Embedded UICC Protection Profile
Version 1.0
22 September 2014

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

List of Tables

List of Figures

References

Ref	Doc Number	Title
[1]	PP-JCS	Common Criteria Protection Profile Java Card™ System Open Configuration, Version 3.0, May 2012, ANSSI-CC-PP-2010/03
[2]	PP0084	Security IC Platform Protection Profile with Augmentation Packages Version 1.0 - BSI-CC-PP-0084-2014
[3]	SGP.02	GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification, Version 1.0, 30 January 2014
[4]	PP-USIM	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations Evolutive Certification Scheme for (U)SIM cards
[5]	GP-SecurityGuidelines-BasicApplications	GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications - Version 1.0 - June 2012 – ref. GPC_GUI_050
[6]	SSCD-PP	Protection Profile Secure Signature Creation Device Type 3, BSI-PP-0006-2002, also short SSCD-PP or CWA14169.
[7]	ETSI_102221	ETSI TS 102 221 - Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 9)
[8]	JIL-CCforIC	Joint Interpretation Library – The application of CC to integrated crircuits – Version 3.0 – February 2009
[9]	CC1	Common Criteria for Information Technology Security Evaluation, Part 1
[10]	CC2	Common Criteria for Information Technology Security Evaluation, Part 2
[11]	CC3	Common Criteria for Information Technology Security Evaluation, Part 3
[12]	GlobalPlatform_Card_Specification	GlobalPlatform Card Specification v2.2.1 including • GlobalPlatform Card Specification v.2.2.1 UICC Configuration - v1.0.1 • GlobalPlatform Card Specification v.2.2 Amendment B: Remote Application Management over HTTP v1.1.1 • GlobalPlatform Card Specification v.2.2 Amendment C: Contactless Services v1.1 • GlobalPlatform Card Specification v.2.2 Amendment D: Secure Channel Protocol 03 v1.1 • GlobalPlatform Card Specification v.2.2 Amendment E: Security Upgrade for Card Content Management v1.0
[13]	ETSI_102225	SCP80 ETSI TS 102 225 [Secured packet structure for UICC based applications; Release 9]
[14]	ETSI_102226	SCP81 ETSI TS 102 226 [Remote APDU structure for UICC based applications; Release 9]
[15]	Composite-Product-	Joint Interpretation Library – Composite Product Evaluation for

Ref	Doc Number	Title
	Evaluation	Smart Cards and similar devices – Version 1.2 – January 2012
[16]	SIM API	3GPP TS 43.019 version 6.0.0 - Subscriber Identity Module Application Programming; Interface (SIM API) for Java Card (Release 6)
[17]	UICC API	ETSI TS 102 241 V9.2.0 (2012-03) - UICC Application Programming Interface (UICC API) for Java Card (Release 9)
[18]	(U)SIM API	3GPP TS 31.130 version 9.4.0 - (U)SIM API for Java™ Card (Release 9)
[19]	ISIM API	3GPP TS 31.133 version 9.2.0 - ISIM API for Java Card™ (Release 9)
[20]	SGP.01	SGP.01 GSMA Embedded SIM Remote Provisioning Architecture v1.1
[21]	MILENAGE	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 11): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; • Document 1: General • Document 2: Algorithm Specification • Document 3: Implementors' Test Data • Document 4: Design Conformance Test Data Document 5: Summary and results of design and evaluation
[22]	TUAK	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233 (Release 12) • Document 1: Algorithm specification • Document 2: Implementers' test data Document 3: Design conformance test data

Definitions

Besides the terms described in the next table, the terminology and abbreviations of Common Criteria apply (see [9], [10] and [11]).

Term	Description
Actor	Physical entity (person, company or organisation) that can assume a Role in the functional architecture. It is possible for an Actor to assume multiple Roles in the same functional architecture.
Application Firewall	This term is used to describe the functions of the eUICC Runtime Environment that restrict the capability of applications to access or

Term	Description
	modify data belonging to other applications. The Java Card System Firewall is an example of such Application Firewall
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.
Device	Equipment into which an Embedded UICC and a communication module are inserted during assembly. Examples include Utility meter, car and camera.
Disabled (Profile)	The state of a Profile where all files and applications (for example NAA) present in the Profile are not selectable over the UICC-Terminal interface.
Embedded UICC	A UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the Device, and enables the secure changing of Profiles.
Enabled (Profile)	The state of a Profile when its files and/or applications (for example, NAA) are selectable over the UICC-Terminal interface.
eUICC Certificate	A certificate issued by the EUM for a specific eUICC. This certificate can be verified using the EUM Certificate.
eUICC Manufacturer	Supplier of the eUICCs and resident software (for example firmware and operating system).
EUM Certificate	A certificate issued to a GSMA accredited EUM which can be used to verify eUICC Certificates. This certificate can be verified using the Root Certificate.
Fallback (or Fall-back)	The Fall-back Mechanism shall be activated in case of loss of network connectivity by the current Enabled Profile. The eUICC shall disable the current Enabled Profile and enable the Profile with Fall-back Attribute set. Only one Profile can have the Fall-back attribute set.
Integrated Circuit Card ID	Unique number to identify a Profile in an eUICC. Note: the ICCID throughout this specification is used to identify the Profile.
International Mobile Subscriber Identity	Unique identifier owned and issued by Mobile operators to (U)SIM applications to enable Devices to attach to a network and use services.
Issuer Security Domain (ISD)	A security domain on the UICC as defined by [GlobalPlatform Card Specification]. This Protection Profile defines an ISD called ISD-P for the SM-DP, and an ISD called ISD-R for the SM-SR.
JCS	Java Card System

Term	Description
Mobile Network Operator	An entity providing access capability and communication services to its Customers through a mobile network infrastructure.
Mobile Network Operator Security Domain	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.
Network Access Application	An application residing on a UICC which provides authorization to access a network for example a USIM application.
Operational Profile	A Profile containing network authentication parameters as well as MNO's applications and 3rd party applications.
Orphaned Profile	A Profile whose Policy Rules have become unmanageable, for example due to the termination of the Customer's contract with the MNO.
OTA Keys	The credentials included in the Profile, used in conjunction with OTA Platforms.
OTA Platform	An MNO Platform for remote management of UICCs and the content of Enabled MNO Profiles on eUICCs.
Platform Management	A set of functions related to the enabling, disabling and deletion of a Profile on and the transport of Profile Management functions to an eUICC. Platform Management actions are protected by Platform Management Credentials shared between the SM-SR and the ISD-R. Platform Management does not affect the content of a Profile.
Platform Management Credentials	Data required within an eUICC so that a secured communication can be set up between an external entity and the eUICC in order to enable, disable and delete Profiles on the eUICC and to transport Profile Management functions.
Platform Support Functions	A (set of) service(s) and/or application(s) of the TOE supporting the Security Domains, typically including GlobalPlatform functions and policy enforcement capacities.
Policy	Principles reflected in a set of rules that governs the behaviour of eUICC and/or entities involved in the remote management of the eUICC.
Policy Rule	Defines the atomic action of a Policy and the conditions under which it is executed.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which allows, when enabled, access to a specific mobile network infrastructure.
Profile Management	A set of functions related to the downloading, installation and content update of a Profile in a dedicated ISD-P on the eUICC. Download and installation are protected by Profile Management Credentials shared between the SM-DP and the ISD-P.
Profile Management Credentials	Data required within an eUICC so that a Profile downloaded from an external entity can be decrypted and installed on the eUICC.

Term	Description
Provisioning Profile	A Profile contains NAA parameters to enable access to communication network(s) to provide transport capability for eUICC management and Profile Management between the eUICC and an SM-SR.
Role(s)	Role(s) are representing a logical grouping of functions.
Root Certificate	Self-signed certificate of the CI, used to authenticate certificates issued to other entities.
Security Domains	Privileged applications defined in [12]
Security IC	Integrated circuit whose security functionality is described in [2]
Subscriber	An entity (associated with one or more users) that is engaged in a Subscription with a Telecommunication Service Provider. The Subscriber is allowed to subscribe and unsubscribe to services, to register a user or a list of users authorised to use those services, and also to set the limits relative to the use that associated users make of those services.
Subscription Manager Data Preparation	Role that prepares the Profiles and manages the secure download and installation of these Profiles onto the eUICC.
Subscription Manager Secure Routing	Role that securely performs functions of Platform Management commands and the transport of Profile Management commands.
Telecom Framework	A (set of) service(s) and/or application(s) of the TOE supporting the NAA by providing network authentication algorithms.

Abbreviations

Besides the terms described in the next table, the terminology and abbreviations of Common Criteria apply (see [9], [10] and [11]).

Term	Description
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application programming interface
CASD	Controlling Authority Security Domain
CERT	Certificate
CI	Certificate Issuer
DPA	Differential Power Analysis
ECASD	eUICC Controlling Authority Security Domain
ECDSA	Elliptic Curve cryptography Digital Signature Algorithm
ECKA	Elliptic Curve cryptography Key Agreement algorithm
EID	eUICC-ID
ETSI	European Telecommunications Standards Institute
eUICC	Embedded UICC
EUM	eUICC Manufacturer
GP	GlobalPlatform
GSMA	GSM Association
IC	Integrated Circuit
IMSI	International Mobile Subscriber Identity
ISD	Issuer Security Domain
ISDP or ISD-P	Issuer Security Domain Profile
ISDR or ISD-R	Issuer Security Domain Root
JCAPI	Java Card API
JCRE	Java Card Runtime Environment
JCS	Java Card System
JCVM	Java Card Virtual Machine
JIL	Joint Interpretation Library
M2M	Machine to machine
MNO	Mobile Network Operator
MNO-SD	Mobile Network Operator Security Domain
NAA	Network Access Application
OS	Operational System
OTA	Over The Air

PIN	Personal Identification Number
POL1	Policy Rules within the Profile
PP	Protection Profile
PSF	Platform Support Functions
RE	Runtime Environment
SCP	Secure Channel Protocol
SD	Security Domain
SIM	Subscriber Identity Module
SM	Subscription Manager
SM-DP	Subscription Manager Data Preparation
SM-SR	Subscription Manager Secure Routing
SSCD	Secure Signature Creation Device
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
USIM or (U)SIM	Universal Subscriber Identity Module

1 Introduction

This document defines a Protection Profile for the remote provisioning and management of the Embedded UICC in machine-to-machine Devices.

Profile

1.1 Protection Profile Identification

Title:	Embedded UICC Protection Profile
Author:	GSMA
Editor:	Trusted Labs
Reference:	GSMA SGP 05
Version:	1.0
CC Version:	3.1 revision 4
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General Status:	Evaluation draft
Registration:	Pending
Keywords:	Embedded UICC, remote provisioning

1.2 TOE Overview

This section presents the architecture and common usages of the Target of Evaluation (TOE). The TOE of this Protection Profile is a set of applications loaded on a Security IC, which is itself embedded onto a M2M Device. The TOE includes:

- Security Domains: Privileged applications providing the remote provisioning and administration functionality (the notion of Security Domain follows the definition given by [12]);
- A set of functions providing support to these Security Domains:
    - *Platform Support Functions*, which include Policy enforcement functions and extended GP OPEN capabilities;
    - A *Telecom Framework* providing network authentication algorithms.

The Security IC and its embedded software are considered as the environment of the eUICC, covered by security objectives. Nevertheless, any eUICC evaluation against this PP shall comprehend the whole including:

- The complete TOE of this PP;

- The Security IC Platform and OS;
- The Runtime Environment (for example Java Card System).

1.2.1 TOE Type

The eUICC is an UICC embedded in a machine-to-machine Device. Whether the eUICC has a form factor enabling replacement is not considered here: the eUICC is not intended to be removable once it is rolled out. The eUICC is connected to a given mobile network, by the means of its currently enabled MNO Profile.

The Security target of the eUICC shall include the whole eUICC – however this Protection Profile only includes the bricks showed (in blue) on the figure hereafter. The TOE includes in particular Platform management capabilities, which provide an interface to manage applications in a secure way. These capabilities are inspired from GlobalPlatform (GP), albeit with a few modifications, especially regarding the state machine. The GP OPEN may implement part of the *Platform Support Functions* functionality.

The Runtime Environment (RE) is not part of the TOE. However the TOE requires that the underlying RE meets a series of security objectives (see objectives OE.RE.* in §4.2.2) that are met by the Java Card System Protection Profile [1]. The figure hereafter takes such Java Card System as an example of RE.

The Profiles are not part of the TOE.

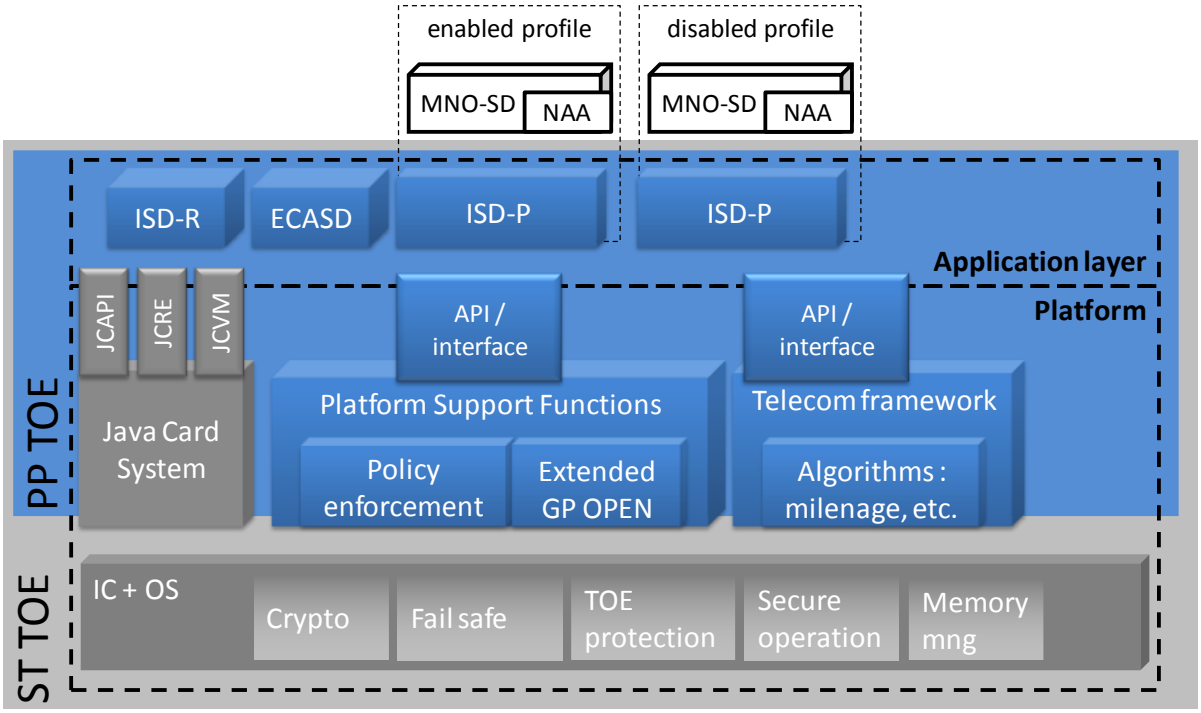

Figure 1 : scope of the TOE

1.2.1.1 Application Layer

The goal of this Application layer is to implement the eUICC functionalities described in [3], which rely on the notion of a Profile. A Profile is the combination of a file structure, data and applications to be provisioned onto, or present on, 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.

This document will use the term "Profile" to describe either Provisioning Profiles or Operational 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 relies on the Platform layer to have them enforced on the eUICC.

The Profile structure, composed of a set of Profile Components, is specified by, and under the full control of, the MNO. The full Profile structure shall be contained in a unique ISD-P. The Profile structure shall contain a Profile Component, called MNO-SD, which performs an identical Role as the ISD for a UICC. The Profile structure shall include:

- The MNO-SD
- At least one NAA
- POL1, even if not used
- The file system

More details on the Profile can be found in [3]

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 [20], the ISD-P shall:

a) Be a separate and independent entity on the eUICC
b) Contain a Profile including file system, NAAs and Policy Rules;
c) Contain a state machine related to creating, enabling and disabling the Profile;
d) Contain keys for Profile Management for the loading and installation phase;
e) Implement a key establishment protocol to generate a keyset for the personalisation of the ISD-P;
f) Be able to receive and decrypt, load and install the Profile created by the SMDP;
g) Be able to set its own state to disabled once the Profile is installed;
h) Provide SCP03 capabilities to secure its communication with the SM-DP;
i) 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.

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 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 [20], the ISD-R shall:

a) Be created within an eUICC at time of manufacture;

b) Be associated to an SM-SR;

c) Not be deleted or disabled;

d) Provides a secure OTA channel using Platform Management Credentials (SCP80 or SCP81) to the SM-SR;

e) Implement a key establishment protocol for the support of the change of SM-SR;

f) Offers wrapping and unwrapping service of the transport part during Profile download;

g) Be able to create new ISD-Ps with the required memory quota;

h) Not be able to create any SD except an ISD-P;

i) Executes Platform Management functions in accordance to the Policy Rules;

j) 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.

MNO-SD

The MNO-SD is the on-card representative of the MNO Platform. It is, according to [3], 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 [20], the MNO-SD shall:

a) Be associated to itself;

b) Contain the MNO OTA Keys;

c) Provide a secure OTA channel (SCP80 or SCP81);

d) Have the capability to host Supplementary Security Domains.

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 [20], the ECASD:

a) Is created within an eUICC at time of manufacture;

b) Cannot be deleted or disabled after delivery;

c) Is based on the concept of CASD from Global Platform;

d) Is configured by the eUICC Manufacturer at pre-issuance;

e) Contains a non-modifiable eUICC private key, the associated Certificate, the CI's root public keys and the EUM keyset for key/certificate renewal;

f) Is associated to the ISD-R, which provides the underlying secure OTA channel;

g) Is required for, and is not limited to, the establishment of new keysets in the ISD-P(s) and ISD-R;

h) Does not support the Mandated DAP verification feature.

1.2.1.2 Platform Layer

This PP does not assume that the platform code is realized by applications, native applications/libraries or OS services. The Platform capabilities include:

- The Platform Support Functions (PSF), which are responsible for the administration of the eUICC. This PP does not mandate any specific design for these functions and the exact structure of the PSF is implementation-dependent, however it must include the following capabilities:
    - *Extended GlobalPlatform OPEN functions*, which extend the capabilities of a GP OPEN and Trusted Framework and must at least provide:
        - API for SDs
        - APDU dispatching to SDs
        - SDs selection
        - eUICC content management, which typically includes loading, installation, enabling, disabling, deletion of SDs
        - Trusted communications between SDs

      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 3 of [3]).
    - *Policy Enforcement functions*, which are in charge of the verification and application of POL1 rules during Platform Management activities.

A developer may choose, if possible, to implement some of these functions in the SDs, for example the policy enforcement may be realized completely by the ISD-R. The PSM is only defined here to identify the platform code supporting the SDs *if it exists*.

- The Telecom Framework, which includes algorithms used by Network Access Applications (NAA) to access mobile networks. The NAAs are part of the Profiles, but the algorithms, as part of the Telecom Framework, are provisioned onto the eUICC during manufacturing.

The RE code is out of scope of this Protection Profile.

1.2.2 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.

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

1.2.3 TOE Lifecycle

1.2.3.1 Lifecycle compared to a Security IC Platform lifecycle

The TOE life cycle is different from a traditional smartcard lifecycle, due to the post-issuance provisioning functionality.

The figures hereafter show the description of the TOE lifecycle, compared to the [PP0084] lifecycle. The delivery of the TOE may be performed at different stages.

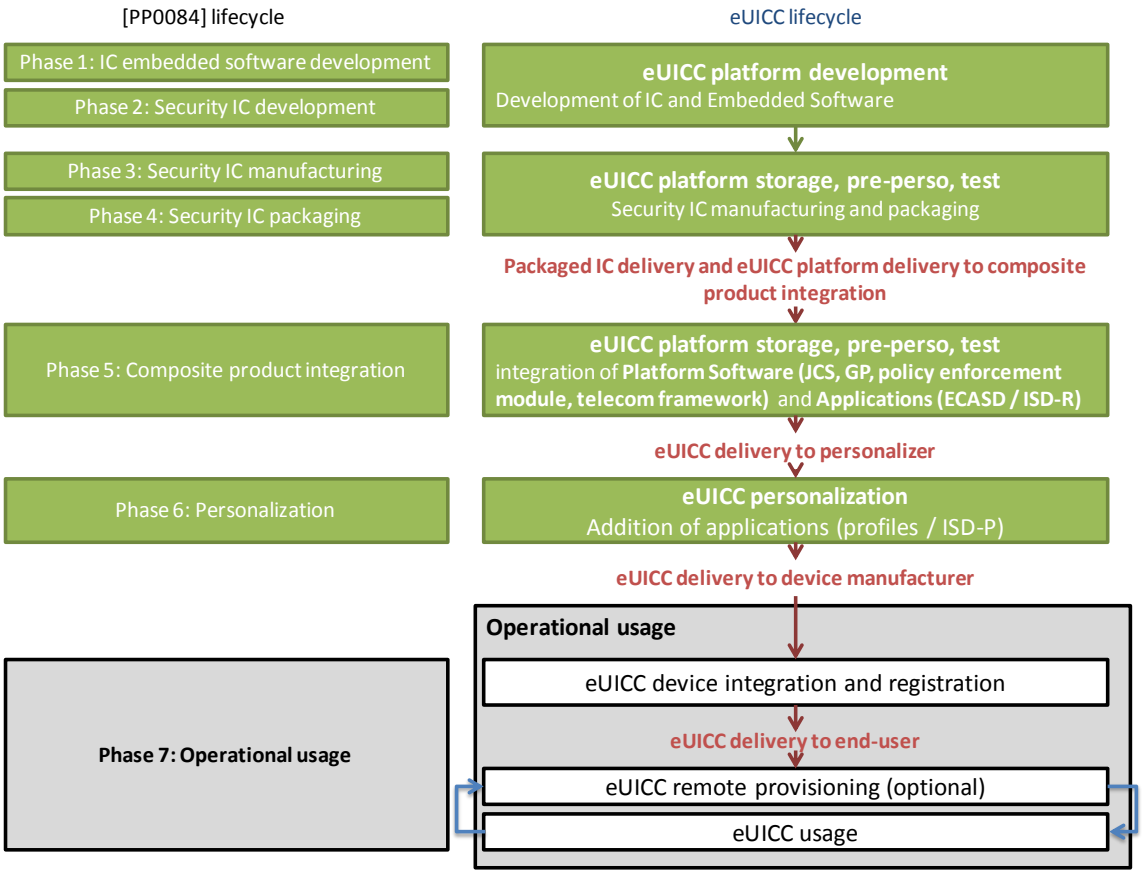

Figure 2 : TOE Lifecycle – TOE Delivery

The reader may refer to [PP0084] for a thorough description of Phases 1 to 7:

- Phases 1 and 2 compose the product development: Embedded Software (IC Dedicated Software, OS, Runtime Environment, applications, other Platform components such as PSF, Applications) and IC development.
- Phase 3 and 4 correspond to IC manufacturing and packaging, respectively. Some IC pre-personalisation steps may occur in Phase 3.
- Phase 5 concerns the embedding of software components within the IC.
- Phase 6 is dedicated to the product personalisation prior final use.
- Phase 7 is the product operational phase.

The eUICC life cycle is composed of the following stages:

- Development corresponds to the first two stages of the IC development
- Storage, pre-personalisation and test cover the stages related to manufacturing, packaging and the embedding of software products onto the eUICC,
- The TOE may be delivered to a personalizer different from the eUICC Manufacturer (TOE delivery after phase 5);
- The eUICC undergoes personalization (and test) – the personalization consists in inserting provisioning Profiles and Operational Profiles onto the eUICC;
- The TOE is delivered to the Device Manufacturer (if the personalizer is the eUICC Manufacturer: TOE delivery after phase 6)

- After the TOE delivery: operational usage of the TOE (the TOE must be auto-protected)
- eUICC integration onto the Device is performed by the Device Manufacturer. The Device Manufacturer and/or the eUICC Manufacturer also register the eUICC in a given SM-SR;
- The eUICC is then used to provide connectivity to the Device end-user. The eUICC may be provisioned again, at post-issuance, using the remote provisioning infrastructure.

In order to have a possible compliance of the Security Target with the (U)SIM PP, the delivery of the eUICC may occur also either during Security IC manufacturing (Phase 3) or during Composite Product Integration (Phase 5). It is also possible that part of the eUICC is delivered in Phase 3 and the rest is delivered in Phase 5. eUICC Platform storage is not necessarily a single step in the life cycle since it can be stored in parts. eUICC Platform delivery occurs before storage and may take place more than once if the TOE is delivered in parts. Delivery and acceptance procedures shall guarantee the authenticity, the confidentiality and integrity of the exchanged pieces.

1.2.3.2 Actors of the TOE

The eUICC delivered to the end-user is embedded onto the 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, this PP also considers that the MNO is not an Actor of the TOE.

The only Actors having an interface to the TOE are:

- The Device Manufacturer, when integrating the eUICC onto the 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).

1.2.4 Non-TOE HW/SW/FW Available to the TOE

1.2.4.1 TOE interfaces

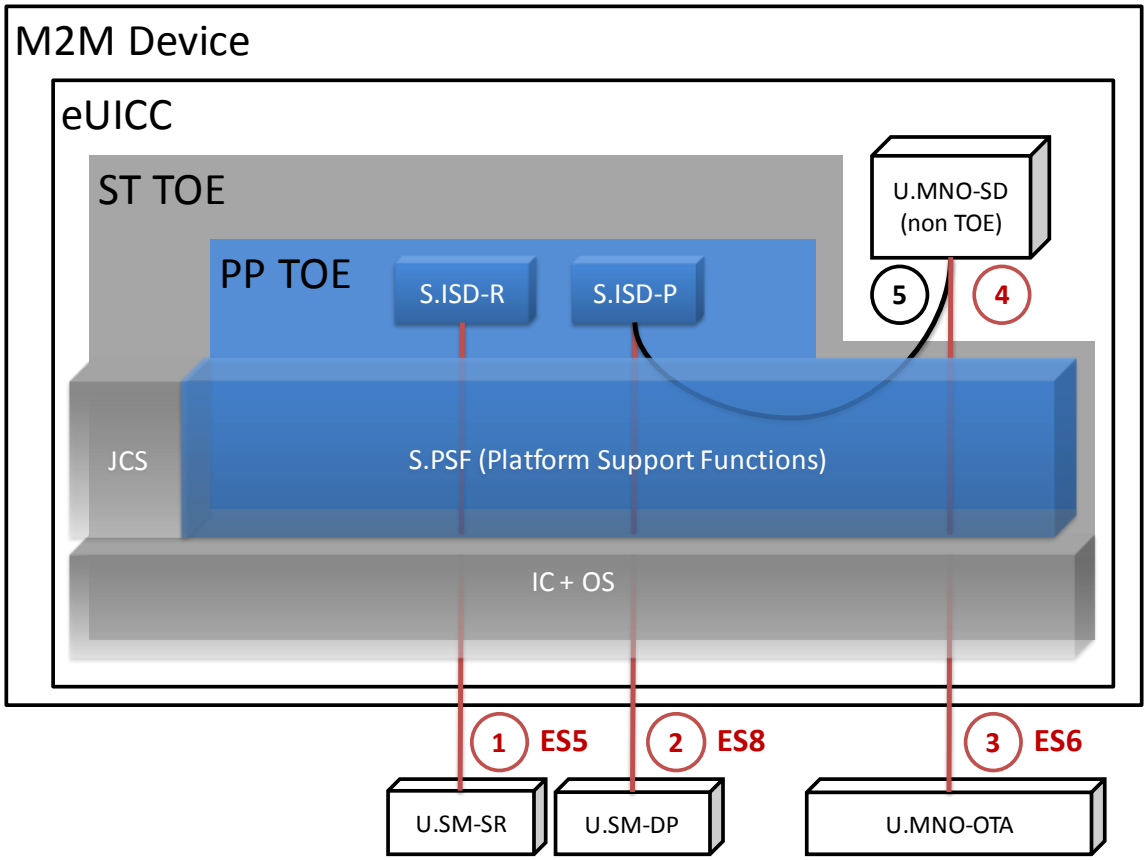

Figure 3 : TOE Interfaces

The TOE of this protection Profile is a part of the complete eUICC. The TOE of the Security Target will include the complete eUICC except:

- The loaded Profiles consisting in a MNO-SD and associated applications;
- Any other non-TOE software, such as applications loaded on the eUICC and not belonging to a profile.

Note: The ST writer may choose to include these items in the ST TOE but it is not mandatory.

As shown on previous figure, the ST TOE has the following interfaces:

- With the provisioning infrastructure, consisting in SM-SR, SM-DP and MNO OTA Platform (interfaces 1 to 3, identified ES5, ES6 and ES8 in [3])
- With the MNO-SD:
  - The interface 4 is used to enforce the trusted channel between the MNO-SD and the MNO OTA Platform
  - The interface 5 is used to enforce an internal trusted channel between the MNO-SD and the ISD-P.

As the MNO-SD is not part of the TOE, part of the enforcement of these trusted channels is ensured by the operational environment of the TOE.

All communications are supported by the Platform Support Functions, which provide a secure APDU dispatching and an extension of the GP Trusted Framework to support secure communications between SDs.

The RE also supports communications by providing applications with means to protect the confidentiality and integrity of their communications (see OE.RE.SECURE-COMM)

The RE itself relies on the Security IC and its embedded software.

1.2.4.2 Description of Non-TOE HW/SW and Systems

Integrated Circuit or Chip

The TOE is based on a Security Integrated Circuit (IC) which is a hardware Device composed of a processing unit, memories, security components and I/O interfaces. It has to implement security features able to ensure:

- The confidentiality and the integrity of information processed and flowing through the Device,
- The resistance of the Security IC to externals attacks such as physical tampering, environmental stress or any other attacks that could compromise the sensitive assets stored or flowing through it.

This Security IC may also include extra features or embedded proprietary software (called IC Dedicated Software or firmware) which provides additional services (such as low level routines) to facilitate the usage of the Security IC.

The IC security features are expected to be similar to those described in [PP0084].

Embedded Software

The TOE relies on an Embedded Software (ES) loaded into the Security IC and which manages the features and resources provided by the chip. It is, generally divided into two levels:

1) Low level:

- Drivers related to the I/O, RAM, ROM, EEPROM, Flash memory if any, and any other hardware component present on the Security IC,

2) High Level:

- Protocols and handlers to manage I/O,
- Memory and file manager,
- Cryptographic services and any other high level services provided by the OS.

The ES is expected to provide the following security features:

- Crypto: Provides secure low-level cryptographic processing
- Layer separation: enforces that access to low-level functionality is done only via APIs (incl. integrity/confidentiality of private data/code)

- TOE protection: does not allow any native code or application to be bypassed or altered
- Secure operation: supports the needs for any update to a single persistent object or class field to be atomic and provides low level transaction concurrency control.
- Memory management: provides
    - storage in persistent or volatile memory, depending on the needs.
    - low-level control accesses (segmentation fault detection)
    - a means to perform memory operations atomically.

Runtime Environment

Following [12], the Runtime Environment is responsible for:

- Providing an interface to all Applications that ensures that the Runtime Environment security mechanisms cannot be bypassed, deactivated, corrupted or otherwise circumvented;
- Performing secure memory management to ensure that:
    - Each Application's code and data (including transient session data) as well as the Runtime Environment itself and its data (including transient session data) is protected from unauthorized access from within the card. The Runtime Environment provides isolation between Security Domains via an Application Firewall.
    - When more than one logical channel is supported, each concurrently selected Application's code and data (including transient session data) as well as the Runtime Environment itself and its data (including transient session data) is protected from unauthorized access from within the card; The previous contents of the memory is not accessible when that memory is reused;
    - The memory recovery process is secure and consistent in case of a loss of power or withdrawal of the card from the card reader while an operation is in progress;
- Providing communication services with off-card entities that ensures the proper transmission (according to the specific communication protocol rules) of unaltered command and response messages

The Runtime Environment also provides applications with cryptographic means to protect their communications.

A Java Card System compliant to [1] typically meets these objectives, while compliance to [1] is not required by this PP.

This PP uses the Java Card System as a reference for the expected Runtime Environment. Consequently, the SFRs of this PP:

- Use the notion of AID, as described in [1], as an identification for applications for the Runtime Environment as well as the TOE.
- Refer to some SFRs of the Protection Profile [1]

If the ST writer uses another Runtime Environment, corresponding SFRs must be adapted to describe equivalent mechanisms.

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.

The M2M Device may not be easily reachable, and is not expected to include a user interface, at least related to the eUICC functionality. For this reason, the eUICC does not include applications requiring user interaction such as PIN entry.

No security certification is expected to be performed on the Device itself, and the eUICC may not rely on the Device security to protect its assets.

MNO-SD and applications

The Profile controlled by each ISD-P consists in a MNO-SD security domains, which itself may manage several applications, in the same meaning as intended by [4].

Basic applications

Basic applications stand for applications that do not require any particular security for their own.

Basic applications must be compliant with the security rules as defined in [5].

Secure Applications

Secure applications are applications requiring a high level of security for their own assets. It is indeed necessary to protect application assets in confidentiality, integrity or availability at different security levels depending on the AP Security Policy.

As such, secure applications follow a Common Criteria evaluation and certification in composition with the previously certified underlying Platform.

Remote provisioning infrastructure

The eUICC interfaces with the following remote provisioning architecture, that are responsible for the management of Profiles on the eUICC.

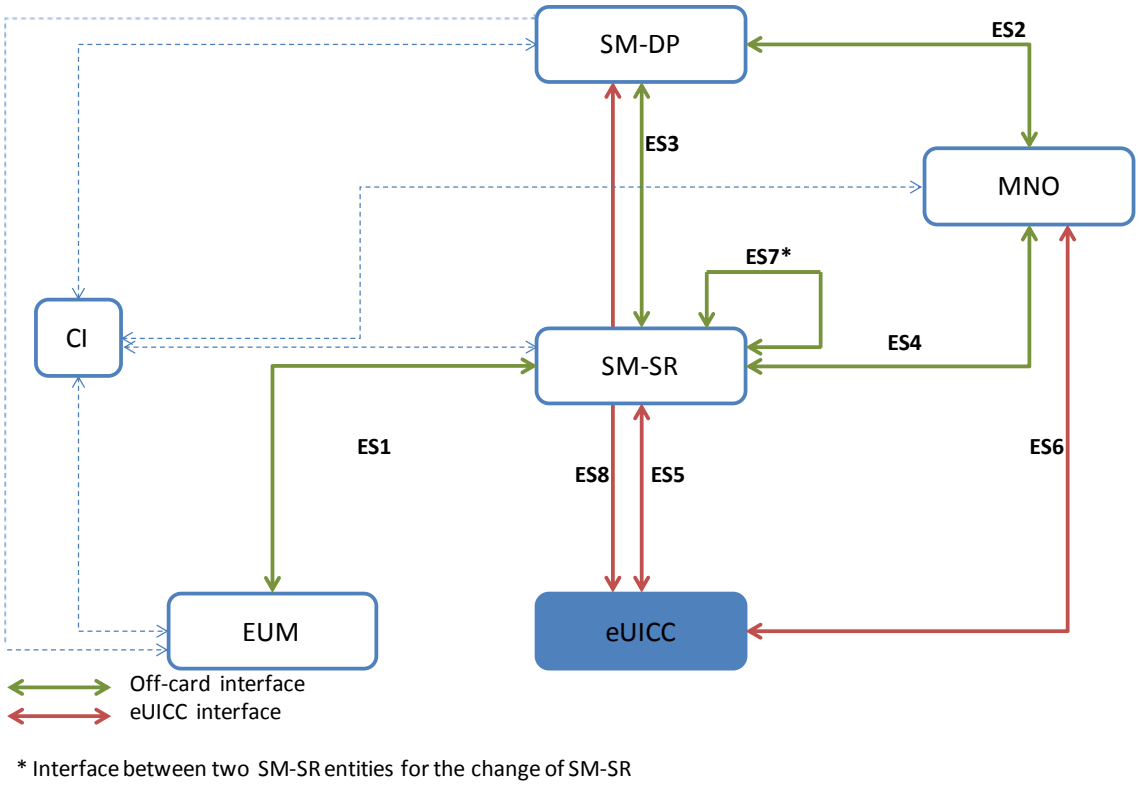

Figure 4 : eUICC Remote Provisioning infrastructure

The TOE communicates with remote servers of

- SM-SR, which provides Platform management commands and secure routing for SM-DP
- SM-DP, which provides Profile Management commands and Profiles
- MNO OTA Platforms

The TOE shall require 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 a HSM) from which the keys are obtained are referred as Trusted IT products.

1.2.5 Protection Profile Usage

The TOE of a Security Target conformant with this PP is the whole embedded eUICC made of the IC, OS, RE and the TOE of this PP. The objectives for the environment (that is for the IC, OS and RE) specified in this PP shall become objectives for the TOE in the Security Target. These objectives shall be (1) either fulfilled by a previous certificate or (2) translated into SFRs by the ST author, or (3) a combination of both. Taking the example where the RE is implemented by a Java Card System:

- The first scenario corresponds to a composite evaluation in the sense of [15], with the IC, OS and JCS already certified, and the embedded eUICC certified on top of them. The Security Target shall refer to the IC, OS and JCS Security Target(s) to fulfill the corresponding security objectives.
- The second scenario corresponds to a unified evaluation of the whole product. The ST shall define SFRs for the IC, OS and JCS in addition to those specified in this PP.
- The third scenario arises for instance when the embedded eUICC is embedded in a certified IC, but the OS and JCS features have not been certified. Therefore, the ST shall refer to the IC Security Target to fulfill the IC objectives and shall introduce SFRs in order to meet the objectives for the OS and JCS. This is a composite evaluation of the system composed of the eUICC software, JCS and OS on top of a certified IC.

The ST author is allowed to add objectives for the TOE regarding other aspects than those specified in this Protection Profile provided the CC conformance rules are met. This may arise, for instance, if the product

- Is intended to include MNO Profiles that must fulfill [4]
- includes a secure application with specific requirements (for example a signature application that must fulfill [PP-SSCD]).

In particular, in a composite evaluation [15], a composite product Security Target (typically for a TOE composed of the eUICC with secure applications) will have to comply with several application security requirements:

- Where there is no application Protection Profile, the composite product Security Target describes the security requirements of the secure application embedded into the previously certified TOE.
- When an application Protection Profile has already been certified, the security requirements of this PP are described within the new composite product Security Target.

A secure application embedded into the eUICC can be certified in composition [15] at a maximum assurance level of EAL4+, which is the EAL of this PP. For specific needs, some security functions of the secure application may envisage to pursue a higher security assurance level (typically using formal methods) for the secure application only and outside composition activities. The additional elements of evidence on the secure application reinforce the trust on the security level of the application.

1.3 Summary of the Security Problem and Features

This section aims to provide contextual information regarding the Security Problem Definition, Security Objectives and Security Functional Requirements described in this Protection Profile. This high-level view of the Protection Profile describes:

- The threat agents;
- The main threat categories, and the corresponding categories of security objectives;
- The security policies corresponding to the objectives.

1.3.1 Threat Agents

The two threat agents considered specifically in this Protection Profile are:

- An off-card Actor;
- An on-card application.

Both types of agents have a High attack potential.

The off-card Actor may be any Actor using the external interfaces of the eUICC, whether they are intended or not to be used.

The intended interfaces of the eUICC are:

- The interfaces with remote provisioning architecture or MNO (OTA interfaces, mobile network)
- The interface with the communication module of the Device, which shall conform to the terminal requirements within [7]

The unintended interfaces of the eUICC are mainly the IC surface as defined in [8] (which may include voltage, electro-magnetism, temperature, and so on).

The on-card application is stored on a MNO Profile and uses the following interfaces:

- APIs
    - GP API,
    - APIs that may be dependent on the Runtime Environment such as the JavaCard API, SIM API ([16]), UICC API ([17]), USIM API ([18]), ISIM API ([19]))
- Policy enforcement interface
- APDU buffer / global byte array;
- RE interfaces such as Java Card VM and Java Card RE.

An application may also try to compromise the TOE by directly using an unintended interface such as:

- eUICC memory (via a buffer overflow);
- Access to APDU buffer or global byte array when another application is selected.

This application may also be described as a "malicious on-card application" or "malicious application" in the remainder of this document.

NB: The Platform code is not considered a threat agent, since the TOE that will be defined in the Security Target includes all the Platform, including the Security IC and embedded software.

1.3.2 High-level View of Threats

The threats considered in this Protection Profile (see section 3.3) correspond to the high-level scenarios described hereafter.

1.3.2.1 "First-Level" Threats

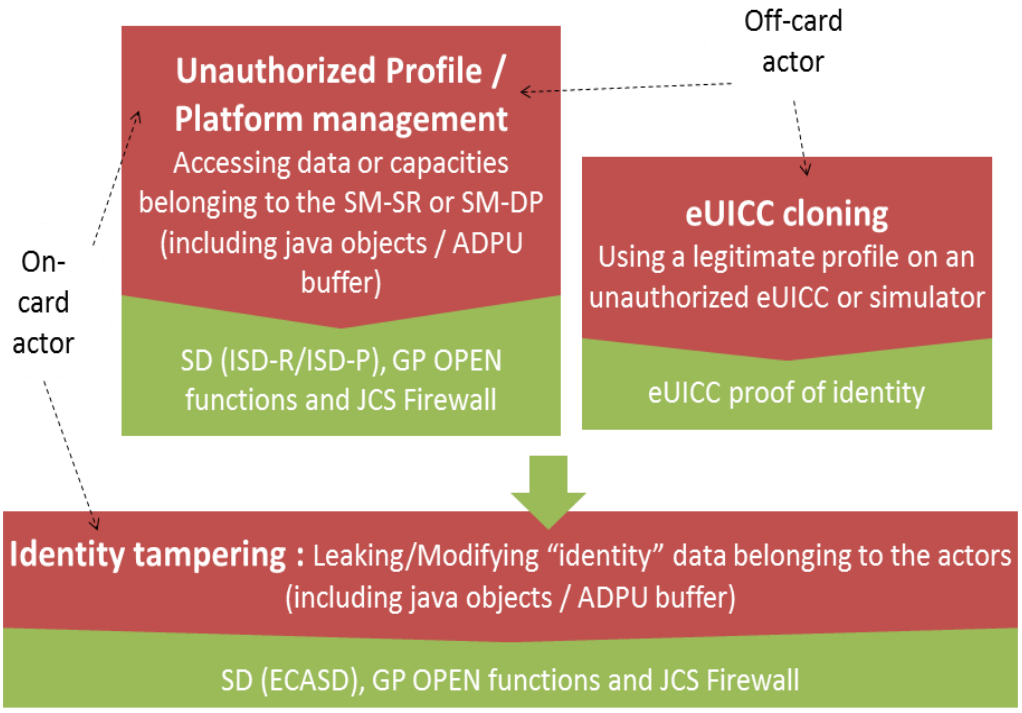

Figure 5 : "First-Level" Threats (1)

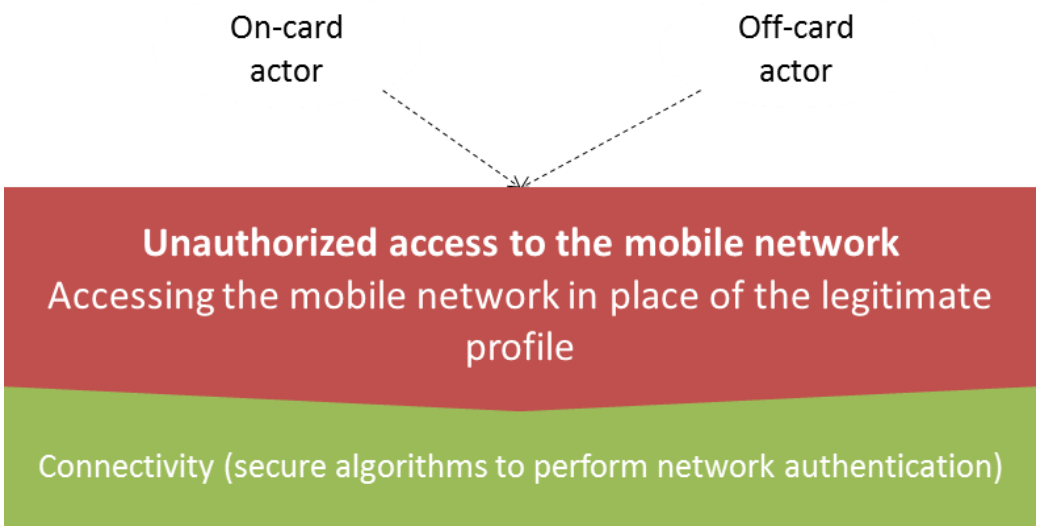

Figure 6 : "First-Level" Threats (2)

Unauthorized Profile / Platform Management

An off-card Actor or on-card application may try to compromise the eUICC in two different ways, by trying to perform:

- Unauthorized Profile Management (typically altering Profile data before or after installation);

- Unauthorized Platform management (typically trying to disable an enabled Profile);

This Protection Profile covers these threats by defining Security Domains: data and capabilities associated to a Security Domain are accessible only to its legitimate owner.

The Security Domains are supported by the extended GP OPEN capacities of the *Platform Support functions*. Their isolation is also supported by the Application Firewall provided by the Runtime Environment of the TOE.

The security domain related to the Profile Management is the ISD-P, while the security domain in charge of Platform management is the ISD-R. More details on these threats can be found in section 3.3.1.

Identity tampering

An attacker may try to bypass the protections against the two categories of threats defined above. A possible vector would consist in directly modifying the identity of the eUICC, or identities of actors via an on-card application. This may be performed, for example, by modifying secrets generated for session establishment, or modifying the CI root public key.

The security objectives covering this threat consist in defining a dedicated Security Domain (ECASD). Identity data such as the CI root public key is under the control of the ECASD and cannot be modified by other actors of the TOE. Some capabilities of the ECASD (such as the generation of secrets) can be used by ISD-R and ISD-P.

The ECASD is supported by the extended GP OPEN capacities of the *Platform Support functions*. Its isolation is also supported by the Application Firewall provided by the Runtime Environment of the TOE.

More details on this threat can be found in section 3.3.2.

eUICC cloning

An off-card Actor may also try to use a legitimate Profile on an unauthorized eUICC, or on a simulator. The Protection Profile prevents cloning by guaranteeing the identity of the eUICC to an off-card Actor before a Profile can be downloaded, or during the usage of the eUICC. The objects used to prove the eUICC identity are controlled by the ECASD security domain. More details on this threat can be found in section 3.3.3.

Note: this PP does not define any means to prove the identity of the eUICC to an on-card application. Such functionality may be included in a future version of the PP.

Unauthorized access to the mobile network

An Actor may try to leverage upon flaws of the network authentication algorithms to gain access to network authentication keys, in order to later authenticate in place of a legitimate Profile. More details on this threat can be found in section 3.3.4.

1.3.2.2 "Second-level" threats

An attacker may try to bypass the protections against the "first-level threats" described in previous section. This PP describes this as "second-level" threats.

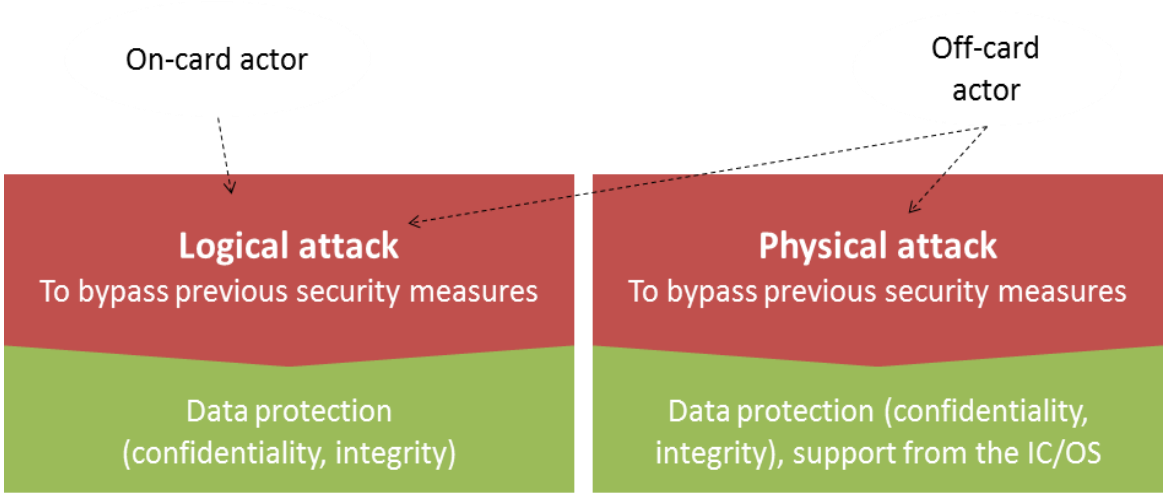

Figure 7 : "second-level" threats

Logical attacks

An on-card malicious application, or an off-card Actor, may try to use unintended side-effects of legitimate eUICC functions or commands to bypass the protections of the TSF. This protection Profile covers these threats in two different ways:

- The underlying RE protects the Security Domains within the TOE (ISD-R, ISD-P, ECASD) from other applications;
- The Platform code belonging to the TOE is not protected from applications by the RE, thus requiring explicit security objectives.

More details on this threat can be found in section 3.3.5.

Physical attacks

An off-card Actor may try to bypass *Platform Support Functions* by several types of attacks. Typically, the off-card Actor may try to perform a side-channel analysis to leak the protected keys, or perform a fault injection to alter the behavior of the TOE. This protection Profile includes security objectives for the underlying IC, which ensures protection against physical attacks.

More details on these last threats can be found in section 3.3.5.

2 Conformance Claims

2.1 CC Conformance Claims

This protection Profile is conformant to Common Criteria version 3.1 revision 4.

More precisely, this protection Profile is conformant to:

- CC Part 1 [9],
- CC Part 2 [10] (extended)
- CC Part 3 [11] (conformant)

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

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

2.2 Conformance Claims to this PP

This Protection Profile requires demonstrable conformance (as defined in [9]) of any ST or PP claiming conformance to this PP.

2.3 PP Conformance Claims

This Protection Profile does not require formal compliance to a specific IC Protection Profile, OS Protection Profile or Runtime Environment, but those IC and JCS evaluated against [2] and [1] respectively, fully meet the objectives.

3 Security Problem Definition

3.1 Assets

Assets are security-relevant elements to be directly protected by the TOE. They are divided into two groups. The first one contains the data created by and for the user (User data) and the second one includes the data created by and for the TOE (TSF data). For each asset it is specified the kind of risks they run.

Note that, while assets listed in the underlying Runtime Environment are not included in this Protection Profile, the ST writer shall still take into account every asset of [1].

3.1.1 User data

User data includes:

User data controlled by the ISD-R:

- The ISD-R keyset (D.ISDR_KEYS)

User data controlled by the ISD-P:

- The ISD-P keyset (D.ISDP_KEYS)
- At least one Network Authentication Application (part of D.PROFILE-CODE) and its associated parameters (D.PROFILE_NAA_PARAMS)
- The POL1 policy file (D.PROFILE_POL1)
- The file system (included in D.PROFILE-CODE)
- The MNO-SD (D.MNO_SD), which may include other applications, as well as
  - The identity associated with the profile (D.PROFILE_IDENTITY)
  - The MNO-SD keyset (D.MNO_KEYS)

This Protection Profile aims at protecting the data and applications of the Profile, regardless of the format. Therefore, in the asset description, the format will not be detailed.

3.1.1.1 Keys

Cryptographic keys owned by the Security Domains. All keys are to be protected from unauthorized disclosure and modification.

D.MNO_KEYS

Keys used by MNO OTA Platform to request management operations from the ISD-P. The keys are loaded during provisioning and stored under the control of the MNO SD.

D.ISDR_KEYS

This Platform Management keyset is used by SM-SR to perform Platform Management functions, via its on-card representative (ISD-R).

D.ISDP_KEYS

This Profile Management keyset is used by SM-DP to perform Profile Management functions via its on-card representative (ISD-P).

3.1.1.2 Profile data

Confidential sensitive data of the applications, like the data contained in an object, a static field of a package, a local variable of the currently executed method, or a position of the operand stack.

To be protected from unauthorized disclosure and unauthorized 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.

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.

The IMSI shall 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.

POL1 shall be protected from unauthorized modification.

3.1.1.3 Profile code

D.PROFILE_CODE

The profile applications include first and second level applications ([7]), in particular:

- The MNO-SD and the Security Domains under the control of the MNO-SD (CASD, SSD)
- The other applications that may be provisioned within the MNO-SD (network access applications, and so on)

This asset also includes, by convention, the file system of the Profile.

All these applications are under the control of the MNO SD.

These assets have to be protected from unauthorized modification.

3.1.2 TSF data

The TSF data includes three categories of data:

- TSF code, ensuring the protection of Profile data
- Management data, ensuring that the management of applications will enforce a set of rules (for example privileges, lifecycle, and so on)
- Identity management data, guaranteeing the identities of eUICC and remote actors

3.1.2.1 TSF Code

D.TSF_CODE

The TSF Code distinguishes between

- the ISD-R, ISD-Ps and ECASD
- the Platform code

All these assets have to be protected from unauthorized disclosure and modification. Knowledge of this code may allow bypassing the TSF. This concerns logical attacks at runtime in order to gain a read access to executable code, typically by executing an application that tries to read the memory area where a piece of code is stored.

Application Note:

- this does not include applications within the MNO-SD, which are part of the user data (Profile applications)
- the notion of unauthorized disclosure and modification is the same as used in [1]

3.1.2.2 Management data

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 [3].

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.

3.1.2.3 Identity management data

Identity management data is used to guarantee the authenticity of actor's identities. It includes:

- EID, eUICC certificate and associated private key, which are used to guarantee the identity of the eUICC
- CI's root public key, which is used to verify all actor's certificates
- Shared secrets used to generate credentials

NB: The EUM keyset for key/certificate renewal is not considered in current version of the PP, since there is no scenario defined for key renewal.

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.

It must 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.

The eUICC certificate has to be protected from unauthorized modification.

Application Note:

In order to verify the certification chain of the eUICC, one requires the EUM certificate and CI's root certificate. However this version of the Protection Profile does not consider the EUM certificate yet, since no use case has been defined regarding its lifecycle in the eUICC.

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.

The CI's root public key must 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.

The EID shall 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.

The shared secrets shall be protected from unauthorized disclosure and modification.

3.2 Users / Subjects

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 PP.

3.2.1 Users

U.PROFILE-APP

The applications included in Profiles

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.

An eUICC can contain more than one MNO-SD.

3.2.2 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.

3.3 Threats

3.3.1 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;
- 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 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

The PP 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 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 behaviour.

Directly threatens the assets: D.ISDP_KEYS, D.MNO_KEYS, D.TSF_CODE (ISD-P), D.PROFILE_*

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 behaviour 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:

- o disclose, replace or modify the SM-SR credentials transmitted during SM-SR handover;
- o 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 behaviour 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.

3.3.2 Identity tampering

T.UNAUTHORIZED-IDENTITY-MNG

A malicious on-card application:

- o 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
- o discloses or modifies functionalities of the ECASD

Such a threat typically includes for example:

- o direct access to fields or methods of the Java objects
- o exploitation of the APDU buffer and global byte array
- o 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

- o use them on another eUICC or on a simulator
- o modify them / replace them with other credentials.

This includes:

- o 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

3.3.3 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

3.3.4 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

3.3.5 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:
  - the extended GP OPEN
  - 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.

Application Note:

This Protection Profile does not require formal compliance to a specific IC Protection Profile or a smart card OS Protection Profile but those IC evaluated against [2] fully meet the objectives.

3.4 Organisational Security Policies

3.4.1 Lifecycle

OSP.LIFECYCLE

The TOE must enforce the eUICC lifecycle defined in [3]. 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:

[3] also includes a fallback functionality ensuring that the eUICC is able to detect a loss of connectivity, then fall-back to a secure provisioning profile and notify the SM-SR. This function is not addressed by this PP.

3.5 Assumptions

A.ACTORS

Actors of the infrastructure (CI, SM-DP, SM-SR and MNO) securely manage their own credentials and otherwise sensitive data.

A.APPLICATIONS

The applications follow the guidelines stated in [5] to ensure that:

- they do not use older versions of shared libraries than the versions provided by the runtime environment
- they do not include any modified shared library without incrementing the library's version accordingly
- they do not introduce any command causing a misuse of GlobalPlatform CVM
- they do pass the latest bytecode verification process by Oracle or the Platform Developer

Application Note:

The use of these guidelines aims to provide a reasonable assurance that an application will not pose a security risk to another application loaded on this product, even before considering the security features provided by the platform.

4 Security Objectives

4.1 Security Objectives for the TOE

4.1.1 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: 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.

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:

- o that incoming messages are properly provided unaltered to the corresponding Security Domain;
- o 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.

4.1.2 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.

Application Note:

This proof may, for instance, be obtained by including the EID value in the eUICC certificate, which is signed by the eUICC Manufacturer.

4.1.3 Platform services

O.OPERATE

The PSF and Telecom framework belonging to the TOE shall ensure the correct operation of their security functions.

Application Note:

Startup of the TOE (TSF-testing) can be covered by FPT_TST.1. As in [1], this SFR component is not mandatory. Testing could also occur randomly. Self-tests may become mandatory in order to comply with other certification programs.

O.API

The Platform code belonging to the TOE shall provide an API to

- o provide atomic transaction to its services, and
- o control the access to its services. The TOE must prevent the unauthorised use of commands.

4.1.4 Data protection

O.DATA-CONFIDENTIALITY

The TOE shall avoid unauthorised 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 unauthorised 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.

4.1.5 Connectivity

O.ALGORITHMS

The eUICC shall provide a mechanism for the authentication to the mobile networks.

4.2 Security Objectives for the Operational Environment

4.2.1 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, SM-DP and MNO. The CI must ensure the security of the private keys associated with the EUM Certificates and SM-DP certificates.

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 SM-SR 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 SM-DP 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.

Application Note:

The SM-DP replaces the OE.PERSONALIZER as defined in [4]

OE.MNO

The MNOs must ensure that any key used in the profile (ISD-P, MNO SD, and any other SSD) are securely generated before they are transmitted on the eUICC via the MNO OTA Platform. The MNOs must ensure that any key used in the profile (ISD-P, MNO SD, and any other SSD) are not compromised before they are transmitted on the eUICC via the MNO OTA Platform.

Administrators of the mobile operator OTA servers shall be trusted people. They shall be trained to use and administer those servers. They have the means and the equipment to perform their tasks. They must be aware of the sensitivity of the assets they manage and the responsibilities associated with the administration of OTA servers. OTA Platform communication on ES6 makes use of at least a minimum security settings defined for ES5 in [3], section 2.4.

Application Note:

One possible realisation of this assumption is the enforcement of security rules defined in an OTA server security guidance document with regular site inspections to check the applicability of the rules

4.2.2 Platform

OE.IC.PROOF_OF_IDENTITY

The underlying IC used by the TOE is uniquely identified

OE.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.

Application Note:

NB: Equivalent to OE.SCP-SUPPORT of [1].

OE.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.

OE.RE.PSF

The Runtime Environment shall provide secure means for card management activities, including:

- o load of a package file
- o installation of a package file
- o extradition of a package file or an application
- o personalization of an application or a Security Domain
- o deletion of a package file or an application
- o privileges update of an application or a Security Domain
- o access to an application outside of its expected availability

Application Note:

This PP does not require full compliance to [1], but Java Card Systems certified under [1] fully meet this objective. The ST writer may translate this objective by reusing the security objectives of [1] related to the following threats: T.DELETION, T.INSTALL.

OE.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 provides

- o an Application Firewall
- o Cryptographic functions that applications may use to actually protect the exchanged information This PP does not require full compliance to [1], but Java Card Systems certified under [1] fully meet this objective. The ST writer may translate this objective by reusing the security objectives of [1] related to the following threats: T.CONFID-APPLI-DATA and T.INTEG-APPLI-DATA.

OE.RE.API

The Runtime Environment shall ensure that native code can be invoked only via an API.

Application Note:

This PP does not require full compliance to [1], but Java Card Systems certified under [1] fully meet this objective. The ST writer may translate this objective by reusing the security objectives of [1] related to the following threats: T.CONFID-JCS-CODE, T.INTEG-JCS-CODE, T.CONFID-JCS-DATA, T.INTEG-JCS-DATA.

OE.RE.DATA-CONFIDENTIALITY

The Runtime Environment shall provide a means to protect at all times the confidentiality of the TOE sensitive data it processes

Application Note:

This PP does not require full compliance to [1], but Java Card Systems certified under [1] fully meet this objective. The ST writer may translate this objective by

- o reusing the security objectives of [1] related to the following threats: T.CONFID-APPLI-DATA

- refining the ADV_ARC "non-bypassability" requirements to explicit the coverage of side channel attacks by the security architecture of the ST TOE.

OE.RE.DATA-INTEGRITY

The Runtime Environment shall provide a means to protect at all times the integrity of the TOE sensitive data it processes.

Application Note:

This PP does not require full compliance to [1], but Java Card Systems certified under [1] fully meet this objective. The ST writer may translate this objective by reusing the security objectives of [1] related to the following threats: T.INTEG-APPLI-DATA, T.INTEG-APPLI-DATA.LOAD, T.INTEG-APPLI-CODE, T.INTEG-APPLI-CODE.LOAD

OE.RE.IDENTITY

The Runtime Environment shall ensure the secure identification of the applications it executes

OE.RE.CODE-EXE

The Runtime Environment shall prevent unauthorized code execution by applications

Application Note:

This PP does not require full compliance to [1], but Java Card Systems certified under [1] fully meet this objective. The ST writer may translate this objective by reusing the security objectives of [1] related to the following threats: T.EXE-CODE.1, T.EXE-CODE.2, T.EXE-CODE-REMOTE and T.NATIVE.

4.2.3 Profile

OE.APPLICATIONS

The applications shall follow the guidelines stated in [5] to ensure that:

- they do not use older versions of shared libraries than the versions provided by the runtime environment
- they do not include any modified shared library without incrementing the library's version accordingly
- they do not introduce any command causing a misuse of GlobalPlatform CVM
- they do pass the latest bytecode verification process by Oracle or the Platform Developer

Application Note:

The use of these guidelines aims to provide a reasonable assurance that an application will not pose a security risk to another application loaded on this product, even before considering the security features provided by the platform.

This objective implies the objective OE.VERIFICATION from the JCS Protection Profile ([1]).

OE.MNOSD

The Security Domain U.MNO-SD must use the secure channel SCP80/81 provided by the TOE according to [3].

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Unauthorized Profile and Platform Management

T.UNAUTHORIZED-PROFILE-MNG This threat is covered by requiring authentication and authorization from the legitimate actors:

- O.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 (OE.RE.DATA-CONFIDENTIALITY and OE.RE.DATA-INTEGRITY).

The authentication is supported by corresponding secure channels:

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

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

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

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

4.3.1.2 Identity tampering

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 (OE.RE.DATA-CONFIDENTIALITY and OE.RE.DATA-INTEGRITY).

OE.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 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 (OE.RE.SECURE-COMM).

NB: No secure channel can be established to the ECASD in this version of the 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.

4.3.1.3 Profile cloning

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

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

4.3.1.4 Unauthorized access to the mobile network

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

4.3.1.5 Second level threats

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 (OE.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 (OE.RE.DATA-CONFIDENTIALITY, OE.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.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY)

The following objectives for the operational environment are also required:

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

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

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

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

4.3.2 Organisational Security Policies

4.3.2.1 Lifecycle

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 OE.RE.PSF. O.PSF ensures that there is a single ISD-P enabled at a time

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

4.3.3 Assumptions

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.

4.3.4 SPD and Security Objectives

Threats	Security Objectives
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP, OE.MNO, O.PSF, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.MNOSD
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PSF, O.SECURE-CHANNELS, OE.SM-SR, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY
T.PROFILE-MNG-INTERCEPTION	OE.SM-DP, OE.MNO, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.MNOSD
T.PLATFORM-MNG-INTERCEPTION	O.SECURE-CHANNELS, OE.SM-SR, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PSF, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.RE.IDENTITY
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, OE.IC.PROOF_OF_IDENTITY
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS
T.LOGICAL-ATTACK	OE.IC.SUPPORT, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, O.OPERATE, OE.RE.API, OE.RE.CODE-EXE
T.PHYSICAL-ATTACK	OE.IC.SUPPORT, OE.IC.RECOVERY, O.OPERATE, O.DATA-CONFIDENTIALITY, OE.RE.DATA-CONFIDENTIALITY

Table 1 Threats and Security Objectives - Coverage

Security Objectives	Threats
O.PSF	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-SR	T.UNAUTHORIZED-PLATFORM-MNG, T.PLATFORM-MNG-INTERCEPTION
OE.SM-DP	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
OE.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
OE.IC.RECOVERY	T.PHYSICAL-ATTACK
OE.RE.PSF	
OE.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.IDENTITY-INTERCEPTION

Security Objectives	Threats
OE.RE.API	T.LOGICAL-ATTACK
OE.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.PHYSICAL-ATTACK
OE.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
OE.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
OE.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.LOGICAL-ATTACK
OE.MNOSD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION

Table 2 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives
OSP.LIFECYCLE	O.PSF, OE.RE.PSF, O.OPERATE

Table 3 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
O.PSF	OSP.LIFECYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFECYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-SR	
OE.SM-DP	
OE.MNO	
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PSF	OSP.LIFECYCLE
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.APPLICATIONS	
OE.MNOSD	

Table 4 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.ACTORS	OE.CI, OE.SM-SR, OE.SM-DP, OE.MNO	Section 2.3.3
A.APPLICATIONS	OE.APPLICATIONS	Section 2.3.3

Table 5 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-SR	A.ACTORS
OE.SM-DP	A.ACTORS
OE.MNO	A.ACTORS
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PSF	
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.APPLICATIONS	A.APPLICATIONS
OE.MNOSD	

Table 6 Security Objectives for the Operational Environment and Assumptions - Coverage

5 Extended Requirements

5.1 Extended Families

5.1.1 Extended Family FIA_API - Authentication Proof of Identity

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 (cf. [3], chapter "Extended components definition (APE_ECD)") from a TOE point of view.

Family Behaviour:

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.

Management:

FIA_API.1 The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit:

FIA_API.1 There are no actions defined to be auditable.

5.1.1.1 Extended Components

Extended Component FIA_API.1

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.

Dependencies: No dependencies.

5.1.2 Extended Family FPT_EMS - TOE Emanation

5.1.2.1 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. The definition of the family FPT_EMS is taken from the Protection Profile Secure Signature Creation Device [SSCD-PP].

FPT_EMS TOE Emanation

Family behaviour:

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.

Management:

FPT_EMS.1

There are no management activities foreseen.

Audit:

FPT_EMS.1

There are no actions identified that shall be auditable if FAU_GEN (Security audit data generation) is included in a PP or ST using FPT_EMS.1.

5.1.2.2 Extended Components

Extended Component FPT_EMS.1

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].

Dependencies: No dependencies.

6 Security Requirements

6.1 Security Functional Requirements

6.1.1 Introduction

This protection Profile defines the following security policies:

- 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 3.2. 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).

6.1.1.1 Secure Channel Protocol information flow control SFP

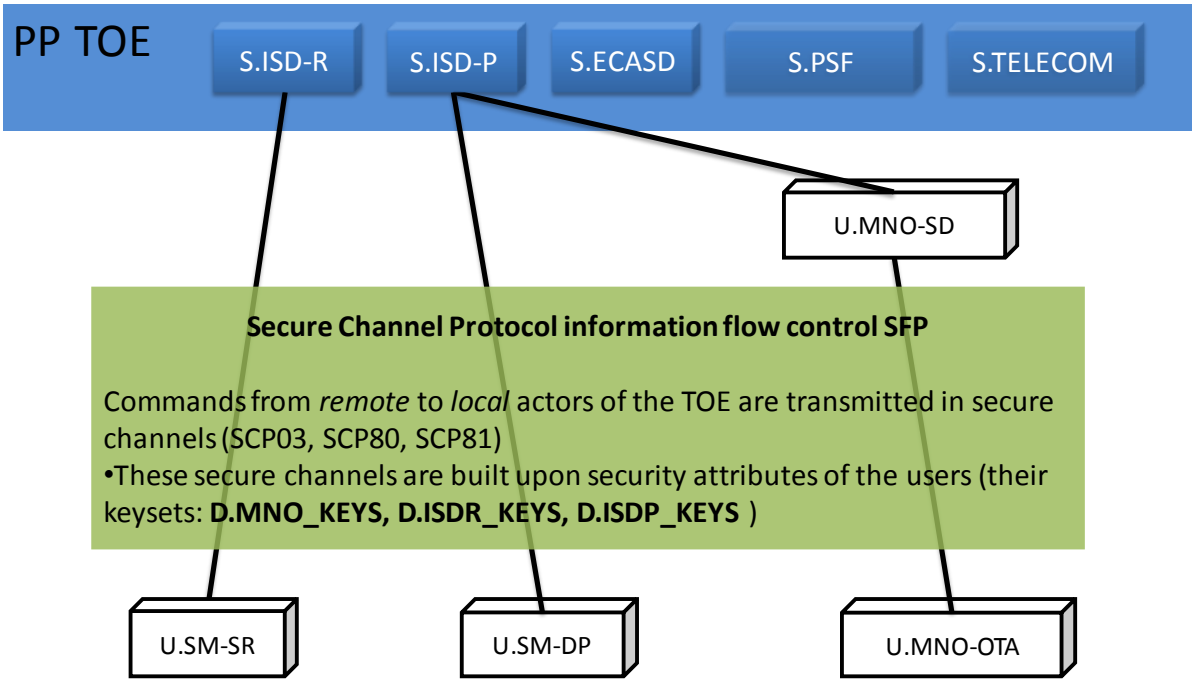

Figure 8: Secure Channel Protocol Information flow control SFP

6.1.1.2 Platform services information flow control SFP

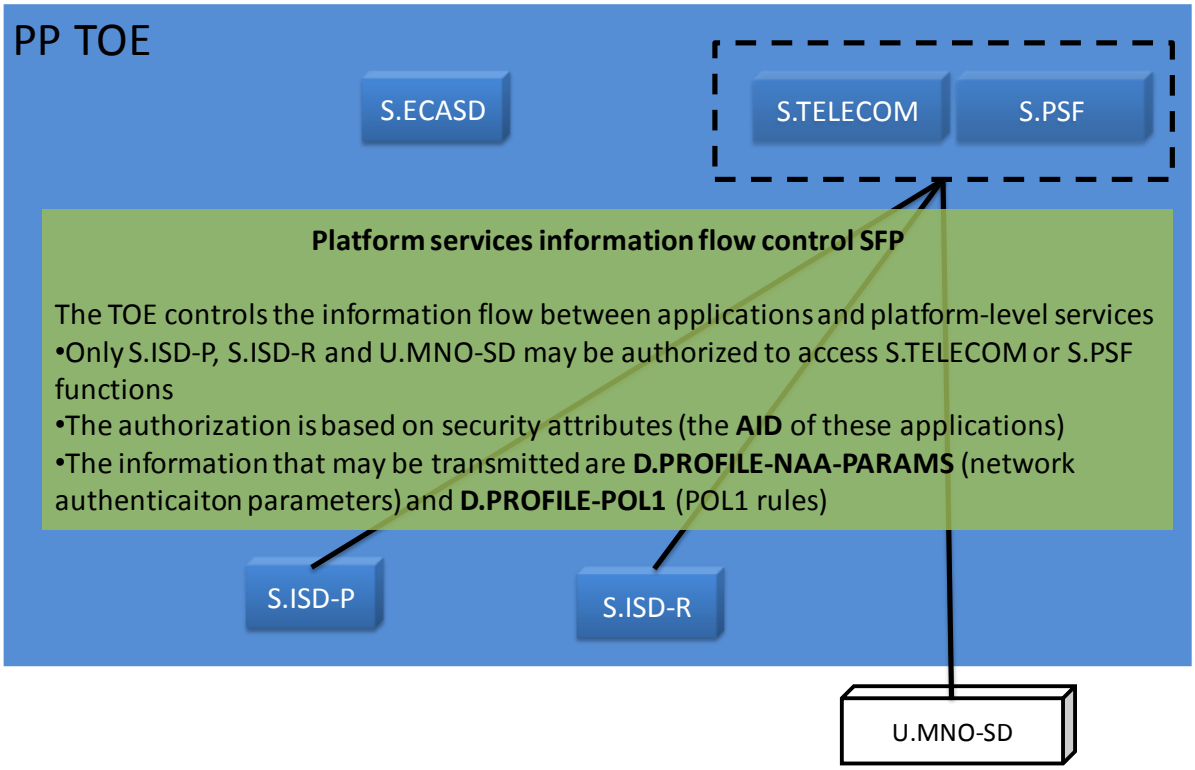

Figure 9: Platform services information flow control SFP

6.1.1.3 ISD-R access control SFP

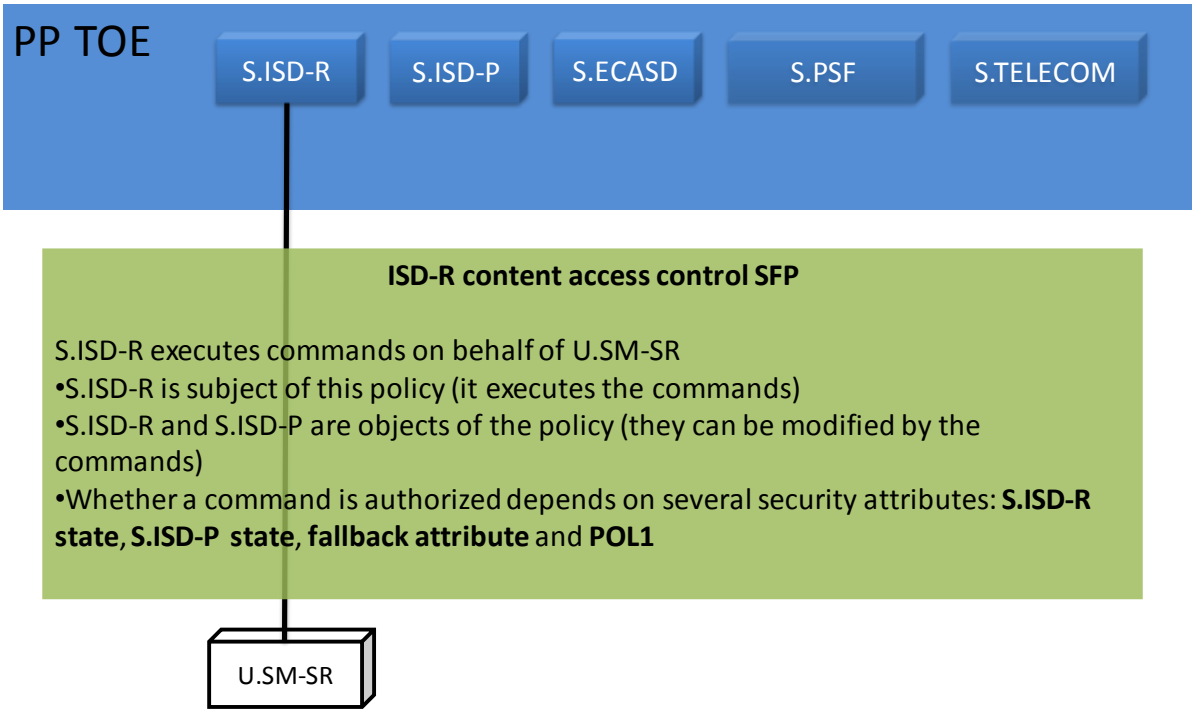

Figure 10: ISD-R access control SFP

6.1.1.4 ISD-P access control SFP

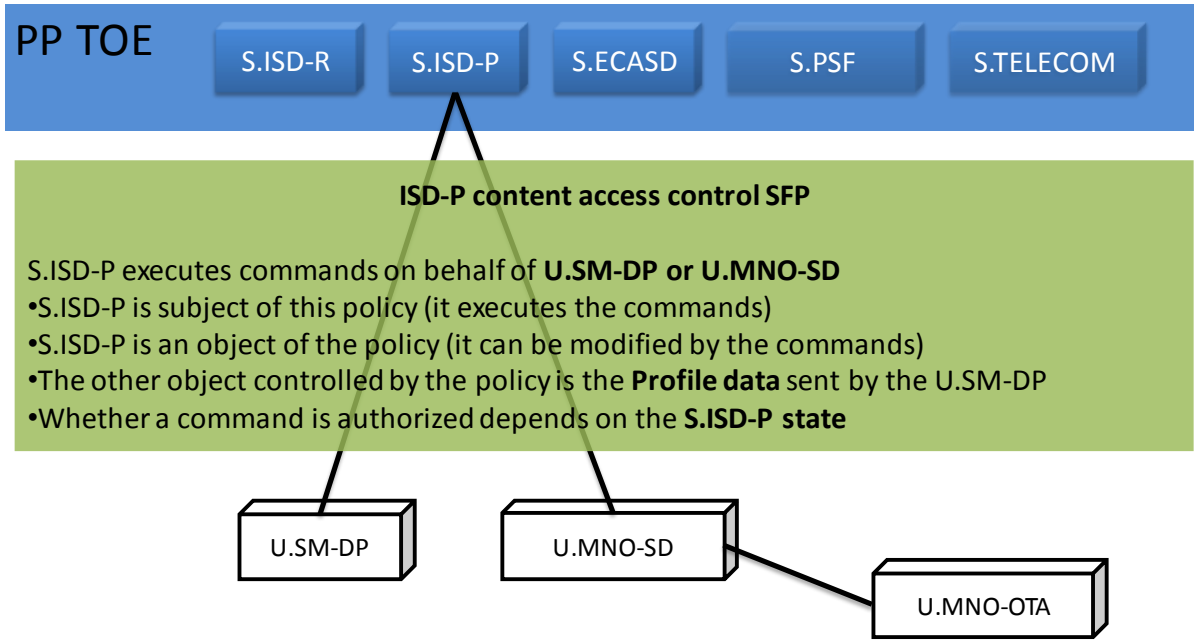

Figure 11: ISD-P content access control SFP

6.1.1.5 ECASD content access control SFP

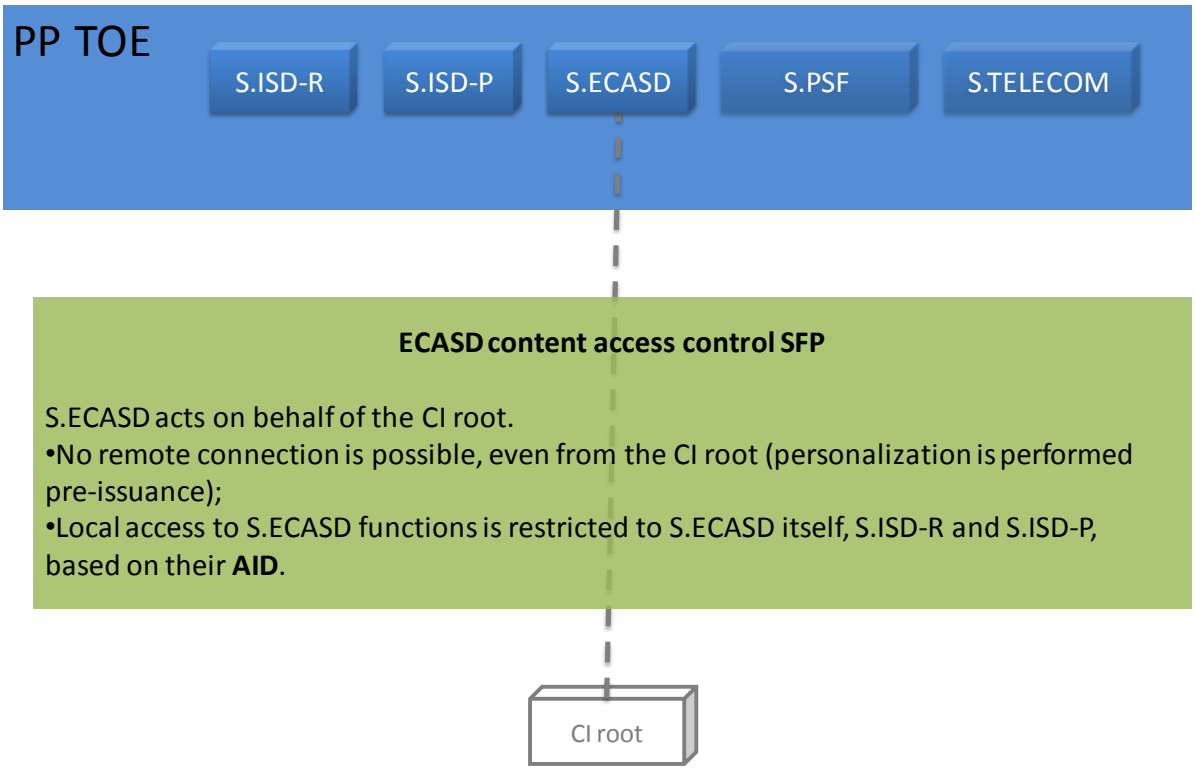

Figure 12: ECASD content access control SFP

6.1.1.6 Security attributes used in SFRs

Security attribute	Details	Relationship to assets
AID	The AID is an identifier for the applications in a JCS runtime environment. As this Protection Profile does not mandate JCS, the ST writer may use another, equivalent, mean to identify applications.	The AID belongs to the runtime environment (is an asset of the JCS Protection Profile [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 the D.PSF_DATA described in § *3.1.2.2 Management data*
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 the D.PSF_DATA described in § *3.1.2.2 Management data*
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 the D.PSF_DATA described in § *3.1.2.2 Management data*
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 § *3.1.1.2 Profile data*

Security attribute	Details	Relationship to assets
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 §*3.1.1.1 Keys*
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 Protection profile. The CI root public key is described as the asset D.CI_ROOT_PUBKEY in § *3.1.2.23 Identity management data*
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 life-time. 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 life-time.	These attributes included in the D.PSF_DATA described in § *3.1.2.2 Management data*
EID	The EID is the identifier of the physical eUICC on which the TOE is implemented.	The EID is a hardware identifier and is not part of the assets of this protection profile.

Table 7: Definition of the security attributes

6.1.2 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 keyset);
  - via SCP03 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.

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

FIA_UID.1/EXT Timing of identification

FIA_UID.1.1/EXT The TSF shall allow

- **application selection**
- **requesting data that identifies the eUICC**
- **[assignment: list of additional TSF mediated actions].**

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

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

Application Note:

This SFR is related to the identification of the 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**
- **[assignment: list of additional TSF mediated actions]**

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

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

Application Note:

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

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

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

The ST writer shall add FCS_COP.1 requirements to include the requirements stated by [3]:

- A new U.SM-SR must be authenticated by verifying its ECDSA signature, 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 a SCP80 secure channel according to [13] or optionally SCP81 according to [14]
- A new U.SM-DP must be authenticated by verifying its ECDSA signature, 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 secure channels, according to FCS_CKM.1/SCP-SM).
- Once the D.ISDP_KEYS keyset is created, U.SM-DP must be authenticated using a SCP03 secure channel according to [12], amendment D
- U.MNO-OTA must be authenticated using a SCP80 secure channel according to [13], or optionally SCP81 according to [14] (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO)

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with one of the following:

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

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 behalf of that user:
- **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 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 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)

The ST writer must be aware that U.MNO-SD is not a subject of the TOE, but an external on-card user acting on behalf of U.MNO-OTA, which is an external off-card user.

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.MNO-SD 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 the 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.ISD-P; 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.

6.1.3 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/SCP-MNO)

FDP_IFC.1/SCP Subset information flow control

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

- **users/subjects:**
  - **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.MNO-SD in a SCP80 or SCP81 secure channel**.

FDP_IFF.1.3/SCP The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/SCP The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

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 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 [3]

- For SM-SR: §2.2.5.1 and §2.4
- For SM-DP: §2.2.5.2 and §2.5
- For MNO-SD: §2.2.5.3 and §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 **[assignment: list of functions for which a trusted channel is required]**.

Application Note:

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the requirements stated by [3], §2.2.5:

- The secure channels to SM-DP must be SCP03 secure channels. Identification of endpoints is addressed by the use of AES according to [12] Amendment D
- 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 perform the same functions than the SCP80 secure channel. The identification of endpoints is addressed by
  - For SCP80: the use of AES according to [13]
  - For SCP81: the use of TLS V1.2 (RFC 5246) according to [14]

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 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 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 secure channel to transmit the following Platform Management commands:

- ES5.EnableProfile
- ES5.DisableProfile
- ES5.DeleteProfile
- ES5.eUICCCapabilityAudit
- ES5.MasterDelete
- ES5.SetFallbackAttribute
- ES5.HandleNotificationConfirmation

The TSF shall permit the SM-SR to open a SCP80 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 secure channel to modify the connectivity parameters of the SM-DP:

- The TSF shall then permit the SM-DP to open a SCP03 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

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

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

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

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

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

FDP_ITC.2.5/SCP The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

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 **[assignment: list of interpretation rules to be applied by the TSF]** 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_IFC.1/SCP and the Downloaded objects related to this SFR FPT_TDC.1/SCP are listed below:

- SM-SR commands
  - ES5.CreateISDP
  - ES5.EnableProfile
  - ES5.DisableProfile
  - ES5.DeleteProfile
  - ES5.eUICCCapabilityAudit
  - ES5.MasterDelete
  - ES5.SetFallbackAttribute
  - ES5.EstablishISDRKeySet

  - ES5.FinaliseISDRhandover
  - ES5.UpdateSMSRAddressingParameters
- 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 unauthorised 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

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the requirements stated by [3]: Confidentiality of communication must be addressed by the use of AES in CBC mode (NIST 800-38A) with a minimum key size of 128 bits.

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

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.

As the cryptographic mechanisms used for the trusted channel may be provided by the underlying Platform, this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the requirements stated by [3]: Integrity of communication must be addressed by the use of AES in CMAC mode (NIST SP 800-38B) with a minimum key size of 128 bits.

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

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

The Elliptic Curve cryptography used for this key agreement may be provided by the underlying Platform. Consequently this PP does not include the corresponding FCS_COP.1 SFR. The ST writer shall add a FCS_COP.1 requirement to include the following requirements: The underlying cryptography for this key agreement is ECKA-EG, compliant with one of the following:

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

FCS_CKM.2/SCP-MNO Cryptographic key distribution

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

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)

Note: 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 **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Application Note:

This SFR is related to the destruction of the following keys:

- D.ISDP_KEYS
- 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 **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Application Note:

This SFR is related to the destruction of the following keys:

- D.MNO_KEYS

6.1.4 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)**
  - **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 [3]
- 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)**
  - **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"**
- **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.**
- **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.**

o **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 authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

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

o **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 [3], 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 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 [3] 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**

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 (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 is authorized only if S.ISD-P's attribute "state" is "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 authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

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 [3]:

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

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 [3]:

- 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.MNO-SD, 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**
- **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**.

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 authorise 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**.

6.1.5 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 the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/Platform_services The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/Platform_services The TSF shall explicitly deny an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly deny information flows]**.

Application Note:

This SFR aims to control which subject is able to transmit POL1 or network authentication keys to the PSF and Telecom Framework. Differences in implementation are allowed, since this PP requires demonstrable conformance. Is it consequently possible for the ST writer to replace this SFR by another instance of FDP_IFF.1 as long as it addresses the control of information flow for these data. Examples of such adaptations could be due to cases such as:

- D.PROFILE-POL1 transmitted from S.ISD-P to S.ISD-R, then from S.ISD-R to S.PSF
- D.PROFILE-NAA-PARAMS transmitted from U.MNO-SD to S.ISD-P, then by ISD-P to S.TELECOM

FPT_FLS.1/Platform_Services Failure with preservation of secure state

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

- **failure that leads to a potential security violation during the processing of a S.PSF or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **POL1 enforcement**
  - **Network authentication**

- **[assignment: other type of failure]**.

Application Note:

The ST writer shall include both:

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

6.1.6 Security management

This package includes several supporting security functions:

- 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 (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)

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

- **D.SECRETS;**
- **D.eUICC_PRIVKEY**

and **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 **[assignment: type of users]** are unable to use the following interface **[assignment: type of connection]** to gain access to

- **D.SECRETS;**
- **D.eUICC_PRIVKEY**

and **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:

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

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

FDP_SDI.1 Stored data integrity monitoring

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

Refinement:

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

- D.MNO_KEYS
- 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:

- **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 **the following parts of D.PSF_DATA:**

- **ISD-P state**
- **fallback attribute**

to

- **S.ISD-R to modify 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-P to modify ISD-P state**
  - **from "SELECTABLE" to "PERSONALIZED" (during profile personalization)**
  - **from "PERSONALIZED" to "DISABLED" (during profile personalization)**
- **S.PSF to modify ISD-P state**

  - **from "ENABLED" to "DISABLED" (during fall-back)**
- **S.ISD-R to modify the fallback attribute (when setting the fallback attribute)**.

Application Note:

- In case part of the PSF functionality is performed by GlobalPlatform packages, the role of S.PSF may for instance be partly attributed to the OPEN.
- [3] includes a fallback functionality ensuring that the eUICC is able to detect a loss of connectivity, then fall-back to a secure provisioning profile and notify the SM-SR. This function is not addressed by this PP. 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 **Security Channel protocol information flow SFP, ISD-P access control SFP and ISD-R access control SFP** to restrict the ability to **change_default, query, modify and delete** the security attributes

- **D.PROFILE_POL1**

to

- **S.ISD-P to change_default, upon request of U.SM-DP via "ES8.DownloadAndInstallation"**
- **S.ISD-R, S.ISD-P to query**
- **S.ISD-P to modify, upon request of U.MNO-SD via "ES6.UpdatePOL1byMNO"**
- **S.ISD-R to delete, upon request of U.SM-SR by "ES5.DeleteProfile"**.

FMT_MSA.1/CERT_KEYS Management of security attributes

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

- **CERT.DP.ECDSA**
- **CERT.SR.ECDSA**
- **D.ISDP_KEYS**
- **D.ISDR_KEYS**
- **D.MNO_KEYS**

to

- **S.ISD-P for:**
  - **query CERT.DP.ECDSA**

- **change_default D.ISDP_KEYS, upon request of U.SM-DP via "ES8.EstablishISDPKeySet"**
- **change_default D.MNO_KEYS, upon request of U.SM-DP via "ES8.DownloadAndInstallation"**
- **query D.ISDP_KEYS**

o **S.ISD-R for:**

- **query CERT.SR.ECDSA**
- **change_default D.ISDR_KEYS, upon request of U.SM-SR via "ES5.EstablishISDRKeySet"**
- **query D.ISDR_KEYS**
- **delete D.ISDR_KEYS, upon request of U.SM-SR via "ES5.FinaliseISDRhandover"**
- **delete D.ISDP_KEYS and D.MNO_KEYS, upon request of U.SM-SR by "ES5.DeleteProfile"**

o **no actor for other operations**.

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 initialisation

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

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

FMT_SMF.1 Specification of Management Functions

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

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

o **External users:**

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

- **U.MNO-OTA**

o **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 §3.2

6.1.7 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 (FCS_CKM.2/Mobile_network 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 **[selection: MILENAGE, Tuak, other]** and cryptographic key sizes **according to the corresponding standard** that meet the following:

- o **MILENAGE according to standard [21]**
- o **Tuak according to [22]**.

Application Note:

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

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

key distribution method] that meets the following: **[assignment: list of standards]**.

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 **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

6.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

The only refined SAR is ADV_ARC, as shown hereafter.

6.2.1 ADV_ARC Security Architecture

ADV_ARC.1 Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

Refinement:

In order to enforce the domain separation, the security architecture may require applications loaded on the eUICC containing the TOE to comply with some rules. But in this case, the security architecture shall not require more rules than the ones specified in A.APPLICATIONS.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3 Security Requirements Rationale

6.3.1 Objectives

6.3.1.1 Security Objectives for the TOE

Platform Support Functions

O.PSF All SFRs related to Security Domains (FDP_ACC.1/* and FDP_ACF.1/*) 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, which ensures that lifecycle modifications 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).

NB: The master delete is also described as a secure failure mode in FPT_FLS.1.

O.eUICC-DOMAIN-RIGHTS The requirements FDP_ACC.1/* and FDP_ACF.1/* 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 and FMT_MSA.3 address the management of the security attributes used by the SFP.

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 All SFRs relative to the ES5, ES6 and ES8 interfaces (*/SCP, */SCP-SM and */SCP-MNO) 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

Identification and authentication SFRs (FIA/*) 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.

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 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 de-allocated resources.

eUICC proof of identity

O.PROOF_OF_IDENTITY This objective is covered by the extended requirement FIA_API.1.

Platform services

O.OPERATE FPT_FLS.1/Platform_services requires that failures do not impact on the security of the TOE.

O.API FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FMT_MSA.3 and FMT_MSA.1 state the policy for controlling the access to TOE services and resources by the Application Layer ("API information flow control policy").

Atomicity and rollback are provided by FDP_ROL.1/Platform_services and the FPT_FLS.1/Platform_services requirement.

Data protection

O.DATA-CONFIDENTIALITY FDP_UCT.1 addresses the reception of data from off-card actors, while the access control SFPs (FDP_ACC.1/*) 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_COP1/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 FDP_UIT.1 addresses the reception of data from off-card actors, while the access control SFPs (FDP_ACC.1/*) 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).

FPT_TST.1 contributes to the protection of integrity.

Connectivity

O.ALGORITHMS The algorithms are defined in FCS_COP.1. FCS_CKM.2 describes how the keys are distributed within the MNO profiles, and FCS_CKM.4 describes the destruction of the keys.

6.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements
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/PSF_DATA, FMT_MSA.1/POL1
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
O.SECURE-CHANNELS	FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FIA_UID.1/EXT, FIA_UAU.4/EXT, FIA_ATD.1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FDP_IFC.1/SCP, FDP_IFF.1/SCP, FIA_UID.1/MNO-SD, FCS_CKM.4/SCP-SM, FCS_CKM.4/SCP-MNO, FIA_USB.1/MNO-SD, FIA_USB.1/EXT, FMT_SMF.1, FMT_SMR.1, FIA_UAU.1/EXT
O.INTERNAL-SECURE-CHANNELS	FDP_RIP.1, FDP_SDI.1, FPT_EMS.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, FPT_FLS.1/Platform_Services, FMT_SMR.1, FMT_SMF.1, FMT_MSA.3
O.DATA-CONFIDENTIALITY	FDP_RIP.1, FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network, FPT_EMS.1
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FDP_SDI.1

Security Objectives	Security Functional Requirements
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network

Table 8 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FIA_UID.1/EXT	O.SECURE-CHANNELS
FIA_UAU.1/EXT	O.SECURE-CHANNELS
FIA_USB.1/EXT	O.SECURE-CHANNELS
FIA_UAU.4/EXT	O.SECURE-CHANNELS
FIA_UID.1/MNO-SD	O.SECURE-CHANNELS
FIA_USB.1/MNO-SD	O.SECURE-CHANNELS
FIA_ATD.1	O.SECURE-CHANNELS
FIA_API.1	O.PROOF_OF_IDENTITY
FDP_IFC.1/SCP	O.SECURE-CHANNELS
FDP_IFF.1/SCP	O.SECURE-CHANNELS
FTP_ITC.1/SCP	O.eUICC-DOMAIN-RIGHTS, O.SECURE-CHANNELS
FDP_ITC.2/SCP	O.SECURE-CHANNELS
FPT_TDC.1/SCP	O.SECURE-CHANNELS
FDP_UCT.1/SCP	O.SECURE-CHANNELS, O.DATA-CONFIDENTIALITY
FDP_UIT.1/SCP	O.SECURE-CHANNELS, O.DATA-INTEGRITY
FCS_CKM.1/SCP-SM	O.SECURE-CHANNELS
FCS_CKM.2/SCP-MNO	O.SECURE-CHANNELS
FCS_CKM.4/SCP-SM	O.SECURE-CHANNELS
FCS_CKM.4/SCP-MNO	O.SECURE-CHANNELS
FDP_ACC.1/ISDR	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ISDR	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ISDP	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ISDP	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ECASD	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ECASD	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_IFC.1/Platform_services	O.API
FDP_IFF.1/Platform_services	O.API

Security Functional Requirements	Security Objectives
FPT_FLS.1/Platform_Services	O.OPERATE, O.API
FPT_EMS.1	O.INTERNAL-SECURE-CHANNELS, O.DATA-CONFIDENTIALITY
FDP_SDI.1	O.INTERNAL-SECURE-CHANNELS, O.DATA-INTEGRITY
FDP_RIP.1	O.INTERNAL-SECURE-CHANNELS, O.DATA-CONFIDENTIALITY
FPT_FLS.1	
FMT_MSA.1/PSF_DATA	O.PSF
FMT_MSA.1/POL1	O.PSF
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS
FMT_MSA.3	O.SECURE-CHANNELS, O.API
FMT_SMF.1	O.SECURE-CHANNELS, O.API
FMT_SMR.1	O.SECURE-CHANNELS, O.API
FCS_COP.1/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS
FCS_CKM.2/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS
FCS_CKM.4/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS

Table 9 SFRs and Security Objectives

6.3.3 Dependencies

6.3.3.1 SFRs Dependencies

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

Requirements	CC Dependencies	Satisfied Dependencies
FCS_CKM.4/SCP-SM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FCS_CKM.4/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	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
FPT_FLS.1/Platform_Services	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, 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, FMT_SMF.1, FMT_SMR.1

Requirements	CC Dependencies	Satisfied Dependencies
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	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/SCP-MNO
FCS_CKM.4/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP

Table 10 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.2 or FCS_COP.1 of FCS_CKM.1/SCP-SM is discarded. The dependency to FCS_COP.1 is left unsatisfied, since the TOE uses the cryptographic libraries provided by its underlying Platform

6.3.3.2 SARs Dependencies

Requirements	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_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	
ALC_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

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

Table 11 SARs Dependencies

6.3.4 Rationale for the Security Assurance Requirements

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

6.3.4.1 ALC_DVS.2 Sufficiency of security measures

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

6.3.4.2 AVA_VAN.5 Advanced methodical vulnerability analysis

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

7 Notice

This document has been generated with TL SET version 3.1.1 Full (for CC3). For more information about the security editor tool of Trusted Labs visit our website at www.trusted-labs.com.

Formatting throughout the document is restricted by use of TL SET therefore, some deviations from AD.11 GSMA House Style have occurred. In particular, section 3 to 6 (generated by TLSET) have to meet the naming conventions and terminology of Common Criteria (not GSMA house style). In particular, capitalization rules are those from Common Criteria. Ultimately, Common Criteria terms cannot be defined in this document, and the reader must refer to Common Criteria for Information Technology Security Evaluation [9], [10] and [11] for definitions.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	13 October 2013	First release of PRD	GSMA PSMC	Trusted Labs / ESIM WI1

A.2 Other Information

Type	Description
Document Owner	SIM Group
Editor / Company	Trusted Labs

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com.

Your comments or suggestions & questions are always welcome.

Index

U