are active in different logical channels. Multiselectable applet instances within a same CAP file must share the transient memory segment if they are concurrently active ([JCRE310], §4.3).

FDP_ROL.1/FIREWALL Basic rollback

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

FDP_ROL.1.2/FIREWALL The TSF shall permit operations to be rolled back within the **scope of a select(), deselect(), process(), install() or uninstall() call, notwithstanding the restrictions given in [JCRE310], §7.7, within the bounds of the Commit Capacity ([JCRE310], §7.8), and those described in [JCAPI310]**.

Application note: transactions are a service offered by the APIs to applets. It is also used by some APIs to guarantee the atomicity of some operation. This mechanism is either implemented in Java Card platform or relies on the transaction mechanism offered by the underlying platform. Some operations of the API are not conditionally updated, as documented in [JCAPI310] (see for instance, PIN-blocking, PIN-checking, update of Transient objects).

Card Security Management

FAU_ARP.1 Security alarms

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

- **throw an exception,**
- **lock the card session,**
- **reinitialize the Java Card System and its data,**
- **none**[127]

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(), [JCAPI310] and ([JCRE310], §7.6.2)**
- **violation of the Firewall or JCVM SFPs,**
- **unavailability of resources,**
- **array overflow,**
- **GlobalPlatform card state inconsistency**[128]

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

FDP_SDI.2/DATA Stored data integrity monitoring and action

FDP_SDI.2.1/DATA The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors**[129] on all objects, based on the following attributes: **integrity check data**[130].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **mute the card and decrease the global fault detection counter. Once the global fault detection counter reaches 0, the card is put in degraded mode.**[131]

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

- Key (i.e. objects instance of classes implemented the interface Key)
- PIN (objects instance of class OwnerPin)
- Package
- GlobalPlatform card state (OP_READY, SECURED)[132]

FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that **any user**[133] are unable to observe the operation **read, write, cryptographic operations**[134] on **PIN, Key**[135] by **any other user or subject**[136].

[127] [assignment: list of other actions]
[128] [assignment: list of other runtime errors]
[129] [assignment: integrity errors]
[130] [assignment: user data attributes]
[131] [assignment: action to be taken]
[132] The CARD_LOCKED and TERMINATE states are not mentioned as they cannot be reached in eUICC product.
[133] [assignment: list of users and/or subjects]
[134] [assignment: list of operations]
[135] [assignment: list of objects]
[136] [assignment: list of protected users and/or subjects]

FPT_FLS.1/JCS Failure with preservation of secure state

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

Application note: the Java Card RE Context is the Current context when the Java Card VM begins running after a card reset ([JCRE310], §6.2.3) or after a proximity card (PICC) activation sequence ([JCRE310]). Behavior of the TOE on power loss and reset is described in [JCRE310], §3.6 and §7.1. Behavior of the TOE on RF signal loss is described in [JCRE310], §3.6.1.

FPT_TDC.1 Inter-TSF basic TSF data consistency

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

FPT_TDC.1.2 The TSF shall use

- **the rules defined in [JCVM310] specification,**
- **the API tokens defined in the export files of reference implementation,**
- **none**[137]

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.

AID management

FIA_ATD.1/AID User attribute definition

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

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

Refinement: "Individual users" stand for applets.

FIA_UID.2/AID User identification before any action

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

Application note:

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

[137] [assignment: list of interpretation rules to be applied by the TSF]

FIA_USB.1/AID User-subject binding

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

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **CAP file AID are defined with associated value during loading and with context identifier**[138].

FIA_USB.1.3/AID The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **None**[139].

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

FMT_MTD.1/JCRE Management of TSF data

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

Application note:

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

FMT_MTD.3/JCRE Secure TSF data

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

ADELG Security Functional Requirements

This group consists of the SFRs related to the deletion of applets and/or CAP files, enforcing the applet deletion manager (ADEL) policy on security aspects outside the runtime. Deletion is a critical operation and therefore requires specific treatment.

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

FDP_ACC.2/ADEL Complete access control

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

Refinement: the operations involved in the policy are: OP.DELETE_APPLET, OP.DELETE_CAP_FILE, and OP.DELETE_CAP_FILE_APPLET.

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

[138] [assignment: rules for the initial association of attributes]
[139] [assignment: rules for the changing of attributes]

FDP_ACF.1/ADEL Security attribute based access control

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

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

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

- **In the context of this policy, an object O is reachable if and only one of the following conditions hold:**
  1) **the owner of O is a registered applet instance A (O is reachable from A),**
  2) **a static field of a resident package P contains a reference to O (O is reachable from P),**
  3) **there exists a valid remote reference to O (O is remote reachable),**
  4) **there exists an object O' that is reachable according to either (1) or (2) or (3) above and O' contains a reference to O (the reachability status of O is that of O').**
- **The following access control rules determine when an operation among controlled subjects and objects is allowed by the policy:**
  - ➢ **R.JAVA.14 ([JCRE310], §11.3.4.2, Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon an O.APPLET only if,**
    1) **S.ADEL is currently selected,**
    2) **there is no instance in the context of O.APPLET that is active in any logical channel and**
    3) **there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance distinct from O.APPLET, or O.JAVAOBJECT is reachable from a package P, or ([JCRE3], §8.5) O.JAVAOBJECT is remote reachable.**
  - ➢ **R.JAVA.15 ([JCRE310], §11.3.4.2.1, Multiple Applet Instance Deletion): S.ADEL may perform OP.DELETE_APPLET upon several O.APPLET only if,**
    1) **S.ADEL is currently selected,**
    2) **there is no instance of any of the O.APPLET being deleted that is active in any logical channel and**
    3) **there is no O.JAVAOBJECT owned by any of the O.APPLET being deleted such that either O.JAVAOBJECT is reachable from an applet instance distinct from any of those O.APPLET, or O.JAVAOBJECT is reachable from a CAP file P, or ([JCRE310], §8.5) O.JAVAOBJECT is remote reachable.**
  - ➢ **R.JAVA.16 ([JCRE310], §11.3.4.3, Applet/Library CAP file Deletion): S.ADEL may perform OP.DELETE_CAP_FILE upon an O.CODE_CAP_FILE only if,**
    1) **S.ADEL is currently selected,**
    2) **no reachable O.JAVAOBJECT, from a CAP file distinct from O.CODE_CAP_FILE that is an instance of a class that belongs to O.CODE_CAP_FILE, exists on the card and**
    3) **there is no resident package on the card that depends on O.CODE_CAP_FILE.**
  - ➢ **R.JAVA.17 ([JCRE310], §11.3.4.4, Applet CAP file and Contained Instances Deletion): S.ADEL may perform OP.DELETE_CAP_FILE_APPLET upon an O.CODE_CAP_FILE only if,**
    1) **S.ADEL is currently selected,**
    2) **no reachable O.JAVAOBJECT, from a CAP file distinct from O.CODE_CAP_FILE, which is an instance of a class that belongs to O.CODE_CAP_FILE exists on the card,**
    3) **there is no CAP file loaded on the card that depends on O.CODE_CAP_FILE, and**
    4) **for every O.APPLET of those being deleted it holds that: (i) there is no instance in the context of O.APPLET that is active in any logical channel and (ii) there is no O.JAVAOBJECT owned by O.APPLET such that either O.JAVAOBJECT is reachable from an applet instance not being deleted, or O.JAVAOBJECT is reachable from a CAP file not being deleted, or ([JCRE310], §8.5) O.JAVAOBJECT is remote reachable.**

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

FDP_ACF.1.4/ADEL The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **any subject but S.ADEL to O.CODE_PKG or O.APPLET for the purpose of deleting them from the card**.

Application note, FDP_ACF.1.2/ADEL:

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

FDP_RIP.1/ADEL Subset residual information protection

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

Application note: deleted freed resources (both code and data) may be reused, depending on the way they were deleted (logically or physically). Requirements on de-allocation during applet/CAP file deletion are described in [JCRE310], §11.3.4.1, §11.3.4.2 and §11.3.4.3.

FMT_MSA.1/ADEL Management of security attributes

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

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

FMT_MSA.3/ADEL Static attribute initialization

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

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

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

FMT_SMF.1/ADEL Specification of Management Functions

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

FMT_SMR.1/ADEL Security roles

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

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

FPT_FLS.1/ADEL Failure with preservation of secure state

FPT_FLS.1.1/ADEL The TSF shall preserve a secure state when the following types of failures occur: **the applet deletion manager fails to delete a CAP file/applet as described in [JCRE310], §11.3.4**.

Application note:

- The TOE may provide additional feedback information to the card manager in case of a potential security violation (see FAU_ARP.1).
- The CAP file/applet instance deletion must be atomic. The "secure state" referred to in the requirement must comply with Java Card specification ([JCRE310], §11.3.4.)

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

ODELG Security Functional Requirements

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

FDP_RIP.1/ODEL Subset residual information protection

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

Application note:

- Freed data resources resulting from the invocation of the method javacard.framework.JCSystem.requestObjectDeletion() may be reused. Requirements on de-allocation after the invocation of the method are described in [JCAPI310].
- There is no conflict with FDP_ROL.1 here because of the bounds on the rollback mechanism: the execution of requestObjectDeletion() is not in the scope of the rollback because it must be performed in between APDU command processing, and therefore no transaction can be in progress.

FPT_FLS.1/ODEL Failure with preservation of secure state

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

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

SCP Security Functional Requirements

This section states the security functional requirements for the Smart Card Platform.

Operating System

This section presents those requirements of the Smart Card Platform group that concern the Operating System. Due to the enlargement of the evaluation scope, the requirements related to OS are now assigned to the TOE and no more to the environment[140]. Other internal security mechanisms are not addressed by SFR but ADV_ARC activities.

[140] This explains why “FPT_RCV.3/OS” and “FPT_RCV.4/OS” are not actually present in [PP-JCS], however these two SFRs cover environmental security objectives initially defined in [PP-JCS] and then

FPT_RCV.3/OS Automated recovery without undue loss

FPT_RCV.3.1/OS When automated recovery from **none, see application note below**[141] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_RCV.3.2/OS For **execution access to a memory zone reserved for TSF data, writing access to a memory zone reserved for TSF's code, and any segmentation fault performed by a Java Card applet**[142] the TSF shall ensure the return of the TOE to a secure state using automated procedures.

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

- **the contents of Java Card static fields, instance fields, and array positions that fall under the scope of an open transaction;**
- **the Java Card objects that were allocated into the scope of an open transaction;**
- **the contents of Java Card transient objects;**
- **any possible Executable Load File being loaded when the failure occurred**[143]

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

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

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

FPT_RCV.4/OS Function recovery

FPT_RCV.4.1/OS The TSF shall ensure that **reading from and writing to static and objects' fields interrupted by power loss**[144] have the property that the function either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

9.2 SECURITY ASSURANCE REQUIREMENTS

This ST is based on the EAL4 assurance package augmented with the components AVA_VAN.5 and ALC_DVS.2.

9.3 SECURITY REQUIREMENTS RATIONALE

9.3.1 *TOE security objectives coverage – Mapping table*

Security Objective	SFRs
O.PSF	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FMT_MSA.1/POL1, FMT_MSA.1/PSF_DATA, FPT_FLS.1, FCS_RNG.1

refined in [PP-SGP05] (OE.IC.RECOVERY and OE.IC.SUPPORT) which have become TOE security objectives in the present ST (O.IC.RECOVERY and O.IC.SUPPORT).

[141] [assignment: list of failures/service discontinuities during card content management operations]

[142] [assignment: list of failures/service discontinuities during card content management operations]

[143] [assignment: quantification]

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

Security Objective	SFRs
O.eUICC-DOMAIN-RIGHTS	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FTP_ITC.1/SCP, FMT_MSA.1/POL1, FMT_MSA.1/PSF_DATA, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FCS_RNG.1
O.SECURE-CHANNELS	FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP, FCS_CKM.1/SCP-SM, FCS_COP.1/ECKA-EG, FCS_CKM.2/SCP-MNO, FCS_CKM.4/SCP-SM, FCS_CKM.4/SCP-MNO, FIA_UID.1/EXT, FIA_UAU.1/EXT, FCS_COP.1/AUTH_SMSR, FCS_COP.1/AUTH_SMDP, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD , FIA_USB.1/MNO-SD, FIA_USB.1/EXT, FIA_ATD.1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
O.INTERNAL-SECURE-CHANNELS	FPT_EMS.1, FDP_SDI.1, FDP_RIP.1
O.PROOF_OF_IDENTITY	FIA_API.1
O.OPERATE	FPT_FLS.1/Platform_services
O.API	FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FMT_MSA.3, FMT_SMR.1, FMT_SMF.1, FPT_FLS.1/Platform_services
O.DATA-CONFIDENTIALITY	FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FPT_EMS.1, FDP_RIP.1, FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network FCS_CKM.4/Mobile_network
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FDP_SDI.1
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network, FCS_CKM.4/Mobile_network
O.IC.PROOF_OF_IDENTITY	Addressed by FAU_SAS.1 of [ST_IC]
O.IC.SUPPORT	FPT_RCV.4/OS
O.IC.RECOVERY	FPT_RCV.3/OS
O.RE.PSF	FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_ITC.2/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL, FDP_ITC.2/GP-KL, FMT_MSA.1/GP, FMT_MSA.3/GP, FMT_SMR.1/GP, FMT_SMF.1/GP, FPT_RCV.3/GP, FPT_FLS.1/GP, FPT_TDC.1/GP, FTP_ITC.1/GP, FCO_NRO.2/GP, FIA_UID.1/GP, FDP_UIT.1/GP, FDP_ROL.1/GP, FDP_UCT.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FIA_AFL.1/GP, FCS_CKM.4/GP, FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP, FDP_ACC.1/GP-ELFU, FDP_ACF.1/GP-ELFU, FDP_ROL.1/GP-ELFU, FMT_MSA.1/GP-ELFU, FMT_MSA.3/GP-ELFU, FMT_SMF.1/GP-ELFU, FPT_FLS.1/GP-ELFU, FPT_TDC.1, FMT_MTD.1/JCRE, FDP_ACC.2/ADEL, FDP_ACF.1/ADEL, FDP_RIP.1/ADEL, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL, FPT_FLS.1/ADEL
O.RE.SECURE-COMM	FCS_CKM.1/GP-SCP, FCS_CKM.4/GP, FCS_COP.1/GP-SCP, FMT_MSA.1/GP, FMT_MSA.3/GP, FMT_SMR.1/GP, FMT_SMF.1/GP, FPT_TDC.1/GP, FTP_ITC.1/GP, FIA_UID.1/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FPR_UNO.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FIA_AFL.1/GP, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_RIP.1/APDU,

Security Objective	SFRs
	FDP_RIP.1/KEYS, FAU_ARP.1, FDP_SDI.2/DATA, FPR_UNO.1, FPT_FLS.1/JCS
O.RE.API	FDP_ACF.1/FIREWALL
O.RE.DATA-CONFIDENTIALITY	FPR_UNO.1/GP, FIA_AFL.1/ETSI-PIN, FPR_UNO.1/ETSI-PIN, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FDP_RIP.1/OBJECTS, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_RIP.1/ABORT, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT, FDP_ROL.1/FIREWALL, FAU_ARP.1, FPR_UNO.1, FPT_FLS.1/JCS, FDP_RIP.1/ADEL, FDP_RIP.1/ODEL, FPT_FLS.1/ODEL
O.RE.DATA-INTEGRITY	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_ROL.1/FIREWALL, FAU_ARP.1, FDP_SDI.2/DATA, FPT_FLS.1/JCS
O.RE.IDENTITY	FIA_ATD.1/AID, FIA_UID.2/AID, FIA_USB.1/AID, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE
O.RE.CODE-EXE	FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS
O.SECURE_LOAD_ACODE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC, FCS_COP.1/OS-UPDATE-VER, FPT_FLS.1/OS-UPDATE, FCS_CKM.4/GP
O.SECURE_AC_ACTIVATION	FMT_SMF.1/OS-UPDATE, FPT_FLS.1/OS-UPDATE
O.TOE_IDENTIFICATION	FIA_ATD.1/OS-UPDATE
O.CONFID-UPDATE-IMAGE.LOAD	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FTP_TRP.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-DEC, FCS_CKM.4/GP
O.AUTH-LOAD-UPDATE-IMAGE	FDP_ACC.1/OS-UPDATE, FDP_ACF.1/OS-UPDATE, FMT_MSA.3/OS-UPDATE, FMT_SMR.1/OS-UPDATE, FCS_COP.1/OS-UPDATE-VER, FPT_FLS.1/OS-UPDATE, FCS_CKM.4/GP

Table 14: TOE Security Objectives coverage by SFRs – Mapping table

9.3.2 *TOE security objectives coverage – Rationale*

O.PSF is fulfilled by the following SFRs:

- All SFRs related to Security Domains (FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD and FDP_ACF.1/ECASD) cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that meets the card content management rules.
- FMT_MSA.1/POL1 supports these SFRs by ensuring management of the POL1 policy file and connectivity parameters file, which ensures that lifecycle modifications and connection to remote entity are made according to the authorized policy.
- FMT_MSA.1/PSF_DATA restricts the state transitions that can apply to PSF data (ISD-P state and Fallback attribute) that are used as security attributes by other security policies of the TSF (ISD-R access control SFP and ISD-P access control SFP).
- The objective also requires a secure failure mode as described in FPT_FLS.1.

- FCS_RNG.1 is required to support FDP_ACF.1/ECASD.

O.eUICC-DOMAIN-RIGHTS is fulfilled by the following SFRs:

- The requirements FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD and FDP_ACF.1/ECASD ensure that ISD-R, ISD-P, MNO-SD and ECASD functionality and content are only accessible to the corresponding authenticated user. FTP_ITC.1/SCP provide the corresponding secure channels to the authorized users.
- FMT_MSA.1/POL1, FMT_MSA.1/PSF_DATA, FMT_MSA.1/CERT_KEYS and FMT_MSA.3 address the management of the security attributes used by the SFP.
- FCS_RNG.1 is required to support FDP_ACF.1/ECASD.

NB: there is no secure channel to access ECASD, since its services can be accessed by on-card actors, but its content cannot be modified during the lifecycle of the eUICC.

O.SECURE-CHANNELS is fulfilled by the following SFRs:

- The requirements FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP, cover this security objective by enforcing Secure Channel Protocol information flow control SFP that ensures that transmitted commands and data are protected from unauthorized disclosure and modification. They rely on FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.4/SCP-SM and FCS_CKM.4/SCP-MNO for key management. FCS_COP.1/ECKA-EG is also involved as it supports FCS_CKM.1/SCP-SM.
- Identification and authentication SFRs (FIA_UID.1/EXT, FIA_UAU.1/EXT, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD , FIA_USB.1/MNO-SD, FIA_USB.1/EXT) support this security objective by requiring authentication and identification from the distant SM-DP, SM-SR and MNO OTA Platform in order to establish these secure channels. FCS_COP.1/AUTH_SMSR and FCS_COP.1/AUTH_SMDP are also involved as it supports FIA_UAU.1/EXT.
- FIA_ATD.1, FMT_MSA.1/CERT_KEYS and FMT_MSA.3 address the management of the security attributes used by the SFP.
- FMT_SMF.1 and FMT_SMR.1 support these SFRs by providing management of roles and management of functions.

O.INTERNAL-SECURE-CHANNELS is fulfilled by the following SFRs:

- FPT_EMS.1 ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks. This includes in particular the shared secrets transmitted between ECASD and ISD-R/ISD-P.
- FDP_SDI.1 ensures that the shared secret cannot be modified during this transmission.
- FDP_RIP.1 ensures that the shared secret cannot be recovered from deallocated resources.

O.PROOF_OF_IDENTITY is covered by the extended requirement FIA_API.1.

O.OPERATE is covered by FPT_FLS.1/Platform_services which requires that failures do not impact the security of the TOE.

O.API is fulfilled by the following SFRs:

- FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FMT_MSA.3 and FMT_SMR.1 and FMT_SMF.1 state the policy for controlling the access to TOE services and resources by the Application Layer ("API information flow control policy").
- Atomicity is provided by the FPT_FLS.1/Platform_services requirement.

O.DATA-CONFIDENTIALITY is fulfilled by the following SFRs:

- FDP_UCT.1/SCP addresses the reception of data from off-card actors, while the access control SFPs (FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD) address the isolation between Security Domains.
- FPT_EMS.1 ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks.
- FDP_RIP.1 ensures that no residual confidential data is available.

- FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network and FCS_CKM.4/Mobile_network address the cryptographic algorithms present in the Telecom Framework, the distribution and the destruction of associated keys.

O.DATA-INTEGRITY is fulfilled by the following SFRs:

- FDP_UIT.1/SCP addresses the reception of data from off-card actors, while the access control SFPs (FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD) address the isolation between Security Domains.
- FDP_SDI.1 specifies the Profile data that is monitored in case of an integrity breach (for example modification of the received profile during the installation operation).

O.ALGORITHMS is fulfilled by the following SFRs:

- The algorithms are defined in FCS_COP.1/Mobile_network.
- FCS_CKM.2/Mobile_network describes how the keys are distributed within the MNO profiles, and FCS_CKM.4/Mobile_network describes the destruction of the keys.

O.IC.PROOF_OF_IDENTITY states that the underlying IC used by the TOE is uniquely identified; as such it directly targets the IC. It is directly covered by FAU_SAS.1 of [ST_IC], which deals with “Audit storage, addressing Lack of TOE identification”, as mentioned in [ST_IC] table 7.

O.IC.SUPPORT is addressed by FPT_RCV.4/OS which deals with recovery operations.

O.IC.RECOVERY is addressed by FPT_RCV.3/OS which deals with recovery operations.

O.RE.PSF is fulfilled by the following SFRs:

- SFRs from [PP-GP]:
  - FDP_IFC.2/GP-ELF, FDP_IFF.1/GP-ELF, FDP_IFC.2/GP-KL, FDP_IFF.1/GP-KL enforce the information flow control policy for managing, authenticating, and protecting the Card management commands and responses between off-card and on-card entities.
  - FDP_ITC.2/GP-ELF enforces the ELF loading information flow policy when importing ELFs.
  - FDP_ITC.2/GP-KL enforces the Data & Key information flow policy when importing keys and data.
  - FMT_MSA.1/GP and FMT_MSA.3/GP specify security attributes enabling to ensure the authenticity, integrity, and/or confidentiality of card management commands.
  - FIA_UID.1/GP, FIA_UAU.1/GP and FIA_UAU.4/GP ensure appropriate identification and authentication mechanisms. In addition, these SFRs specify the actions being performed before the authentication of the origin of the received APDU commands takes place.
  - FTP_ITC.1/GP requires a trusted channel for authenticating the card management commands and for securely protecting (authenticity, integrity, and/or confidentiality) the loading of ELF/data.
  - FPT_FLS.1/GP requires the card to preserve a secure state when failures occur during loading/installing/deleting an Executable File / application instance.
  - FCS_COP.1/GP-DAP_SHA, FCS_COP.1/GP-DAP_VER, FCO_NRO.2/GP-DAP ensure that ELFs received by the TOE have been generated by an authorized actor (integrity and authenticity evidence).
  - FDP_UIT.1/GP ensures the integrity of card management operations.
  - FDP_UCT.1/GP ensures the confidentiality of card management operations.
  - FMT_SMF.1/GP enforces the card management operations (Loading, Installation, etc.), the privileges, the life cycle states and transition by defining the protective actions for the belonging commands.
  - FDP_ROL.1/GP ensures the rollback of the installation or removal operation on the executable files and application instances.
  - FCO_NRO.2/GP enforces the evidence of the origin during the loading of Executable Load Files, SD/Application data and keys.
  - FPT_TDC.1/GP specifies requirements preventing any possible misinterpretation of the Security Domain keys used to implement a Secure Channel when those are loaded from the off-card entity.

  - FPT_RCV.3/GP ensures safe recovery from failure.
  - FIA_AFL.1/GP supports the objective by bounding the number of signatures that the attacker may try to attach to a message to authenticate its origin.
  - FCS_CKM.4/GP which deals with the secure destruction of DAP keys
  - FMT_SMR.1/GP maintains the roles S.OPEN, S.SD, Application and is able to associate these roles to the users owning SDs.
  - All the SFRs dealing with the ELF Upgrade capability according to [Amd H]: FDP_ACC.1/GP-ELFU, FDP_ACF.1/GP-ELFU, FDP_ROL.1/GP-ELFU, FMT_MSA.1/GP-ELFU, FMT_MSA.3/GP-ELFU, FMT_SMF.1/GP-ELFU, FPT_FLS.1/GP-ELFU
- SFRs from [PP-JCS]:
  - All the SFRs dealing with applet deletion: FDP_ACC.2/ADEL, FDP_ACF.1/ADEL, FDP_RIP.1/ADEL, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL, FPT_FLS.1/ADEL
  - FPT_TDC.1 dealing with the correct interpretation of CAP files, bytecodes and associated data
  - FMT_MTD.1/JCRE which ensures that JCRE is the only subject able to modify the list of registered applets' AIDs

O.RE.SECURE-COMM is fulfilled by the following SFRs:

- SFRs from [PP-GP]:
  - All SFRs supporting or related to Secure Channel: FCS_CKM.1/GP-SCP, FCS_COP.1/GP-SCP, FCS_CKM.4/GP, FIA_UID.1/GP, FDP_UIT.1/GP, FDP_UCT.1/GP, FIA_UAU.1/GP, FIA_UAU.4/GP, FIA_AFL.1/GP, FTP_ITC.1/GP, FPR_UNO.1/GP, FPT_TDC.1/GP
  - Associated requirements of the class FMT: FMT_MSA.1/GP, FMT_MSA.3/GP, FMT_SMR.1/GP, FMT_SMF.1/GP
- SFRs from [PP-JCS]:
  - FDP_ACC.2/FIREWALL and FDP_ACF.1/FIREWALL (FIREWALL access control policy)
  - FDP_IFF.1/JCVM, FDP_IFC.1/JCVM (JCVM information flow control policy
  - Associated requirements of the class FMT: FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FMT_SMR.1/JCS, FMT_SMF.1/JCS, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM also indirectly contribute to meet this objective.
  - FDP_RIP.1/APDU, FDP_RIP.1/KEYS, FPR_UNO.1 which address confidentiality protection of the APDU buffer and of cryptographic keys.
  - FDP_SDI.2/DATA which addresses integrity protection of cryptographic keys
  - FAU_ARP.1 and FPT_FLS.1/JCS which defines the security reaction to a firewall violation and ensures the TOE remains in a secure state.

O.RE.API is covered by FDP_ACF.1/FIREWALL: the only means to execute native code is the invocation of a Java Card API method.

O.RE.DATA-CONFIDENTIALITY is fulfilled by the following SFRs:

- SFRs from [PP-GP]:
  - FPR_UNO.1/GP and FPR_UNO.1/ETSI-PIN which ensure unobservability of operations on PIN and keys
  - FIA_AFL.1/ETSI-PIN which ensures PIN protection against brute-force attacks
- SFRs from [PP-JCS]:
  - All SFRs related to the enforcement of the Javacard firewall: FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FDP_ROL.1/FIREWALL, FMT_SMF.1/JCS, FMT_SMR.1/JCS
  - FPR_UNO.1 which ensures unobservability of operations on PIN and keys

  - SFRs related to residual information protection: FDP_RIP.1/OBJECTS, FDP_RIP.1/ABORT, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT, FDP_RIP.1/ADEL, FDP_RIP.1/ODEL
  - SFRs dealing with security reaction: FAU_ARP.1, FPT_FLS.1/JCS, FPT_FLS.1/ODEL

O.RE.DATA-INTEGRITY is fulfilled by the following SFRs from [PP-JCS]:

- All SFRs related to the enforcement of the Javacard firewall: FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS, FDP_ROL.1/FIREWALL
- SFRs dealing with security reaction: FAU_ARP.1, FPT_FLS.1/JCS
- FDP_SDI.2/DATA which deals with integrity protection of sensitive data such as PIN and keys.

O.RE.IDENTITY is fulfilled by the following SFRs from [PP-JCS] related to AID management: FIA_ATD.1/AID, FIA_UID.2/AID, FIA_USB.1/AID, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE.

O.RE.CODE-EXE is fulfilled by the following [PP-JCS] SFRs which enforce the Javacard firewall: FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_SMF.1/JCS, FMT_SMR.1/JCS

O.SECURE_LOAD_ACODE is fulfilled by the following SFRs:

- FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code.
- FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code.
- FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation.
- FCS_COP.1/OS-UPDATE-DEC specifies the cryptographic algorithms used to decrypt the additional code prior to installation.
- FCS_COP.1/OS-UPDATE-VER specifies the cryptographic algorithms used to perform digital signature verification of the additional code to be loaded.
- FPT_FLS.1/OS-UPDATE ensures that the TOE always remains in a secure state during the loading, installation, and activation of additional code.
- FCS_CKM.4/GP which deals with the secure destruction of OS Update keys

O.SECURE_AC_ACTIVATION is fulfilled by the following SFRs:

- FMT_SMF.1/OS-UPDATE manages the activation of additional code.
- FPT_FLS.1/OS-UPDATE ensures that the TOE always remains in a secure state during the loading, installation, and activation of additional code.

O.TOE_IDENTIFICATION is directly fulfilled by FIA_ATD.1/OS-UPDATE which maintains the additional code ID for each activated additional code.

O.CONFID-UPDATE-IMAGE.LOAD is fulfilled by the following SFRs:

- FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code.
- FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation.
- FTP_TRP.1/OS-UPDATE provides a trusted path during the transmission of the additional code to the TOE for loading.
- FCS_COP.1/OS-UPDATE-DEC specifies the cryptographic algorithms used to decrypt the additional code prior to installation.
- FCS_CKM.4/GP which deals with the secure destruction of OS Update keys.

O.AUTH-LOAD-UPDATE-IMAGE is fulfilled by the following SFRs:

- FDP_ACC.1/OS-UPDATE and FDP_ACF.1/OS-UPDATE enforce the OS Update Access Control Policy on the loading, installation, and activation of additional code.

- FMT_MSA.3/OS-UPDATE specifies security attributes that support management of the loading, installation, and activation of additional code.
- FMT_SMR.1/OS-UPDATE maintains the role of OS Developer, which is responsible for signature verification and decryption of additional code before Loading, Installation, and Activation.
- FCS_COP.1/OS-UPDATE-VER specifies the cryptographic algorithms used to perform digital signature verification of the additional code to be loaded.
- FPT_FLS.1/OS-UPDATE ensures that the TOE always remains in a secure state during the loading, installation, and activation of additional code.
- FCS_CKM.4/GP which deals with the secure destruction of OS Update keys.

9.3.3 *SFR dependency rationale*

Security Functional Requirement	CC dependencies	Satisfied dependencies
FIA_UID.1/EXT	No dependencies	▨
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FCS_COP.1/AUTH_SMSR	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/SCP-SM
FCS_COP.1/AUTH_SMDP	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/SCP-SM
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1
FIA_UAU.4/EXT	No dependencies	▨
FIA_UID.1/MNO-SD	No dependencies	▨
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1	No dependencies	▨
FIA_API.1	No dependencies	▨
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP FMT_MSA.3
FTP_ITC.1/SCP	No dependencies	▨
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP FTP_ITC.1/SCP FPT_TDC.1/SCP
FPT_TDC.1/SCP	No dependencies	▨
FDP_UCT.1/SCP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.1/SCP FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FCS_COP.1/ECKA-EG FCS_COP.1/GP-SCP
FCS_COP.1/ECKA-EG	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM FDP_ITC.2/SCP
FCS_CKM.2/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/SCP-MNO
FCS_CKM.4/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP FCS_CKM.1/SCP-SM
FCS_CKM.4/SCP-MNO	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP FCS_CKM.1/SCP-SM
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR FMT_MSA.3
FDP_ACC.1/ISDP	(FDP_ACF.1)	FDP_ACF.1/ISDP
FDP_ACF.1/ISDP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDP FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services FMT_MSA.3

Security Functional Requirement	CC dependencies	Satisfied dependencies
FPT_FLS.1/Platform_Services	No dependencies	
FCS_RNG.1	No dependencies	
FPT_EMS.1	No dependencies	
FDP_SDI.1	No dependencies	
FDP_RIP.1	No dependencies	
FPT_FLS.1	No dependencies	
FMT_MSA.1/PSF_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_ACC.1/ISDP FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/POL1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_ACC.1/ISDP FDP_IFC.1/SCP FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR FDP_ACC.1/ISDP FDP_IFC.1/SCP FDP_ACC.1/ECASD FMT_SMF.1 FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PSF_DATA FMT_MSA.1/POL1 FMT_MSA.1/CERT_KEYS FMT_SMR.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT FIA_UID.1/MNO-SD
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/Mobile_network
FCS_CKM.2/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and (FCS_CKM.4)	FDP_ITC.2/SCP FCS_CKM.4/Mobile_network
FCS_CKM.4/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/SCP
FDP_IFC.2/GP-ELF	(FDP_IFF.1)	FDP_IFF.1/GP-ELF
FDP_IFF.1/GP-ELF	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-ELF FMT_MSA.3/GP
FDP_ITC.2/GP-ELF	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FPT_TDC.1/GP FTP_ITC.1/GP
FDP_IFC.2/GP-KL	(FDP_IFF.1)	FDP_IFF.1/GP-KL
FDP_IFF.1/GP-KL	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/GP-KL FMT_MSA.3/GP
FDP_ITC.2/GP-KL	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-KL FPT_TDC.1/GP FTP_ITC.1/GP
FCS_CKM.1/GP-SCP	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1/GP-SCP FCS_CKM.4/GP
FCS_COP.1/GP-SCP	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1/GP-SCP FCS_CKM.4/GP
FMT_MSA.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FMT_SMR.1/GP FMT_SMF.1/GP
FMT_MSA.3/GP	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP FMT_SMR.1/GP
FMT_SMR.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/GP	No dependencies	
FPT_RCV.3/GP	(AGD_OPE.1)	AGD_OPE.1
FPT_FLS.1/GP	No dependencies	
FPT_TDC.1/GP	No dependencies	
FTP_ITC.1/GP	No dependencies	
FCO_NRO.2/GP	(FIA_UID.1)	FIA_UID.1/GP

Security Functional Requirement	CC dependencies	Satisfied dependencies
FIA_UID.1/GP	No dependencies	▨
FDP_UIT.1/GP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FDP_ROL.1/GP	(FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL
FDP_UCT.1/GP	(FTP_ITC.1 or FTP_TRP.1) and (FDP_ACC.1 or FDP_IFC.1)	FDP_IFC.2/GP-ELF FDP_IFC.2/GP-KL FTP_ITC.1/GP
FPR_UNO.1/GP	No dependencies	▨
FIA_UAU.1/GP	(FIA_UID.1)	FIA_UID.1/GP
FIA_UAU.4/GP	No dependencies	▨
FIA_AFL.1/GP	(FIA_UAU.1)	FIA_UAU.1/GP
FCS_CKM.4/GP	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FDP_ITC.2/GP-ELF FDP_ITC.2/GP-KL FCS_CKM.1/GP-SCP
FIA_AFL.1/ETSI-PIN	(FIA_UAU.1)	FIA_UAU.1/GP
FPR_UNO.1/ETSI-PIN	No dependencies	▨
FCS_COP.1/GP-DAP_SHA	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/GP-ELF FCS_CKM.4/GP
FCS_COP.1/GP-DAP_VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/GP-ELF FCS_CKM.4/GP
FCO_NRO.2/GP-DAP	(FIA_UID.1)	FIA_UID.1/GP
FDP_ACC.1/GP-ELFU	(FDP_ACF.1)	FDP_ACF.1/GP-ELFU
FDP_ACF.1/GP-ELFU	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/GP-ELFU FMT_MSA.3/GP-ELFU
FDP_ROL.1/GP-ELFU	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/GP-ELFU
FMT_MSA.1/GP-ELFU	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/GP-ELFU FMT_SMR.1/GP FMT_SMF.1/GP-ELFU
FMT_MSA.3/GP-ELFU	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/GP-ELFU FMT_SMR.1/GP
FMT_SMF.1/GP-ELFU	No dependencies	▨
FPT_FLS.1/GP-ELFU	No dependencies	▨
FDP_ACC.1/OS-UPDATE	(FDP_ACF.1)	FDP_ACF.1/OS-UPDATE
FDP_ACF.1/OS-UPDATE	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/OS-UPDATE FMT_MSA.3/OS-UPDATE
FMT_MSA.3/OS-UPDATE	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1/OS-UPDATE **See rationale**
FMT_SMR.1/OS-UPDATE	(FIA_UID.1)	FIA_UID.1/GP
FMT_SMF.1/OS-UPDATE	No dependencies	▨
FIA_ATD.1/OS-UPDATE	No dependencies	▨
FTP_TRP.1/OS-UPDATE	No dependencies	▨
FCS_COP.1/OS-UPDATE-DEC	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/GP-ELF FCS_CKM.4/GP
FCS_COP.1/OS-UPDATE-VER	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/GP-ELF FCS_CKM.4/GP
FPT_FLS.1/OS-UPDATE	No dependencies	▨
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/JCS **See rationale**
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM FMT_SMF.1/JCS FMT_SMR.1/JCS

Security Functional Requirement	CC dependencies	Satisfied dependencies
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/JCS
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_SMR.1/JCS
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM FMT_SMR.1/JCS
FMT_SMF.1/JCS	No dependencies	
FMT_SMR.1/JCS	(FIA_UID.1)	FIA_UID.2/AID
FDP_RIP.1/ABORT	No dependencies	
FDP_RIP.1/APDU	No dependencies	
FDP_RIP.1/GlobalArray	No dependencies	
FDP_RIP.1/bArray	No dependencies	
FDP_RIP.1/KEYS	No dependencies	
FDP_RIP.1/TRANSIENT	No dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAA.1)	**See rationale**
FDP_SDI.2/DATA	No dependencies	
FPR_UNO.1	No dependencies	
FPT_FLS.1/JCS	No dependencies	
FPT_TDC.1	No dependencies	
FIA_ATD.1/AID	No dependencies	
FIA_UID.2/AID	No dependencies	
FIA_USB.1/AID	(FIA_ATD.1)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1/JCS FMT_SMR.1/JCS
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL FMT_SMF.1/ADEL FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	**See rationale**
FPT_FLS.1/ADEL	No dependencies	
FDP_RIP.1/ODEL	No dependencies	
FPT_FLS.1/ODEL	No dependencies	
FPT_RCV.3/OS	(AGD_OPE.1)	AGD_OPE.1
FPT_RCV.4/OS	No dependencies	

Rationale for the exclusion of dependencies:

- **The dependency FMT_MSA.1 of FMT_MSA.3/OS-UPDATE is unsupported.**
  No history information has to be kept by the TOE.
- **The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is unsupported.**
  The dependency between FMT_MSA.1/JCRE and FMT_SMF.1 is not satisfied because no management functions are required for the Java Card RE.
- **The dependency FAU_SAA.1 of FAU_ARP.1 is unsupported**
  The dependency of FAU_ARP.1 on FAU_SAA.1 assumes that a “potential security violation” generates an audit event. On the contrary, the events listed in FAU_ARP.1 are self-contained (arithmetic exception, ill-formed bytecodes, access failure) and ask for a straightforward reaction of the TSFs on their occurrence at runtime. The JCVM or other components of the TOE

detect these events during their usual working order. Thus, there is no mandatory audit recording in this ST.

- **The dependency FIA_UID.1 of FMT_SMR.1/ADEL is unsupported**
  This ST does not require the identification of the “deletion manager” since it can be considered as part of the TSF.

9.3.4 *SAR – Evaluation Assurance Level Rationale*

The EAL4 package and addition of ALC_DVS.2 and AVA_VAN.5 are required by [PP-SGP05].

9.3.5 *SAR – Dependency rationale*

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

Security Assurance Requirement	CC dependencies	Satisfied dependencies
		ATE_DPT.1

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

9.4 Composition Tasks – SFR Part

The following table (see next page) lists the SFRs that are declared in the security target [ST_IC], and separates them in relevant platform[145]-SFRs (RP_SFR-SERV and RP_SFR-MECH[146]) and irrelevant platform-SFRs (IP_SFR), as requested in [CCDB]. The table also provides the link between the relevant platform-SFRs and the composite product SFRs.

[145] Using the composition tasks terminology, the platform is the ST33K1M5 chip.

[146] RP_SFR-SERV designates relevant IC SFRs used by the composite TOE to implement security services with associated TSFI. RP_SFR-MECH designates relevant IC SFRs used by the composite TOE as mechanisms to provide global protection against attacks.

Platform-SFR	Platform-SFR title	Addressing (as stated in platform ST)	RP_SFR -SERV	RP_SFR-MECH	IP_SFR	Composite product SFRs
FRU_FLT.2	Limited fault tolerance	Malfunction		X		No direct link to composite TOE SFRs but provides global protection against attacks.
FPT_FLS.1	Failure with preservation of secure state			X		
FMT_LIM.1/Test	Limited capabilities – Test	Abuse of Test functionality		X		No direct link to composite TOE SFRs but provides global protection against attacks.
FMT_LIM.2/Test	Limited availability – Test			X		
FAU_SAS.1	Audit storage	Lack of TOE identification		X		No direct link to composite TOE SFRs but used for the composite-product identification.
FDP_SDC.1	Stored data confidentiality	Physical manipulation and probing		X		No direct link to composite TOE SFRs but provides global protection against attacks.
FDP_SDI.2	Stored data integrity monitoring and action			X		
FPT_PHP.3	Resistance to physical attack			X		
FDP_ITT.1	Basic internal transfer protection	Leakage		X		FPR_UNO.1
FPT_ITT.1	Basic internal TSF data transfer protection			X		
FDP_IFC.1	Subset information flow control			X		
FCS_RNG.1 / PTG.2	Random number generation - PTG.2	Weak cryptographic quality of random numbers	X			FCS_RNG.1
FCS_COP.1	Cryptographic operation	Cipher scheme support	X			FCS_COP.1/Mobile_network FCS_COP.1/GP-SCP FCS_COP.1/GP-DAP_VER FCS_COP.1/OS-UPDATE-DEC FCS_COP.1/OS-UPDATE-VER
FDP_ACC.2/Memories	Complete access control – Memories	Memory access violation	X			FDP_ACC.2/FIREWALL
FDP_ACF.1/Memories	Security attribute based access control - Memories		X			FDP_ACF.1/FIREWALL
FMT_MSA.3/Memories	Static attribute initialization – Memories	Correct operation	X			FMT_MSA.3/FIREWALL FMT_MSA.3/JCVM
FMT_MSA.1/Memories	Management of security attributes – Memories		X			FMT_MSA.1/JCRE FMT_MSA.1/JCVM

Platform-SFR	Platform-SFR title	Addressing (as stated in platform ST)	RP_SFR -SERV	RP_SFR-MECH	IP_SFR	Composite product SFRs
FMT_SMF.1/Memories	Specification of management functions - Memories		X			FMT_SMF.1/JCS
FIA_API.1	Authentication Proof of Identity	Masquerade		X		No direct link to composite TOE SFRs. Note that the IC Loader is no more available after phase c. However, this IC SFR is essential to protect the composite TOE during phases b and c.
FMT_LIM.1/Loader	Limited capabilities - Loader	Abuse of Loader functionality			X	Not applicable to the composite TOE, as the IC Loader is no more available after phase c.
FMT_LIM.2/Loader	Limited availability - Loader			X		No direct link to composite TOE SFRs, however this IC SFR participates to the composite TOE protection during phases d and e.
FTP_ITC.1/Loader	Inter-TSF trusted channel - Loader	Loader violation		X		No direct link to composite TOE SFRs. Note that the IC Loader is no more available after phase c. However, these IC SFRs are essential to protect the composite TOE during phases b and c.
FDP_UCT.1/Loader	Basic data exchange confidentiality - Loader			X		
FDP_UIT.1/Loader	Data exchange integrity - Loader			X		
FDP_ACC.1/Loader	Subset access control - Loader			X		
FDP_ACF.1/Loader	Security attribute based access control - Loader			X		
FMT_MSA.3/Loader	Static attribute initialization - Loader	Correct Loader operation		X		No direct link to composite TOE SFRs. Note that the IC Loader is no more available after phase c. However, these IC SFRs are essential to protect the composite TOE during phases b and c.
FMT_MSA.1/Loader	Management of security attributes - Loader			X		
FMT_SMR.1/Loader	Security roles – Loader			X		
FIA_UID.1/Loader	Timing of identification - Loader			X		
FIA_UAU.1/Loader	Timing of authentication – Loader			X		
FMT_SMF.1/Loader	Specification of management functions - Loader			X		

Platform-SFR	Platform-SFR title	Addressing (as stated in platform ST)	RP_SFR -SERV	RP_SFR-MECH	IP_SFR	Composite product SFRs
FPT_FLS.1/Loader	Failure with preservation of secure state – Loader			X		
FAU_SAR.1/Loader	Audit review – Loader	Lack of TOE identification		X		No contradiction with composite TOE SFRs.
FAU_SAS.1/Loader	Audit storage – Loader			X		
FTP_ITC.1/Sdiag	Inter-TSF trusted channel – Secure Diagnostic	Abuse of Secure Diagnostic functionality		X		No direct link to composite TOE SFRs, however these IC SFRs are essential to ensure that the Secure Diagnostic capability cannot be used during phases d and e by an unauthorized actor to bypass the SFRs of the composite TOE.
FAU_SAR.1/Sdiag	Audit review – Secure Diagnostic			X		
FMT_LIM.1/Sdiag	Limited capabilities – Secure Diagnostic			X		
FMT_LIM.2/Sdiag	Limited availability – Secure Diagnostic			X		

10 TOE summary specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The security functionalities concerning the IC are described in [ST_IC] and are not redefined in this security target, although they must be considered for the TOE.

10.1 SECURITY FUNCTIONS RELATED TO RSP AND TELECOM FEATURES

GSMA.Ident-Auth

This security function handles the identification and authentication of TOE external actors, according to the [GSMA] specifications:

- Identification and authentication of U.SM-SR
- Identification and authentication of U.SM-DP
- Identification and authentication of U.MNO-OTA
- Identification and authentication of U.MNO-SD

For each actor, all aspects of identification and authentication are implemented according to the [GSMA] specifications, such as:

- Allowed operations before identification/authentication is performed
- Authentication processes (through certificate verification, SCP establishment…)
- Related cryptographic operations
- Definition of security attributes
- User/subject binding
- Prevention of the reuse of authentication data

This security function also provides a proof of the identity of the eUICC to external actors. This proof is obtained by including the EID value in the eUICC certificate, which is signed by the eUICC Manufacturer.

GSMA.SecureChannels

This security function handles the secure channel requirements specified by [GSMA]:

- Between U.SM-SR and S.ISD-R
- Between U.SM-DP and S.ISD-P
- Between U.MNO-OTA and U.MNO-SD
- The related SCPs are SCP03(t), SCP80 and SCP81
- The related SM-SR, SM-DP and MNO-OTA commands, as well as the required protection level (integrity and/or confidentiality), are those specified in [GSMA].
- The generation of ISD-R and ISD-P keysets is also handled by this security function. This operation is also implemented according to [GSMA] specifications.

GSMA.SecurityDomains

This security function implements the [GSMA] requirements related to the ISD-R, ISD-P and e-CASD security domains:

- Enforcement of the ISD-R Access Control policy
- Enforcement of the ISD-P Access Control policy
- Enforcement of the e-CASD Access Control policy.

GSMA.PlatformServices

This security function monitors the information flow between S.ISD-R, S.ISD-P, U.MNO-SD and the underlying Telecom environment during profile installation, network authentication and profile policy enforcement. In particular, the security function ensures that:

- D.PROFILE-NAA-PARAMS can be transmitted only:
  - by U.MNO-SD to S.TELECOM in order to execute the "Network authentication" API function
  - by S.ISD-P to S.PSF using the "Installation" API function.

- D.PROFILE-POL1 can be transmitted only by S.ISD-P to S.PSF in order to execute the "POL1 enforcement" function.

This security function also ensures that the TOE remains in a secure state in case some failures occur during such information flow.

GSMA.SecurityMngt

This security function handles general security requirements related to the GSMA assets, such as:

- Integrity protection of the following GSMA assets: D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS, D.PROFILE_NAA_PARAMS, D.PROFILE_IDENTITY, D.PROFILE_POL1, D.eUICC_PRIVKEY, D.eUICC_CERT, D.CI_ROOT_PUBKEY, D.EID, D.SECRETS.
- Removal of the content of the following GSMA assets/objects upon deallocation/allocation: D.SECRETS, D.eUICC_PRIVKEY, D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS, D.PROFILE_NAA_PARAMS.
- Ensuring that the TOE remains in a secure state in case of failure during creation of a new ISD-P by ISD-R, during creation of a profile by ISD-P or during installation due to the presence of an orphaned profile.
- Management of ISD-P state and related transitions, and of the fallback attribute, according to the [GSMA] specifications.
- Management of the operations on D.PROFILE_POL1 according to the [GSMA] specifications.
- Management of the operations on CERT.DP.ECDSA, CERT.SR.ECDSA, D.ISDP_KEYS, D.ISDR_KEYS, D.MNO_KEYS according to the [GSMA] specifications.
- Management of roles according to [GSMA] specifications.

GSMA.NetworkAuthent

This security function handles mobile network authentication using the MILENAGE, TUAK or CAVE algorithms. The related keys are distributed according to the [GSMA] specifications.

ETSI.PIN

This security function implements the controls on the ETSI PIN objects defined in [TS 102 221]. The ETSI PIN is blocked after 3 unsuccessful (and consecutive) PIN verification attempts. The comparison between the PIN value provided by the owner of the M2M device and the reference PIN is done securely within the TOE (in particular, without any leakage that could allow an observer to gain information on the PIN value).

10.2 SECURITY FUNCTIONS RELATED TO GP/JCS FEATURES

GP.CardContentManagement

This security function provides the capability and a dedicated flow control for the loading, installation, extradition, registry update, selection and removal of eUICC content and especially executable files and application instances. It supports Delegated management (DM), Authorized management (AM) and it can use DAP or Mandated DAP verification and generation of Reception token. It also checks that only the eUICC management commands specified and allowed at each state of the eUICC life cycle are accepted, and ill-formed ones are rejected with an appropriate error response.

GP.KeyLoading

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

GP.SecurityDomain

This security function provides security domain management, as SD creation, SD selection, SD privileges setting and SD deletion in SD hierarchy. It provides means to associate or extradite an

application to a security domain in order to provide services (as secure channel) to the dedicated application without sharing the related keys stored in SD. It also provides Keyset Management in SD, with Key Set creation, Key set deletion, key importation, replacement, or deletion in Key Set.
Security Domains are privileged Applications as defined in [GPCS] § 7, holding cryptographic keys to be used to support Secure Channel Protocol operations and/or to authorize card content management functions. There are different types of security domain with dedicated privileges and associated operations, such as ISD Security domain, Supplementary Security domains, and Controlling Authority Security domains.

GP.SecureChannel

This security function provides a secure communication channel between the eUICC and an external entity during an Application Session according to [GPCS], [Amd B], [Amd D], [Amd F], [TS 102.225] and [TS 102.226]. It provides an APDU flow control using the Command security level check according to eUICC Life cycle and type of APDU.
A Secure Channel Session is divided into three sequential phases:

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

The following services are provided by the Secure Channel:

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

The following Secure Channel Protocols are supported by the TOE: SCP02, SCP03(t), SCP11, SCP80 and SCP81.

GP.GPRegistry

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

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

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

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

GP.DAP

The TOE implements the verification of DAP (and Mandated DAP) blocks as specified in [GPCS] sections C.2 and C.3. The following algorithms are supported:

- SHA-256, SHA-384, or SHA-512 for the hash computation
- TDES (112 bits or 168 bits key length), AES (128, 192, or 256 bits key length), RSA (1024 or 2048 bits key length) or ECC (256, 384, or 512 bits key length) for the DAP signature verification. This verification is done at the time an ELF with DAP is received.

GP.ELFU

The TOE implements the ELF Upgrade capability according to [Amd H]. Associated access control rules are enforced, as defined in [Amd H]. Management functions include the Saving, Loading, Restore phases of the Executable Load File Process, the management of the ELF upgrade session status and the eSE management during the ELF upgrade session. Rollback of deletion operations is supported under the following rules:

- If the deletion of the application instances and ELF(s) (atomic and irreversible operation) was started and then interrupted and/or disturbed by for example unexpected power-down, it shall automatically restart and complete at next power-up.
- If the interruption occurred during the Deletion Sequence and the latter did not complete automatically (i.e. the irreversible deletion operation did not start already), the Deletion Sequence shall restart.

A secure state is preserved when the following types of failures occur:

- The required minimum amount of memory is not available at the time the command MANAGE ELF UPGRADE is received
- A fatal error occurs using the new ELF version during the Restore Phase
- The ELF Upgrade Recovery Procedure fails
- The installation of an Application instance fails
- An interruption occurred during the Installation, Saving, Restore, or Consolidation Sequences.

GP.OS-UPDATE

The TOE implements an OS Update capability by means of the GemActivate proprietary mechanism, allowing the MultiSIM M2M 4.3.0 Platform to be updated post-issuance (during phase e of the TOE life-cycle). OS updates are performed through the loading, installation and activation of related ELFs, fulfilling the same rules as for any other ELF. DAP verification (AES128 CMAC) is mandatory for ELFs containing OS updates, ensuring the authenticity and integrity protection of the code update, and the content of the ELF is directly encrypted (AES128 in CBC mode) with a dedicated encryption key, ensuring the confidentiality protection. Note that both the DAP signature verification key and the encryption key are GemActivate keys, meaning that OS updates can only be issued and decrypted by Thales. Verification of TOE identification data is also enforced before allowing any OS update. The whole OS update operation is done through an atomic process, ensuring the permanent consistency between the MultiSIM M2M 4.3.0 Platform active code and its identification data.

A secure state is preserved in case of failure during the OS update process. More precisely:

- There are 3 steps in an OS Update operation:
  - step 1: loading
  - step 2: activation
  - step 3: update of TOE identification data

  Steps 2 and 3 are performed atomically, so that the TOE active code and identification data always remain consistent.
- If a failure (interruption or incident) occurs during step 1 (loading), then the TOE remains in its initial state (no update, neither of code nor of the TOE identification data).

- If a failure (interruption or incident) occurs during the atomic sequence step 2 / step 3 (activation / update of TOE identification data), then the enforced behavior depends on the nature of the update:
    - For java code updates, the TOE remains in its initial state and the OS Update operation is aborted.
    - For native code updates, the TOE does some retries to complete the atomic sequence step 2 / step 3 (activation / update of TOE identification data) until it is successful.
    - In any case, only two possible secure states are possible at any given time:
        - Either activation is not done and the TOE identification data is not updated (i.e. initial state)
        - Or the atomic sequence completes successfully, i.e. the OS update is activated and the TOE identification data is updated accordingly.

JCS.APDUBuffer

The security function maintains a byte array buffer accessible from any applet context. This buffer is used to transfer incoming APDU header and data bytes as well as outgoing data according to [JCAPI310]. The APDU class API is designed to be transport protocol independent (T=0, T=1…), as defined in ISO 7816-3.

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

JCS.ByteCodeExecution

This security function handles applet bytecode execution according to the rules defined in [JCVM310]. The JCVM execution may be summarized in JCVM interpreter start-up, bytecode execution and JCVM interpreter loop. The applet bytecode execution consists in:

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

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

JCS.Firewall

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

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

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

JCS.Package

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

JCS.KeyManagement

This security function enforces key management for the different associated operations: key importation, key exportation, key masking and key destruction using the standard API defined in [JCAPI310].

- Key importation and exportation is done using method protecting confidentiality and integrity of key.
- Key masking protects the confidentiality of cryptographic keys from being read out from the memory. It ensures the service of accessing and modifying them.
- Key destruction (implemented through the method clearKey() of the Key class) disables the use of a key both logically and physically.

JCS.CryptoAPI

This security function offers cryptographic services through the JavaCard API [JCAPI310]:

- Generation of random numbers as defined in [JCAPI310], to be used for key values or challenges during external exchanges. The Random Number Generator (RNG) is hybrid deterministic and conformant to [AIS31] DRG.4, providing enhanced backward secrecy & enhanced forward secrecy. It passes [AIS31] test procedure A.
- Encryption and decryption using TDES algorithm as defined in [JCAPI310] Cipher class. Both TDES 2-keys (112 bits key length) and TDES 3-keys (168 bits key length) are supported.
- Generation of 4-byte or 8-byte MAC using TDES algorithm as defined in [JCAPI310] Signature class. Both TDES 2-keys (112 bits key length) and TDES 3-keys (168 bits key length) are supported.
- Encryption and decryption using AES (128, 192 or 256 bits key) algorithm as defined in [JCAPI310] Cipher and AEADCipher classes.
- Generation of 16-byte, 24-byte or 32-byte MAC using AES algorithm (128, 192 or 256 bits key) in CBC mode as defined in [JCAPI310] Signature class.
- Data hash computation as defined in [JCAPI310] MessageDigest class.
- Verification of ECDSA signatures as defined in [JCAPI310] Signature class. Elliptic curve cryptography over GF(p) is considered here, with P ranging from 160 to 521 bits.
- Secret key agreement according to the ECDH algorithm, as defined in [JCAPI310] KeyAgreement class. Elliptic curve cryptography over GF(p) is considered here, with P ranging from 160 to 521 bits.

Note that these cryptographic services are made available both to applications and to other security functions of the TOE (e.g. Secure Channel Protocols).

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

JCS.OwnerPIN

This security function provides to applets a means to perform user identification and authentication with the OwnerPin class conformant to [JCAPI310].

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

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

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

JCS.EraseResidualData

This security function ensures that sensitive data are locked upon the following operations as defined in [JCRE310]:

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

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

This security function also ensures that the sensitive temporary buffers (transient object, bArray object, Global Array object, APDU buffer, Cryptographic buffer) are securely cleared after their usage with respect to their life-cycle and interface as defined in [JCRE310], transient object at reset or allocation and persistent object are erased at allocation for new object.

JCS.OutOfLifeDataUndisclosure
This security function ensures that sensitive data are locked until postponed erasure on the following operations: Deletion of persistent and transient objects according to [JCRE310].

JCS.RunTimeExecution
This security function provides a secure run time environment conformant to [JCRE310] and deals with:

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

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

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

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

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

10.3 TSS RATIONALE

Security Functional Requirement	Coverage by TSS Security Function(s)
FIA_UID.1/EXT	This SFR is covered by GSMA.Ident-Auth.
FIA_UAU.1/EXT	This SFR is covered by GSMA.Ident-Auth.

Security Functional Requirement	Coverage by TSS Security Function(s)
FCS_COP.1/AUTH_SMSR	This SFR is covered by GSMA.Ident-Auth.
FCS_COP.1/AUTH_SMDP	This SFR is covered by GSMA.Ident-Auth.
FIA_USB.1/EXT	This SFR is covered by GSMA.Ident-Auth.
FIA_UAU.4/EXT	This SFR is covered by GSMA.Ident-Auth.
FIA_UID.1/MNO-SD	This SFR is covered by GSMA.Ident-Auth.
FIA_USB.1/MNO-SD	This SFR is covered by GSMA.Ident-Auth.
FIA_ATD.1	This SFR is covered by GSMA.Ident-Auth.
FIA_API.1	This SFR is covered by GSMA.Ident-Auth.
FDP_IFC.1/SCP	This SFR is covered by GSMA.SecureChannels.
FDP_IFF.1/SCP	This SFR is covered by GSMA.SecureChannels.
FTP_ITC.1/SCP	This SFR is covered by GSMA.SecureChannels and GP.SecureChannel.
FDP_ITC.2/SCP	This SFR is covered by GSMA.SecureChannels.
FPT_TDC.1/SCP	This SFR is covered by GSMA.SecureChannels.
FDP_UCT.1/SCP	This SFR is covered by GSMA.SecureChannels and GP.SecureChannel.
FDP_UIT.1/SCP	This SFR is covered by GSMA.SecureChannels and GP.SecureChannel.
FCS_CKM.1/SCP-SM	This SFR is covered by GSMA.SecureChannels.
FCS_COP.1/ECKA-EG	This SFR is covered by GSMA.SecureChannels.
FCS_CKM.2/SCP-MNO	This SFR is covered by GSMA.SecureChannels.
FCS_CKM.4/SCP-SM	This SFR is covered by JCS.KeyManagement.
FCS_CKM.4/SCP-MNO	This SFR is covered by JCS.KeyManagement.
FDP_ACC.1/ISDR	This SFR is covered by GSMA.SecurityDomains.
FDP_ACF.1/ISDR	This SFR is covered by GSMA.SecurityDomains.
FDP_ACC.1/ISDP	This SFR is covered by GSMA.SecurityDomains.
FDP_ACF.1/ISDP	This SFR is covered by GSMA.SecurityDomains.
FDP_ACC.1/ECASD	This SFR is covered by GSMA.SecurityDomains.
FDP_ACF.1/ECASD	This SFR is covered by GSMA.SecurityDomains.
FDP_IFC.1/Platform_services	This SFR is covered by GSMA.PlatformServices.
FDP_IFF.1/Platform_services	This SFR is covered by GSMA.PlatformServices.
FPT_FLS.1/Platform_Services	This SFR is covered by GSMA.PlatformServices.
FCS_RNG.1	This SFR is covered by JCS.CryptoAPI.
FPT_EMS.1	This SFR is covered by JCS.KeyManagement and JCS.CryptoAPI.
FDP_SDI.1	This SFR is covered by GSMA.SecurityMngt.
FDP_RIP.1	This SFR is covered by GSMA.SecurityMngt.
FPT_FLS.1	This SFR is covered by GSMA.SecurityMngt.
FMT_MSA.1/PSF_DATA	This SFR is covered by GSMA.SecurityMngt.
FMT_MSA.1/POL1	This SFR is covered by GSMA.SecurityMngt.
FMT_MSA.1/CERT_KEYS	This SFR is covered by GSMA.SecurityMngt.
FMT_MSA.3	This SFR is covered by GSMA.SecureChannels and GSMA.SecurityDomains.
FMT_SMF.1	This SFR is covered by GSMA.SecureChannels and GSMA.SecurityDomains.
FMT_SMR.1	This SFR is covered by GSMA.SecurityMngt.
FCS_COP.1/Mobile_network	This SFR is covered by GSMA.NetworkAuthent.
FCS_CKM.2/Mobile_network	This SFR is covered by GSMA.NetworkAuthent.
FCS_CKM.4/Mobile_network	This SFR is covered by JCS.KeyManagement.
FDP_IFC.2/GP-ELF	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_IFF.1/GP-ELF	This SFR is covered by GP.CardContentManagement managing flow control for loading and installing application instances.
FDP_ITC.2/GP-ELF	This SFR is covered by JCS.Package checking the binary compatibility of dependent packages using their version numbers and AIDs prior to installation operations.
FDP_IFC.2/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FDP_IFF.1/GP-KL	This SFR is covered by GP.KeyLoading, GP.SecurityDomain and GP.SecureChannel.
FDP_ITC.2/GP-KL	This SFR is covered by GP.KeyLoading.
FCS_CKM.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FCS_COP.1/GP-SCP	This SFR is covered by GP.SecureChannel.
FMT_MSA.1/GP	This SFR is covered by GP.SecureChannel providing an APDU flow control using the Command security level check according to Card Life cycle and type of APDU.

Security Functional Requirement	Coverage by TSS Security Function(s)
FMT_MSA.3/GP	This SFR is covered by GP.SecureChannel providing setting of the default value.
FMT_SMR.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain managing the roles: S.OPEN, S.SD, Applications.
FMT_SMF.1/GP	This SFR is covered by GP.SecurityDomain and GP.SecureChannel.
FPT_RCV.3/GP	This SFR is addressed by JCS.RunTimeExecution, OS.MemoryManagement, GP.GPRegistry and GP.CardContentManagement covering the applet instance erasure when applet instance registration operation fails.
FPT_FLS.1/GP	This SFR is addressed by JCS.Package, JCS.RunTimeExecution and GP.CardContentManagement covering the applet instance registration operations and associated error handling.
FPT_TDC.1/GP	This SFR is addressed by GP.CardContentManagement, GP.SecureChannel and GP.KeyLoading.
FTP_ITC.1/GP	This SFR is addressed by GP.SecureChannel.
FCO_NRO.2/GP	This SFR is covered by GP.SecureChannel managing the secure channel protocol where several checks are performed prior ELF or Key loading: * mutual authentication between the external entity (Issuer or Application provider) and the selected security Domain, including creation of a session key, * by the verification of a (chained) MAC that the Issuer or Application provider attaches to each file or data block sent, * by the erase of the session key at the end of the session.
FIA_UID.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain controlling accessible action prior identification and action when SD or application associated to SD are selected.
FDP_UIT.1/GP	This SFR is covered by GP.SecureChannel providing a session key generation. It ensures that the whole package or data has been correctly received.
FDP_ROL.1/GP	This SFR is addressed by GP.CardContentManagement, GP.KeyLoading and OS.Atomicity.
FDP_UCT.1/GP	This SFR is covered by GP.SecureChannel which provides confidentiality protection for sensitive data (such as secret keys).
FPR_UNO.1/GP	This SFR is covered by JCS.RunTimeExecution and JCS.CryptoAPI.
FIA_UAU.1/GP	This SFR is covered by JCS.RunTimeExecution and GP.SecurityDomain (as for FIA_UID.1/GP).
FIA_UAU.4/GP	This SFR is covered by GP.SecureChannel.
FIA_AFL.1/GP	This SFR is covered by GP.SecureChannel.
FCS_CKM.4/GP	This SFR is covered by JCS.KeyManagement.
FIA_AFL.1/ETSI-PIN	This SFR is addressed by ETSI.PIN.
FPR_UNO.1/ETSI-PIN	This SFR is addressed by ETSI.PIN.
FCS_COP.1/GP-DAP_SHA	This SFR is addressed by GP.DAP.
FCS_COP.1/GP-DAP_VER	This SFR is addressed by GP.DAP.
FCO_NRO.2/GP-DAP	This SFR is addressed by GP.DAP.
FDP_ACC.1/GP-ELFU	This SFR is addressed by GP.ELFU.
FDP_ACF.1/GP-ELFU	This SFR is addressed by GP.ELFU.
FDP_ROL.1/GP-ELFU	This SFR is addressed by GP.ELFU.
FMT_MSA.1/GP-ELFU	This SFR is addressed by GP.ELFU.
FMT_MSA.3/GP-ELFU	This SFR is addressed by GP.ELFU.
FMT_SMF.1/GP-ELFU	This SFR is addressed by GP.ELFU.
FPT_FLS.1/GP-ELFU	This SFR is addressed by GP.ELFU.
FDP_ACC.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FDP_ACF.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FMT_MSA.3/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FMT_SMR.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FMT_SMF.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FIA_ATD.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FTP_TRP.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FCS_COP.1/OS-UPDATE-DEC	This SFR is addressed by GP.OS-UPDATE.
FCS_COP.1/OS-UPDATE-VER	This SFR is addressed by GP.OS-UPDATE.
FPT_FLS.1/OS-UPDATE	This SFR is addressed by GP.OS-UPDATE.
FDP_ACC.2/FIREWALL	This SFR is covered by JCS.Firewall.
FDP_ACF.1/FIREWALL	This SFR is covered by JCS.Firewall.

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_IFC.1/JCVM	This SFR is covered by JCS.Firewall and JCS.APDUBuffer controlling unauthorized access or invalid storage of reference.
FDP_IFF.1/JCVM	This SFR is covered by JCS.Firewall.
FDP_RIP.1/OBJECTS	This SFR is covered by JCS.OutOfLifeDataUndisclosure (to avoid access to data prior erase) and JCS.EraseResidualData (to erase data).
FMT_MSA.1/JCRE	This SFR is covered by JCS.RunTimeExecution covering context switch and application selection.
FMT_MSA.1/JCVM	This SFR is covered by JCS.ByteCodeExecution requiring context switch for specific code execution and JCS.RunTimeExecution covering context switch and modification of the Currently Active Context according to given rules.
FMT_MSA.2/FIREWALL_JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_MSA.3/JCVM	This SFR is addressed by JCS.RunTimeExecution covering object sharing.
FMT_SMF.1/JCS	This SFR is addressed by JCS.RunTimeExecution covering context management and instance registration.
FMT_SMR.1/JCS	This SFR is addressed by JCS.RunTimeExecution covering JCVM and JCRE roles.
FDP_RIP.1/ABORT	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/APDU	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/GlobalArray	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/bArray	This SFR is addressed by JCS.OutOfLifeDataUndisclosure and JCS.EraseResidualData covering data erasure.
FDP_RIP.1/KEYS	This SFR is addressed by JCS.EraseResidualData covering data erasure.
FDP_RIP.1/TRANSIENT	This SFR is covered by JCS.OutOfLifeDataUndisclosure managing the access control to transient object to be erased prior the erasure of the content in memory.
FDP_ROL.1/FIREWALL	This SFR is addressed by JCS.RunTimeExecution covering transaction rollback during specific operations.
FAU_ARP.1	This SFR is addressed by JCS.RunTimeExecution, JCS.Exception, JCS.Firewall, and OS.MemoryManagement covering exception handling with different specific operations.
FDP_SDI.2/DATA	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, OS.Atomicity and OS.MemoryManagement covering integrity handling with specific operations.
FPR_UNO.1	This SFR is addressed by JCS.OwnerPIN, JCS.KeyManagement, JCS.CryptoAPI and OS.MemoryManagement covering data handling with specific operations avoiding observation.
FPT_FLS.1/JCS	This SFR is covered by JCS.Exception, JCS.ByteCodeExecution, JCS.RunTimeExecution, and OS.Atomicity preserving a secure state when unexpected events occur during specific operations.
FPT_TDC.1	This SFR is covered by JCS.Package enforcing export check, CAP file translation and link specific operations.
FIA_ATD.1/AID	This SFR is covered by JCS.RunTimeExecution and GP.GPRegistry controlling applet registration and uninstallation.
FIA_UID.2/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing user identity (package AID) during applet selection and identify associated context provided.
FIA_USB.1/AID	This SFR is covered by GP.GPRegistry and JCS.RunTimeExecution managing registration of each applet and associated package during its installation with its AID.
FMT_MTD.1/JCRE	This SFR is covered by JCS.RunTimeExecution offering services for applet registration and uninstallation managing associated access rights.
FMT_MTD.3/JCRE	This SFR is fully covered by JCS.RunTimeExecution managing presence and legacy of AID with ISO rules.
FDP_ACC.2/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.
FDP_ACF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.GPRegistry and JCS.RunTimeExecution checking rules for applet instance uninstallation and deletion dependency rules.

Security Functional Requirement	Coverage by TSS Security Function(s)
FDP_RIP.1/ADEL	This SFR is covered by GP.CardContentManagement and JCS.OutOfLifeDataUndisclosure by checking operations to avoid access to freed resources prior to its reuse.
FMT_MSA.1/ADEL	This SFR is covered by GP.GPRegistry, GP.CardContentManagement and JCS.RunTimeExecution responsible of checking rules concerning applet attributes, implicit and explicit selection rules prior to authorize deletion operation.
FMT_MSA.3/ADEL	This SFR is covered by JCS.RunTimeExecution and GP.CardContentManagement dealing with Security Attributes initialization, providing secure, restrictive default values for the security attributes of subject and objects involved in applet deletion.
FMT_SMF.1/ADEL	This SFR is covered by GP.CardContentManagement, GP.SecurityDomain and JCS.RunTimeExecution.
FMT_SMR.1/ADEL	This SFR is covered by GP.SecurityDomain maintaining the SD roles responsible of applet deletion. This SFR is also covered by JCS.RunTimeExecution maintaining the JCRE role for applet uninstallation.
FPT_FLS.1/ADEL	This SFR is covered by GP.GPRegistry, JCS.RunTimeExecution and OS.Atomicity preserving a secure state when unexpected events occur during package or instance deletion, managing the transaction part of the deletion operation by either rolling back, or completing it.
FDP_RIP.1/ODEL	This SFR is covered by JCS.EraseResidualData and OS.MemoryManagement ensuring that the content of deleted objects is erased upon the deletion and by JCS.OutOfLifeDataUndisclosure making unavailable for disclosure upon further reallocation of the freed space.
FPT_FLS.1/ODEL	This SFR is covered by JCS.RunTimeExecution and OS.MemoryManagement performing memory management to release no more used memory on unreferenced objects and preserves a secure state when unexpected events occur during object deletion.
FPT_RCV.3/OS	This SFR is covered by OS.Atomicity.
FPT_RCV.4/OS	This SFR is covered by OS.MemoryManagement.

END OF DOCUMENT