eUICC for Consumer and IoT Devices Protection Profile
Version 2.0
19 December 2023

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Contents

Figures **5**
Tables **6**
0.1 References **7**
0.2 Definition of Terms **10**
0.3 Abbrevitions **15**
1 Introduction **18**
1.1 Protection Profile identification 18
1.2 TOE overview 18
1.2.1 TOE type and TOE major security features 19
1.2.2 TOE usage 23
1.2.3 TOE life-cycle 23
1.2.4 Non-TOE HW/SW/FW Available to the TOE 26
1.2.5 Protection Profile Usage 32
1.3 Summary of the security problem and features 33
1.3.1 Threat agents 33
1.3.2 High-level view of threats 34
2 Conformance Claims **39**
2.1 CC Conformance Claims 39
2.2 Conformance Claims to this PP 39
2.3 PP Conformance Claims 39
3 Security Problem Definition **40**
3.1 Assets 40
3.1.1 User data 40
3.1.2 TSF data 41
3.2 Users / Subjects 44
3.2.1 Users 44
3.2.2 Subjects 45
3.3 Threats 46
3.3.1 Unauthorized profile and platform management 46
3.3.2 Identity tampering 47
3.3.3 eUICC cloning 48
3.3.4 LPAd/IPAd impersonation 48
3.3.5 Unauthorized access to the mobile network 49
3.3.6 Second level threats 49
3.4 Organisational Security Policies 49
3.4.1 Life-cycle 49
3.5 Assumptions 50
3.5.1 Device assumptions 50
3.5.2 Miscellaneous 50
4 Security Objectives **51**
4.1 Security objectives for the TOE 51
4.1.1 Platform support functions 51
4.1.2 eUICC proof of identity 52

4.1.3 Platform services 52
4.1.4 Data protection 52
4.1.5 Connectivity 53
4.2 Security Objectives for the Operational Environment 54
4.2.1 Actors 54
4.2.2 Platform 55
4.2.3 Profile 57
4.3 Security Objectives Rationale 58
4.3.1 Threats 58
4.3.2 Organisational Security Policies 60
4.3.3 Assumptions 61
4.3.4 SPD and Security Objectives 61
5 Extended requirements 66
6 Security Requirements 66
6.1 Security Functional Requirements 66
6.1.1 Introduction 66
6.1.2 Identification and authentication 71
6.1.3 Comminication 76
6.1.4 Security Domains 84
6.1.5 Platform Services 87
6.1.6 Security management 89
6.1.7 Mobile Network authentication 94
6.2 Security Functional Rationale 95
6.2.1 Refinements regarding Architectural design (ADV_ARC.1) 96
6.3 Security Requirements Rationale 97
6.3.1 Objectives 97
6.3.2 Rationale tables of Security Objectives and SFRs 99
6.3.3 Dependencies 101
6.3.4 Rationale for the Security Assurance Requirements 105
7 LPAe PP-Module 106
7.1 Introduction 106
7.1.1 PP-Module Identification 106
7.1.2 Base-PP 106
7.1.3 TOE Overview 106
7.1.4 Summary of the security problem 109
7.2 Consistency Rationale 110
7.3 Conformance Claims 111
7.3.1 Conformance Claims to this PP 112
7.4 Security Problem Definition 112
7.4.1 Assets 112
7.4.2 Users / Subjects 113
7.4.3 Threats 114
7.4.4 Assumptions 115
7.5 Security Objectives 116
7.5.1 Security Objectives for the TOE 116

7.5.2 Security Objectives for the Operational Environment 117
7.5.3 Security Objectives Rationale 117
7.6 Extended Requirements 120
7.6.1 Extended Families 120
7.7 Security Requirements 121
7.7.1 Security Functional Requirements 122
7.7.2 Security Assurance Requirements 132
7.7.3 Security Requirements Rationale 132
8 LPAe PP-configuration 136
8.1 Reference 136
8.2 Components statement 136
8.3 Conformance statement 136
8.4 SAR statement 136
9 IPAe PP-module 137
9.1 Introduction 137
9.1.1 PP-Module Identification 137
9.1.2 Base-PP 137
9.1.3 TOE Overview 137
9.1.4 Summary of the security problem 140
9.2 Consistency Rationale 141
9.3 Conformance Claims 142
9.3.1 Conformance Claims to this PP 142
9.4 Security Problem Definition 142
9.4.1 Assets 142
9.4.2 Users / Subjects 144
9.4.3 Threats 144
9.4.4 Assumptions 145
9.5 Security Objectives 146
9.5.1 Security Objectives for the TOE 146
9.5.2 Security Objectives for the Operational Environment 147
9.5.3 Security Objectives Rationale 147
9.6 Extended Requirements 150
9.6.1 Extended Families 150
9.7 Security Requirements 151
9.7.1 Security Functional Requirements 152
9.7.2 Security Assurance Requirements 163
9.7.3 Security Requirements Rationale 163
10 IPAe PP-configuration 167
10.1 Reference 167
10.2 Components statement 167
10.3 Conformance statement 167
10.4 SAR statement 167
Annex A PP Module OS Update 167
A.1 Scope 167
A.2 Security Problem Definition (SPD) 168

A.2.1 Assets 168
A.2.2 Security Aspects 168
A.2.3 Threats 168
A.2.4 Subjects 169
A.3 Security Objectives 169
A.3.1 Security Objectives for the TOE 169
A.3.2 Security Objectives for the Operational Environment 170
A.3.3 Security Objectives Rationale 170
Annex B Annex B Document Management 172
B.1 Document History 172
B.2 Other Information 174

Figures

Figure 1 Scope of the TOE based on [PP0084] 20
Figure 2 Scope of the TOE based on [PP0117] 20
Figure 3 TOE life-cycle – TOE delivery compared to the [PP0084] 24
Figure 4 TOE lifecycle – TOE delivery compared to the [PP0117] 25
Figure 5 TOE interfaces based on [PP0084] 26
Figure 6 TOE interfaces based on [PP0117] 27
Figure 7 Remote SIM Provisioning System, LPA in the Device 31
Figure 8 Remote SIM Provisioning System, IPA in the IoT Device 32
Figure 9 “First-level” threats (1) 35
Figure 10 “First-level” threats (2) 36
Figure 11 “Second Level Threats” 37
Figure 12 Secure Channel Protocol Information flow control SFP 67
Figure 13 Platform services information flow control SFP 68
Figure 14: ISD-R access control SFP 68
Figure 15 ISD-P content access control SFP 69
Figure 16 ECASD access control SFP 69
Figure 17 Scope of the TOE 107
Figure 18 TOE interfaces 108
Figure 19 Remote SIM Provisioning System, LPA in the eUICC 109
Figure 20: LPAe Information flow control SFP 122
Figure 21 Scope of the TOE 138
Figure 22 TOE interfaces 139
Figure 23 Remote Provisioning System, IPA in the eUICC 140
Figure 24 IPAe Information flow control SFP 152

Tables

Table 1 Threats and Security Objectives – Coverage 62
Table 2 Security Objectives and Threats – Coverage 63
Table 3 OSPs and Security Objectives – Coverage 63
Table 4 Security Objectives and OSPs – Coverage 64
Table 5 Assumptions and Security Objectives for the Operational Environment – Coverage 64
Table 6 Security Objectives for the Operational Environment and Assumptions – Coverage 65
Table 7 Definition of the security attributes 71
Table 8 Security Objectives and SFRs – Coverage 99
Table 9 SFRs and Security Objectives 101
Table 10 SFRs Dependencies 104
Table 11 SARs Dependencies 105
Table 12 Threats and Security Objectives – Coverage 119
Table 13 Security Objectives and Threats – Coverage 120
Table 14 Assumptions and Security Objectives for the Operational Environment – Coverage 120
Table 15 Security Objectives for the Operational Environment and Assumptions - Coverage 120
Table 16 Definition of the security attributes of LPAe module 123
Table 17 Security Objectives and SFRs – Coverage 134
Table 18 SFRs and Security Objectives 134
Table 19 SFRs Dependencies 136
Table 20 Threats and Security Objectives - Coverage 149
Table 21 Security Objectives and Threats – Coverage 150
Table 22 Assumptions and Security Objectives for the Operational Environment – Coverage 150
Table 23 Security Objectives for the Operational Environment and Assumptions – Coverage 150
Table 24 Definition of the security attributes of IPAe module 153
Table 25 Security Objectives and SFRs – Coverage 164
Table 26 SFRs and Security Objectives 165
Table 27 SFRs Dependencies 166

0.1 References

Ref	Doc Number	Title
[1]	PP-JCS	Java Card™ System - Open Configuration Protection Profile, version 3.0.5, December 2017, BSI-CC-PP-0099-2017.
[2]	PP0084	Security IC Platform Protection Profile with Augmentation Packages version 1.0, February 2014, BSI-CC-PP-0084-2014.
[3]	SGP.02	GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification - Version 2.0, October 2014 - Version 3.0, 30 June 2015 - Version 4.2, 07 July 2020 References to *[3]* in this PP may be interpreted as *any of the three versions of this document*. References to *[3] version 2.0* (respectively *[3] version 3.0*) shall be interpreted as *only the version 2.0* (respectively *3.0*) *of the document*.
[4]	PP-USIM	(U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations, version 2.0.2, July 2010, ANSSI-CC-PP-2010/05.
[5]	GP-SecurityGuidelines-BasicApplications	GlobalPlatform Card Composition Model Security Guidelines for Basic Applications, version 2.0, December 2014 – ref. GPC_GUI_050.
[6]	ETSI_TS_102221	ETSI TS 102 221 - Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 9).
[7]	JIL-CC forIC	Joint Interpretation Library – The application of CC to integrated circuits, version 3.0, February 2009.
[8]	Void	Void
[9]	Void	Void
[10]	Void	Void

[11]	GlobalPlatform_Card_Specification	GlobalPlatform Card Specification v2.3 including • Card Confidential Card Content Management Card Specification v2.3 - Amendment A v1.1; • Card Remote Application Management over HTTP Card Specification v2.2 – Amendment B v1.1.3; • Card Technology Contactless Services Card Specification v2.3 - Amendment C v1.2; • Card Technology Secure Channel Protocol '03' Card Specification v2.2 – Amendment D V1.1.1; • Secure Channel Protocol '11' Card Specification v.2.2 – Amendment F V1.0.
[12]	SCP80	ETSI TS 102 225 - Secured packet structure for UICC based applications, version 9.0.0, release 9, April 2010. ETSI TS 102 226 - Remote APDU structure for UICC based applications, version 12.0.0, release 9, February 2015.
[13]	SCP81	GlobalPlatform Card Specification Amendment B – Remote Application Management over HTTP, version 1.1.3, May 2015.
[14]	Composite-Product-Evaluation	Joint Interpretation Library – Composite Product Evaluation for Smart Cards and similar devices, Version 1.4, August 2015.
[15]	SIM API	3GPP TS 43.019 - Subscriber Identity Module Application Programming; Interface (SIM API) for Java Card, version 6.0.0, release 6, December 2004.
[16]	UICC API	ETSI TS 102 241 - UICC Application Programming Interface (UICC API) for Java Card, version 9.2.0, release 9, March 2012.
[17]	(U)SIM API	3GPP TS 31.130 - (U)SIM API for Java™ Card, version 9.4.0, release 9, April 2012.
[18]	ISIM API	3GPP TS 31.133 - ISIM API for Java Card™, version 9.2.0 - release 9, May 2011.
[19]	AIS 20/31	W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators“, version 2.0, September, 2011.
[20]	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: Implementers Test Data; • Document 4: Design Conformance Test Data; • Document 5: Summary and results of design and evaluation.

[21]	Tuak	3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233, version 12.1.0 , release 12, December 2014. • Document 1: Algorithm specification; • Document 2: Implementers' test data; • Document 3: Design conformance test data.
[22]	3GPP Authent	3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture, version 12.2.0, release 12, December 2014. 3GPP TS 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture, version 12.16.0, release 12, December 2015.
[23]	SGP.21	Remote SIM Provisioning (RSP) Architecture, version: • 2.1, GSM Association, February 2017. • 2.2, GSM Association, September 2017. • 2.3, GSM Association, June 2021. • 2.4, GSM Association, August 2021. • 2.5, GSM Association, November 2022. • 3.0, GSM Association, March 2022.
[24]	SGP.22	Remote SIM Provisioning (RSP) Technical Specification, version: • 2.1, GSM Association, February 2017. • 2.2.x GSM Association, June 2020. • 2.3, GSM Association, June 2021. • 2.4, GSM Association, October 2021. • 2.5, GSMA Association, May 2023. • 3.0, GSM Association, October 2022.
[25]	3GPP Numbering	3GPP TS 23.003 version 15.3.0 - Numbering, addressing and identification (Release 15).
[26]	NFC Req	GSMA TS.26 – NFC Handset Requirements, version 11.0, June 2017.
[27]	JIL	Security requirements for post-delivery code loading, Joint Interpretation Library, Version 1.0, February 2016
[28]	GP SE PP	GlobalPlatform Secure Element Protection Profile
[29]	SGP.24	RSP Compliance Process, version, GSMA Association, version 2.3, October 2020.
[30]	eUICC Profile Package	Trusted Connectivity Alliance (formerly SIMalliance) eUICC Profile Package: Interoperable Format Technical Specification, version 2.1 or Higher
[31]	SGP.29	GSMA EID Definition and Assignment Process V1.0
[32]	TS.48	GSMA Generic eUICC Test Profile for Device Testing
[33]	ETSI TS 102 220	Smart Cards; ETSI numbering system for telecommunication application providers

[34]	PP0117	Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, Version 1.5, BSI-CC-PP-0117-2022
[35]	SGP.31	eSIM IoT Architecture and Requirements, version: • 1.0, GSM Association, April 2022. • 1.1, GSM Association, May 2023.
[36]	SGP.32	eSIM IoT Technical Specification, version: • 1.0, GSM Association, May 2023.
[37]	CC1v2022	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version CC:2022 Revision 1, November 2022.
[38]	CC2v2022	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version CC:2022 Revision 1, November 2022.
[39]	CC3v2022	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version CC:2022 Revision 1, November 2022.
[40]	CC5v2022	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, version CC:2022 Revision 1, November 2022.

0.2 Definition of Terms

Besides the terms described in the next table, the terminology and abbreviations of Common Criteria apply (see [37], [38], [39] and [40]).

Term	Description
Additional Code	Code activated by the Atomic Activation on the Initial TOE to generate the final TOE. For instance, Additional Code could: correct flaws, add new functionalities, update the operating system (definition from [27]).
Alternative SM-DS	SM-DS used in cascade mode with a Root SM-DS to redirect Event Registration from an SM-DP+ to the Root SM-DS.
Consumer Device	As per the definition of Device in SGP.22[24].
Device	Consumer Device or IoT Device
Disabled (Profile)	The state of a Profile where all files and applications (e.g. NAA) present in the Profile are not selectable over the eUICC- Terminal interface.
Discrete eUICC	An eUICC implemented on discrete standalone hardware, including its own dedicated volatile and non-volatile memory. A Discrete eUICC can be removable or non-removable.
eIM Configuration Operation	As defined in SGP.32[36].

Enabled (Profile)	The state of a Profile when its files and/or applications (e.g., NAA) are selectable over the UICC-Terminal interface.
Enterprise	A business, organization or government entity that subscribes to mobile services to be utilized by its workforce in support of the business or activities of the Enterprise. The Enterprise as the Subscriber owns the relationship with the Mobile Service Provider(s).
Enterprise Capable Device	A Device that supports the installation and enforcement of Enterprise Rules.
Enterprise Profile	An Operational Profile for which the Subscriber is an Enterprise. This profile may include restrictions on the End User of the Device.
Enterprise Rule	A rule stored in an Enterprise Profile that can be used by the Profile Owner to restrict End User controllability for enabling and installing Profiles on Enterprise Capable Devices.
eSIM CA	As defined in SGP.21 [23] V3.0.
eSIM IoT Remote Manager	As defined in SGP.32 [36].
eUICC	A UICC which enables the remote and/or local management of Profiles in a secure way. NOTE: The term originates from “embedded UICC”.
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 (e.g. firmware and operating system).
eUICC-ID	Unique identifier for the eUICC as defined in the SGP.02 [24] or alternatively with the new format as defined in SGP.29 [31] See further explanation on section 4.3.1 of SGP.22 [24]
eUICC OS Update	Mechanism to correct existing features on an eUICC by the original OS Manufacturer when the eUICC is in the field.
eUICC Package	As defined in SGP.32 [36].
Event	A Profile download which is set by an SM-DP+ on behalf of an Operator, to be processed by a specific eUICC.
EventID	Unique identifier of an Event for a specific EID generated by the SM-DP+ / SM-DS.
Event Record	The set of information stored on the SM-DS for a specific Event, via the Event Registration procedure. This information consists of either: • the Event-ID, EID, and SM-DP+ address or • the Event-ID, EID, and SM-DS address.
Event Registration	A process notifying the SM-DS on the availability of information on either a specific SM-DP+ or a specific SM-DS for a specific eUICC.

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.
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.
Integrated eUICC	An eUICC implemented on an Integrated TRE.
Integrated TRE	A TRE implemented inside a System-on-Chip (SoC), optionally making use of remote volatile and/or non-volatile memory.
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 as defined in 3GPP TS 23.003 [25] section 2.2.
IoT Device	As defined in SGP.32 [36].
IoT Profile Assistant	As defined in SGP.32 [36].
Issuer Identifier Number	The first 8 digits of the EID.
Issuer Security Domain	A security domain on the UICC as defined by GlobalPlatform Card Specification [11].
Local Profile Assistant	A functional element in the Device or in the eUICC that provides the LPD, LDS and LUI features. When LPA is located in the Device, these elements are noted LPAd, LPDd, LUId, LDSd. When LPA is located in the eUICC, these elements are noted LPAe, LPDe, LUIe, LDSe. Where LPA, LPD, LDS or LUI are used, it applies to the element independent of its location in the Device or in the eUICC.
Local Profile Management	Local Profile Management are operations that are locally initiated on the End User (ESeu) interface.
Local Profile Management Operation	Local Profile Management Operations include enable Profile, disable Profile, delete Profile, query Profile Metadata, eUICC Memory Reset, eUICC Test Memory Reset and Set Nickname.
MatchingID	Equivalent to “Activation Code Token“as defined in SGP.21 [23]: “A part of the Activation Code information provided by the Operator/ Mobile Service Provider to reference a Subscription“.
Mobile Network Operator	An entity providing access capability and communication services to its End User through a mobile network infrastructure.

Mobile Network Operator Security Domain (MNO-SD)	Part of the Profile, owned by the Operator, providing the Secured Channel to the Operator's Over The Air (OTA) Platform. It is used to manage the content of a Profile once the Profile is enabled.
Network Constrained Device	As defined in SGP.32 [36].
NFC Device	A Device compliant with GSMA TS.26 [26].
Notification	A report about a Profile download and Local Profile Management Operation processed by the eUICC.
Managing SM-DP+	An SM-DP+ that is authorised by the Profile Owner to perform RPM to the eUICC on which their Profile resides.
Operational Profile	A Profile that allows connectivity to a commercial mobile network.
OTA Keys	The credentials included in the Profile, used in conjunction with OTA Platforms.
OTA Platform	An Operator platform for remote management of UICCs and the content of Enabled Operator Profiles on eUICCs.
Platform Management	A set of functions related to the, enabling, disabling and deletion of a Profile and/or the transport of Profile Management functions to an eUICC. Platform Management does not affect the contents of a Profile.
Profile	Combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC and which typically allows, when enabled, the access to a specific network A Profile can be an Operational, Provisioning or Test Profile.
Profile Component	A Profile Component is an element of the Profile, when installed in the eUICC, and MAY be one of the following: • An element of the file system like an MF, EF or DF; • An Application, including NAA and Security Domain; • Profile metadata, including Profile Policy Rules; • An MNO-SD.
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.
Profile Management Operation	Local or Remote Profile Management operation: Enable Profile, Disable Profile, Delete Profile
Profile Nickname	Alternative name of the Profile set by the End User.
Profile Policy Authorisation Rule	A set of data that governs the ability of a Profile Owner to make use of a Profile Policy Rule in a Profile.
Profile Policy Rule	Defines a qualification for or enforcement of an action to be performed on a Profile when a certain condition occurs.

Profile State Management Operation	As defined in SGP.32[36].
Profile Type	Operator specific defined type of Profile. This is equivalent to the “Profile Description ID“as described in Annex B of SGP.21 [23]
Provisioning Profile	A Profile that allows connectivity to a commercial mobile network solely to provide system services, such as the provisioning of Profiles.
Reference Enterprise Rule	The Enterprise Rule that is currently being enforced by the eUICC.
Remote Profile Management	Profile Management operations performed by a Managing SM-DP+ at the request of the Profile Owner.
Roles	Roles are representing a logical grouping of functions.
Root SM-DS	A globally identified central access point for finding Events from one or more SM-DP+(s).
Rules Authorisation Table	A set of Profile Policy Authorisation Rules that, together, determines the ability of a Profile Owner to make use of a set of Profile Policy Rules in a Profile.
SCP-SGP22	Protocol for Profile Protection and eUICC Binding defined in [24] and based on SCP11 ([11] Amendment F)
Mobile Service Provider	As defined in SGP.21[23]
SM-DP+ OID	Identifier of the SM-DP+ that is globally unique and is included as part of the SM-DP+ Certificate.
SM-DS OID	Identifier of the SM-DS that is globally unique and is included as part of the SM-DS Certificate.
Subscription	Describes the commercial relationship between the End User and the Mobile Service Provider.
Subscription Manager Data Preparation+ (SM-DP+)	This role prepares Profile Packages, secures them with a Profile protection key, stores Profile protection keys in a secure manner and the Protected Profile Packages in a Profile Package repository, and allocates the Protected Profile Packages to specified EIDs. The SM-DP+ binds Protected Profile Packages to the respective EID and securely downloads these Bound Profile Packages to the LPA of the respective eUICC. The SM-DP+ also performs Remote Profile Management.
Subscription Manager Discovery Server (SM-DS)	This is responsible for providing addresses of one or more SM-DP+(s) to a LDS.
Tamper Resistant Element	A security module consisting of hardware and low-level software providing resistance against software and hardware attacks, capable of securely hosting operating systems together with applications and their confidential and cryptographic data.
Test Profile	As defined in SGP.22 [24].

UI Constrained Device	As defined in SGP.32[36].
User Intent	As defined in SGP.22 [24].

0.3 Abbrevitions

Besides the terms described in the next table, the terminology and abbreviations of Common Criteria apply (see [37], [38], [39] and [40]).

Abbreviation	Description
AID	Application Identifier
ASN.1	Abstract Syntax Notation One
CERT.CI.ECDSA	Certificate of the eSIM CA for its Public ECDSA Key
CERT.DPauth.ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for SM-DP+ authentication
CERT.DPpb.ECDSA	Certificate of the SM-DP+ for its Public ECDSA key used for Profile Package Binding
CERT.DSauth.ECDSA	Certificate of the SM-DS for its Public ECDSA key used for SM-DS authentication
CERT.EUICC.ECDSA	Certificate of the eUICC for its Public ECDSA key
CERT.EUM.ECDSA	Certificate of the EUM for its Public ECDSA key
CERT.DP.TLS	Certificate of the SM-DP+ for securing TLS connections (version >= 1.2)
CERT.DS.TLS	Certificate of the SM-DS for securing TLS connections (version >= 1.2)
CERT.EIM.ECDSA	Certificate of the eIM for signing eUICC Packages.
CERT.EIM.TLS	Certificate of the eIM for securing TLS/DTLS connections (version >= 1.2)
CMAC	Cipher-based MAC
CRL	Certificate Revocation List
DH	Diffie-Hellman
ECASD	eUICC Controlling Authority Security Domain
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve cryptography Digital Signature Algorithm
ECKA	Elliptic Curve cryptography Key Agreement algorithm
eCO	eIM Configuration Operation
EID	eUICC-ID
eIM	eSIM IoT Remote Manager
ETSI	European Telecommunications Standards Institute
EUM	eUICC Manufacturer

GP	GlobalPlatform
GSMA	GSM Association
HLR	Home Location Register
ICCID	Integrated Circuit Card ID
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IPA	IoT Profile Assistant
IPAd	IoT Profile Assistant in the IoT Device
IPAe	IoT Profile Assistant in the eUICC
ISD	Issuer Security Domain
ISD-P	Issuer Security Domain Profile
ISD-R	Issuer Security Domain Root
ISO	International Standards Organisation
ITU	International Telecommunications Union
LDS	Local Discovery Service
LDSd	Local Discovery Service when LPA is in the Consumer Device
LDSe	Local Discovery Service when LPA is in the eUICC
LPA	Local Profile Assistant
LPAd	Local Profile Assistant when LPA is in the Consumer Device
LPAe	Local Profile Assistant when LPA is in the eUICC
LPD	Local Profile Download
LPDd	Local Profile Download when LPA is in the Consumer Device
LPDe	Local Profile Download when LPA is in the eUICC
LTE	Long Term Evolution
LUI	Local User Interface
LUId	Local User Interface when LPA is in the Consumer Device
LUIe	Local User Interface when LPA is in the eUICC
MAC	Message Authentication Code
MEP	Multiple Enabled Profiles
MNO	Mobile Network Operator
NAA	Network Access Application
PSMO	Profile State Management Operation
NCD	Network Constrained Device
OTA	Over The Air
otPK.DP.ECKA	One-time Public Key of the SM-DP+ for ECKA
otPK.DP.KAeac	One-time Public Key of the SM-DP+ for ECKA for Device Change (optional)
otPK.EUICC.ECKA	One-time Public Key of the eUICC for ECKA
otSK.DP.ECKA	One-time Private Key of the SM-DP+ for ECKA
otSK.EUICC.ECKA	One-time Private Key of the eUICC for ECKA

otSK.EUICC.ECKAeac	One-time Private Key of the eUICC for ECKA for Device Change (optional)
PE	Profile Element
PKI	Public Key Infrastructure
PK.CI.ECDSA	Public Key of the eSIM CA, part of the CERT.CI.ECDSA
PK.DPauth.ECDSA	Public Key of the SM-DP+ part of the CERT.DPauth.ECDSA
PK.DPpb.ECDSA	Public Key of the SM-DP+ part of the CERT.DPpb.ECDSA
PK.DSauth.ECDSA	Public Key of the SM-DS part of the CERT.DSauth.ECDSA
PK.EIM.ECDSA	Public Key of the eIM, optionally part of the CERT.EIM.ECDSA
PK.EUICC.ECDSA	Public Key of the eUICC, part of the CERT.EUICC.ECDSA
PK.EUM.ECDSA	Public Key of the EUM, part of the CERT.EUM.ECDSA
POS	Point Of Sale
PPI	Profile Package Interpreter
PPE	Profile Policy Enabler
PRE	Profile Rules Enforcer
PPR	Profile Policy Rule
RAT	Rules Authorisation Table
RPM	Remote Profile Management
RSP	Remote SIM Provisioning
SAS	Security Accreditation Scheme
SCP	Secure Channel Protocol
SD	Security Domain
S-ENC	Session key for message encryption/decryption
S-MAC	Session Key for message MAC generation/verification
SoC	System on Chip
ShS	Shared Secret
SK.CI.ECDSA	Private key of the eSIM CA for signing certificates
SK.DPauth.ECDSA	Private Key of the of SM-DP+ for creating signatures for SM-DP+ authentication
SK.DPpb.ECDSA	Private key of the SM-DP+ used to provide signatures for Profile binding
SK.DSauth.ECDSA	Private Key of the of SM-DS for creating signatures for SM-DS authentication
SK.EUICC.ECDSA	Private key of the eUICC for creating signatures
SK.EUM.ECDSA	Private key of the EUM for creating signatures
SK.DP.TLS	Private key of the SM-DP+ for securing TLS connection connections (version >= 1.2)
SK.DS.TLS	Private key of the SM-DS for securing TLS connection connections (version >= 1.2)
SM-DP+	Subscription Manager Data Preparation (Enhanced compared to the SM-DP in SGP.02 [3])
SM-DS	Subscription Manager Discovery Server

SVN	SGP.22 Specification Version Number (referred to as 'eSVN' in SGP.21 [23]).
TLS	Transport Layer Security (version >= 1.2)
TRE	Tamper Resistant Element
UICD	UI Constrained Device
USIM	Universal Subscriber Identity Module
3S	Secure Sub-System

1 Introduction

This document defines a Protection Profile (PP) for the remote provisioning and management of the eUICC in Consumer and IoT Devices, following the modular approach from [37], and consisting of:

- Base-PP (described in sections 1 to 6),
- LPAe PP-Module (described in section 7),
- LPAe PP-Configuration (defined in section 8),
- IPAe PP-Module (defined in section 9) and
- IPAe PP-Configuration(defined in section 10).

1.1 Protection Profile identification

Title: eUICC for Consumer and IoT Devices Protection Profile

Author: GSMA

Editor: GSMA

Reference: SGP.25.Base

Version: 2.0

CC Version: CC:2022 release 1

Assurance Level: EAL4 augmented with ALC_DVS.2 and AVA_VAN.5

General Status: Complete

Keywords: eUICC, Consumer Devices, IoT Devices, Remote SIM 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 the embedded UICC software that implements the GSMA RSP Architecture Specification [23] and Technical Specification [24] for Consumer Devices or eSIM IoT Architecture and Requirements [35] and eSIM IoT Technical Specification [36] for IoT Devices. The ST writer SHALL indicate which versions of the specifications are implemented by the TOE.

This TOE is loaded on a secure IC. The secure IC itself can be embedded or integrated onto a Device, but it can also be removable (for more details on the scope of the TOE, see Figure 1).

The TOE includes:

- The Application Layer: privileged applications, such as Security Domains, providing the remote provisioning and administration functionality (the notion of Security Domain follows the definition given by [11]):

  - An ISD-R, including LPA/IPA Services, providing life-cycle management of profiles;
  - An ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication;
  - ISD-P security domains, each one hosting a unique profile.
- The Platform Layer: a set of functions providing support to the Application Layer:
  - A Telecom Framework providing network authentication algorithms;
  - A Profile Package Interpreter translating Profile Package data into an installed Profile;
  - And a Profile Rules Enforcer which comprises the Profile Policy Enabler (Profile Policy verification and enforcement functions) and the enforcement of Enterprise Rules.

The secure 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 the PP;
- The secure IC platform and OS;
- The Runtime Environment (for example Java Card System).

Remark: If the TOE provides eUICC OS Update functionality then the use of eUICC OS Update PP-Module is mandatory. The ST author should provide their own rationale for meeting the defined security objectives (See Appendix A).

1.2.1 TOE type and TOE major security features

The TOE type is software.

The eUICC is a component in a Device. 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 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 section 4.2.2) that are met by the Java Card System Protection Profile [1]. The figure hereafter takes such a Java Card System as an example of RE.

The Profiles are not part of the TOE.

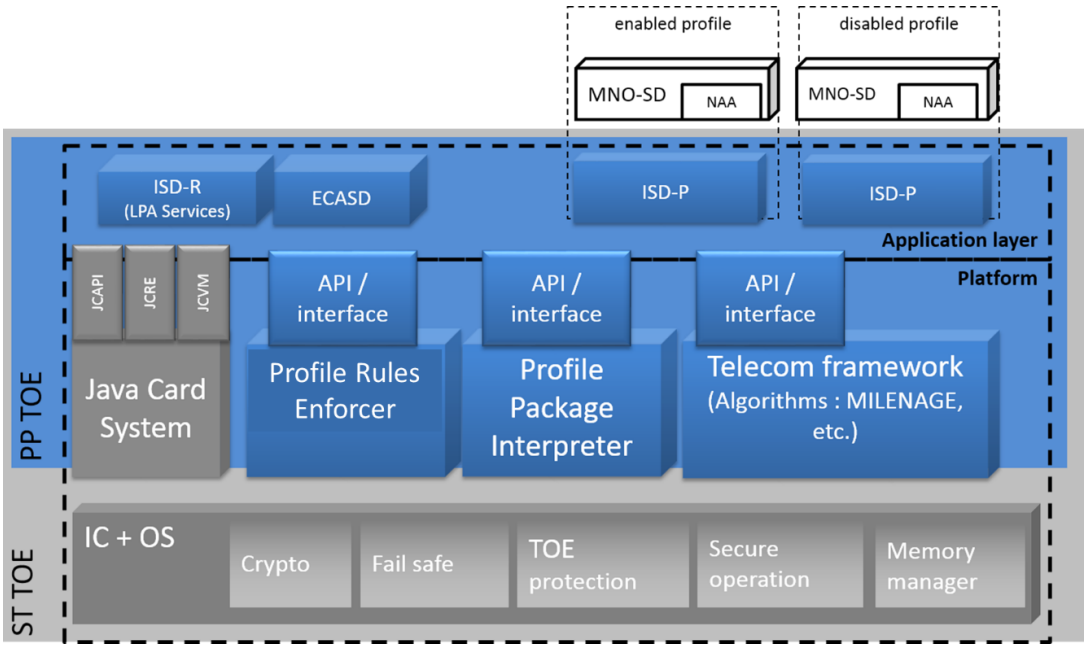


Figure 1 Scope of the TOE based on [PP0084]

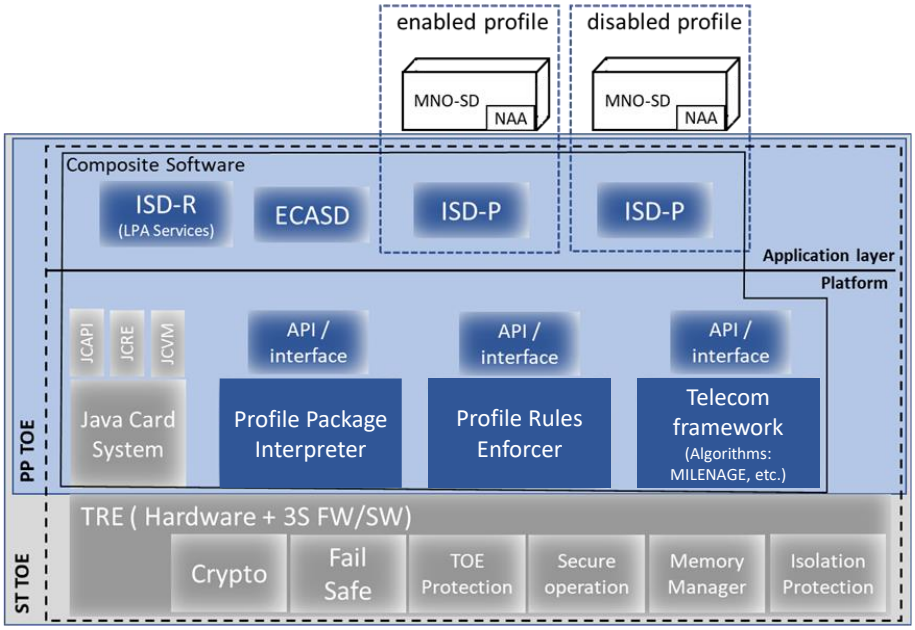


Figure 2 Scope of the TOE based on [PP0117]

1.2.1.1 Application Layer

The goal of the Application layer is to implement the eUICC functionalities described in [23] and [24], which rely on the notion of a Profile. A Profile is the combination of a file structure, data and applications to be provisioned onto, or present on, an eUICC. Each Profile, combined with the functionality of the eUICC, behaves basically as a SIM card. An eUICC may contain more than one Profile, but one and only one is activated at a time. Each Profile is controlled by a unique ISD-P.

A Profile can have several forms:

- A Provisioning Profile: A Profile that allows connectivity to a mobile network solely to

provide the provisioning of Profiles;

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

NOTE: The GSMA Generic Test Profile [32] is an example of a Test Profile that supports a wide range of development, certification, and repair/refurbishment testing activities.

This document will use the term “Profile” to describe either Provisioning Profiles, Operational Profiles, or Test Profiles.

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

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

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

More details on the Profile can be found in [23] and [24].

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

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

ISD-P

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

As defined in [24], the ISD-P shall ensure that:

a) It hosts a unique Profile;

b) Only the following Application Layer components shall have access to the profiles:

   - ISD-P;
   - ISD-R, which shall only have access to the metadata of the profiles;

c) A Profile component shall not have any visibility of, or access to, components outside its ISD-P. An ISD-P shall not have any visibility of, or access to, any other ISD-P;

d) Deletion of a Profile shall remove the containing ISD-P and all Profile components of the Profile.

ISD-R

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

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

As defined in [24]:

a) There shall be only one ISD-R on an eUICC;

b) The ISD-R shall be installed and personalized by the EUM during eUICC manufacturing. The ISD-R shall be associated with itself;

c) The ISD-R cannot be deleted or disabled.

LPA/IPA Services

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

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

LPA Services are mandatory even if the LPAe is provided in the eUICC. LPA/IPA Services code is located in the ISD-R.

MNO-SD

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

ECASD

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

As defined in [23], the ECASD has the following properties:

a) There can only be one ECASD on an eUICC;

b) It is installed and personalised by the EUM during the eUICC manufacturing as described in [11];

c) It has eUICC private key(s) for creating signatures;

d) It has associated certificate(s) for eUICC authentication;

e) It has the eSIM CA public key(s) for verifying SM-DP+ and SM-DS certificates;

f) It has the certificate of the EUM;

g) It MAY have the eIM public key(s) or certificate(s) for verifying eIM messages (SGP.32).

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, that is, the Platform layer is *not* meant to relate to "platform" as a pseudonym for a runtime environment (e.g. Java Card). The Platform capabilities include:

- The Telecom Framework, which includes algorithms used by Network Access Applications (NAA) to access mobile networks. The NAAs are part of the Profiles, but the algorithms, as part of the Telecom Framework, are provisioned onto the eUICC during manufacturing.
- The Profile Package Interpreter, an eUICC Operating System service that translates the Profile Package data as defined in eUICC Profile Package Specification [30] into an installed Profile using the specific internal format of the target eUICC.
- The Profile Rules Enforcer, which implements the enforcement of Enterprise Rules, and the Profile Policy Enabler (PPE). The PPE has two functions:
    - Verification that a Profile containing PPRs is authorised by the RAT;
    - Enforcement of the PPRs of a Profile.

A developer may choose, if at all possible, to implement some of Profile management functions in the SDs, for example the policy enforcement may be realized completely by the ISD-R. The Profile Package Interpreter and Profile Rules Enforcer are only defined here to identify the platform code supporting the SDs *if it exists*.

Application Note 1:

Authentication to a Public Mobile Network (PMN) is done in accordance with the 3GPP standards [22]. According to these standards (especially TS 33.102) the 3G and 4G authentication mechanisms allow the response values RES to have a length that is any multiple of 8 bits between 32 and 128 bits inclusive. In practice, either 32-bit or 64-bit RES is used. This protection profile covers products only when used to create 64-bit RES. Operators choosing to use 32-bit RES will therefore be using the product outside the scope of this protection profile.

The protection profile includes origin authentication of the PMN that owns the customer subscription to the Profile. It includes also entity authentication of the Profile to the PMN in which a customer subscriber is roaming on. It does not include entity authentication of this visited PMN to the Profile, except in 4G authentication.

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 MNO's property, and stores MNO specific information.

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

1.2.3 TOE life-cycle

1.2.3.1 Life-cycle compared to a secure IC Platform life-cycle

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

The figures hereafter show the description of the TOE life-cycle, compared to the [2] life-cycle. The delivery of the TOE may be performed at different stages.

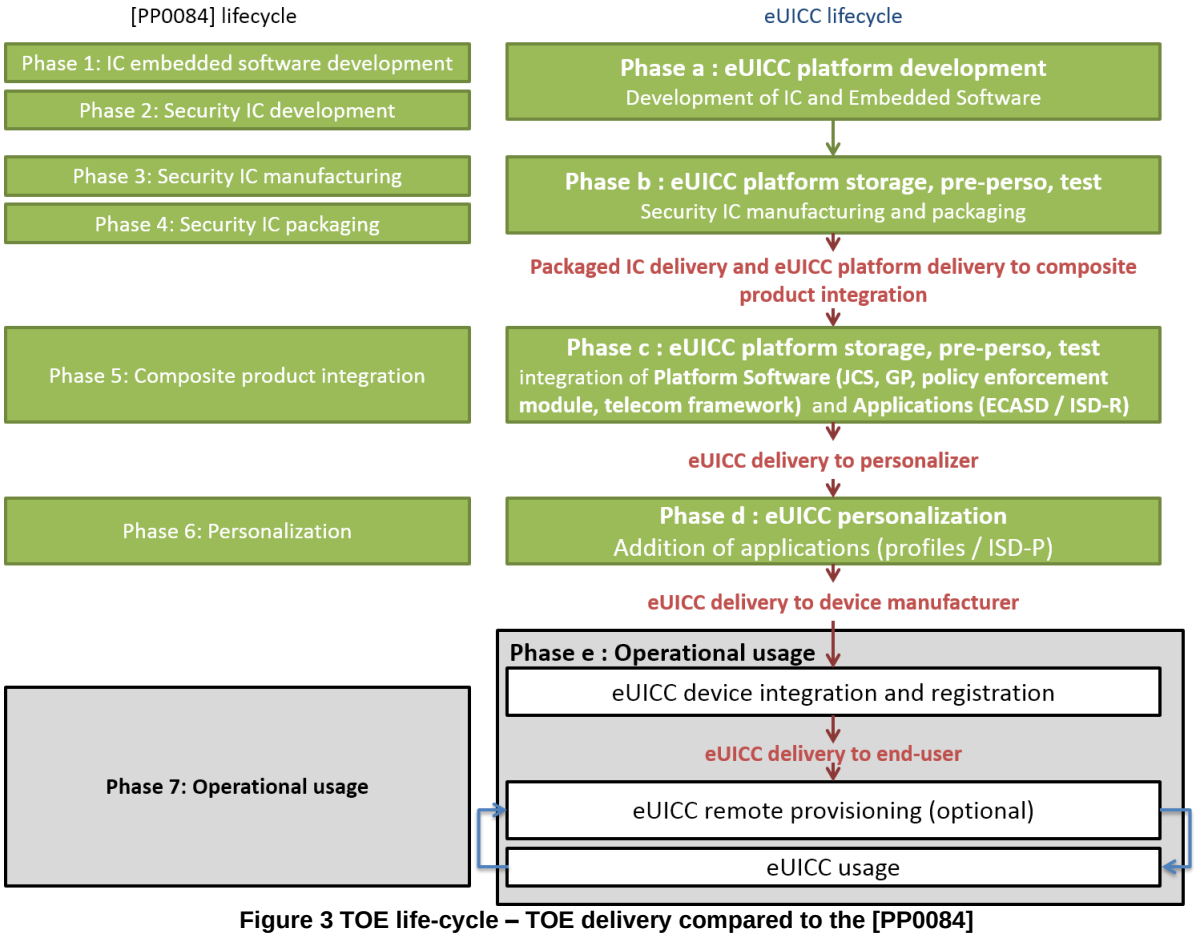


Figure 3 TOE life-cycle – TOE delivery compared to the [PP0084]

The reader may refer to [2] for a thorough description of Phases 1 to 7:

- Phases 1 and 2 compose the product development: Embedded Software (IC Dedicated Software, OS, RE, applications, other Platform components such as PPI, PRE, 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:

- **Phase a :** Development corresponds to the first two stages of the IC development;
- **Phase b :** Storage, pre-personalisation and test cover the stages related to manufacturing and packaging of the IC;
- *TOE Delivery [optional]: At this phase the delivery of the TOE to the customer of the eUICC manufacturer could happen, if the TOE is already self-protected;*

- **Phase c :** eUICC platform storage, pre-personalization, test covers the stage of the embedding of software products onto the eUICC;
- *TOE Delivery [optional]: At this phase the delivery of the TOE to the customer of the eUICC manufacturer could happen, if the TOE is already self-protected;*
- **Phase d :** eUICC personalization covers the insertion of provisioning Profiles and Operational Profiles onto the eUICC;
- *TOE Delivery [optional]: At this phase the delivery of the TOE to the customer of the eUICC manufacturer happens at the latest;*
- **Phase e :** operational usage of the TOE covers the following steps:
  - 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-DS;
  - 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.

Application Note 2:

The ST writer must describe which delivery activities are required in their own life-cycle model and at which phase the delivery of the self-protected TOE happens.

1.2.3.2 Lifecycle compared to a 3S Platform lifecycle

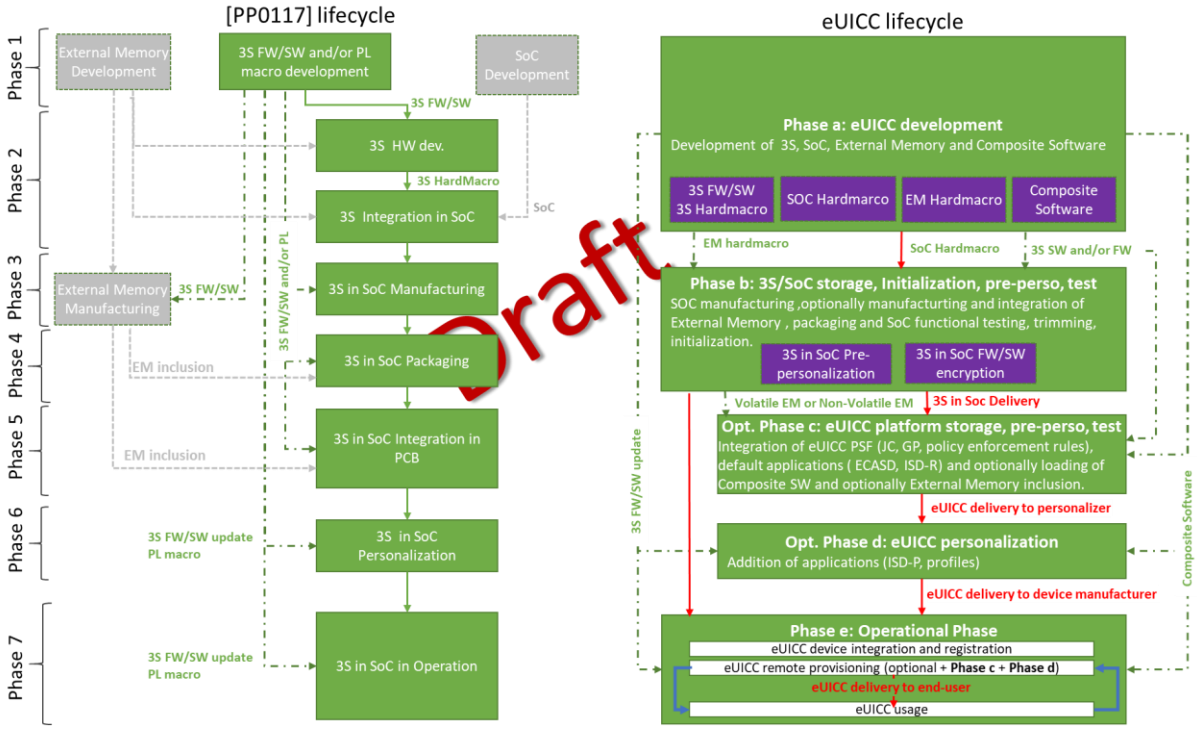


Figure 4 TOE lifecycle – TOE delivery compared to the [PP0117]

Application Note 3:
For simplicity reasons, the right side of the Figure 4 does not include the eUICC implementation based on PL macro.

1.2.3.3 Actors of the TOE

The eUICC delivered to the end-user can be either embedded onto the Device or

removable. In addition, the end-user can 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);
- And, the End User, through the Local User Interface, but possibly also via the direct interface to the eUICC in the case when this later is removable.
- 3S FW / SW developer, 3S integrator or SoC manufacturer on its behalf, will have interfaces for updating the 3S FW / SW and Composite Software.

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

1.2.4.1 TOE interfaces

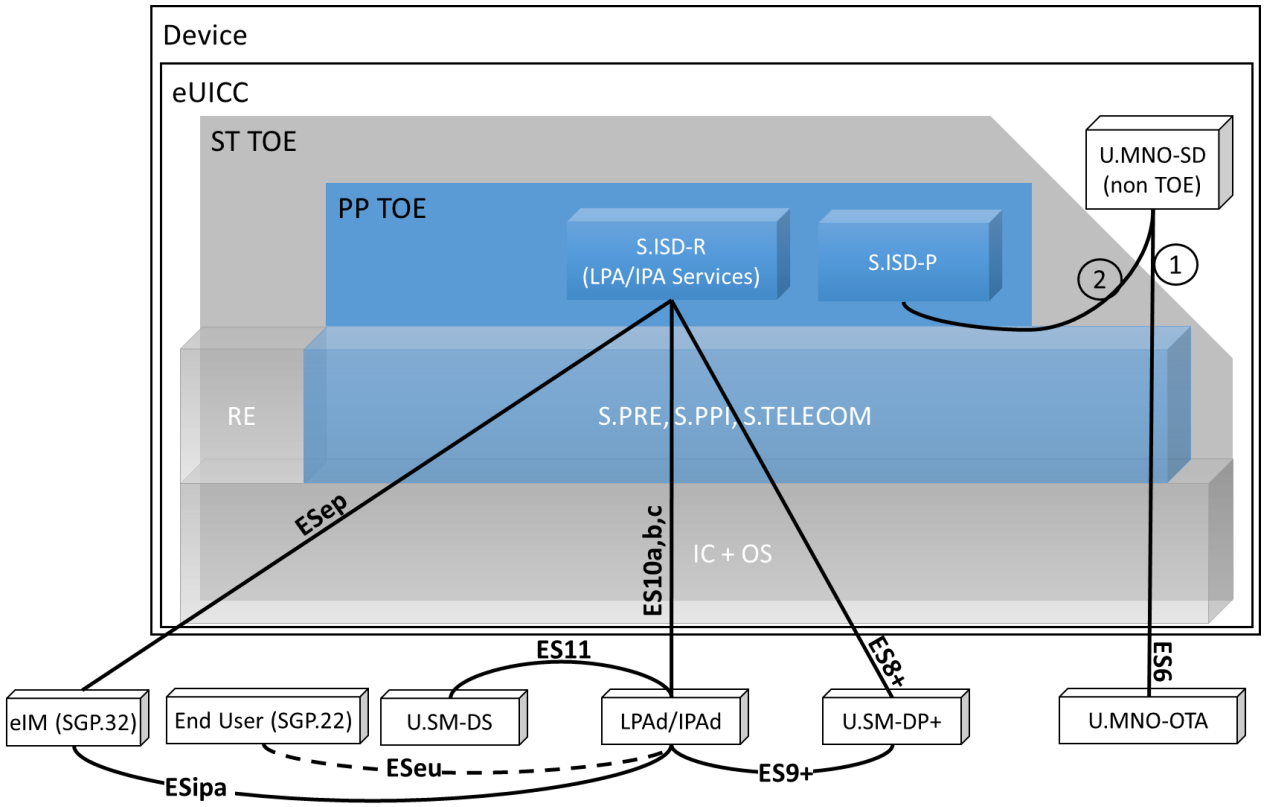


Figure 5 TOE interfaces based on [PP0084]

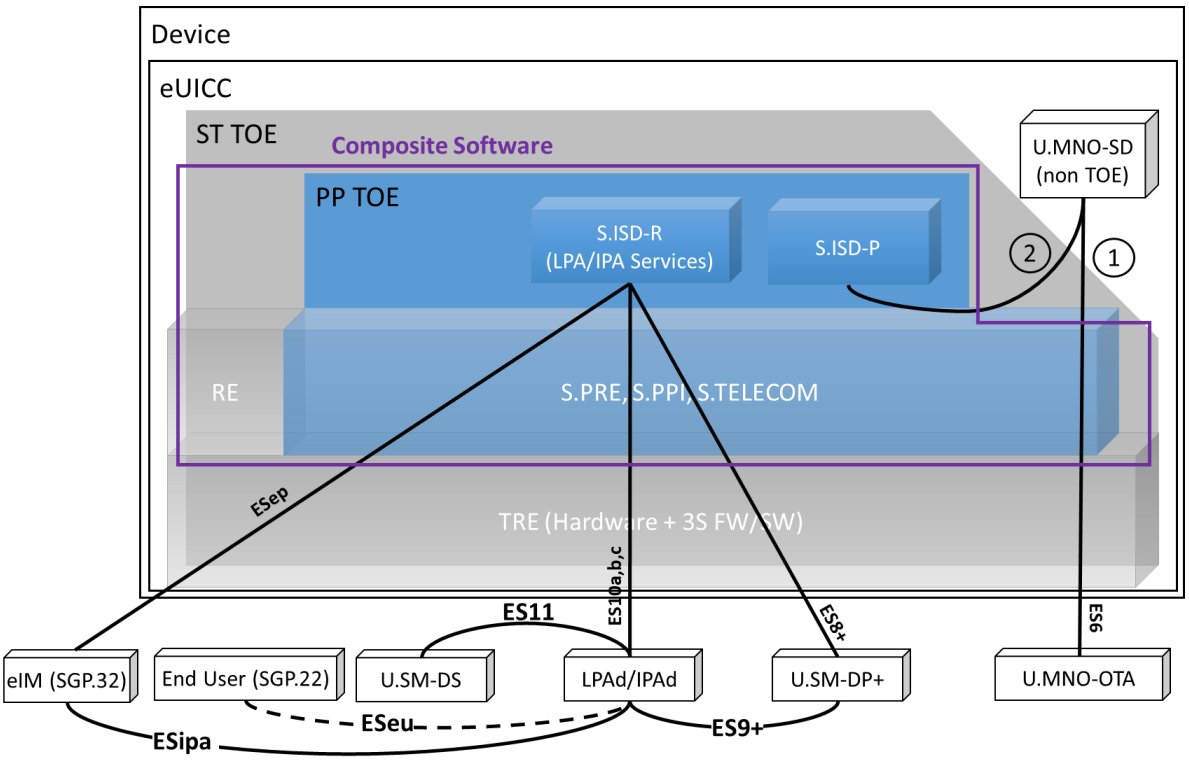


Figure 6 TOE interfaces based on [PP0117]

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.

Application Note 4:

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

As shown on Figure 5 and Figure 6, the ST TOE has the following interfaces:

- With the provisioning infrastructure, consisting in SM-DS, SM-DP+, MNO OTA Platform, and LPAd interfaces (identified ES6, ES8+, ES10a-c in [24]), ESep and ESipa [36] as well as the End User interface (ESeu (SGP.22));
- With the MNO-SD:
  - The interface 1 is used to enforce the trusted channel between the MNO-SD and the MNO OTA Platform;
  - The interface 2 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, a part of the enforcement of these trusted channels is ensured by the operational environment of the TOE.

All communications are supported by the Platform functions, which provide a secure APDU dispatching and support for 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 secure IC and its embedded software.

1.2.4.2 Description of Non-TOE HW/FW/SW and systems

Integrated Circuit (IC) or Chip

The TOE is based on a secure 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 secure 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.

The IC security features are required to be certified according to [2] or [34].

LPAd/IPAd

The TOE for Consumer eUICC relies on a Local Profile Assistant (LPA) or IoT Profile Assistant (IPA) component [24] and [36]. It can either be implemented at the application level as LPAe/IPAe (the case covered by the LPAe/IPAe PP-Module), or it can be implemented as a non-TOE on-device unit called LPAd/IPAd.

Although LPAd/IPAd is a non-TOE component it uses the LPA/IPAd Services already mentioned in section 1.2.1.1.

Embedded software (ES)

The TOE relies on an Embedded Software (ES) loaded into the secure 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 secure 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 modification 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 [11], 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].

Application Note 5 :

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

Device

The eUICC is intended to be used in a Consumer or IoT Device.

The Consumer Device is expected to include a user interface, at least related to the eUICC functionality. In this case, the eUICC includes the Local User Interface (LUI) part of the LPA.

The IoT Device can be either a Network Constrained Device or a User Interface Constrained Device.

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

MNO-SD and applications

The Profile controlled by each ISD-P consists in a MNO-SD security domain, 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].

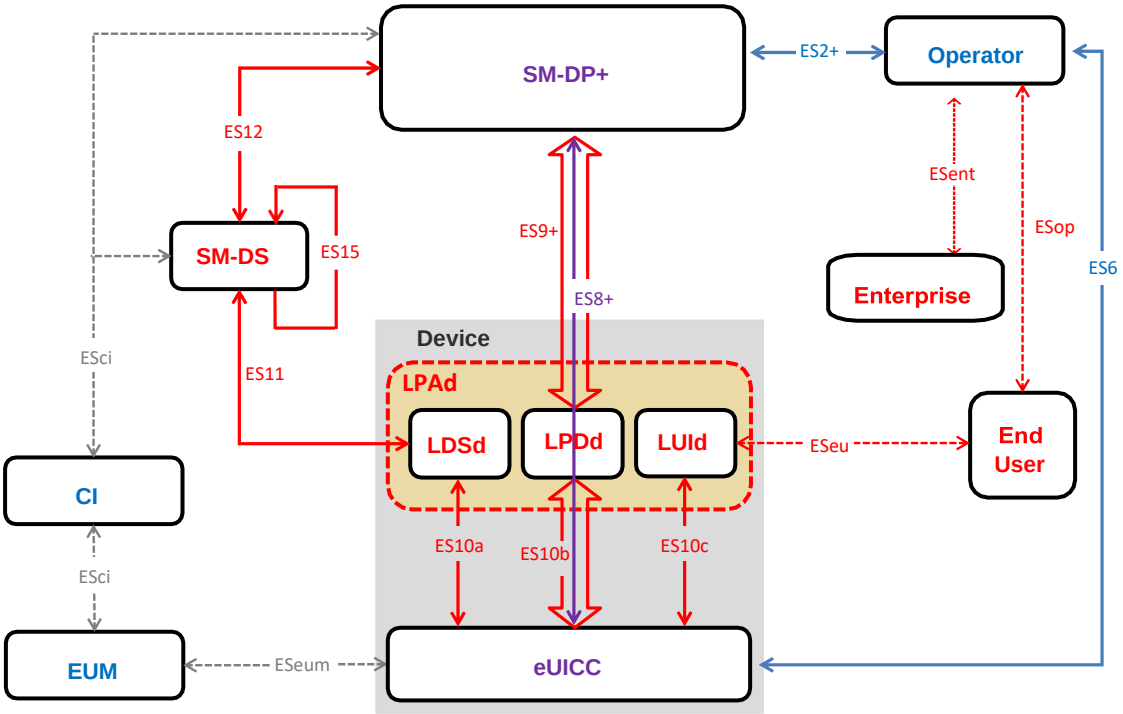
Secure Applications

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 for Consumer Devices

The eUICC interfaces with the following remote provisioning entities that are responsible for the management of Profiles on the eUICC. Figure 7 describes the communication channels of the architecture when the LPA is located in the Consumer Device (LPAd).



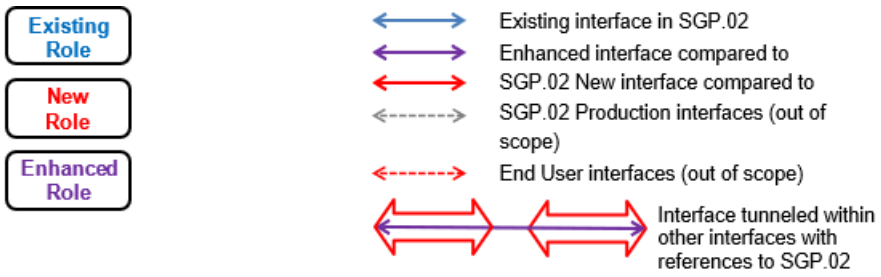


Figure 7 Remote SIM Provisioning System, LPA in the Device

The TOE communicates with remote servers of:

- SM-DP+, which provides Platform and Profile management commands as well as Profiles.

The TOE shall require the use of secure channels for these interfaces. The keys and certificates required for these operations on the TOE are exchanged/generated during operational use of the TOE. Identities (in terms of certificates) rely on a single root of trust called the eSIM CA, whose public key is stored pre-issuance on the eUICC.

The remote servers and, if any, the security component (such as an HSM) from which the keys are obtained are referred as Trusted IT products.

Remote provisioning infrastructure for IoT Devices

The eUICC interfaces with the following remote provisioning entities that are responsible for the management of Profiles on the eUICC. Figure 8 describes the communication channels of the architecture when the IPA is located in the IoT Device (IPAd).

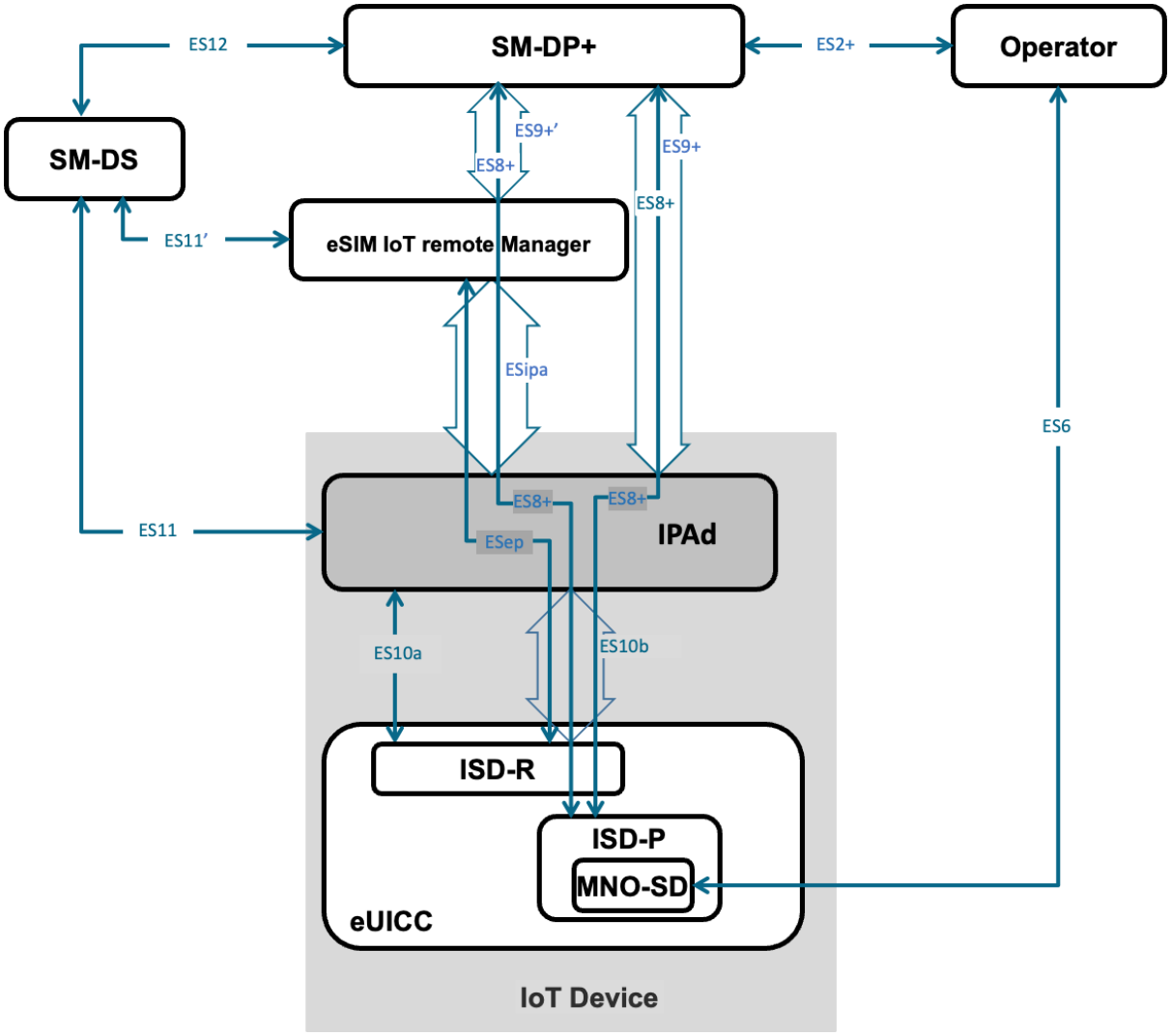


Figure 8 Remote SIM Provisioning System, IPA in the IoT Device

The TOE communicates with remote servers of:

- SM-DP+, which provides Platform and Profile State Management commands as well as Profiles.
- eIM which provides Profile State Management Operations and eIM Configuration Operations.

The TOE shall require the use of secure channels for these interfaces. The keys and certificates required for these operations on the TOE are exchanged/generated during operational use of the TOE. Identities (in terms of certificates) rely on a single root of trust called the CA, whose public key is stored pre-issuance on the eUICC.

The remote servers and, if any, the security components (such as an HSM) from which the keys are obtained are referred as Trusted IT products.

1.2.5 Protection Profile Usage

The TOE of a Security Target conformant with this PP is the whole 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 [14], with the IC, OS and JCS already certified, and the eUICC certified on top of them.

  The Security Target shall refer to the IC, OS and JCS Security Target(s) to fulfil 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 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 fulfil 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 fulfil [4].

In particular, in a composite evaluation [14], 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 [14] 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 described in this Protection Profile. This high-level view of the Protection Profile describes:

- The threat agents;
- The main threat categories;
- The organizational security policies and assumptions.

1.3.1 Threat agents

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

- An off-card Actor;

- An on-card application.

All two 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 (TLS interfaces (version 1.2 or later), OTA interfaces, mobile network);
- The interface with the communication module of the Device, which shall conform to the terminal requirements within [6];
- The interfaces with the LPAd.

The unintended interfaces of the eUICC are mainly the IC surface as defined in [7] (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 Java Card API, SIM API ([15]), UICC API ([16]), USIM API ([17]), ISIM API ([18]));
- Policy enforcement interfaces (PRE, PPI);
- 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.

The Platform code itself is not considered a threat agent, since

- Either the runtime environment will be previously certified according to [1];
- Or the runtime environment will be part of the TOE.

In both cases, the IC and its embedded software will be previously certified according to PP0084 [2] or PP0117 [34].

1.3.2 High-level view of threats

The threats considered in this Protection Profile correspond to the high-level scenarios described hereafter.

“First-level” threats

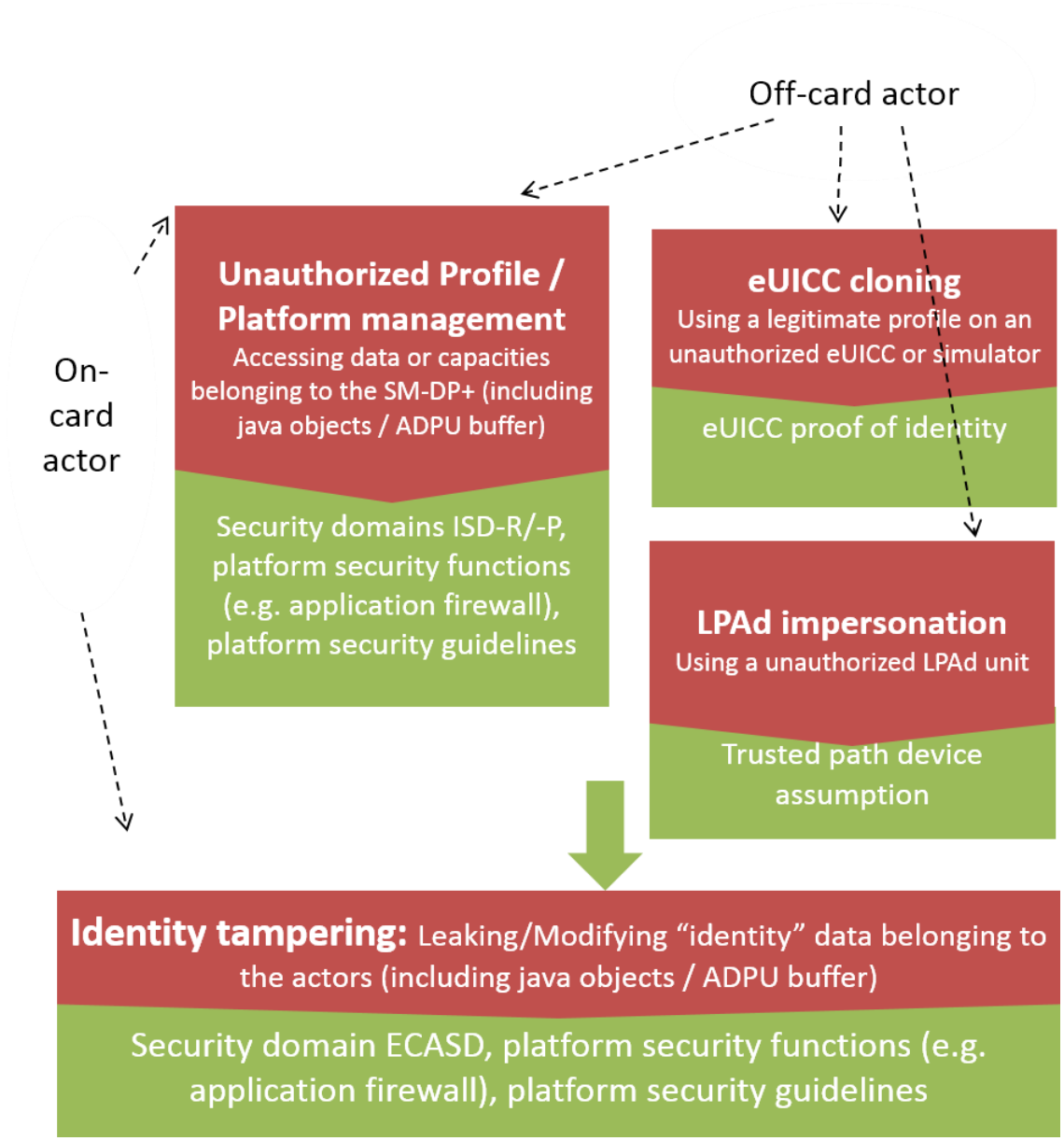


Figure 9 “First-level” threats (1)

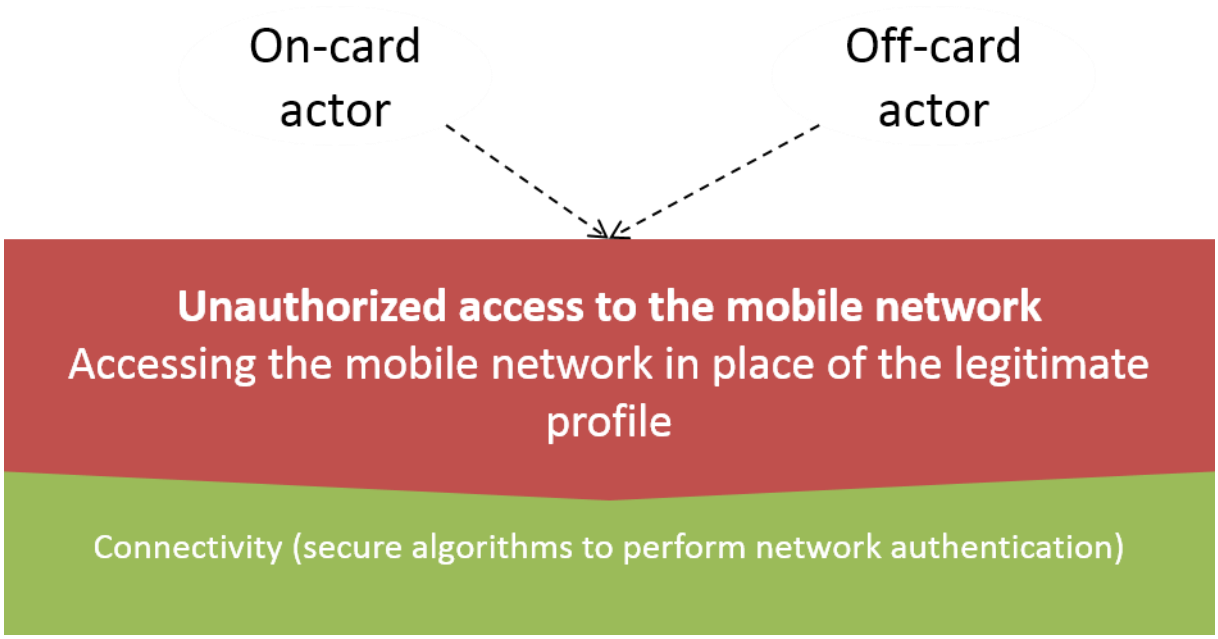


Figure 10 "First-level" threats (2)

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 platform 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.

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 eSIM CA public key.

The security objectives covering this threat consist in defining a dedicated Security Domain (ECASD). Identity data such as the eSIM CA 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 LPA.

The ECASD is supported by the platform functions. Its isolation is also supported by the Application Firewall provided by the Runtime Environment of the TOE.

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.

Application Note 6:

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.

LPAd impersonation

Within the eUICC, the interfaces to connect to an LPAd are always present, even if the off-eUICC LPAd itself is not present. The attacker can exploit those interfaces to impersonate the LPAd (Man-in-the-middle, masquerade).

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.

"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.

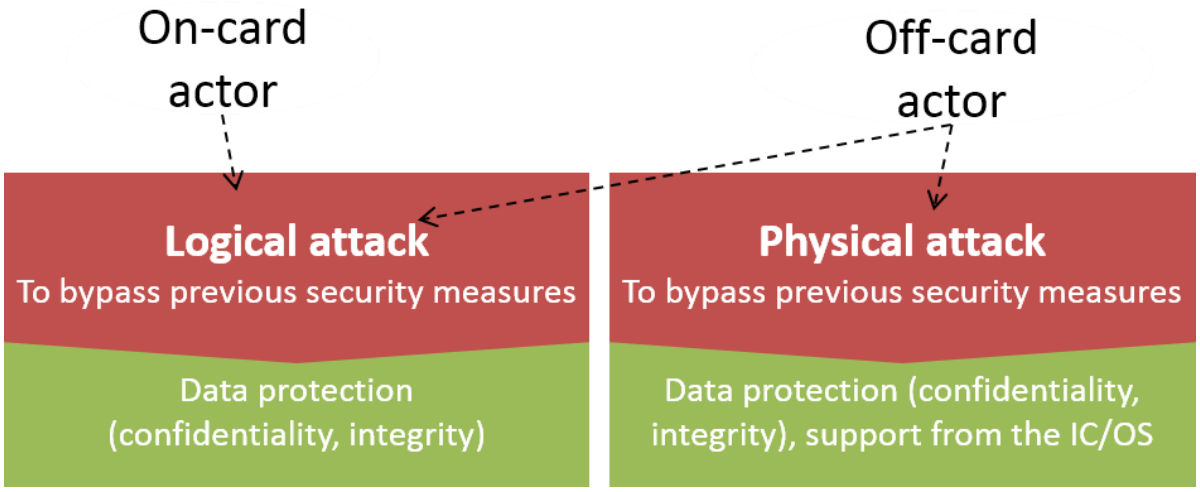


Figure 11 "Second Level Threats"

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;
- Within the eUICC, the interfaces to connect to an LPAd are always present, even if the off-eUICC LPAd itself is not present. The attacker can exploit a *logical* flaw in the interfaces to modify or disclose sensitive assets, or execute code.

Physical attacks

An off-card Actor may try to bypass the platform TOE 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 behaviour of the TOE. This protection Profile includes security objectives for the underlying IC, which ensures protection against physical attacks.

Within the eUICC, the interfaces to connect to an LPAd are always present, even if the off-eUICC LPAd itself is not present. The attacker can exploit a *physical* flaw in the interfaces to modify or disclose sensitive assets, or execute code.

2 Conformance Claims

2.1 CC Conformance Claims

This protection Profile is conformant to Common Criteria 2022 release 1.

This protection Profile is conformant to:

- CC Part 1 [37],
- CC Part 2 [38] (conformant),
- CC Part 3 [39] (conformant),
- CC Part 5 [40].

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,

The following assurance requirement augmentation is optional but suggested:

- ALC_FLR.2 Flaw Reporting Procedures.

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

This PP does not claim conformance to any other PP.

2.2 Conformance Claims to this PP

This Protection Profile requires demonstrable conformance (as defined in [37]) of any ST or PP claiming conformance to this PP.

2.3 PP Conformance Claims

This Protection Profile:

- Requires composite evaluation atop an IC previously certified according to PP0084 [2] or PP0117 [24];
- Does not require a certified platform. The ST writer might use a previously certified JCS (according to the Protection Profile [1]) using composition, but they also may chose instead to:
    - add the runtime environment (that may use another technology than Java Card) in the TOE,
    - transform the objectives OE.RE.* into objectives for the TOE,
    - add SFRs and demonstrate that the objectives are covered.

Application Note 7:

The evaluation of cryptographic functions might be required at several steps of the evaluation:

- during the certification of the IC, for cryptographic operations provided by the IC such as the RNG;
- during the certification of the JCS platform, if composition is used over a certified JCS;
- during the full product evaluation, for example,
    - when the TOE uses a non-evaluated RE that includes cryptographic functions,

- when the TOE is evaluated by composition over a RE that does not define telecom authentication algorithms (forcing the TOE to implement these algorithms on top of the RE).

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-P:
  - At least one Network Authentication Application (part of D.PROFILE_CODE) and its associated parameters (D.PROFILE_NAA_PARAMS);
  - The PPR policy file and Enterprise Rules (optional) (D.PROFILE _RULES);
  - The file system (included in D.PROFILE_CODE);
  - The 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);
  - The user codes that may be associated to the profile download (D.PROFILE_USER_CODES).

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.

3.1.1.2 Profile data

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, including confidential sensitive data.

D.PROFILE_NAA_PARAMS

Parameters used for network authentication, including keys. Such parameters may include for example elliptic curve parameters. Parameters are loaded during provisioning and storedunder the control of the ISD-P. They may be transmitted to the Telecom Framework,

which contains the authentication algorithms.

To be protected from unauthorized disclosure and unauthorized modification.

D.PROFILE_IDENTITY

The International Mobile Subscriber Identity is the user credential when authenticating on a MNO's network via an Authentication algorithm. The IMSI is a representation of the subscriber's identity and will be used by the MNO as an index for the subscriber in 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_POLICY_RULES

Data describing the profile policy rules (PPRs) of a profile , and the Enterprise Rules (optional).

These rules are loaded during provisioning and stored under the control of the ISD-P. They are managed by the MNO OTA Platform.

PPRs and Enterprise Rules shall be protected from unauthorized modification.

D.PROFILE_USER_CODES (SGP.22)

This asset consists of:

- the optional Activation Code that End User may use to initiate a Profile Download and Installation via the Local User Interface (LUId);
- the hash of the optional Confirmation Code (Hashed Confirmation Code) that End User may use to confirm a Profile Download and Installation via the Local User Interface (LUId).

Note that although these codes are input by End User at the LUId, which is outside of the TOE, the codes are sent to the TOE for signature (ex. euiccSigned2 data structure).

To be protected from unauthorized modification.

3.1.1.3 Profile code

D.PROFILE_CODE

The profile applications include first and second level applications ([6]), 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, life-cycle, 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 8:

- 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.PLATFORM_DATA

The data of the platform environment, like for instance,

- the identifiers and privileges including SM-DS OID, MNO OID, SM-DP+ OID, and eIM Identifier (SGP.32);
- the eUICC life-cycle state of the ISD-P security domain (see Annex A of [24]).

This data may be partially implemented in the logic of ISD-R and the Platform code, instead of being “data” properly speaking. As a consequence, this asset is strongly linked with D.TSF_CODE.

To be protected from unauthorized modification.

D.DEVICE_INFO

This asset includes the security-sensitive elements of Device Information data, such as the device type allocation code (TAC) or the device capabilities (ex. Support for updating of certificate revocation lists (CRLs)), that is provided to the eUICC by the LPAd/IPAd.

To be protected from unauthorized modification.

D.PLATFORM_RAT

Data describing the Rules Authorisation Table (RAT) of the eUICC.

These rules are initialised at eUICC manufacturing time or during the initial device setup provided that there is no installed operational profile. The OEM or EUM is responsible for setting the content of the RAT. RAT is stored in the eUICC.

To be protected from unauthorized modification.

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;

- 'eSIM CA certificate';
- EUM's certificates;
- eIM's certificates and/or associated public keys which are used to verify the eUICC Packages sent by the eIM.
- Shared secrets used to generate credentials.

D.SK.EUICC.ECDSA

The eUICC private key(s), stored in ECASD, used by the eUICC to prove its identity, generate shared secrets with remote actors, and generate signatures.

It must be protected from unauthorized disclosure and modification.

D.CERT.EUICC.ECDSA

Certificate(s) issued by the EUM for a specific, individual, eUICC. Certificates contain public keys PK.EUICC.ECDSA and are stored in ECASD. This certificate(s) can be verified using the EUM Certificate.

The eUICC certificate(s) has to be protected from unauthorized modification.

D.PK.CI.ECDSA

The 'eSIM CA public key (PK.CI.ECDSA) used to verify the certification chain of eUICC and remote actors. It is stored in ECASD.

It must be protected from unauthorized modification.

ECASD MAY contain several public keys belonging to the same eSIM CA or different eSIM CA.

Each PK.CI.ECDSA SHALL be stored with information coming from the CERT.CI.ECDSA the key is included in, at least:

- Certificate serial number: required to manage eSIM CA revocation by CRL;
- eSIM CA Identifier: eSIM CA OID;
- Subject Key Identifier: required to verify the Certification chain of the off-card entity.

D.PK.EIM.ECDSA (SGP.32)

The eIM public key (PK.EIM.ECDSA) used to verify the eUICC Package signature. It is stored in ECASD.

It must be protected from unauthorized modification.

ECASD MAY contain several public keys belonging to different eIMs.

Optionally, each PK.EIM.ECDSA MAY be stored with information coming from the CERT.EIM.ECDSA the key is included in, at least:

- Certificate serial number;
- eIM Identifier: eimID;
- Subject Key Identifier: required to verify the Certification chain of the off-card entity.

D.EID

The EID (eUICC-ID) uniquely identifies the eUICC. This identifier is set by the eUICC manufacturer and does not change during operational life of the eUICC. It is stored in ECASD. The EID is used as a key by SM-DP+ and SM-DS to identify eUICCs in their

databases.
The EID shall be protected from unauthorized modification.

D.SECRETS

This asset includes:

- the one-time keys of the eUICC and the SM-DP+: otSK.EUICC.ECKA, otPK.EUICC.ECKA, otSK.EUICC.ECKAeac (optional), otPK.EUICC.ECKAeac (optional) and otPK.DP.ECKA;
- the shared secret (ShS) used to protect the Profile download; and
- session keys (S-ENC and S-MAC) and the initial MAC chaining value.

These asset shall be protected from unauthorized disclosure and modification.

D.CERT.EUM.ECDSA

The Certificate(s) of the EUM
(CERT.EUM.ECDSA). To be protected from
unauthorised modification.

D.CRLs

The optional certificate revocation lists (extract) stored in the eUICC.
To be protected against unauthorised modification.

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.SM-Dpplus

Role that prepares the Profiles and manages the secure download and installation of these Profiles onto the eUICC.

U.SM-DS

Role that securely performs functions of discovery.

U.MNO-OTA

An MNO platform for remote management of UICCs and the content of Enabled MNO Profiles on eUICCs.

U.MNO-SD

A MNO-SD is a Security Domain part of the Profile, owned by the MNO, providing the Secured Channel to the MNO's OTA Platform (U.MNO-OTA). It is used to manage the content of a Profile once the Profile is enabled.

An eUICC can contain more than one MNO-SD.

U.3S-DEV

A role that develops the 3S SW / FW and their updates.

U.eIM (SGP.32)

Role that securely performs functions of Profile State Management Operations, eIM Configuration Operations and Profile Donwnload.

3.2.2 Subjects

S.ISD-R

The ISD-R is responsible for the creation of new ISD-Ps and life-cycle management of all ISD-Ps.

The ISD-R includes LPA/IPA Services that provides the necessary access to the services and data required by LPA/IPA functions. LPA/IPA Services are mandatory, regardless of the fact whether it is LPAe/IPAe or LPAd/IPAd which is active.

S.ISD-P

The ISD-P is the on-card representative of the SM-DP+ and is a secure container (Security Domain) for the hosting of a Profile.

S.ECASD

The Embedded UICC Controlling Authority Security Domain (ECASD) is responsible for secure storage of credentials required to support the required security domains on the eUICC.

S.PPI

Profile Package Interpreter, an eUICC Operating System service that translates the Profile Package data as defined in eUICC Profile Package Specification [30] into an installed Profile using the specific internal format of the target eUICC.

S.PPE

Profile Rules Enforcer (PRE), which enforces the reference Enterprise Rules and contains the Profile Policy Enabler (PPE). The PPE has two functions:

- Verification that a Profile containing PPRs is authorised by the RAT;
- Enforcement of the PPRs of a Profile.

S.TELECOM

The Telecom Framework is an Operating System service that provides standardised network authentication algorithms to the NAAs hosted in the ISD-Ps.

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 or trying to add unauthorized eIM to the eUICC (SGP.32)).

T.UNAUTHORIZED-PROFILE-MNG

A malicious on-card application:

- o modifies or discloses profile data belonging to ISD-P or MNO-SD;
- o executes or modifies operations from profile applications (ISD-P, MNO-SD and applications controlled by MNO-SD);
- o modifies or discloses the ISD-P or MNO-SD application.

Such 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.

The PP does not address the following cases:

- o An application within a ISD-P tries to compromise its own MNO-SD;
- o 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:

- o An application within a ISD-P tries to compromise another MNO-SD or ISD-P;
- o An application within a ISD-P tries to compromise an application under the control of another MNO-SD or ISD-P;
- o 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.

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

T.UNAUTHORIZED-PLATFORM-MNG

A malicious on-card application:

- o modifies or discloses data of the ISD-R or PRE;
- o executes or modifies operations from ISD-R or PRE;
- o modifies the rules authorisation table (RAT) stored in the

PRE. 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

Directly threatened assets are D.TSF_CODE, D.PLATFORM_DATA and D.PLATFORM_RAT.

By altering the behaviour of ISD-R or PRE, the attacker indirectly threatens the provisioning status of the eUICC, thus also threatens the same assets as T.UNAUTHORIZED-PROFILE-

MNG.

T.PROFILE-MNG-INTERCEPTION

An actor alters or eavesdrops the transmission between eUICC and SM-DP+ (ES8+), or eUICC and MNO OTA Platform (ES6), Device and eUICC in case of RPM (UpdateMetadataRequest)), or eIM and eUICC in case of eUICC Package (PSMO or eCO) 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 Profile Metadata (ex. The Profile Policy Rules (PPR), Enterprise Rules, …) data when updated by the MNO OTA platform or by RPM request;
- Replace or modify the content of eUICC Package (SGP.32).

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.MNO_KEYS, D.TSF_CODE (ISD-P and ISD-R), D.PROFILE_*.

T.PROFILE-MNG-ELIGIBILITY

An actor alters or eavesdrops the transmission between eUICC and SM-DP+ (ES8+), or alters the Device Information when provided from the LPAd/IPAd to the eUICC, in order to compromise the eligibility of the eUICC, for example:

- downgrade the security of the profile sent to the eUICC by claiming compliance to a previous version of the specification, or lack of cryptographic support;
- obtain an unauthorized profile by modifying the Device Info or eUICC identifier.

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.TSF_CODE, D.DEVICE_INFO, D.EID.

3.3.2 Identity tampering

T.UNAUTHORIZED-IDENTITY-MNG

A malicious on-card application:

- discloses or modifies data belonging to the “Identity management data” or the “TSF Code” asset category:
  - discloses or modifies D.SK.EUICC.ECDSA, D.SECRETS,
  - modifies D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, D.PK.EIM.ECDSA (SGP.32),
  - modifies the generation method (part of D.TSF_CODE) for shared secrets, one-time keys or session keys (i.e. methods used to generate D.SECRETS);
- discloses or modifies functionalities of the ECASD (part of D.TSF_CODE).

Such a threat typically includes for example:

- direct access to fields or methods of the Java objects

- exploitation of the APDU buffer and global byte array
- impersonation of an application, of the Runtime Environment, or modification of privileges of an application

Directly threatens the assets: D.TSF_CODE, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs, D.PK.EIM.ECDSA (SGP.32).

S.IDENTITY-INTERCEPTION

An attacker may try to intercept credentials, either on-card or off-card, in order to

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

This includes on-card interception of:

- the shared secrets used in profile download (D.SECRETS)
- the eUICC-ID (D.EID)

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)

Directly threatens the assets: D.SECRETS, D.EID.

3.3.3 eUICC 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.SK.EUICC.ECDSA,D.EID, D.SECRETS.

3.3.4 LPAd/IPAd impersonation

T.LPAd-INTERFACE-EXPLOIT

The attacker exploits the interfaces to LPAd/IPAd (interfaces ES10a, ES10b and ES10c (SGP.22)) to: o either impersonate the LPAd/IPAd (Man-in-the-middle, masquerade), or

o exploit a flaw in the interface to modify or disclose sensitive assets, or execute code (extension of T.LOGICAL-ATTACK and T.PHYSICAL-ATTACK targeting specifically the interfaces to LPAd/IPAd).

The attacker could thus perform unauthorised profile and platform management, for instance by circumventing the End User confirmation (SGP.22) needed for such actions, execute eUICCMemoryReset (SGP.32), or Add Initial eIM (SGP.32).

The attacker could also compromise the eligibility check process by compromising the Device Information that is normally passed on from the LPA/IPAd to the eUICC before profile download and installation.

The difference to the threats T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, and T.PROFILE-MNG-ELIGIBILITY, is on the interfaces used to perform the attack (ES10a,b,c).

Directly threatened asset: D.DEVICE_INFO, D.PLATFORM_DATA.

3.3.5 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.

3.3.6 Second level threats

T.LOGICAL-ATTACK

An on-card malicious application bypasses the Platform security 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 Profile Rules Enforcer
- the Profile Package Interpreter
- 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 _RULES, D.PLATFORM_DATA, D.PLATFORM_RAT.

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.

3.4 Organisational Security Policies

3.4.1 Life-cycle

OSP.LIFE-CYCLE

The TOE must enforce the eUICC life-cycle defined in [24]. In particular:

- There is a limit on the number of ISD-Ps enabled at a time:
  - if the eUICC supports MEP, the limit is greater than one
  - otherwise, the limit is one

- The eUICC must enforce the profile policy rules (PPR) in case a profile state change is attempted (installation, disabling or deletion of a profile), except during the memory reset or test memory reset functions: in this case, the eUICC may disable and delete the currently enabled profile, even if a PPR states that the profile cannot be disabled or deleted;

- The eUICC must enforce the rules authorisation table (RAT) before a profile containing PPRs is authorised to be installed on the eUICC.

3.5 Assumptions

3.5.1 Device assumptions

A.TRUSTED-PATHS-LPAd-IPAd

It is assumed that the interfaces ES10a, ES10b and ES10c (SGP.22) are trusted paths between the eUICC and LPAd/IPAd, when LPAd/IPAd is present and active. It is also assumed that the LPAd/IPAd is a trusted component.

It is assumed that LPAd has a means to authenticate the End User (SGP.22).

It is assumed that IPAd is protected against misuse (SGP.32).

It is assumed that the Device manufacturer is securing the following operations (SGP.32):

- Add of an initial eIM Configuration Data by the IPA.
- Complete removal of eIM Configuration Data by the IPA.

3.5.2 Miscellaneous

A.ACTORS

Actors of the infrastructure (eSIM CA, EUM, SM-DP+, SM-DS, eIM (SGP.32), and MNO) securely manage their own credentials and otherwise sensitive data. In particular for the overall mobile authentication mechanism defined in 3GPP TS 33.102 [22] to be secure, certain properties need to hold that are outside the scope of the eUICC. In particular, subscriber keys need to be strongly generated and securely managed. The following assumptions are therefore stated:

- The key K is randomly generated during profile preparation and is securely transported to the Authentication Centre belonging to the MNO;
- The random challenge RAND is generated with sufficient entropy in the Authentication Centre belonging to the MNO;
- The Authentication Centre belonging to the MNO generates unique sequence numbers SQN, so that each quintuplet can only be used once;
- Triplets / quintuplets are communicated securely between MNOs for roaming.

A.APPLICATIONS

The applications shall comply with the security guidelines document for the used platform (operating system). These guideline must substantially describe the application writing style and the platform security mechanisms (e.g. security domains, application firewall) that shall be used to ensure that the applications do not harm the TOE.

4 Security Objectives

4.1 Security objectives for the TOE

4.1.1 Platform support functions

O.PRE-PPI

The TOE shall provide the functionalities of platform management (loading, installation, enabling, disabling, and deletion of applications) in charge of the life-cycle of the whole eUICC and installed applications, as well as the corresponding authorization control, provided by the Profile Rules Enforcer (PRE) and the Profile Package Interpreter (PPI).

In particular, the PRE ensures that:

- There is a limit on the number of ISD-Ps enabled at a time:
  - if the eUICC supports MEP, the limit is greater than one
  - otherwise, the limit is one
- Verification that a Profile containing PPRs is authorised by the RAT;
- Enforcement of the PPRs of a Profile.
- Enforcement of the reference Enterprise Rule.

The PPI translates the Profile Package data as defined in eUICC Profile Package Specification [30] into an installed Profile using the specific internal format of the target eUICC.

This functionality shall rely on the Runtime Environment secure services for package loading, application installation and deletion.

Application Note 9:

The PRE and PPI will in practice be tightly connected with the rest of the TOE, which in return shall very likely rely on the PRE and PPI for the effective enforcement of some of its security functions. The Platform guarantees that only the ISD-R or the Mobile 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 PPR and RAT. 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 MNO-SD keys. Modification of this Security Domain keyset is restricted to its corresponding owner (MNO OTA Platform).

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 management 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 o ISD-R and SM-DP+;

- MNO-SD and MNO OTA Platform.

- ISD-R and eIM (SGP.32)

The TOE shall ensure at any time:

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

Communications shall be protected from unauthorized disclosure, modification and replay.

This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment and the PPE/PPI (see O.PPE-PPI).

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 10:

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 PRE, PPI and Telecom framework belonging to the TOE shall ensure the correct operation of their security functions.

Application Note 11:

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

- provide atomic transaction to its services, and
- 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.SK.EUICC.ECDSA;

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

Application Note 12:

Amongst the components of the TOE,

- PRE, PPI 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:

- The following keysets:
  - D.MNO_KEY

S; o Profile data:

- D.PROFILE_NAA_PARAMS,
- D.PROFILE_IDENTITY,
- D.PROFILE _RULES,
- D.PROFILE_USER_COD

ES; o Management data:

- D.PLATFORM_DATA,
- D.DEVICE_INFO,
- D.PLATFORM_RAT;

- Identity management data:
  - D.SK.EUICC.ECDSA,
  - D.CERT.EUICC.ECDSA,
  - D.PK.CI.ECDSA,
  - D.EID,
  - D.CERT.EUM.ECDSA,
  - D.CRLs,
  - D.SECRETS,
  - D.PK.EIM.ECDSA (SGP.32).

Application Note 13:

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 eSIM CA is a trusted third-party for the purpose of authentication of the entities of the system. The eSIM CA provides certificates for the EUM, SM-DS and SM-DP+. The eSIM CA must ensure the security of its own private keys.

OE.SM-Dpplus

The SM-DP+ shall be a trusted actor responsible for the data preparation and the associated OTA servers. The SM-DP+ site must be accredited following GSMA SAS.

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),
- 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 14:

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

OE.SM-DS

The SM-DS shall be a trusted actor responsible for the Discovery Service. The SM-DS site must be accredited following GSMA SAS. The SM-DS has secure communication channels with SM-DP+ or another SM-DS.

The SM-DS must ensure the security of credentials received from the SM-DP+ or another SM-DS.

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 15:

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.

OE.EIM (SGP.32)

The eIM shall ensure the authenticity and integrity for its generated eUICC Packages containing Profile State Management Operations (PSMO) or eIM Configuration Operations (eCO).

Administrators of the eIM shall be trusted people.

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 Profile Rules Enforcer, Profile Package Interpreter, and Telecom Framework (S.PRE, S.PPI, and S.TELECOM).
- (3) It allows the S.PRE, S.PPI, and S.TELECOM to store data in “persistent technology memory” or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection).
- (4) It provides a means to perform memory operations atomically for S.PRE, S.PPI, and S.TELECOM.

Application Note 16:

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.PRE-PPI

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

- load of a package file,
- installation of a package file,
- extradition of a package file or an application,
- personalization of an application or a Security Domain,
- deletion of a package file or an application,

- o privileges update of an application or a Security Domain,
- o

Application Note 17:

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 18:

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 19:

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 20:

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;
- o 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 21:

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.
Application Note 21.1:

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.SID.1, T.SID.2

OE.RE.CODE-EXE

The Runtime Environment shall prevent unauthorized code execution by applications.
Application Note 22:

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.

OE.TRUSTED-PATHS-LPAd-IPAd

The interfaces ES10a, ES10b and ES10c (SGP.22) are trusted paths between the eUICC and LPAd/IPAd, when LPAd/IPAd is present and active.

4.2.3 Profile

OE.APPLICATIONS

The applications shall comply with the security guidelines document for the platform (operating system) used. These guideline must substantially describe the application writing style and the platform security mechanisms (e.g. security domains, application firewall) that shall be used to ensure that the applications do not harm the TOE.

Application Note 23:

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]).
Application Note 24:

In the case when GlobalPlatform is the used platform, the guidelines of [5] shall be applied.

OE.MNO-SD

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.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors (SM-DP+ and MNO OTA Platform) will access the Security Domains functions and content;
- OE.SM-Dpplus 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.MNO-SD).

In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required:

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

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

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

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

In order to ensure the secure operation of the Application Firewall, the following objectives for the operational environment are also required:

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

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

Consequently, the TSF ensures:

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

underlying Runtime Environment, which protects the applications communications (OE.RE.SECURE- COMM).

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

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

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

Consequently, the TSF ensures:

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

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

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

4.3.1.2 Identity tampering

T.UNAUTHORIZED-IDENTITY-MNG O.PRE-PPI and O.eUICC-DOMAIN-RIGHTS coversthis 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.

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).

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

4.3.1.3 eUICC cloning

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

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

4.3.1.4 LPAd impersonation

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

4.3.1.5 Unauthorized access to the mobile network

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

impersonation by an attacker.

4.3.1.6 Second level threats

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

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

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

- the TOE itself must ensure the correct operation of PRE, PPI and Telecom Framework (O.OPERATE), and
- PRE, PPI and Telecom Framework must protect the confidentiality and integrity of the sensitive data they process, 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 Runtime Environment (to which Java Card System can be an implementation) security architecture must cover side channels (OE.RE.DATA-CONFIDENTIALITY).

4.3.2 Organisational Security Policies

4.3.2.1 Life-cycle

OSP.LIFE-CYCLE O.PRE-PPI ensures that there is a single ISD-P enabled at a time.

The profile deletion capability relies on the secure application deletion mechanisms provided by OE.RE.PRE-PPI.

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

4.3.3 Assumptions

4.3.3.1 Device assumptions

A.TRUSTED-PATHS-LPAd-IPAd This assumption is upheld by OE.TRUSTED-PATHS-LPAd-IPAd.

4.3.3.2 Miscellaneous

A.ACTORS This assumption is upheld by objectives OE.CI, OE.SM-Dpplus, OE.MNO, and OE.EIM (SGP.32) 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	Rationale
T.UNAUTHORIZED- PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-Dpplus, OE.MNO, O.PRE-PPI , O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.RE.DATA- CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.MNO-SD	Section 4.3.1
T.UNAUTHORIZED- PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI , OE.APPLICATIONS, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.EIM (SGP.32)	Section 4.3.1
T.PROFILE-MNG-INTERCEPTION	OE.SM-Dpplus, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE- COMM, OE.MNO-SD, OE.EIM (SGP.32)	Section 4.3.1
T.PROFILE-MNG-ELIGIBILITY	OE.SM-Dpplus, OE.RE.SECURE-COMM, O.SECURE- CHANNELS, O.INTERNAL-SECURE-CHANNELS, OE.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	Section 4.3.1
T.UNAUTHORIZED- IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PRE-PPI , OE.RE.DATA- CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.RE.IDENTITY	Section 4.3.1
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM	Section 4.3.1
T.UNAUTHORIZED- eUICC	O.PROOF_OF_IDENTITY, OE.IC.PROOF_OF_IDENTITY	Section 4.3.1
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd-IPAd	Section 4.3.1
T.UNAUTHORIZED- MOBILE-ACCESS	O.ALGORITHMS	Section 4.3.1

T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, O.OPERATE, OE.RE.API, OE.RE.CODE-EXE, OE.IC.SUPPORT, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	Section 4.3.1
T.PHYSICAL-ATTACK	OE.IC.SUPPORT, OE.IC.RECOVERY, O.DATA-CONFIDENTIALITY, OE.RE.DATA-CONFIDENTIALITY	Section 4.3.1

Table 1 Threats and Security Objectives – Coverage

Security Objectives	Threats
O.PRE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY- INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL- ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-Dpplus	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.EIM (SGP.32)	T.UNAUTHORIZED-PLATFORM-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.PRE-PPI	
OE.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY- INTERCEPTION
OE.RE.API	T.LOGICAL-ATTACK
OE.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
OE.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
OE.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
OE.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd-IPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION

Table 2 Security Objectives and Threats – Coverage

Organisational Security Policies	Security Objectives	Rationale
OSP.LIFE-CYCLE	O.PRE-PPI, OE.RE.PRE-PPI , O.OPERATE	Section 4.3.2

Table 3 OSPs and Security Objectives – Coverage

Security Objectives	Organisational Security Policies
O.PRE-PPI	OSP.LIFE-CYCLE

O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-Dpplus	
OE.MNO	
OE.EIM (SGP.32)	
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PRE-PPI	OSP.LIFE-CYCLE
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd-IPAd	
OE.APPLICATIONS	
OE.MNO-SD	
OE.SM-DS	

Table 4 Security Objectives and OSPs – Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.TRUSTED-PATHS-LPAd-IPAd	OE.TRUSTED-PATHS-LPAd-IPAd	Section 4.3.3
A.ACTORS	OE.CI, OE.SM-Dpplus, OE.MNO, OE.EIM (SGP.32)	Section 4.3.3
A.APPLICATIONS	OE.APPLICATIONS	Section 4.3.3

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

Security Objectives for the Operational Environment	Assumptions
OE.CI	A.ACTORS
OE.SM-Dpplus	A.ACTORS

OE.MNO	A.ACTORS
OE.EIM (SGP.32)	A.ACTORS
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PRE-PPI	
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd-IPAd	A.TRUSTED-PATHS- LPAd-IPAd
OE.APPLICATIONS	A.APPLICATIONS
OE.MNO-SD	

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

5 Extended requirements

Void.

6 Security Requirements

In order to define the Security Functional Requirements, Part 2 of the Common Criteria was used.

Some Security Functional Requirements have been refined. The refinements are described below the associated SFR. The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. These refinements are interpretation refinement, and are described as an extra paragraph, starting with the word “Refinement”.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are 66nitializa. Please, note that there are specific selection operations related to the eSIM IoT SGP.32 [36] specification. These selection operations are indicated by referencing the SGP.32 [36] and they are mandatory to be used when the TOE is compatible with SGP.32 [36].

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as bold text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are 66nitializa.

In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is both bold and italicized (see for example the SFR FCS_COP.1/Mobile_network).

In some other cases the assignment made by the PP authors defines an assignment to be performed by the ST author. Thus this text is both bold and italicized (see for example the SFR FIA_UID.1/EXT).

The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

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 content access control SFP,
- ECASD 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-Dpplus, U.MNO OTA Platform, U.EIM (SGP.32)) or local (U.MNO-SD, which is an application on the eUICC).

6.1.1.1 Secure Channel Protocol information flow control SFP

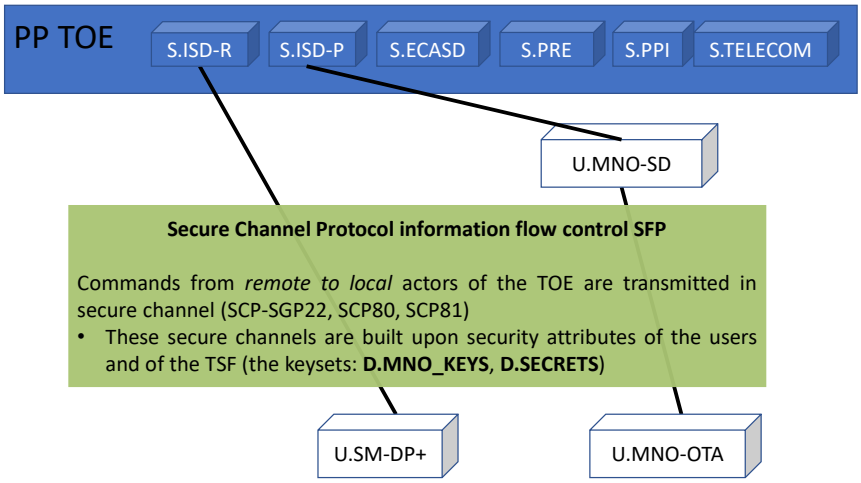


Figure 12 Secure Channel Protocol Information flow control SFP

The eUICC shall support SCP-SGP22, SCP80, SCP81 (see section Terms and definitions and References for more details).

6.1.1.2 Platform services information flow control SFP

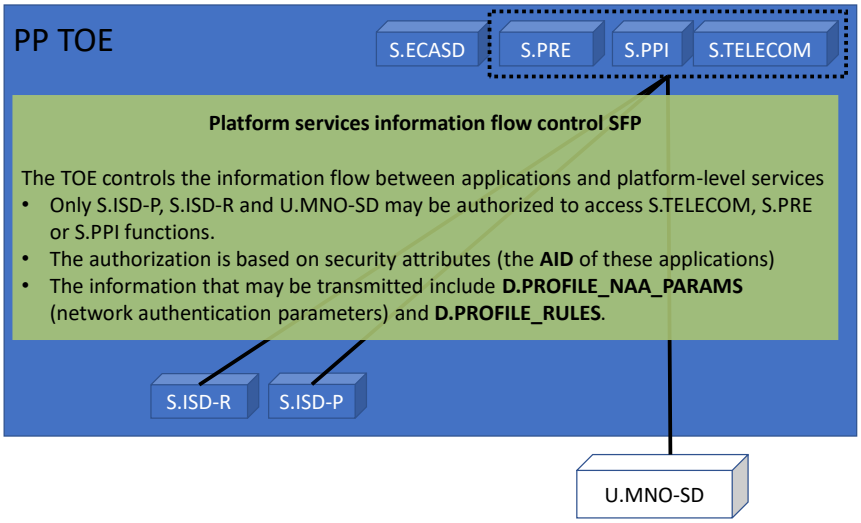


Figure 13 Platform services information flow control SFP

6.1.1.3 ISD-R access control SFP

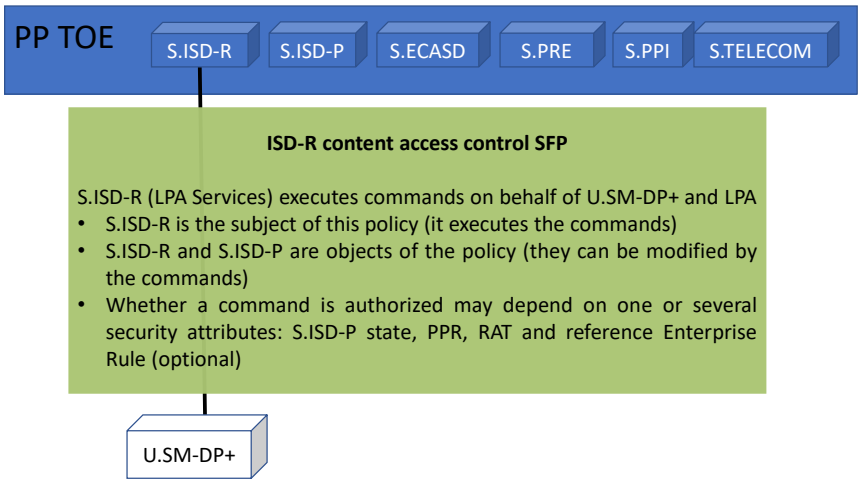


Figure 14: ISD-R access control SFP

6.1.1.4 ISD-P content access control SFP

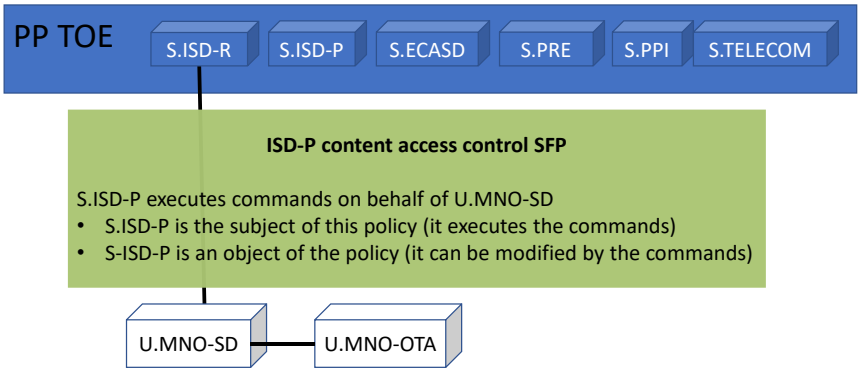


Figure 15 ISD-P content access control SFP

6.1.1.5 ECASD access control SFP

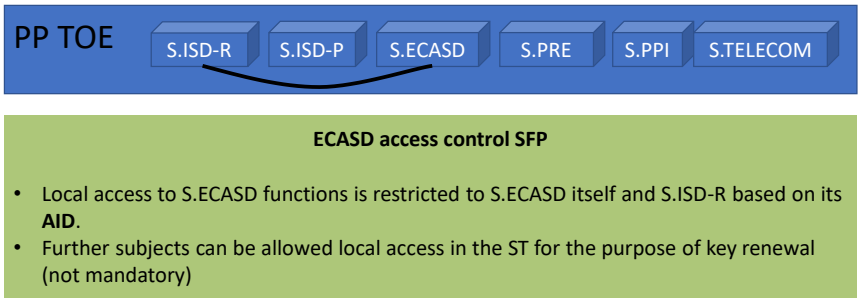


Figure 16 ECASD access control SFP

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-P state	The state of the subject S.ISD-P. The possible value for this state are: • ENABLED • DISABLED • INSTALLED • SELECTABLE	This attribute is a part of the D.PLATFORM_DATA described in section 3.1.2.2 Management data
PPR	The Profile Policy 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. PPR may include one or several of the following rules: • (PPR1) 'Disabling of this Profile is not allowed' • (PPR2) 'Deletion of this Profile is not allowed'	This attribute is described as part of D.PROFILE _RULES in section 3.1.1.2 Profile data
Reference Enterprise Rule	The Reference Enterprise Rule is associated to a given S.ISD-P and is used by the TOE to assess whether other ISD-Ps enablement is authorized. If MEP is supported, it is possible that multiple Enterprise profiles are enabled at a time. Then, only the Reference Enterprise Rule is considered.	This attribute is described as part of D.PROFILE_RULES in section 3.1.1.2 Profile data
Enterprise Rule	A rule stored in an Enterprise Profile that can be used by the Profile Owner to restrict End User controllability for enabling and installing Profiles on Enterprise Capable Devices.	This attribute is described as part of D.PROFILE_RULES in section 3.1.1.2 Profile data
RAT	The Rules Authorisation Table is installed at eUICC personalization time and is used by the PPE and the LPA to determine whether or not a Profile that contains PPRs is authorised and can be installed on the eUICC.	
Keysets and session keys (D.MNO_KEYS, D.SECRETS)	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.SECRETS) are defined in section 3.1.1.1 Keys

CERT.Dpauth.E CDSA CERT.DPpb.ECDSA	Certificates of U.SM-Dpplus that are used by the TOE to authenticate this user. These certificates are issued by the eSIM CA. The TOE can verify this certificate using the eSIM CA public key.	These attributes are not assets of this Protection profile. The eSIM CA public key is described as the asset D.PK.CI.ECDSA in section 3.1.2.3 Identity management data
SM-DP+ OID MNO OID	SM-DP+ OID is the identification of the default SM-DP+. This value can be empty, in which case either the SM-DS discovery procedure or the SM-DP+ address contained in an Activation Code have to be used. The default SM-DP+ address can be modified or deleted during the lifetime of the eUICC; Memory Reset resets the SM–DP+ OID to its initial value. MNO OID is the identification of the MNO owner of the Profile. Once thisinformation is associated to the Profile, it remains unchanged during the Profile's life-time.	These attributes included in the D.PLATFORM_DATA described in section 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.
CERT.EIM.ECDSA (SGP.32)	Certificates of U.EIM that are used by the TOE to authenticate this user. The TOE can verify this certificate using the eIM public key	The eIM public key is described as the asset D.PK.EIM.ECDSA in section 3.1.2.3 Identity management data

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-Dpplus by its SM-DP+ OID;
- identify the remote user U.MNO-OTA by its MNO OID;identify the on-card user U.MNO-SD by its AID, according to [33];
- identify the remote user U.EIM by its eIM Identifier (SGP.32).

The TOE must:

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

- authenticate U.EIM using PK.EIM.ECDSA (SGP.32).

U.M NO-SD is not authenticated by the TOE. It is created on the eUICC during the profile download and installation by the U.SM-Dpplus. 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-Dpplus is bound to S.ISD-R;
- U.MNO-OTA is bound to U.MNO-SD, and U.MNO-SD is bound to the S.ISD-P managing the corresponding MNO profile;
- U.EIM is bound to S.ISD-R (SGP.32).

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 25:

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

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

The identification of the only local user (U.MNO-SD) is addressed by the FIA_UID.1/MNO-SD SFR.

Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user.

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 26:

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

- U.SM-Dpplus;,
- U.MNO-OTA;
- U.EIM (SGP.32).

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 [24]:

- A U.SM-Dpplus must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.Dpauth.ECDSA and CERT.DPpb.ECDSA), as well as the public key of the CI (D.PK.CI.ECDSA).
- U.MNO-OTA must be authenticated using a SCP80 secure channel according to [12] using the parameters defined in [3] section 2.4.3, or optionally SCP81 according to [13] using the parameters defined in [3] section 2.4.4 (The keyset used for this operation is distributed according to FCS_CKM.2/SCP-MNO).

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with at least one of the elliptic curves referenced for that purpose in SGP.22 [24] or SGP.32 [36].

FIA_USB.1/EXT User-subject binding

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

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

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

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

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

- **change of SM-DP+ OID requires U.SM-Dpplus to be authenticated via "CERT.Dpauth.ECDSA"**
- **change of MNO OID is not allowed.**

Application Note 27:

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

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

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

FIA_UAU.4/EXT Single-use authentication mechanisms

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

- **U.SM-Dpplus**
- **U.MNO-OTA**
- **[Selection: none, U.EIM]**

Application Note 28:

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

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

The ST writer shall choose the selections related to SGP.32 if the TOE supports eSIM for IoT specifications.

FIA_UID.1/MNO-SD Timing of identification

FIA_UID.1.1/MNO-SD The TSF shall allow

[assignment: *list of TSF-mediated actions*] 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 29:

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-Dpplus via the subject S.ISD-R (see FDP_ACF.1/ISDR), and the binding between U.SM-Dpplus and S.ISD-R requires authentication of U.SM-DP+, as described in FIA_USB.1/EXT.

FIA_USB.1/MNO-SD User-subject binding

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

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

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

Application Note 30:

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

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

In order to perform operations such as PPR update, U.MNO-OTA authenticates, then sends a command to U.MNO-SD, which transmits it to S.ISD-P; the 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-R: The S.ISD-R 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.Dpauth.ECDSA, CERT.DPpb.ECDSA, and SM-DP+ OID belonging to U.SM-Dpplus;**
- **MNO OID belonging to U.MNO-OTA;**
- **AID belonging to U.MNO-SD.**

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1 The TSF shall provide a **cryptographic authentication mechanism**

based on the EID of the eUICC to prove the identity of the TOE by including the following properties **the EID value in the eUICC certificate** to an external entity.

Application Note 31:

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

6.1.3 Comminication

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-Dpplus and S.ISD-R;
- between U.MNO-OTA and U.MNO-SD.

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

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

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

FDP_IFC.1/SCP Subset information flow control

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

- **users/subjects:**
  - **U.SM-Dpplus and S.ISD-R**
  - **U.MNO-OTA and U.MNO-SD**
- **information: transmission of commands**.

FDP_IFF.1/SCP Simple security attributes

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

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

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

- **The TOE shall permit communication between U.MNO-OTA and U.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-Dpplus and S.ISD-R if it is not performed in a SCP-SGP22 secure channel.**

Application Note 32:

More details on the secure channels can be found in [24]

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

FTP_ITC.1/SCP Inter-TSF trusted channel

FTP_ITC.1.1/SCP The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and

provides assured identification of its end points and protection of the channel data from modification or disclosure.

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

FTP_ITC.1.3/SCP The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application Note 33:

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 [24]:

- The secure channels to SM-DP+ must be SCP-SGP22 secure channels. Identification of endpoints is addressed by the use of AES according to [11] Amendment F using the parameters defined in [24], sections 2.6 and 5.5.
- SCP80 must be provided to build secure channels to MNO OTA Platform (section 5.4 of [24]). The TSF may also permit to use a SCP81 secure channel to perform

the same functions than the SCP80 secure channel.

Related keys are:

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

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

- The TSF shall permit the SM-DP+ to open a SCP-SGP22 secure channel to transmit the following operations:
  - ES8+.InitialiseSecureChannel
  - ES8+.ConfigureISDP
  - ES8+.StoreMetadata
  - ES8+.ReplaceSessionKeys
  - ES8+.LoadProfileElements.
- The TSF shall permit the LPAd/IPAd to transmit the following operations:
- ES10a.GetEuiccConfiguredData (SGP.22 v3.0 or higher)
  - ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.x)
  - ES10a.SetDefaultDpAddress
  - ES10b.PrepareDownload
  - ES10b.LoadBoundProfilePackage
  - ES10b.GetEUICCChallenge
  - ES10b.GetEUICCInfo
  - ES10b.ListNotification
  - ES10b.RetrieveNotificationsList
  - ES10b.RemoveNotificationFromList
  - ES10b.AuthenticateServer
  - ES10b.CancelSession
  - ES10b.LoadEuiccPackage (SGP.32)
  - ES10b.AddInitialEim (SGP.32)
  - ES10b.GetCerts (SGP.32)
  - ES10b.EnableUsingDD (SGP.32)
  - ES10b.ProfileRollback (SGP.32)
  - ES10b.ConfigureAutomaticProfileEnabling (SGP.32)
  - ES10b.GetEimConfigurationData (SGP.32)
  - ES10b.GetProfilesInfo (SGP.32)ES10c.GetProfilesInfo (SGP.22)
  - ES10c.EnableProfile (SGP.22)
  - ES10c.DisableProfile (SGP.22)
  - ES10c.DeleteProfile (SGP.22)
  - ES10c.eUICCMemoryReset (SGP.22)

  - ES10b.GetEID (SGP.32)
  - ES10c.GetEID (SGP.22)
  - ES10c.SetNickname
  - ES10c.GetRAT.
- The TSF may permit the LPAd/IPAd to transmit the following operations:
  - ES10b.LoadCRL (SGP.22 V2.x)
  - ES10c.LPA alerting (SGP.22 v3.0 or higher)
  - ES10c.VerifySmdsResponse (SGP.22 v3.0 or higher)
  - ES10b.LoadRPMPackage (SGP.22 v3.0 or higher)
  - ES10b.PrepareDeviceChange (SGP.22 v3.0 or higher)
  - ES10b.VerifyDeviceChange (SGP.22 v3.0 or higher).
  - ES10b.eUICCMemoryReset (SGP.32).
- The TSF shall permit the remote OTA Platform to open a SCP80 or SCP81 secure channel to transmit the following operation:
  - ES6.UpdateMetadata.

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-Dpplus and U.MNO-OTA**
  - **Downloaded objects from U.SM-Dpplus and U.MNO-OTA**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SCP The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Application Note 34:

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

- SM-DP+ commands
  - ES8+.InitialiseSecureChannel
  - ES8+.ConfigureISDP
  - ES8+.StoreMetadata
  - ES8+.ReplaceSessionKeys
  - ES8+.LoadProfileElements
- LPAd/IPAd commands
  - ES10a.GetEuiccConfiguredData (SGP.22 v3.0 or higher)
  - ES10a.GetEuiccConfiguredAddresses (SGP.22 v2.x)
  - ES10a.SetDefaultDpAddress
  - ES10b.PrepareDownload
  - ES10b.LoadBoundProfilePackage
  - ES10b.GetEUICCChallenge
  - ES10b.GetEUICCInfo
  - ES10b.ListNotification
  - ES10b.RetrieveNotificationsList
  - ES10b.RemoveNotificationFromList
  - ES10b.LoadCRL (SGP.22 V2.x)ES10b.AuthenticateServer
  - ES10b.CancelSession
  - ES10b.LoadEuiccPackage (SGP.32)
  - ES10b.AddInitialEim (SGP.32)
  - ES10b.GetCerts (SGP.32)
  - ES10b.EnableUsingDD (SGP.32)
  - ES10b.ProfileRollback (SGP.32)
  - ES10b.ConfigureAutomaticProfileEnabling (SGP.32)
  - ES10b.GetEimConfigurationData (SGP.32)
  - ES10b.GetProfilesInfo (SGP.32)
  - ES10c.GetProfilesInfo
  - ES10c.EnableProfile
  - ES10c.DisableProfile
  - ES10c.DeleteProfile
  - ES10b.eUICCMemoryReset (SGP.32)
  - ES10c.eUICCMemoryReset (SGP.22)
  - ES10b.GetEID (SGP.32)
  - ES10c.GetEID (SGP.22)
  - ES10c.SetNickname
  - ES10c.GetRAT
  - ES10c.LPA alerting (SGP.22 v3.0 or higher)
  - ES10c.VerifySmdsResponse (SGP.22 v3.0 or higher)
  - ES10b.LoadRPMPackage (SGP.22 v3.0 or higher)

  - o ES10b.PrepareDeviceChange (SGP.22 v3.0 or higher)
  - o ES10b.VerifyDeviceChange (SGP.22 v3.0 or higher)
- Downloaded objects from SM-DP+ o Session keys
  - o Profile Metadata (including PPR data)
- MNO commands
  - o ES6.UpdateMetadata
- Downloaded objects from MNO OTA Platform o Profile Metadata (including PPR data and Enterprise Rules (optional)).

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 35:

This SFR is related to the protection of:

- Profiles downloaded from SM-DP+.

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 [24].

Related keys are:

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

FDP_UIT.1/SCP Data exchange integrity

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

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

Application Note 36:

This SFR is related to the protection of:

- Profiles downloaded from SM-DP+;

- Commands received from SM-DP+ and MNO OTA Platform;
- PPR and Enterprise Rules (optional) 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 [24].

Related keys are:

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

FCS_CKM.1/SCP-SM Cryptographic key generation

FCS_CKM.1.1/SCP-SM The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curves Key agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following:

[**assignment**: *at least one elliptic curve referenced in SGP.22 [24] or SGP.32 [36]*]

o

Application Note 37:

This key generation mechanism is used to generate

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

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

FCS_CKM.2/SCP-MNO Cryptographic key distribution

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

Application Note 38:

This SFR is related to the distribution of

- D.MNO_KEYS during profile download.

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

FCS_CKM.4/SCP-SM Cryptographic key destruction

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 39:

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

- D.MNO_KEYS.

FCS_CKM.6/SCP-SM Cryptographic key destruction

FCS_CKM.6.1/SCP-SM The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction*]].

FCS_CKM.6.2/SCP-SM The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-SM in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note 40:

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

- D.SECRETS
- CERT.DPauth.ECDSA
- CERT.DPpb.ECDSA
- CERT.DP.TLS
- D.CERT.EUICC.ECDSA
- D.SK.EUICC.ECDSA
- D.PK.CI.ECDSA.

FCS_CKM.6/SCP-MNO Cryptographic key destruction

FCS_CKM.6.1/SCP-MNO The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction*]].

FCS_CKM.6.2/SCP-MNO The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/SCP-MNO in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note 41:

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-R can perform ECASD functions and obtain output data from these functions (*ECASD access control SFP* in FDP_ACC.1/ECASD and FDP_ACF.1/ECASD).

FDP_ACC.1/ISDR Subset access control

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

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

Application Note 42:

- This policy describes the rules to be applied to access Platform Management operations. It covers the access to operations by ISD-R required by sections 5.x of [24].

FDP_ACF.1/ISDR Security attribute based access control

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

- **subjects: S.ISD-R**
- **objects:**
  - **S.ISD-P with security attributes “state” “PPR”, and [Selection: “Reference Enterprise Rule”, no additional attributes]**
- **operations:**
  - **Create and configure profile**
  - **Store profile metadata**
  - **Enable profile**

- **Disable profile**
- **Delete profile**
- **Perform a Memory reset**.

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

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

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

Application Note 43:

This policy describes the rules to be applied to access Platform Management or eUICC Management operations. It covers the access to the following operations by ISD-R required by sections 5.x of [24]:

- ES8+.ConfigureISDP (Create and configure profile)
- ES8+.StoreMetadata (Store profile metadata)
- ES10c.EnableProfile (Enable profile)
- ES10c.DisableProfile (Disable profile)
- ES10c.DeleteProfile (Delete profile)
- ES10c.eUICCMemoryReset (Perform a Memory reset)
- ES10b.LoadRpmPackage (Enable/Disable/Delete profile) (SGP.22 v3.0 or higher)

Application Note 44:

The ST writer shall choose the selections related to Enterprise Rules in FDP_ACF.1.1/ISDR and FDP_ACF.1.2/ISDR if the TOE supports Enterprise Profiles.

FDP_ACC.1/ECASD Subset access control

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

- **subjects: S.ISD-R,**
- **objects: S.ECASD,**
- **operations:**
  - **execution of a ECASD function**
  - **access to output data of these functions,**

- **[assignment: additional list of subjects, objects, and operations between subjects and objects covered by the SFP].**

FDP_ACF.1/ECASD Security attribute based access control

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

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

- **[assignment: additional list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes].**

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

- **Authorized users: only S.ISD-R, identified by its AID, shall be authorized to execute the following S.ECASD functions:**
  - **Verification of a certificate CERT.Dpauth.ECDSA, CERT.DPpb.ECDSA, CERT.DP.TLS, CERT.Dsauth.ECDSA, or CERT.DS.TLS, provided by an ISD-R, with the eSIM CA public key (PK.CI.ECDSA)**
  - **Creation of an eUICC signature, using D.SK.EUICC.ECDSA, on material provided by an ISD-R**.
- **[assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].**

FDP_ACF.1.3/ECASD 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/ECASD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

6.1.5 Platform Services

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

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

FDP_IFC.1/Platform_services Subset information flow control

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

- **users/subjects:**
  - **S.ISD-R, S.ISD-P, U.MNO-SD**
  - **Platform code (S.PRE, S.PPI,S.TELECOM)**
- **information:**
  - **D.PROFILE_NAA_PARAMS**
  - **D.PROFILE _RULES**
  - **D.PLATFORM_RAT**
- operations:
  - **installation of a profile**
  - **PPR and RAT enforcement**
  - **network authentication**.
  - **[selection**: **Reference Enterprise Rule enforcement, no additional operations]**

Application Note 45:

The ST writer shall choose the selections related to Enterprise Rules in FDP_IFC.1.1/Platform_services if the TOE supports Enterprise Profiles.

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 _RULES**
  - **D.PLATFORM_RAT**
- **operations:**
  - **installation of a profile**
  - **PPR and RAT enforcement**
  - **network authentication**.
  - **[selection: Reference Enterprise Rule enforcement, no additional operations]**

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

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

FDP_IFF.1.3/Platform_services The TSF shall enforce the [assignment: *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 46:

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

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

S.ISD-P to S.TELECOM.

Application Note 47:

The ST writer shall choose the selections related to Enterprise Rules in FDP_IFF.1.1/Platform_services and FDP_IFF.1.2/Platform_services if the TOE supports Enterprise Profiles.

FPT_FLS.1/Platform_services Failure with preservation of secure state

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

- **failure that lead to a potential security violation during the processing of a S.PRE, S.PPI or S.TELECOM API specific functions:**
  - **Installation of a profile**
  - **PPR and RAT enforcement**
  - **Network authentication**
  - **[selection: Reference Enterprise Rule enforcement, no additional functions]**
- **[assignment: *other type of failure*]**.

Application Note 48:

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].

Application Note 49:

The ST writer shall choose the selections related to Enterprise Rules in FPT_FLS.1.1/Platform_services if the TOE supports Enterprise Profiles.

6.1.6 Security management

This package includes several supporting security functions:

- Random number generation (FCS_RNG.1)
- User data and TSF self-protection measures: o 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:
  - o Management of security attributes such as Platform d ata (FMT_MSA.1/PLATFORM_DATA), PPR and Enterprise Rules (FMT_MSA.1/RULES), (FMT_MSA.1/RAT) and keys (FMT_MSA.1/CERT_KEYS) with restrictive default values (FMT_MSA.3); o Management of roles and security functions (FMT_SMR.1 and FMT_SMF.1).

FCS_RNG.1 Random number generation

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

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

Refinement:
The ST author is required to select one of the above RNG classes as defined in AIS 20/31 [19].

FPT_EMS.1 TOE Emanation of TSF and User data

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

ID	Emission	Attack surface	TSF data	User data
1	[assignment: *types of emissions*]	**Any**	**-**	**o D.SECRETS;** **o D.SK.EUICC.ECDSA** **and the secret keys which are part of the following keysets:** **o D.MNO_KEYS,** **o D.PROFILE_NAA_PARAMS.**

Application Note 50:

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
- Profile data
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE _RULES
  - D.PROFILE_USER

_CODES o

Management data

- D.PLATFORM_DATA
- D.DEVICE_INFO
- D.PLATFORM_RAT

- Identity management data
  - D.SK.EUICC.ECDSA
  - D.CERT.EUICC.ECDSA
  - D.PK.CI.ECDSA
  - D.EID
  - D.SECRETS
  - D.CERT.EUM.ECDSA
  - D.CRLs if existing

FDP_RIP.1 Subset residual information protection

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

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

FPT_FLS.1 Failure with preservation of secure state

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

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

FMT_MSA.1/PLATFORM_DATA Management of security attributes

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

- **ISD-P state**

to

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

Application Note 51:

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

FMT_MSA.1/RULES Management of security attributes

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

- **D.PROFILE _RULES**

to

- **S.ISD-R to change_default, via function "ES8+.ConfigureISDP"**
- **S.ISD-R to query**
- **S.ISD-P to modify, via function "ES6.UpdateMetadata"**
- **S.ISD-R to modify, via function "ES10b.LoadRPMPackage (UpdateMetadataRequest)".** (SGP.22 v3.0 or higher)
- **S.ISD-R to delete, via function "ES10c.DeleteProfile"**.

FMT_MSA.1/CERT_KEYS Management of security attributes

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

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

to

- **S.ISD-R for:**
  - **query D.PK.CI.ECDSA**
  - **delete D.MNO_KEYS, via function "ES10c.DeleteProfile"**
- **no actor for other operations**.

Application Note 52:

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

FMT_SMF.1 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

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

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

Application Note 53:

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

FMT_MSA.1/RAT Management of security attributes

FMT_MSA.1.1/RAT The TSF shall enforce the **Platform services information flow SFP and ISD-R access control SFP** to restrict the ability to query the security attributes

- **D.PLATFORM_RAT**

to

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

FMT_MSA.3 Static attribute initialisation

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

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

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.6/Mobile_network).

FCS_COP.1/Mobile_network Cryptographic operation

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

- **MILENAGE according to standard [20] with the following restrictions:**
  - **Only use 128-bit AES as the kernel function? Do not support other choices**
  - **Allow any value for the constant OP**
  - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [20]**
- **Tuak according to [21] with the following restrictions:**
  - **Allow any value of TOP**
  - **Allow multiple iterations of Keccak**
  - **Support 256-bit K as well as 128-bit**
  - **To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards**.

Application Note 54:

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 55:

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.6/ Mobile_network Cryptographic key destruction

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

FCS_CKM.6.2/ Mobile_network The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/Mobile_network in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

6.2 Security Functional Rationale

The Security Assurance Requirements for the evaluation of the TOE are those taken from

- Evaluation Assurance Level 4 (EAL4)

and augmented by taking the following components:

- ALC_DVS.2 and AVA_VAN.5.

The assurance requirements are:

Class ADV: Development

Architectural design (ADV_ARC.1)

Functional specification (ADV_FSP.4)

Implementation representation (ADV_IMP.1)

TOE design (ADV_TDS.3)

Class AGD: Guidance documents

Operational user guidance (AGD_OPE.1)

Preparative user guidance (AGD_PRE.1)

Class ALC: Life-cycle support

CM capabilities (ALC_CMC.4)

CM scope (ALC_CMS.4)

Delivery (ALC_DEL.1)

Development security (ALC_DVS.2)

Life-cycle definition (ALC_LCD.1)

Tools and techniques (ALC_TAT.1)

Class ASE: Security Target evaluation

Conformance claims (ASE_CCL.1)

Extended components definition (ASE_ECD.1)

ST introduction (ASE_INT.1)

Security objectives (ASE_OBJ.2)

Derived security requirements (ASE_REQ.2)

Security problem definition (ASE_SPD.1)

TOE summary specification (ASE_TSS.1)

Class ATE: Tests

Coverage (ATE_COV.2)

Depth (ATE_DPT.1)

Functional tests (ATE_FUN.1)

Independent testing (ATE_IND.2)

Class AVA: Vulnerability assessment

Vulnerability analysis (AVA_VAN.5)

6.2.1 Refinements regarding Architectural design (ADV_ARC.1)

The following text reflects the requirements of the selected component ADV_ARC.1 and the refinement for the ADV_ARC.1.2C:

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.PRE-PPI 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/RULES and FMT_MSA.1/RAT support these SFRs by ensuring management of the Profile Policy Rules (PPR) and Rules Authorisation Table (RAT) files, which ensure that life- cycle modifications are made according to the authorized policy.

FMT_MSA.1/PLATFORM_DATA restricts the state transitions that can apply to Platform data (ISD-P state) that are used as security attributes by other security policies of the TSF (ISD-R access control SFP and ISD-P content access control SFP).

The objective also requires a secure failure mode as described in

FPT_FLS.1. FCS_RNG.1 is required to support FDP_ACF.1/ECASD.

NB: The memory reset is also described as a secure failure mode in FPT_FLS.1.

O.eUICC-DOMAIN-RIGHTS The requirements FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, and FDP_ACF.1/ECASD ensure that ISD-R 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. FCS_RNG.1 is required to support FDP_ACF.1/ECASD.

O.SECURE-CHANNELS All SFRs relative to the 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+ 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 deallocated 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, FMT_SMR.1 and FMT_SMF.1 state the policy for controlling the access to TOE services and resources by the Application Layer.

Atomicity is provided by the FPT_FLS.1/Platform_services requirement.

Data protection

O.DATA-CONFIDENTIALITY FDP_UCT.1/SCP addresses the reception of data from off-card actors, while the access control SFRs (FDP_ACC.1/ISDR, FDP_ACC.1/ECASD) address the isolation between Security Domains.

FPT_EMS.1 ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks.

FDP_RIP.1 ensures that no residual confidential data is available.

FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network, and FCS_CKM.4/Mobile_network address the cryptographic algorithms present in the Telecom Framework, the distribution and the destruction of associated keys.

O.DATA-INTEGRITY FDP_UIT.1/SCP addresses the reception of data from off-card actors, while the access control SFRs (FDP_ACC.1/ISDR, FDP_ACC.1/ECASD) address the isolation between Security Domains.

FDP_SDI.1 specifies the Profile data that is monitored in case of an integrity breach (for example modification of the received profile during the installation operation).

FPT_TST.1 would contribute to the protection of integrity.

Connectivity

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

6.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.PRE-PPI	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/RULES, FMT_MSA.1/RAT, FCS_RNG.1, FPT_FLS.1, FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD	Section 6.3.1
O.eUICC-DOMAIN-RIGHTS	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FTP_ITC.1/SCP, FCS_RNG.1	Section 6.3.1
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	Section 6.3.1
O.INTERNAL-SECURE-CHANNELS	FDP_RIP.1, FDP_SDI.1, FPT_EMS.1	Section 6.3.1
O.PROOF_OF_IDENTITY	FIA_API.1	Section 6.3.1
O.OPERATE	FPT_FLS.1/Platform_services	Section 6.3.1
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	Section 6.3.1
O.DATA-CONFIDENTIALITY	FDP_RIP.1, FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ECASD, FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network, FPT_EMS.1	Section 6.3.1
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ECASD, FDP_SDI.1	Section 6.3.1
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network	Section 6.3.1

Table 8 Security Objectives and SFRs – Coverage

Security Funtional 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.PRE-PPI, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ISDR	O.PRE-PPI, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ECASD	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ECASD	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS
FDP_IFC.1/Platform_services	O.API
FDP_IFF.1/Platform_services	O.API
FPT_FLS.1/Platform_services	O.OPERATE, O.API
FCS_RNG.1	O.PRE-PPI, O.eUICC-DOMAIN-RIGHTS
FPT_EMS.1	O.INTERNAL-SECURE-CHANNELS, O.DATA- CONFIDENTIALITY
Security Functional Requirements	Security Objectives
FDP_SDI.1	O.INTERNAL-SECURE-CHANNELS, O.DATA- INTEGRITY

FDP_RIP.1	O.INTERNAL-SECURE-CHANNELS, O.DATA- CONFIDENTIALITY
FPT_FLS.1	O.PRE-PPI
FMT_MSA.1/PLATFORM_DATA	O.PRE-PPI
FMT_MSA.1/RULES	O.PRE-PPI
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS
FMT_SMF.1	O.SECURE-CHANNELS, O.API
FMT_SMR.1	O.SECURE-CHANNELS, O.API
FMT_MSA.1/RAT	O.PRE-PPI
FMT_MSA.3	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 SFR Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.2 or FCS_COP.1 of FCS_CKM.1/SCP-SM may be discarded. The dependency to FCS_COP.1 may be discarded if the TOE uses the cryptographic libraries provided by its underlying Platform. Otherwise, the ST MUST IMPLEMENT fcs_cop.1 to satisfy this dependency.

The dependency FCS_CKM.3 of FCS_COP.1/Mobile_network isdiscarded. This dependency is discarded as there is no Interface to access the keys..

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	FDP_IFC.1/SCP, FMT_MSA.3

	(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_CKM.5 or FCS_COP.1) and (FCS_CKM.3) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1 {Either by composition or claim in ST} {*Discarded – No Key Access Interface exists}* FCS_CKM.6/SCP-SM FCS_RNG.1
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
FCS_CKM.4/SCP-SM	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.5) and (FCS_CKM.3) FCS_CKM.1)	FDP_ITC.2/SCP {*Discarded – No Key Access Interface exists}*
FCS_CKM.6/SCP-SM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3

FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services , FMT_MSA.3
FPT_FLS.1/Platform_services	No Dependencies	
FCS_RNG.1	No Dependencies	
FPT_EMS.1	No Dependencies	
FDP_SDI.1	No Dependencies	
FDP_RIP.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/RULES	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, MT_MSA.1/RULES, FMT_MSA.1/CERT_KEYS, FMT_SMR.1, FMT_MSA.1/RAT

FCS_COP.1/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) or FCS_CKM.5) and FCS_CKM.3	FDP_ITC.2/SCP, {*Discarded – No Key Access Interface exists}*
FCS_CKM.2/Mobile_network	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) or FCS_CKM.5) and (FCS_CKM.3)	FDP_ITC.2/SCP {*Discarded – No Key Access Interface exists}*
FCS_CKM.6/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP
FCS_CKM.6/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/SCP

Table 10 SFRs Dependencies

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
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 LPAe PP-Module

7.1 Introduction

7.1.1 PP-Module Identification

Title:	LPAe Module for eUICC for Consumer Devices Protection Profile
Base-PP:	eUICC for Consumer and IoT Devices Protection Profile
Author:	GSMA
Editor:	GSMA
Reference:	SGP.25.LPAe
Version:	3.0
CC Version:	CC:2022 release 1
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General Status:	Complete
Keywords:	eUICC, Consumer Devices, Remote SIM Provisioning

7.1.2 Base-PP

The base protection profile for this PP-module is *eUICC for Consumer and IoT Devices Protection Profile* described in the sections 1–6 of this document.

7.1.3 TOE Overview

The TOE of this PP-Module is the *embedded Local Profile Assistant (LPAe)* which manages the Profile Download and the end-user interface. LPAe is part of the Application Layer.

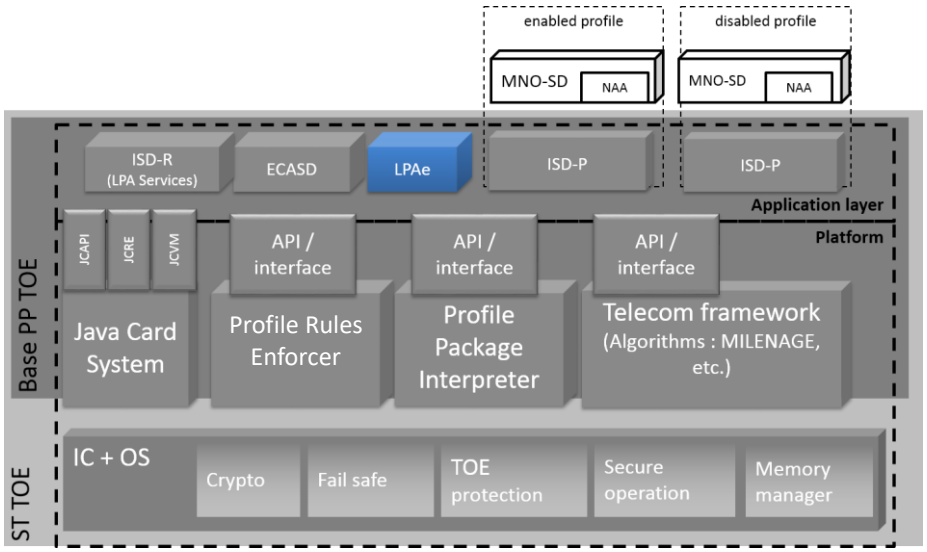


Figure 17 Scope of the TOE

LPAe

Application LayerLPAe is a unit of the Application layer. It has the same functions as the (optional) non-TOE on-device unit LPAd. In particular, it provides the LPDe (local profile download), LDSe (local discovery service), and LUIe (local user interface) features.

The technical implementation of LPAe is up to the EUM. For example, the LPAe may be a feature of the ISD-R.

The LPAe can use the eUICC Rules Authorisation Table (RAT) to determine whether or not a Profile containing Profile Policy Rules (PPRs) is authorised to be installed on the eUICC.

7.1.3.1 TOE type and TOE major security features

The TOE type of this PP-Module is software.
This PP-Module only includes the brick showed (in blue) on the figure hereafter.

7.1.3.2 TOE life-cycle

The LPAe software unit is added at Phase C of the eUICC life-cycle (see Section 1.2.3.1).

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

TOE interfaces

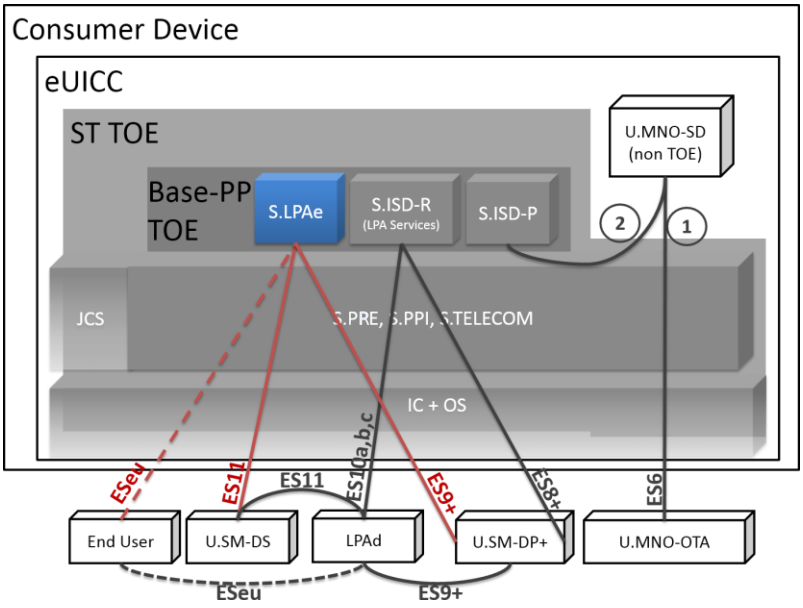


Figure 18 TOE interfaces

As shown on Figure 17, the TOE (shown in blue) has the following interfaces (shown in red):

- With the provisioning infrastructure, consisting in SM-DS and SM-DP+ (identified ES11 and ES9+ in [24]), as well as the End User interface (ESeu).

Description of Non-TOE HW/FW/SW and systems

This PP module inherits all of the non-TOE components of the Base-PP (see Section 1.2.4.2), i.e., the following components: IC, LPAd/IPAd, ES, Runtime Environment, Device, MNO-SD and applications, a Remote provisioning infrastructure.
In addition to the above inherited components, this PP module also interacts with the non- TOE system *LPAe remote provisioning infrastructure*, described in the next subsection.
LPAe remote provisioning infrastructure

The following figure describes the communication channels of the architecture when the LPA is located in the eUICC.

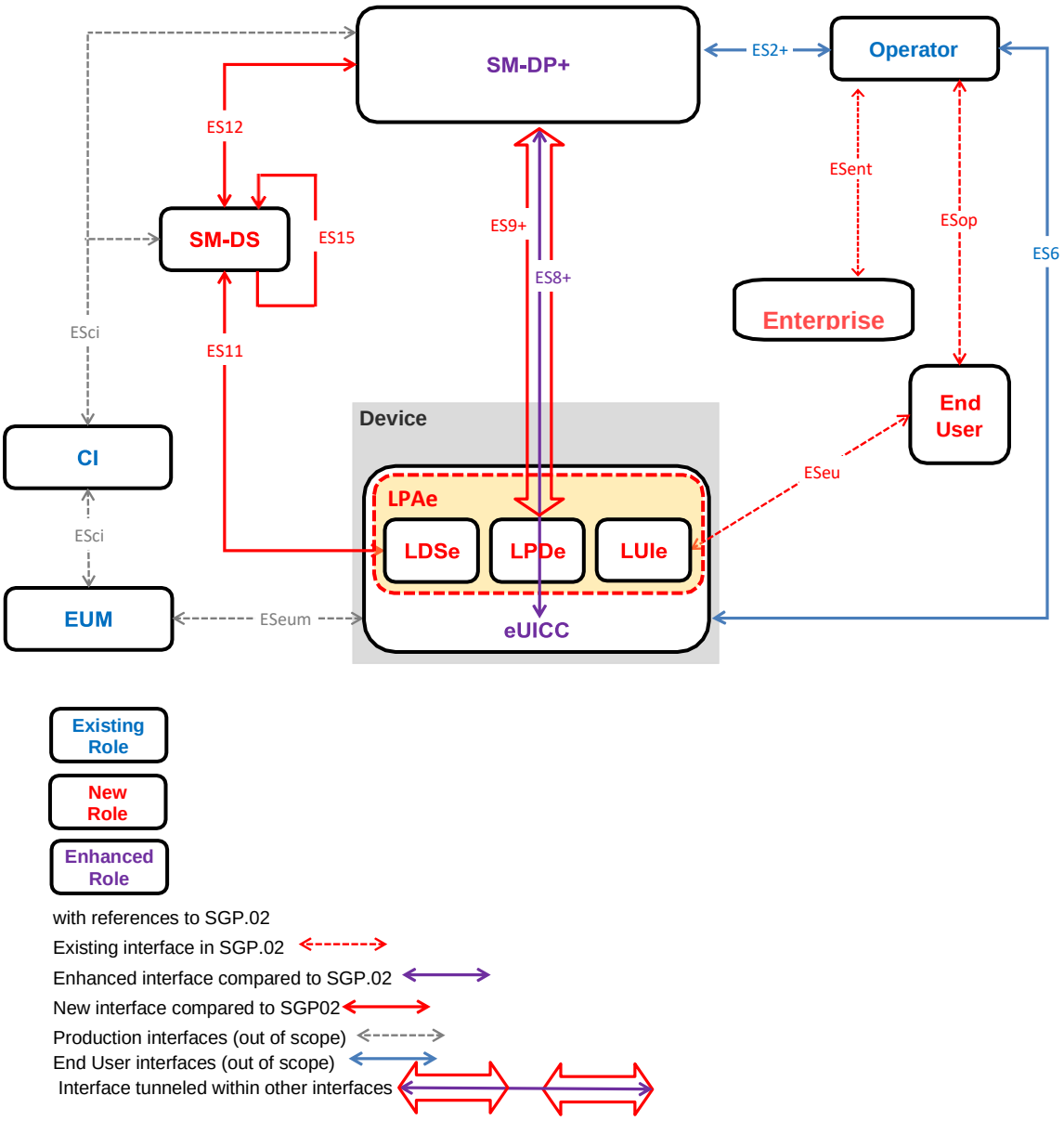


Figure 19 Remote SIM Provisioning System, LPA in the eUICC

The TOE communicates with remote servers of:

- SM-DS, which provides mechanisms for discovery of SM-DP+s;
- SM-DP+, which provides Platform and Profile management commands as well as Profiles.

The TOE shall require the use of secure channels for these interfaces. The keys and certificates required for these operations on the TOE are exchanged/generated during operational use of the TOE. Identities (in terms of certificates) rely on a root of trust called the eSIM CA, 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.

7.1.4 Summary of the security problem

7.1.4.1 High-level view of threats

The threats considered in this PP-Module correspond to the high-level scenarios

described hereafter.

“First-level” threats: Unauthorised Platform Management

These first-level threats arise when the secure links to the LPAe are compromised:

- An attacker alters or eavesdrops the transmission between eUICC and SM-DP+ (link ES9+), in order to compromise the platform management process.
- An attacker alters or eavesdrops the transmission between eUICC and SM-DS (link ES11), in order to compromise the discovery process.
- An attacker alters or eavesdrops the transmission between eUICC and the user (ESeu), in order to.
  - An on-card application:
    - modifies or discloses LPAe data;
    - executes or modifies operations from LPAe.

“Second-level” threats

Logical attacks

An on-card malicious application bypasses the platform security measures by logical means, in order to disclose or modify sensitive data when they are processed by the Platform.

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.

Physical attacks

The attacker discloses or modifies the design of the LPAe, 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.

7.2 Consistency Rationale

The TOE of this PP-Module consists of a new element in the Application Layer, LPAe (Figure 7). No Base-PP TOE component is changed by this PP-Module.

The TOE-external interfaces of this PP-Module are the two interfaces, ES9+ and ES11, which do not exist in the Base-PP (Figure 17). No Base-PP interface is changed by this PP-Module.

Also, the life-cycle of the Base-PP TOE is not changed by this PP-Module.

The union of the Security Problem Definition of this PP-Module (Section 7.4) and the Security Problem Definition of the Base-PP (Section 3) does not lead to a contradiction:

- This PP-Module only adds new assets to the existing assets of the Base-PP;
- This PP-Module only adds a new subject (S.LPAe) to the existing ones of the Base-PP;
- This PP-Module only adds one new assumption (A.ACTORS-LPAe) to the existing assumptions of the Base-PP, and the new assumption is disjoint from the Base-PP

assumption A.ACTORS because it only refers to the user U.SM-DS that does not exists in the Base-PP;

- This PP-Module only adds new threats to the existing threats of the Base-PP. Moreover, the new threats exclusively threaten the PP-Module assets, they do not refer to assets of the Base-PP.

The union of the Security Objectives of this PP-Module (Section 7.5) and the Security Objectives of the Base-PP (Section 4) does not lead to a contradiction:

- As it can be seen from the coverage table Table 13, all Objectives from the PP-Module only cover the proper Threats of the PP-Module, and not the Threats of the Base-PP.
- The PP-Module Objectives only concern assets, subjects, and interfaces (ES9+, ES11) which are proper to the PP-Module, that is, they do not exist in the Base-PP.

Note that some Threats of the PP-Module are also covered by Objectives which already exist in the Base-PP, as can be seen from Table 12.

The union of the SFRs for this PP-Module (Section 7.6) and the SFRs for the Base-PP (Section
6) do not lead to a contradiction:

- This PP-Module only defines a new SFP (LPAe information flow control), for the interfaces that do not exist in the Base-PP (ES9+, ES11).
- Although there are some PP-Module Objectives that also need Base-PP SFRs to be covered (Table 17), the PP-Module SFRs only cover PP-Module Objectives (Table 18),
  i.e. PP-Module SFRs are separate refinements of SFRs and do not override Base-PP SFRs.
- Moreover, Base-PP SFRs do not depend on PP-Module SFRs, as it can be seen from Table 10.

There are no new SARs stated for this PP-Module, since the Base-PP SARs suffice to cover all SFRs.

7.3 Conformance Claims

This protection Profile module is conformant to Common Criteria 2022 release 1.

This protection Profile is conformant to:

- CC Part 1 [37],
- CC Part 2 [38] (conformant),
- CC Part 3 [39] (conformant),
- CC Part 5 [40].

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

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

The following assurance requirement augmentation is optional but suggested:

- ALC_FLR.2 Flaw Reporting Procedures .

ADV_ARC is refined to add a particular set of verifications on top of the existing requirement. This PP does not claim conformance to any other PP.

7.3.1 Conformance Claims to this PP

This Protection Profile module requires demonstrable conformance (as defined in [37]) of any ST or PP claiming conformance to this PP.

7.4 Security Problem Definition

7.4.1 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].

7.4.1.1 User data

User data of the LPAe module includes:

- the codes that the user may enter for profile download (D.LPAe_PROFILE_USER_CODES);
- the profile metadata that is display to the user at the user interface for confirming a platform management action (D.LPAe_PROFILE_DISPLAYED_METADATA).

Profile data

D.LPAe_PROFILE_USER_CODES

This asset consists of:

- o the optional Activation Code that End User may use to initiate Profile Download and Installation via the Local User Interface (LUIe);
- o the optional Confirmation Code that End User may use to confirm Profile Download and Installation via the Local User Interface (LUIe).

D.LPAe_PROFILE_DISPLAYED_METADATA

A copy of the part of Profile Metadata that is displayed by the Local User Interface(LUIe) to the End User for confirmation/information when performing profile management actions. This asset includes in particular the profile class ('operational', 'provisioning', or 'test'), the Profile Policy Rules (PPR), and the profile state ('disabled' or 'enabled').

To be protected against unauthorised modification.

7.4.1.2 TSF data

The TSF data includes:

- TSF code of the LPAe, ensuring the protection of Profile data.

TSF Code

D.LPAe_TSF_CODE

LPAe code is an assets that has 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 56:

- 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].

Management data

D.LPAe_DEVICE_INFO

This asset includes the security-sensitive elements of Device Information data, such as the device type allocation code (TAC) or the device capabilities (ex. support for updating of certificate revocation lists (CRLs)), that is provided to the eUICC by the LPAe.

To be protected from unauthorized modification.

Keys

D.LPAe_KEYS

This asset contains the secret keys (corresponding to the asset D.SECRETS of Base-PP) used by the LPAe to perform platform management functions:

- session keys for the TLS connection (version 1.2 or greater) of LPDe to SM-DP+ along the interface ES9+;
- session keys for the TLS connection (version 1.2 or greater) of LDSe to SM-DS along the interface ES11.

All of these assets are to be protected from unauthorised disclosure and modification.

7.4.2 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.

7.4.2.1 Users

U.SM-DPplus

U.SM-DS

7.4.2.2 Subjects

S.LPAe

The LPAe is a functional element within the TOE that provides the LPDe, LDSe and LUIe features.

7.4.3 Threats

7.4.3.1 Unauthorized platform management

T.PLATFORM-MNG-INTERCEPTION-LPDe

An attacker alters or eavesdrops the transmission between the SM-DP+ and the LPDe on interface ES9+, in order to compromise the platform management process:

- namely, the delivery and the binding of a Profile Package for the eUICC;
- or, delivery of Notifications.

NB: the attacker may be an on-card application intercepting transmissions to the LPDe, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device.

Directly threatened assets: D.LPAe_KEYS, D.LPAe_PROFILE_*.

T.PLATFORM-MNG-INTERCEPTION-LDSe

An attacker alters or eavesdrops the transmission between the SM-DS and the LDSe on interface ES11, in order to compromise the discovery process:

- namely, the Event retrieval process between the LPAe and an SM-DS (Alternative SM-DS or Root SM-DS).

NB: the attacker may be an on-card application intercepting transmissions to the LDSe, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device.

Directly threatened assets: D.LPAe_KEYS.

T.UNAUTHORIZED-PLATFORM-MNG-LPAe

An on-card application:

- modifies or discloses LPAe data;
- executes or modifies operations from LPAe.

In particular, the following cases could happen:

- the Profile Metadata displayed at the LUIe to End User during enabling or disabling a profile could be compromised;
- the Activation Code or the Confirmation Code could be disclosed or modified while being entered at LUIe by End User;
- the Device Information could be modified before being sent to the eUICC causing:
  - a failure of the eligibility check for a profile, or
  - a downgrade of security parameters, such as indicating that the device does not support certificate revocation lists (CRLs).

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

Directly threatens the assets: D.LPAe_TSF_CODE, D.LPAe_PROFILE_*.

T.PROFILE-MNG-ELIGIBILITY-LPAe

An attacker alters the Device Information when provided from the LPAe to the eUICC, in order to compromise the eligibility of the eUICC, for example:

- o obtain an unauthorized profile by modifying the Device Info.

NB: the attacker may be an on-card application intercepting transmissions to the security domains.

Directly threatens the assets: D.LPAe_TSF_CODE, D.LPAe_DEVICE_INFO.

7.4.3.2 Second level threats

T.LOGICAL-ATTACK-LPAe

An on-card malicious application bypasses the Platform security measures by logical means, in order to disclose or modify sensitive data when they are processed by the LPAe.

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 asset: D.LPAe_*.

T.PHYSICAL-ATTACK-LPAe

An off-card actor discloses or modifies the design of the LPAe, 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.

The off-card actor has high attack potential. The off-card actor may be any actor using the external interfaces of the eUICC, whether they are intended to be used or not.
Directly threatens the assets: D.LPAe_*.

7.4.4 Assumptions

A.ACTORS-LPAe

SM-DP+ and SM-DS are actors of the infrastructure that securely manage their own credentials and otherwise sensitive data. More precisely, SM-DP+ and SM-DS are accredited by the GSMA's Security Accreditation Scheme for Subscription Management (SAS-SM). They secure the communication with the LPA (LPAd/LPAe) using TLS with server (e.g. SM-DP+, SM-DS) authentication.

This assumption extends the Base-PP assumption A.ACTORS.

7.5 Security Objectives

7.5.1 Security Objectives for the TOE

7.5.1.1 Platform support functions

O.SECURE-CHANNELS-LPAe

The eUICC shall maintain secure channels

between o LPAe and SM-DP+.

o LPAe and SM-DS.

The TOE shall ensure at any time:

- o that incoming messages are properly provided unaltered to the LPAe;
- 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 the PRE/PPI (see O.PRE-PPI).

O.INTERNAL-SECURE-CHANNELS-LPAe

The TOE ensures that the communication shared secrets transmitted from the ECASD to the LPAe are protected from unauthorized disclosure or modification.

This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment.

7.5.1.2 Data protection

O.DATA-CONFIDENTIALITY-LPAe

The TOE shall avoid unauthorised disclosure of the secret keys which are part of the keyset D.LPAe_KEYS.

Application Note 57:

Amongst the components of the TOE,

- o PRE, PPI and Telecom Framework must protect the confidentiality of the sensitive data they process, while
- o applications must use the protection mechanisms provided by the Runtime Environment.

This objective includes resistance to side channel attacks.

O.DATA-INTEGRITY-LPAe

The TOE shall avoid unauthorised modification of the following data when managed or manipulated by the TOE:

- o Keys:
  - D.LPAe

_KEYS; o

Profile

data:

- D.LPAe_PROFILE_USER_CODES,
- D.LPAe_PROFILE_DISPLAYED_ME

TADATA; o Management data:

- D.LPAe_DEVICE_INFO.

Application Note 58:

Amongst the components of the TOE,

- o PRE, PPI and Telecom Framework must protect the integrity of the sensitive data they process, while
- o applications must use the integrity protection mechanisms provided by the Runtime Environment.

7.5.2 Security Objectives for the Operational Environment

7.5.2.1 Actors

OE.SM-DPplus

OE.SM-DS

7.5.3 Security Objectives Rationale

7.5.3.1 Threats

Unauthorized platform management

T.PLATFORM-MNG-INTERCEPTION-LPDe The SM-DP+ transmits Profiles (Bound Profile Packages) to the LPAe (LPDe).

Consequently, the TSF ensures:

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

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

T.PLATFORM-MNG-INTERCEPTION-LDSe The SM-DS transmits Events to the LPAe (LDSe).

Consequently, the TSF ensures:

- o Security of the transmission to the (O.SECURE-CHANNELS-LPAe and O.INTERNAL- SECURE-CHANNELS-LPAe) by requiring authentication from SM-DS, 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-DS ensures that the credentials related to the secure channels will not be disclosed when used by off-card actors.

T.UNAUTHORIZED-PLATFORM-MNG-LPAe 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).

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-ELIGIBILITY-LPAe Device Info, transmitted by the LPAe to the eUICC for signature, is used by the SM-DP+ to perform the Eligibility Check prior to allowing profile download onto the eUICC.

Consequently, the TSF ensures:

- Security of the transmission among the LPAe and other security domains of the TOE (O.INTERNAL-SECURE-CHANNELS-LPAe) by protecting the transmission from unauthorized disclosure, modification and replay; These secure channel relies upon the underlying Runtime Environment, which protects the applications communications (OE.RE.SECURE-COMM).

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

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

Second level threats

T.LOGICAL-ATTACK-LPAe This threat is covered by controlling the information flow between the LPAe security domain and the platform layer 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 API of LPAe shall ensure atomic transactions (OE.IC.SUPPORT).

Whenever sensitive data of the TOE are processed by LPAe, 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 layer of the TOE, which are not protected by these mechanisms. Consequently,

- the TOE itself must ensure the correct operation of the Platform layer (PRE, PPI, and Telecom Framework (O.OPERATE)), and
- the Platform layer must protect the confidentiality and integrity of the sensitive data it processes, 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 LPAe (OE.RE.CODE-EXE),
- compliance to security guidelines for applications (OE.APPLICATIONS).

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

7.5.3.2 Assumptions

A.ACTORS-LPAe This assumption is upheld by objectives OE.SM-DPplus and OE.SM-DS which ensure that credentials and otherwise sensitive data will be managed correctly by this actors of the infrastructure.

7.5.3.3 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.PLATFORM-MNG-INTERCEPTION-LPDe	OE.RE.SECURE-COMM, OE.SM-DPplus, O.SECURE- CHANNELS-LPAe, O.INTERNAL-SECURE-CHANNELS- LPAe	Section 7.5.3
T.PLATFORM-MNG-INTERCEPTION-LDSe	OE.RE.SECURE-COMM, OE.SM-DS, O.SECURE-CHANNELS-LPAe, O.INTERNAL-SECURE-CHANNELS- LPAe	Section 7.5.3
T.UNAUTHORIZED-PLATFORM-MNG-LPAe	OE.APPLICATIONS, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	Section 7.5.3
T.PROFILE-MNG-ELIGIBILITY-LPAe	OE.RE.SECURE-COMM, O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-INTEGRITY-LPAe, OE.SM- DPplus, OE.RE.DATA-INTEGRITY	Section 7.5.3
T.LOGICAL-ATTACK- LPAe	O.OPERATE, O.API, OE.RE.API, OE.RE.CODE-EXE, OE.APPLICATIONS, O.DATA-CONFIDENTIALITY- LPAe, O.DATA-INTEGRITY-LPAe, OE.IC.SUPPORT, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA- INTEGRITY	Section 7.5.3
T.PHYSICAL-ATTACK- LPAe	O.DATA-CONFIDENTIALITY-LPAe, OE.IC.SUPPORT, OE.IC.RECOVERY, OE.RE.DATA-CONFIDENTIALITY	Section 7.5.3

Table 12 Threats and Security Objectives – Coverage

Security Objectives	Threats
O.SECURE-CHANNELS-LPAe	T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PLATFORM-MNG-INTERCEPTION-LDSe
O.INTERNAL-SECURE-CHANNELS-LPAe	T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PLATFORM-MNG-INTERCEPTION-LDSe, T.PROFILE-MNG-ELIGIBILITY-LPAe
O.DATA-CONFIDENTIALITY- LPAe	T.LOGICAL-ATTACK-LPAe, T.PHYSICAL- ATTACK-LPAe
O.DATA-INTEGRITY-LPAe	T.PROFILE-MNG-ELIGIBILITY-LPAe, T.LOGICAL-ATTACK-LPAe
OE.SM-DPplus	T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PROFILE-MNG-ELIGIBILITY-LPAe

OE.IC.SUPPORT	T.LOGICAL-ATTACK-LPAe, T.PHYSICAL- ATTACK-LPAe
OE.IC.RECOVERY	T.PHYSICAL-ATTACK-LPAe
OE.RE.SECURE-COMM	T.PLATFORM-MNG-INTERCEPTION-LPDe, T.PLATFORM-MNG-INTERCEPTION-LDSe, T.PROFILE-MNG-ELIGIBILITY-LPAe
OE.RE.API	T.LOGICAL-ATTACK-LPAe
OE.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PLATFORM-MNG-LPAe, T.LOGICAL-ATTACK-LPAe, T.PHYSICAL- ATTACK-LPAe
OE.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PLATFORM-MNG-LPAe, T.PROFILE-MNG-ELIGIBILITY-LPAe, T.LOGICAL-ATTACK-LPAe
OE.RE.CODE-EXE	T.LOGICAL-ATTACK-LPAe
OE.APPLICATIONS	T.UNAUTHORIZED-PLATFORM-MNG-LPAe, T.LOGICAL-ATTACK-LPAe
OE.SM-DS	T.PLATFORM-MNG-INTERCEPTION-LDSe

Table 13 Security Objectives and Threats – Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.ACTORS-LPAe	OE.SM-DS	Section 7.5.3

Table 14 Assumptions and Security Objectives for the Operational Environment – Coverage

Security Objectives for the Operational Environment	Assumptions
OE.SM-DS	A.ACTORS-LPAe

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

7.6 Extended Requirements

7.6.1 Extended Families

7.6.1.1 Extended Family FPT_EMS - TOE Emanation

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.

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.

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.

7.7 Security Requirements

In order to define the Security Functional Requirements, Part 2 of the Common Criteria was used.

Some Security Functional Requirements have been refined. The refinements are described below the associated SFR. The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. These refinements are interpretation refinement, and are described as an extra paragraph, starting with the word “Refinement”.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are italicised.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as bold text. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are italicised.

In some other cases the assignment made by the PP authors defines an assignment to be performed by the ST author. Thus this text is both bold and italicized (see for example the SFR FIA_UID.1/LPAe).

The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

7.7.1 Security Functional Requirements

7.7.1.1 Introduction

This Protection Profile module defines the following security policy:

- LPAe information flow control SFP.

All roles used in the security policy are defined either as users or subjects in sections 3.2 and
7.4.2. 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.

This PP-Module only refers to remote users (U.SM-DS and U.SM-DPplus).

LPAe information flow control SFP

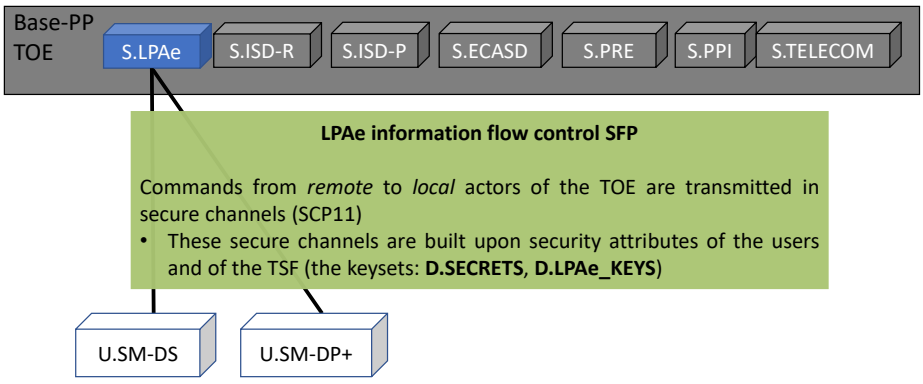


Figure 20: LPAe Information flow control SFP

Security attributes used in SFRs for the LPAe module

Security attribute	Details	Relationship to assets
LPAe session keys (D.LPAe_KEYS)	The session keys for the TLS connection (version 1.2 or greater) between LPAe and SM-DP+ and SM-DS.	This asset is described in section 7.4.1.2 Keys.
CERT.DSauth.E CDSA CERT.DS.TLS CERT.DP.TLS	Certificates of U.SM-DS and U.SM-DPplus that are used by the TOE to authenticate this user. These certificates are issued by the eSIM CA. The TOE can verify this certificate using the eSIM CA public key.	These attributes are not assets of this Protection profile. The eSIM CA public key is described as the asset D.PK.CI.ECDSA in section 3.1.2.3 Identity management data.
SM-DS OID(s)	SM-DS OID is the identification Root SM-DS. The Root SM-DS address(es) are unique and filled in the eUICC. The Root SM-DS(s) are configured at the time of Device manufacture and is invariant.	These attribute is included in the D.PLATFORM_DATA described in section 3.1.2.2 Management data.

Table 16 Definition of the security attributes of LPAe module

7.7.1.2 Identification and Authentication

This package describes the identification and authentication measures of

the TOE: The TOE must:

- identify the remote user U.SM-DS by its SM-

DS OID. The TOE must:

- authenticate U.SM-DS using CERT.DSauth.ECDSA.

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

- U.SM-DPplus is bound to S.LPAe,
- U.SM-DS is bound to S.LPAe.

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

FIA_UID.1/LPAe Timing of identification

FIA_UID.1.1/LPAe 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/LPAe The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note 59:

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

- U.SM-DPplus
- U.SM-DS.

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/LPAe Timing of authentication

FIA_UAU.1.1/LPAe 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/LPAe The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 60:

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

- U.SM-DPplus
- U.SM-DS.

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 [24]:

- A U.SM-DPplus must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.DPauth.ECDSA, CERT.DPpb.ECDSA and CERT.DP.TLS), as well as the public key of the eSIM CA (D.PK.CI.ECDSA).
- A U.SM-DS must be authenticated by verifying its ECDSA signature, using the public keys included in its certificates (CERT.DSauth.ECDSA and CERT.DS.TLS), as well as the public key of the eSIM CA (D.PK.CI.ECDSA).

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with at least one of the elliptic curves referenced for that

purpose in SGP.22 [24].

FIA_USB.1/LPAe User-subject binding

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

- **SM-DP+ OID is associated to S.LPAe, acting on behalf of U.SM-DPplus**
- **SM-DS OID is associated to S.LPAe, acting on behalf of U.SM-DS**.

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

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

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

- **change of SM-DP+ OID requires U.SM-DPplus to be authenticated via "CERT.DPauth.ECDSA"**
- **change of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA"**.

Application Note 61:

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

- U.SM-DPplus binds to a subject (S.LPAe)
- U.SM-DS binds to a subject (S.LPAe)

FIA_UAU.4/LPAe Single-use authentication mechanisms

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

- **U.SM-DPplus**
- **U.SM-DS**.

Application Note 62:

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

- U.SM-DPplus
- U.SM-DS

FIA_ATD.1/LPAe User attribute definition

FIA_ATD.1.1/LPAe The TSF shall maintain the following list of security attributes

belonging to individual users:

- o **CERT.DP.TLS belonging to U.SM-DPplus**
- o **CERT.DSauth.ECDSA, CERT.DS.TLS, and SM-DS OID belonging to U.SM- DS**.

7.7.1.3 Comminication

This package describes how the TSF shall protect communications with external

users. The TSF shall enforce secure channels (FTP_ITC.1/LPAe and

FTP_ITC.2/LPAe):

- between U.SM-DPplus and S.LPAe
- between U.SM-DS and S.LPAe

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/LPAe).

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

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

- generation and deletion of D.LPAe_KEYS and certificates (FCS_CKM.1/SCP-SM, FCS_CKM.6/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.6/SCP-MNO, FCS_CKM.1/LPAe and FCS_CKM.6/LPAe).

FDP_IFC.1/LPAe Subset information flow control

FDP_IFC.1.1/LPAe The TSF shall enforce the **LPAe information flow control SFP**

on o **users/subjects:**

- **U.SM-DPplus and S.LPAe**
- **U.SM-DS and S.LPAe**

- o **information: transmission of commands**.

FDP_IFF.1/LPAe Simple security attributes

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

- o **users/subjects:**
  - **U.SM-DPplus and S.LPAe, with security attribute D.LPAe_KEYS**
  - **U.SM-DS and S.LPAe, with security attribute D.LPAe_KEYS**
- o **information: transmission of commands**.

FDP_IFF.1.2/LPAe The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

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

FDP_IFF.1.4/LPAe 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/LPAe The TSF shall explicitly deny an information flow based on the following rules:

- **The TOE shall reject communication between U.SM-DPplus and S.LPAe if it is not performed in a TLS secure channel;**
- **The TOE shall reject communication between U.SM-DS and S.LPAe if it is not performed in a TLS secure channel**.

Application Note 63:

More details on the secure channels can be found in SGP.22 [24]

- For SM-DP+: Section 5.6
- For SM-DS: Section 5.8

FTP_ITC.1/LPAe Inter-TSF trusted channel

FTP_ITC.1.1/LPAe 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/LPAe The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/LPAe The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application Note 64:

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 [24]:

- The secure channels from the LPAe to SM-DP+ and SM-DS must be TLS with server authentication

Related keys are generated on-card (D.LPAe_KEYS); see FCS_CKM.1/LPAe.

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 LPAe to open a TLS secure channel to SM-DP+ and transmit the following operations:
  - ES9+.InitiateAuthentication
  - ES9+.GetBoundProfilePackage
  - ES9+.AuthenticateClient
  - ES9+.HandeNotification
  - ES9+.CancelSession
- The TSF shall permit the LPAe to open a TLS secure channel to SM-DS and transmit the following operations:
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient

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

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

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

FDP_ITC.2.3/LPAe 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/LPAe 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/LPAe 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/LPAe Inter-TSF basic TSF data consistency

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

- **Commands from U.SM-DPplus and U.SM-DS**
- **Downloaded objects from U.SM-DPplus**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/LPAe 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 65:

The commands related to the SFRs FPT_TDC.1/LPAe, FDP_IFC.1/LPAe, FDP_IFF.1/LPAe and the Downloaded objects related to this SFR FPT_TDC.1/LPAe

are listed below:

- SM-DP+ commands
  - ES9+.InitiateAuthentication
  - ES9+.GetBoundProfilePackage
  - ES9+.AuthenticateClient
  - ES9+.HandeNotification
  - ES9+.CancelSession
- Downloaded objects from SM-DP+
  - Session keys
  - Bound Profile Package
- SM-DS commands
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient

FDP_UCT.1/LPAe Basic data exchange confidentiality

FDP_UCT.1.1/LPAe The TSF shall enforce the **LPAe information flow control SFP** to receive user data in a manner protected from unauthorised disclosure.

Application Note 66:

This SFR is related to the protection of:

- Bound Profile Packages downloaded from SM-DP+.

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 [24]: 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 generated on-card (D.LPAe_KEYS); see FCS_CKM.1/LPAe for further details.

FDP_UIT.1/LPAe Data exchange integrity

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

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

Application Note 67:

This SFR is related to the protection of:

- Bound Profile Packages downloaded from SM-DP+;

- Commands received from to SM-DP+ and SM-DS.

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 [24]: 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 and a MAC length of 64 bits.

Related keys are generated on-card (D.LPAe_KEYS); see FCS_CKM.1/LPAe for further details.

FCS_CKM.1/LPAe Cryptographic key generation

FCS_CKM.1.1/LPAe The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curves Key Agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following:

[**assignment**: *at least one elliptic curve referenced in SGP.22 [24]*]

Application Note 68:

This key generation mechanism is used to generate:

- D.LPAe_KEYS keys.

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

FCS_CKM.4/LPAe Cryptographic key destruction

FCS_CKM.6/LPAe Cryptographic key destruction

FCS_CKM.6.1/LPAe The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction*]].

FCS_CKM.6.2/ LPAe The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/LPAe in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note 69:

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

- D.LPAe_KEYS.

7.7.1.4 Security management

This package includes several supporting security functions:

- User data and TSF self-protection measures: o TOE emanation (FPT_EMS.1/LPAe)
  - o protection from integrity errors (FDP_SDI.1/LPAe)
  - o residual data protection (FDP_RIP.1/LPAe)
- Security management measures:
  - o Management of roles (FMT_SMR.1/LPAe) and function (FMT_SMF.1/LPAe)

FPT_EMS.1/LPAe TOE Emanation

FPT_EMS.1.1/LPAe The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to

- o **D.LPAe_KEYS**

and [assignment: *list of types of user data*].

FPT_EMS.1.2/LPAe The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to

- o **D.LPAe_KEYS**

and [assignment: *list of types of user data*].

Application Note 70:

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/LPAe Stored data integrity monitoring

FDP_SDI.1.1/LPAe 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 following assets that require to be protected against unauthorized modification:

- o Profile data

- D.LPAe_PROFILE_USER_CODES
- D.LPAe_PROFILE_DISPLAYED_M

ETADATA o Management data

- D.LPAe_DEVIC

E_INFO o Keys

- LPAe_KEYS

FDP_RIP.1/LPAe Subset residual information protection

FDP_RIP.1.1/LPAe 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.LPAe_KEYS.**

FMT_SMF.1/LPAe Specification of Management Functions

FMT_SMF.1.1/LPAe 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/LPAe Security roles

FMT_SMR.1.1/LPAe The TSF shall maintain the roles

- **External users:**
  - **U.SM-DS**
- **Subjects:**
  - **S.LPAe**.

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

Application Note 71:

The roles defined here correspond to the users and subjects defined in Section 3.2

7.7.2 Security Assurance Requirements

There are no new SARs stated for this PP-Module, since the Base-PP SARs suffice to cover all SFRs.

7.7.3 Security Requirements Rationale

7.7.3.1 Objectives

Security objectives for the TOE

Platform support functions

O.SECURE-CHANNELS-LPAe All SFRs relative to the ES9+ and ES11 interfaces (FDP_IFC.1/LPAe, FDP_IFF.1/LPAe, FTP_ITC.1/LPAe, FDP_ITC.2/LPAe, FPT_TDC.1/LPAe, FDP_UCT.1/LPAe, FDP_UIT.1/LPAe, FCS_CKM.1/LPAe, FCS_CKM.4/LPAe) cover

this security objective by enforcing the LPAe information flow control SFP that ensures that transmitted commands and data are protected from unauthorized disclosure and modification.

Identification and authentication SFRs (FIA_UID.1/LPAe, FIA_UAU.1/LPAe, FIA_USB.1/LPAe, FIA_UAU.4/LPAe) support this security objective by requiring authentication and identification from the distant SM-DP+ and SM-DS in order to establish these secure channels.

FIA_ATD.1/LPAe, 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/LPAe and FMT_SMR.1/LPAe support these SFRs by providing management of roles and management of functions.

O.INTERNAL-SECURE-CHANNELS-LPAe FPT_EMS.1/LPAe ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks. This includes in particular secrets (asset D.SECRETS) if transmitted between ECASD and LPAe.

FDP_SDI.1/LPAe ensures that the secrets cannot be modified during this transmission. FDP_RIP.1/LPAe ensures that the secrets cannot be recovered from deallocated resources.

Data protection

O.DATA-CONFIDENTIALITY-LPAe FDP_UCT.1/LPAe addresses the reception of data from off-card actor.

FPT_EMS.1/LPAe ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks.

FDP_RIP.1/LPAe ensures that no residual confidential data is available.

O.DATA-INTEGRITY-LPAe FDP_UIT.1/LPAe addresses the reception of data from off-card actors.

FDP_SDI.1/LPAe specifies the data that is monitored in case of an integrity breach.

7.7.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.SECURE-CHANNELS- LPAe	FMT_MSA.1/CERT_KEYS, FMT_SMF.1/LPAe, FMT_SMR.1/LPAe, FIA_UID.1/LPAe, FIA_UAU.1/LPAe, FIA_USB.1/LPAe, FIA_UAU.4/LPAe, FIA_ATD.1/LPAe, FDP_IFF.1/LPAe, FTP_ITC.1/LPAe, FDP_ITC.2/LPAe, FPT_TDC.1/LPAe, FDP_UIT.1/LPAe, FCS_CKM.1/LPAe, FCS_CKM.4/LPAe, FDP_IFC.1/LPAe, FDP_UCT.1/LPAe, FIA_ATD.1, FMT_MSA.3	Section 7.7.3.1
O.INTERNAL-SECURE-CHANNELS-LPAe	FPT_EMS.1/LPAe, FDP_SDI.1/LPAe, FDP_RIP.1/LPAe	Section 7.7.3.1
O.DATA-CONFIDENTIALITY-	FPT_EMS.1/LPAe, FDP_RIP.1/LPAe,	Section 7.7.3.1

LPAe	FDP_UCT.1/LPAe	
O.DATA-INTEGRITY-LPAe	FDP_SDI.1/LPAe, FDP_UIT.1/LPAe	Section 7.7.3.1

Table 17 Security Objectives and SFRs – Coverage

Security Functional Requirements	Security Objectives
FIA_ATD.1	O.SECURE-CHANNELS-LPAe
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS-LPAe
FMT_SMF.1/LPAe	O.SECURE-CHANNELS-LPAe
FMT_MSA.3	O.SECURE-CHANNELS-LPAe
FIA_UID.1/LPAe	O.SECURE-CHANNELS-LPAe
FIA_UAU.1/LPAe	O.SECURE-CHANNELS-LPAe
FIA_USB.1/LPAe	O.SECURE-CHANNELS-LPAe
FIA_UAU.4/LPAe	O.SECURE-CHANNELS-LPAe
FIA_ATD.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_IFC.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_IFF.1/LPAe	O.SECURE-CHANNELS-LPAe
FTP_ITC.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_ITC.2/LPAe	O.SECURE-CHANNELS-LPAe
FPT_TDC.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_UCT.1/LPAe	O.SECURE-CHANNELS-LPAe, O.DATA- CONFIDENTIALITY-LPAe
FDP_UIT.1/LPAe	O.SECURE-CHANNELS-LPAe, O.DATA- INTEGRITY-LPAe
FCS_CKM.1/LPAe	O.SECURE-CHANNELS-LPAe
FCS_CKM.4/LPAe	O.SECURE-CHANNELS-LPAe
FPT_EMS.1/LPAe	O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-CONFIDENTIALITY-LPAe
FDP_SDI.1/LPAe	O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-INTEGRITY-LPAe
FDP_RIP.1/LPAe	O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-CONFIDENTIALITY-LPAe
FMT_SMR.1/LPAe	O.SECURE-CHANNELS-LPAe

Table 18 SFRs and Security Objectives

7.7.3.3 Dependecies

7.7.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies

FIA_UID.1/LPAe	No Dependencies	
FIA_UAU.1/LPAe	(FIA_UID.1)	FIA_UID.1/LPAe
FIA_USB.1/LPAe	(FIA_ATD.1)	FIA_ATD.1/LPAe
FIA_UAU.4/LPAe	No Dependencies	
FIA_ATD.1/LPAe	No Dependencies	
FDP_IFC.1/LPAe	(FDP_IFF.1)	FDP_IFF.1/LPAe
FDP_IFF.1/LPAe	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/LPAe
FTP_ITC.1/LPAe	No Dependencies	
FDP_ITC.2/LPAe	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/LPAe, FTP_ITC.1/LPAe, FPT_TDC.1/LPAe
FPT_TDC.1/LPAe	No Dependencies	
FDP_UCT.1/LPAe	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/LPAe, FTP_ITC.1/LPAe
FDP_UIT.1/LPAe	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/LPAe, FTP_ITC.1/LPAe
FCS_CKM.1/LPAe	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_CKM.3) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1 {Either by composition or claim in ST} {*Discarded – No Key Access Interface exists}* FCS_RNG.1 FCS_CKM.6/LPAe
FCS_CKM.6/LPAe	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/LPAe
FPT_EMS.1/LPAe	No Dependencies	
FDP_SDI.1/LPAe	No Dependencies	
FDP_RIP.1/LPAe	No Dependencies	
FMT_SMF.1/LPAe	No Dependencies	
FMT_SMR.1/LPAe	(FIA_UID.1)	FIA_UID.1/LPAe

Table 19 SFRs Dependencies

Rationale for the exclusion of Dependencies

8 LPAe PP-configuration

8.1 Reference

Title:	LPAe Configuration for eUICC for Consumer Devices Protection Profile
Author:	GSMA
Editor:	GSMA
Reference:	SGP.25.Base+LPAe
Version:	3.0
CC Version:	CC:2022 release 1
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General Status:	Complete
Keywords:	eUICC, Consumer Devices, Remote SIM Provisioning

8.2 Components statement

This PP-Configuration is identified as: *LPAe Configuration for eUICC for Consumer Devices Protection Profile*., version 3.0 and defined in the current section 8.

This configuration has one single Base-PP: *eUICC for Consumer and IoT Devices Protection Profile*, version 3.0 and defined in the current document's sections 1 to 6.

This configuration consists of the Base-PP together with the PP-Module *LPAe Module for eUICC for Consumer Devices Protection Profile*, version 3.0 and defined in the current document's section 7.

8.3 Conformance statement

This Protection Profile requires demonstrable conformance (as defined in [37]) of any ST or PP claiming conformance to this PP Configuration.

8.4 SAR statement

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

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

ADV_ARC.1 is refined to add a particular set of verifications on top of the existing requirement.

9 IPAe PP-module

9.1 Introduction

9.1.1 PP-Module Identification

Title:	IPAe Module for eUICC for IoT Devices Protection Profile
Base-PP:	eUICC for Consumer and IoT Devices Protection Profile
Author:	GSMA
Editor:	GSMA
Reference:	SGP.25.IPAe
Version:	3.0
CC Version:	CC:2022 release 1
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General Status:	Complete
Keywords:	eUICC, IoT Devices, Remote SIM Provisioning

9.1.2 Base-PP

The base protection profile for this PP-module is *eUICC for Consumer and IoT Devices Protection Profile* described in the sections 1–6 of this document.

9.1.3 TOE Overview

The TOE of this PP-Module is the embedded IoT Profile Assistant (IPAe) which provides multiple distinc functions: the Profile Download, the Discovery Service, the Notification Handling, Conveying PSMO, eCO and related results. IPAe is part of the Application Layer.

9.1.3.1 TOE type and TOE major security features

The TOE type of this PP-Module is software.
This PP-Module only includes the brick showed (in blue) on the figure hereafter

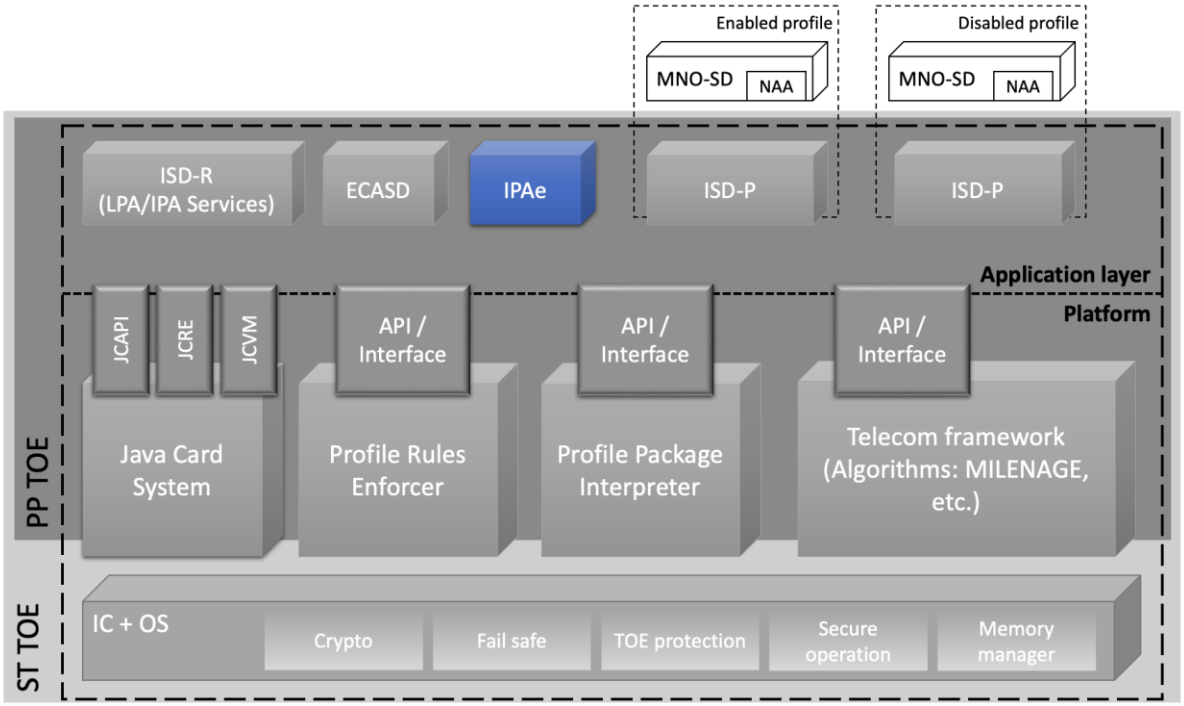


Figure 21 Scope of the TOE

Application Layer

IPAe

IPAe is a unit of the Application layer. It has the same functions as the (optional) non-TOE on-device unit IPAd.

The technical implementation of IPAe is up to the EUM. For example, the IPAe may be a feature of the ISD-R.

The IPAe can use the eUICC Rules Authorisation Table (RAT) to determine whether or not a Profile containing Profile Policy Rules (PPRs) is authorised to be installed on the eUICC.

9.1.3.2 TOE life-cycle

The IPAe software unit is added at Phase C of the eUICC life-cycle (see Section 1.2.3.1).

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

TOE interfaces

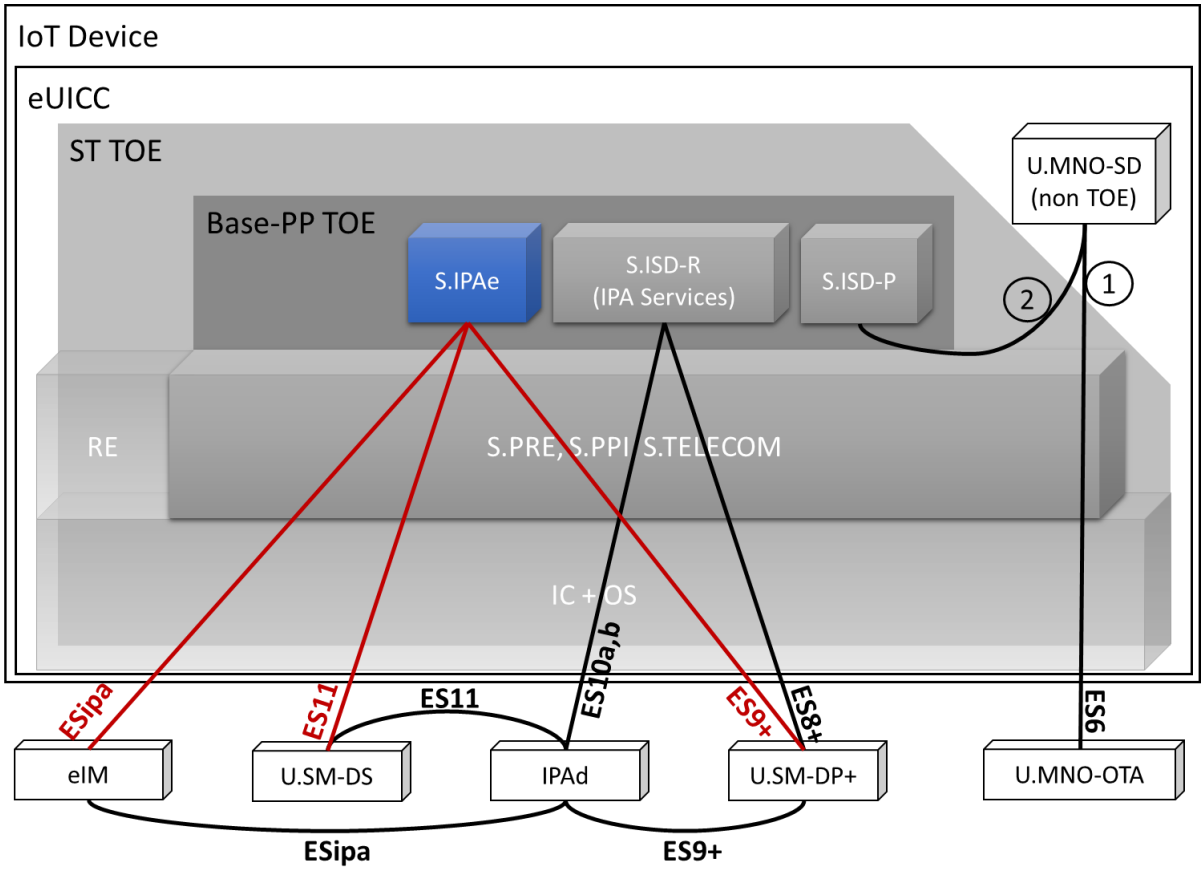


Figure 22 TOE interfaces

As shown on Figure 21, the TOE (shown in blue) has the following interfaces (shown in red):

- With the provisioning infrastructure, consisting in eIM, SM-DS and SM-DP+ (identified ESipa, ES11 and ES9+ in [36]).

Description of Non-TOE HW/FW/SW and systems

This PP module inherits all of the non-TOE components of the Base-PP (see Section 1.2.4.2), i.e., the following components: IC, IPAd, ES, Runtime Environment, IoT Device, MNO- SD and applications, a Remote provisioning infrastructure.

In addition to the above inherited components, this PP module also interacts with the non-TOE system *IPAe remote provisioning infrastructure*, described in the next subsection.

9.1.3.4 IPAe remote provisioning infrastructure

The following figure describes the communication channels of the architecture when the IPA is located in the eUICC.

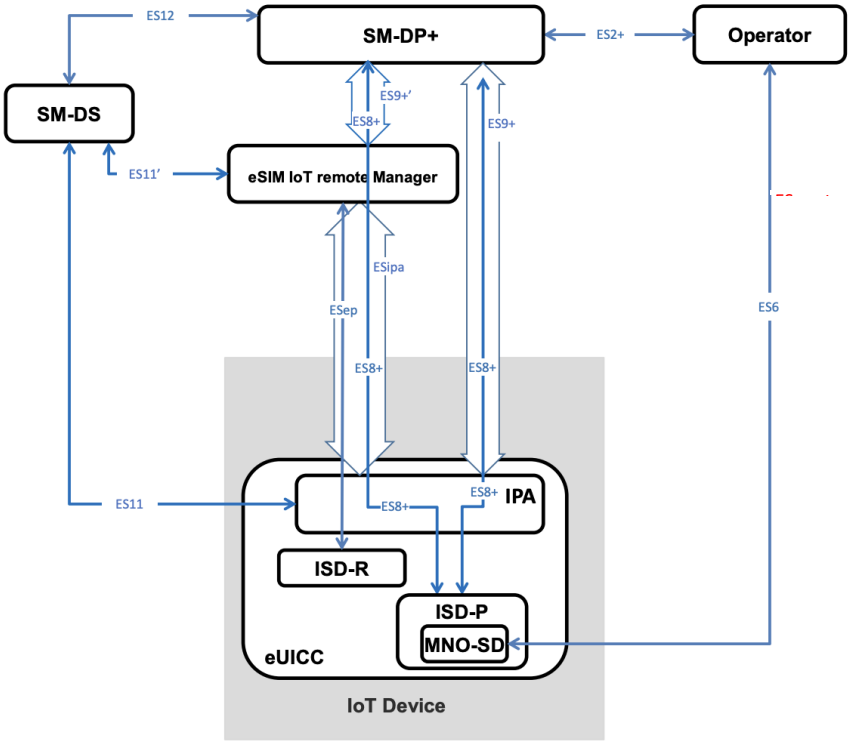


Figure 23 Remote Provisioning System, IPA in the eUICC

The TOE communicates with remote servers of:

- SM-DS, which provides mechanisms for discovery of SM-DP+s;
- SM-DP+, which provides Platform and Profile management commands as well as Profiles.
- eIM, which is responsible for remote Profile State Management Operations (PSMO) on a single IoT Device or a fleet of IoT Devices.

The TOE SHALL require the use of secure channels for these interfaces. The keys and certificates required for these operations on the TOE are exchanged/generated during operational use of the TOE. Identities (in terms of certificates) rely on a root of trust called the eSIM CA, 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.

9.1.4 Summary of the security problem

9.1.4.1 High-level view of threats

The threats considered in this PP-Module correspond to the high-level scenarios described hereafter.

“First-level” threats: Unauthorised Platform Management

These first-level threats arise when the secure links to the IPAe are compromised:

- An attacker alters or eavesdrops the transmission between eUICC and SM-DP+ (link ES9+), in order to compromise the platform management process.
- An attacker alters or eavesdrops the transmission between eUICC and SM-DS (link ES11), in order to compromise the discovery process.
- An attacker alters or eavesdrops the transmission between eUICC and eIM

(ESipa), in order to compromise eIM Profile downloads.

- An on-card application:
  - modifies or discloses IPAe data;
  - executes or modifies operations from IPAe.

“Second-level” threats

Logical attacks

An on-card malicious application bypasses the platform security measures by logical means, in order to disclose or modify sensitive data when they are processed by the Platform.

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.

9.1.4.2 Physical attacks

The attacker discloses or modifies the design of the IPAe, 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.

9.2 Consistency Rationale

The TOE of this PP-Module consists of a new element in the Application Layer, IPAe (Figure 20). No Base-PP TOE component is changed by this PP-Module.
The TOE-external interfaces of this PP-Module are the three interfaces, ES9+, ES11 and ESipa, which do not exist in the Base-PP (Figure 21). No Base-PP interface is changed by this PP-Module.

Also, the life-cycle of the Base-PP TOE is not changed by this PP-Module.

The union of the Security Problem Definition of this PP-Module (Section 9.4) and the Security Problem Definition of the Base-PP (Section 3) does not lead to a contradiction:

- This PP-Module only adds new assets to the existing assets of the Base-PP;
- This PP-Module only adds a new user (U.SM-DS) and a new subject (S.IPAe) to the existing ones of the Base-PP;
- This PP-Module only adds one new assumption (A.ACTORS-IPAe) to the existing assumptions of the Base-PP, and the new assumption is disjoint from the Base-PP assumption A.ACTORS because it only refers to the user U.SM-DS that does not exist in the Base-PP;
- This PP-Module only adds new threats to the existing threats of the Base-PP. Moreover, the new threats exclusively threaten the PP-Module assets, they do not refer to assets of the Base-PP.

The union of the Security Objectives of this PP-Module (Section 9.5) and the Security Objectives of the Base-PP (Section 4) does not lead to a contradiction:

- As it can be seen from the coverage table Table 13, all Objectives from the PP-Module only cover the proper Threats of the PP-Module, and not the Threats of the Base-PP.

- The PP-Module Objectives only concern assets, subjects, and interfaces (ES9+, ES11, and ESipa) which are proper to the PP-Module, that is, they do not exist in the Base-PP.

Note that some Threats of the PP-Module are also covered by Objectives which already exist in the Base-PP, as can be seen from Table 12.

The union of the SFRs for this PP-Module (Section 9.6) and the SFRs for the Base-PP (Section 7) do not lead to a contradiction:

- This PP-Module only defines a new SFP (IPAe information flow control), for the interfaces that do not exist in the Base-PP (ES9+, ES11, and ESipa).
- Although there are some PP-Module Objectives that also need Base-PP SFRs to be covered (Table 17), the PP-Module SFRs only cover PP-Module Objectives (Table 18),
  i.e. PP-Module SFRs are separate refinements of SFRs and do not override Base-PP SFRs.
- Moreover, Base-PP SFRs do not depend on PP-Module SFRs, as it can be seen from Table 10.

There are no new SARs stated for this PP-Module, since the Base-PP SARs suffice to cover all SFRs.

9.3 Conformance Claims

This protection Profile module is conformant to Common Criteria 2022 release 1.

This protection Profile is conformant to:

- CC Part 1 [37],
- CC Part 2 [38] (conformant),
- CC Part 3 [39] (conformant),
- CC Part 5 [40].

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

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

The following assurance requirement augmentation is optional but suggested:

- ALC_FLR.2 Flaw Reporting Procedures.

ADV_ARC is refined to add a particular set of verifications on top of the existing requirement. This PP does not claim conformance to any other PP.

9.3.1 Conformance Claims to this PP

This Protection Profile module requires demonstrable conformance (as defined in [37]) of any ST or PP claiming conformance to this PP.

9.4 Security Problem Definition

9.4.1 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].

9.4.1.1 User data

IPAe does not handle user data.

9.4.1.2 TSF data

The TSF data includes:

- TSF code of the IPAe, ensuring the protection of Profile data.

TSF Code

D.IPAe_TSF_CODE

IPAe code is an assets that has 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 72:

- 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].

Management data

D.IPAe_DEVICE_INFO

This asset includes the security-sensitive elements of Device Information data, such as the device type allocation code (TAC) or the device capabilities (ex. support for updating of certificate revocation lists (CRLs)), that is provided to the eUICC by the IPAe.

To be protected from unauthorized modification.

Keys

D.IPAe_KEYS

This asset contains the secret keys (corresponding to the asset D.SECRETS of Base-PP) used by the IPAe to perform platform management functions:

- session keys for the TLS connection (version 1.2 or greater) of IPAe to SM-DP+ along the interface ES9+;
- session keys for the TLS connection (version 1.2 or greater) of IPAe to SM-DS along the interface ES11.
- session keys for the TLS or DTLS connection (version 1.2 or 1.3) of IPAe to

eIM along the interface ESipa.

All of these assets are to be protected from unauthorised disclosure and modification.

9.4.2 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.

9.4.2.1 Users

U.SM-DS

Role that securely performs functions of discovery.

9.4.2.2 Subjects

S.IPAe

The IPAe is a functional element within the TOE that provides profile download and discovery services features.

9.4.3 Threats

9.4.3.1 Unauthorized platform management

T.PLATFORM-MNG-INTERCEPTION-IPAe

An attacker alters or eavesdrops the transmission between the SM-DP+, SM-DS and eIM and the IPAe on respective interfaces ES9+, ES11 and ESipa, in order to compromise the platform management process:

- the delivery and the binding of a Profile Package for the eUICC;
- or, the event retrieval process between the IPAe and an SM-DS (Alternative SM-DS or Root SM-DS).
- or, the retrieval of profiles from the eIM,
- or, delivery of Notifications.

NB: the attacker may be an on-card application intercepting transmissions to the IPAe, or an off-card actor intercepting OTA transmissions or interface between the eUICC and the Device.

Directly threatened assets: D.IPAe_KEYS.

T.UNAUTHORIZED-PLATFORM-MNG-IPAe

An on-card application:

- modifies or discloses IPAe data;
- executes or modifies operations from IPAe.

In particular, the following cases could happen:

- the Device Information could be modified before being sent to the eUICC causing:
  - a failure of the eligibility check for a Profile, or
  - a downgrade of security parameters, such as indicating that the Device does not support certificate revocation lists (CRLs).

Such a threat typically includes for example:

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

Directly threatens the assets: D.IPAe_TSF_CODE.

T.PROFILE-MNG-ELIGIBILITY-IPAe

An attacker alters the Device Information when provided from the IPAe to the eUICC, in order to compromise the eligibility of the eUICC, for example:

- obtain an unauthorized profile by modifying the Device Info.

NB: the attacker may be an on-card application intercepting transmissions to the security domains.

Directly threatens the assets: D.IPAe_TSF_CODE, D.IPAe_DEVICE_INFO.

9.4.3.2 Second level threats

T.LOGICAL-ATTACK-IPAe

An on-card malicious application bypasses the Platform security measures by logical means, in order to disclose or modify sensitive data when they are processed by the IPAe.

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 asset: D.IPAe_TSF_CODE, D.IPAe_DEVICE_INFO, D.IPAe_IPAe_KEYS.

T.PHYSICAL-ATTACK-IPAe

An off-card actor discloses or modifies the design of the IPAe, 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.

The off-card actor has high attack potential. The off-card actor may be any actor using the external interfaces of the eUICC, whether they are intended to be used or not.

Directly threatens the assets: D.IPAe_TSF_CODE, D.IPAe_DEVICE_INFO, D.IPAe_IPAe_KEYS

9.4.4 Assumptions

A.ACTORS-IPAe

SM-DP+, SM-DS and eIM are actors of the infrastructure that securely manage their own credentials and otherwise sensitive data. More precisely, SM-DP+ and SM-DS

are accredited by the GSMA's Security Accreditation Scheme for Subscription Management (SAS-SM). They secure the communication with the IPA (IPAd/IPAe) using TLS/DTLS, or equivalent, with server (e.g. SM-DP+, SM-DS) authentication.

This assumption extends the Base-PP assumption A.ACTORS.

9.5 Security Objectives

9.5.1 Security Objectives for the TOE

9.5.1.1 Platform support functions

O.SECURE-CHANNELS-IPAe

The eUICC shall maintain secure channels

between o IPAe and SM-DP+.

- o IPAe and SM-DS.
- o IPAe and eIM.

The TOE shall ensure at any time:

- o that incoming messages are properly provided unaltered to the IPAe;
- 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 the PRE/PPI (see O.PRE-PPI).

O.INTERNAL-SECURE-CHANNELS-IPAe

The TOE ensures that the communication shared secrets transmitted from the ECASD to the IPAe are protected from unauthorized disclosure or modification.

This protection mechanism shall rely on the communication protection measures provided by the Runtime Environment.

9.5.1.2 Data protection

O.DATA-CONFIDENTIALITY-IPAe

The TOE shall avoid unauthorised disclosure of the secret keys which are part of the keyset D.IPAe_KEYS.

Application Note 73:

Amongst the components of the TOE,

- o PRE, PPI and Telecom Framework must protect the confidentiality of the sensitive data they process, while
- o applications must use the protection mechanisms provided by the Runtime Environment.

This objective includes resistance to side channel attacks.

O.DATA-INTEGRITY-IPAe

The TOE shall avoid unauthorised modification of the following data when managed or manipulated by the TOE:

- o Keys:
  - D.IPAe_

KEYS

- Management data:
  - D.IPAe_DEVICE_INFO.

Application Note 74:

Amongst the components of the TOE,

- PRE, PPI 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.

9.5.2 Security Objectives for the Operational Environment

9.5.2.1 Actors

OE.SM-DPplus
OE.SM-DS
OE.EIM

9.5.3 Security Objectives Rationale

9.5.3.1 Threats

Unauthorized platform management

T.PLATFORM-MNG-INTERCEPTION-IPAe The SM-DP+ transmits Profiles (Bound Profile Packages) to the IPAe, the SM-DS transmits Events to the IPAe.

Consequently, the TSF ensures:

- Security of the transmission to the IPAe (O.SECURE-CHANNELS-IPAe and O.INTERNAL-SECURE-CHANNELS-IPAe) by requiring authentication from SM-DP+ or SM-DS, 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-DPplus and OE.SM-DS ensure that the credentials related to the secure channels will not be disclosed when used by off-card actors.

T.UNAUTHORIZED-PLATFORM-MNG-IPAe 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).

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-ELIGIBILITY-IPAe Device Info, transmitted by the IPAe to the eUICC for signature, is used by the SM-DP+ to perform the Eligibility Check prior to allowing profile download onto the eUICC.

Consequently, the TSF ensures:

- Security of the transmission among the IPAe and other security domains of the TOE (O.INTERNAL-SECURE-CHANNELS-IPAe) by protecting the transmission from unauthorized disclosure, modification and replay; These secure channel relies upon the underlying Runtime Environment, which protects the applications communications (OE.RE.SECURE-COMM).

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

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

Second level threats

T.LOGICAL-ATTACK-IPAe This threat is covered by controlling the information flow between the IPAe security domain and the platform layer 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 API of IPAe shall ensure atomic transactions (OE.IC.SUPPORT).

Whenever sensitive data of the TOE are processed by IPAe, 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 layer of the TOE, which are not protected by these mechanisms. Consequently,

- the TOE itself must ensure the correct operation of the Platform layer (PRE, PPI, and Telecom Framework (O.OPERATE)), and
- the Platform layer must protect the confidentiality and integrity of the sensitive data it processes, 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 IPAe (OE.RE.CODE-EXE),
- compliance to security guidelines for applications (OE.APPLICATIONS).

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

9.5.3.2 Assumptions

A.ACTORS-IPAe This assumption is upheld by objective OE.SM-DS which ensures that credentials and otherwise sensitive data will be managed correctly by this actor of the infrastructure.

9.5.3.3 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.PLATFORM-MNG-INTERCEPTION-IPAe	OE.RE.SECURE-COMM, OE.SM-DS, O.SECURE-CHANNELS-IPAe, O.INTERNAL-SECURE-CHANNELS- IPAe	Section 9.5.3
T.UNAUTHORIZED-PLATFORM-MNG-IPAe	OE.APPLICATIONS, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	Section 9.5.3
T.PROFILE-MNG-ELIGIBILITY-IPAe	OE.RE.SECURE-COMM, O.INTERNAL-SECURE-CHANNELS-IPAe, O.DATA-INTEGRITY-IPAe, OE.SM- DPplus, OE.RE.DATA-INTEGRITY	Section 9.5.3
T.LOGICAL-ATTACK- IPAe	O.OPERATE, O.API, OE.RE.API, OE.RE.CODE-EXE, OE.APPLICATIONS, O.DATA-CONFIDENTIALITY- IPAe, O.DATA-INTEGRITY-IPAe, OE.IC.SUPPORT, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA- INTEGRITY	Section 9.5.3
T.PHYSICAL-ATTACK- IPAe	O.DATA-CONFIDENTIALITY-IPAe, OE.IC.SUPPORT, OE.IC.RECOVERY, OE.RE.DATA-CONFIDENTIALITY	Section 9.5.3

Table 20 Threats and Security Objectives - Coverage

Security Objectives	Threats
O.SECURE-CHANNELS-IPAe	T.PLATFORM-MNG-INTERCEPTION-IPAe
O.INTERNAL-SECURE-CHANNELS-IPAe	T.PLATFORM-MNG-INTERCEPTION-IPAe, T.PROFILE-MNG-ELIGIBILITY-IPAe
O.DATA-CONFIDENTIALITY- IPAe	T.LOGICAL-ATTACK-IPAe, T.PHYSICAL- ATTACK-IPAe
O.DATA-INTEGRITY-IPAe	T.PROFILE-MNG-ELIGIBILITY-IPAe, T.LOGICAL-ATTACK-IPAe
OE.SM-DPplus	T.PLATFORM-MNG-INTERCEPTION-IPAe, T.PROFILE-MNG-ELIGIBILITY-IPAe
OE.IC.SUPPORT	T.LOGICAL-ATTACK-IPAe, T.PHYSICAL- ATTACK-IPAe
OE.IC.RECOVERY	T.PHYSICAL-ATTACK-IPAe
OE.RE.SECURE-COMM	T.PLATFORM-MNG-INTERCEPTION-IPAe, T.PROFILE-MNG-ELIGIBILITY-IPAe

OE.RE.API	T.LOGICAL-ATTACK-IPAe
OE.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PLATFORM-MNG-IPAe, T.LOGICAL-ATTACK-IPAe, T.PHYSICAL- ATTACK-IPAe
OE.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PLATFORM-MNG-IPAe, T.PROFILE-MNG-ELIGIBILITY-IPAe, T.LOGICAL-ATTACK-IPAe
OE.RE.CODE-EXE	T.LOGICAL-ATTACK-IPAe
OE.APPLICATIONS	T.UNAUTHORIZED-PLATFORM-MNG-IPAe, T.LOGICAL-ATTACK-IPAe
OE.SM-DS	T.PLATFORM-MNG-INTERCEPTION-IPAe

Table 21 Security Objectives and Threats – Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.ACTORS-IPAe	OE.SM-DS	Section 9.5.3

Table 22 Assumptions and Security Objectives for the Operational Environment – Coverage

Security Objectives for the Operational Environment	Assumptions
OE.SM-DS	A.ACTORS-IPAe

Table 23 Security Objectives for the Operational Environment and Assumptions – Coverage

9.6 Extended Requirements

9.6.1 Extended Families

9.6.1.1 Extended Family FPT_EMS - TOE Emanation

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.

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.

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.

9.7 Security Requirements

In order to define the Security Functional Requirements, Part 2 of the Common Criteria was used.
Some Security Functional Requirements have been refined. The refinements are described below the associated SFR. The refinement operation is used to add detail to a requirement, and, thus, further restricts a requirement. These refinements are interpretation refinement, and are described as an extra paragraph, starting with the word “Refinement”.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are italicised.

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as bold text. Assignments to be filled in by the ST

author appear in square brackets with an indication that an assignment is to be made [assignment:] and are italicised.

In some other cases the assignment made by the PP authors defines an assignment to be performed by the ST author. Thus this text is both bold and italicized (see for example the SFR FIA_UID.1/IPAe).

The iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

9.7.1 Security Functional Requirements

9.7.1.1 Introduction

This Protection Profile module defines the following security policy:

- IPAe information flow control SFP.

All roles used in the security policy are defined either as users or subjects in sections 3.2 and
9.4.2. 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.
This PP-Module only refers to remote users (U.EIM, U.SM-DS and U.SM-DPplus).

IPAe information flow control SFP

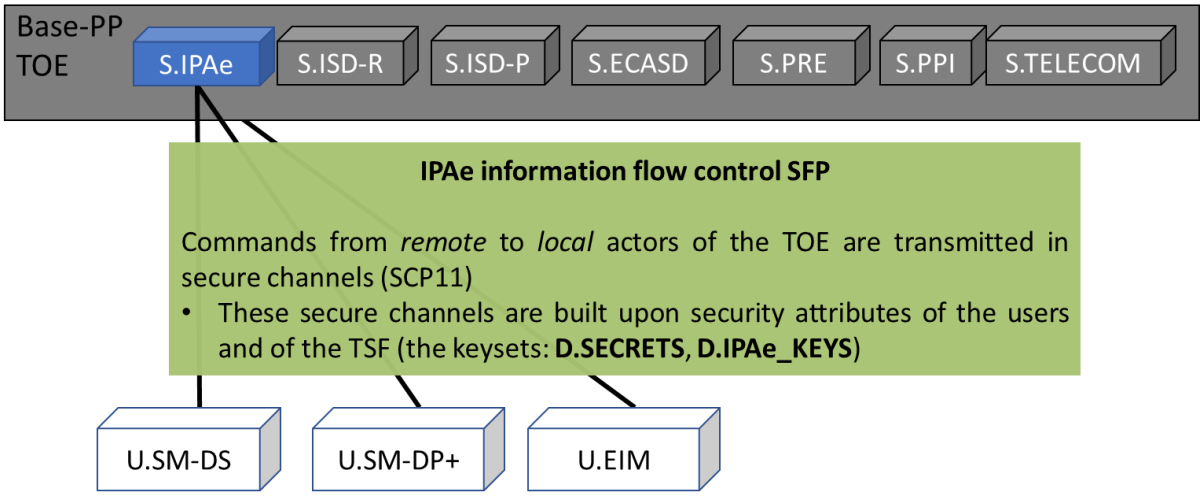


Figure 24 IPAe Information flow control SFP

Security attributes used in SFRs for the IPAe module

Security attribute	Details	Relationship to assets
IPAe session keys (D.IPAe_KEYS)	The session keys for the TLS connection (version 1.2 or greater) between IPAe and SM-DP+, SM-DS, and eIM.	This asset is described in section 8Keys.

CERT.DSauth.E CDSA CERT.DS.TLS CERT.DP.TLS CERT.EIM.TLS	Certificates of U.SM-DS, U.SM-DPplus, and U.EIM that are used by the TOE to authenticate this user. These certificates are issued by the eSIM CA. The TOE can verify this certificate using the eSIM CA public key.	These attributes are not assets of this Protection profile. The eSIM CA public key is described as the asset D.PK.CI.ECDSA in section 3.1.2.3 Identity management data.
SM-DS OID(s) eIM ID	SM-DS OID is the identification Root SM-DS. The Root SM-DS address(es) are unique and filled in the eUICC. The Root SM-DS(s) are configured at the time of Device manufacture and is invariant.	These attribute is included in the D.PLATFORM_DATA described in section 3.1.2.2 Management data.

Table 24 Definition of the security attributes of IPAe module

9.7.1.2 Identification and authentication

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

- identify the remote user U.SM-DS by its SM-DS OID.
- Identify the remote user U.EIM by its eIM ID

The TOE must:

- authenticate U.SM-DS using CERT.DSauth.ECDSA.
- authenticate U.EIM using CERT.EIM.ECDSA.

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

- U.SM-DPplus is bound to S.IPAe,
- U.SM-DS is bound to S.IPAe.
- U.EIM is bound to S.IPAe.

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

FIA_UID.1/IPAe Timing of identification

FIA_UID.1.1/IPAe 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/IPAe The TSF shall require each user to be successfully identified before

allowing any other TSF-mediated actions on behalf of that user.

Application Note 75:

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

- U.SM-DPplus
- U.SM-DS
- U.EIM

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/IPAe Timing of authentication

FIA_UAU.1.1/IPAe 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/IPAe The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 76:

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

- U.SM-DPplus
- U.SM-DS
- U.EIM

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 [36]:

- A U.SM-DPplus must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.DPauth.ECDSA, CERT.DPpb.ECDSA and CERT.DP.TLS), as well as the public key of the CI (D.PK.CI.ECDSA).
- A U.SM-DS must be authenticated by verifying its ECDSA signature, using the public keys included in its certificates (CERT.DSauth.ECDSA and CERT.DS.TLS), as well as the public key of the eSIM CA (D.PK.CI.ECDSA).

A U.EIM must be authenticated by verifying its ECDSA signature, using the public key included in its certificates (CERT.EIM.ECDSA, and CERT.EIM.TLS), as well as the public key of the CI (D.PK.CI.ECDSA).

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

- **SM-DP+ OID is associated to S.IPAe, acting on behalf of U.SM-DPplus**
- **SM-DS OID is associated to S.IPAe, acting on behalf of U.SM-DS.**
- **eIM ID is associated to S.IPAe, acting on behalf of U.EIM.**

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

- **Initial association of SM-DP+ OID requires U.SM-DPplus to be authenticated via "CERT.DPauth.ECDSA"**
- **Initial association of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA".**
- **Initial association of eIM ID requires U.EIM to be authenticated via "CERT.EIM.ECDSA".**

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

- **change of SM-DP+ OID requires U.SM-DPplus to be authenticated via "CERT.DPauth.ECDSA"**
- **change of SM-DS OID requires U.SM-DS to be authenticated via "CERT.DSauth.ECDSA".**
- **change of EIM ID requires U.EIM to be authenticated via "CERT.EIM.ECDSA".**

Application Note 77:

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

- U.SM-DPplus binds to a subject (S.IPAe)
- U.SM-DS binds to a subject (S.IPAe)
- U.EIM binds to a subject (S.IPAe)

FIA_UAU.4/IPAe Single-use authentication mechanisms

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

- **U.SM-DPplus**
- **U.SM-DS**
- **U.EIM**

Application Note 78:

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

- U.SM-DPplus
- U.SM-DS
- U.EIM

FIA_ATD.1/IPAe User attribute definition

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

- **CERT.DP.TLS belonging to U.SM-DPplus**
- **CERT.DSauth.ECDSA, CERT.DS.TLS, and SM-DS OID belonging to U.SM- DS.**

CERT.EIM.TLS, CERT.EIM.ECDSA, and eIM ID belonging to U.EIM.

9.7.1.3 Communication

This package describes how the TSF shall protect communications with external

users. The TSF shall enforce secure channels (FTP_ITC.1/IPAe and

FTP_ITC.2/IPAe):

- between U.SM-DPplus and S.IPAe
- between U.SM-DS and S.IPAe
- between U.EIM and S.IPAe

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/IPAe).

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

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

- generation and deletion of D.IPAe_KEYS and certificates (FCS_CKM.1/SCP-SM, FCS_CKM.6/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.6/SCP-MNO, FCS_CKM.1/IPAe and FCS_CKM.6/IPAe.

FDP_IFC.1/IPAe Subset information flow control

FDP_IFC.1.1/IPAe The TSF shall enforce the **IPAe information flow control SFP**

on o **users/subjects:**

- **U.SM-DPplus and S.IPAe**
- **U.SM-DS and S.IPAe**
- **U.EIM and S.IPAe**

o **information: transmission of commands**.

FDP_IFF.1/IPAe Simple security attributes

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

- **users/subjects:**
  - **U.SM-DPplus and S.IPAe, with security attribute D.IPAe_KEYS**
  - **U.SM-DS and S.IPAe, with security attribute D.IPAe_KEYS**
  - **U.EIM and S.IPAe, with security attribute D.IPAe_KEYS**
- **information: transmission of commands**.

FDP_IFF.1.2/IPAe The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

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

FDP_IFF.1.4/IPAe 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/IPAe The TSF shall explicitly deny an information flow based on the following rules:

- **The TOE shall reject communication between U.SM-DPplus and S.IPAe if it is not performed in a TLS secure channel;**
- **The TOE shall reject communication between U.SM-DS and S.IPAe if it is not performed in a TLS secure channel.**
- **The TOE shall reject communication between U.EIM and S.IPAe if it is not performed in a TLS/DTLS (or equivalent) secure channel.**

Application Note 79:

More details on the secure channels can be found in the following sections of SGP.32 [36]:

- For SM-DP+: Section 5.6
- For SM-DS: Section 5.10
- For eIM: Section 5.14

FTP_ITC.1/IPAe Inter-TSF trusted channel

FTP_ITC.1.1/IPAe 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/IPAe The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3/IPAe The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

Application Note 80:

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 [36]:

- The secure channels from the IPAe to eIM, SM-DP+ and SM-DS must be TLS with server authentication.

Related keys are generated on-card (D.IPAe_KEYS); see FCS_CKM.1/IPAe.

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 IPAe to open a TLS secure channel to SM-DP+ and transmit the following operations:
  - ES9+.InitiateAuthentication
  - ES9+.GetBoundProfilePackage
  - ES9+.AuthenticateClient
  - ES9+.HandeNotification
  - ES9+.CancelSession
  - ES9+.ConfirmDeviceChange
- The TSF shall permit the IPAe to open a TLS secure channel to SM-DS and transmit the following operations:
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient
  - ES11.CheckEvent

- The TSF shall permite the IPAe to open a TLS/DTLS secure channel to eIM and transmit the following operations:

  - ESipa.InitiateAuthentication
  - ESipa.GetBoundProfilePackage
  - ESipa.AuthenticateClient
  - ESipa.HandleNotification
  - ESipa.CancelSession
  - ESipa.GetEimPackage
  - ESipa.TransferEimPackage
  - ESipa.ProvideEimPackageResult

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

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

FDP_ITC.2.2/IPAe The TSF shall use the security attributes associated with the

imported user data.

FDP_ITC.2.3/IPAe 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/IPAe 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/IPAe 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/IPAe Inter-TSF basic TSF data consistency

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

- **Commands from U.SM-DPplus, U.EIM and U.SM-DS**
- **Downloaded objects from U.SM-DPplus and U.EIM**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/IPAe 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 81:

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

- SM-DP+ commands
  - ES9+.InitiateAuthentication
  - ES9+.GetBoundProfilePackage
  - ES9+.AuthenticateClient
  - ES9+.HandeNotification
  - ES9+.CancelSession
  - ES9+.ConfirmDeviceChange
- eIM commands
  - ESipa.InitiateAuthentication
  - ESipa.GetBoundProfilePackage
  - ESipa.AuthenticateClient
  - ESipa.HandleNotification
  - ESipa.CancelSession
  - ESipa.GetEimPackage
  - ESipa.TransferEimPackage
  - ESipa.ProvideEimPackageResult
- Downloaded objects from SM-DP+ and eIM
  - Session keys

  - Bound Profile Package
- SM-DS commands
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient
  - ES11.CheckEvent

FDP_UCT.1/IPAe Basic data exchange confidentiality

FDP_UCT.1.1/IPAe The TSF shall enforce the **IPAe information flow control SFP** to receive user data in a manner protected from unauthorised disclosure.

Application Note 82:

This SFR is related to the protection of:

- Bound Profile Packages downloaded from SM-DP+ and eIM.

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 [36]: Confidentiality of communication must be addressed by the use of AES in CBC mode with a minimum key size of 128 bits.

Related keys are generated on-card (D.IPAe_KEYS); see FCS_CKM.1/IPAe for further details.

FDP_UIT.1/IPAe Data exchange integrity

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

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

Application Note 83:

This SFR is related to the protection of:

- Bound Profile Packages downloaded from SM-DP+ and eIM;
- Commands received from to SM-DP+, eIM and SM-DS.

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 [36]: Integrity of communication must be addressed by the use of AES in CMAC mode with a minimum key size of 128 bits and a MAC length of 64 bits.

Related keys are generated on-card (D.IPAe_KEYS); see FCS_CKM.1/IPAe for further details.

FCS_CKM.1/IPAe Cryptographic key generation

FCS_CKM.1.1/IPAe The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curve Key Agreement (ECKA)** and specified cryptographic key sizes **256** that meet the following *[**assignment**: at least one elliptic curve referenced in SGP.32 [36]].*

Application Note 84:

This key generation mechanism is used to generate:

- D.IPAe_KEYS keys.

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

FCS_CKM.6/IPAe Cryptographic key destruction

FCS_CKM.6.1/IPAe The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction*]].

FCS_CKM.6.2/ IPAe The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1/IPAe in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application Note 85:

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

- D.IPAe_KEYS.

9.7.1.4 Security management

This package includes several supporting security functions:

- User data and TSF self-protection measures:
  - TOE emanation (FPT_EMS.1/IPAe)
  - protection from integrity errors (FDP_SDI.1/IPAe)
  - residual data protection (FDP_RIP.1/IPAe)
- Security management measures:
  - Management of roles (FMT_SMR.1/IPAe) and function (FMT_SMF.1/IPAe)

FPT_EMS.1/IPAe TOE Emanation

FPT_EMS.1.1/IPAe The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to

- **D.IPAe_KEYS**

and [assignment: *list of types of user data*].

FPT_EMS.1.2/IPAe The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to

- **D.IPAe_KEYS**

and [assignment: *list of types of user data*].

Application Note 86:

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/IPAe Stored data integrity monitoring

FDP_SDI.1.1/IPAe 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 following assets that require to be protected against unauthorized modification:

- Management data
  - D.IPAe_DEVICE_INFO
- Keys
  - D.IPAe_KEYS

FDP_RIP.1/IPAe Subset residual information protection

FDP_RIP.1.1/IPAe 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.IPAe_KEYS.**

FMT_SMF.1/IPAe Specification of Management Functions

FMT_SMF.1.1/IPAe 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/IPAe Security roles

FMT_SMR.1.1/IPAe The TSF shall maintain the roles

- **External users:**
  - **U.SM-DS**
  - **U.SM-DPplus**
  - **U.EIM**
- **Subjects:**
  - **S.IPAe**.

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

Application Note 87:

The roles defined here correspond to the users and subjects defined in Section 3.2

9.7.2 Security Assurance Requirements

There are no new SARs stated for this PP-Module, since the Base-PP SARs suffice to cover all SFRs.

9.7.3 Security Requirements Rationale

9.7.3.1 Objectives

Security objectives for the TOE

Platform support functions

O.SECURE-CHANNELS-IPAe All SFRs relative to the ESipa, ES9+ and ES11 interfaces (FDP_IFC.1/IPAe, FDP_IFF.1/IPAe, FTP_ITC.1/IPAe, FDP_ITC.2/IPAe, FPT_TDC.1/IPAe, FDP_UCT.1/IPAe, FDP_UIT.1/IPAe, FCS_CKM.1/IPAe, FCS_CKM.4/IPAe) cover this security objective by enforcing the IPAe information flow control SFP that ensures that transmitted commands and data are protected from unauthorized disclosure and modification.

Identification and authentication SFRs (FIA_UID.1IPAe, FIA_UAU.1/IPAe, FIA_USB.1/IPAe, FIA_UAU.4/IPAe) support this security objective by requiring authentication and identification from the distant eIM, SM-DP+ and SM-DS in order to establish these secure channels.

FIA_ATD.1/IPAe, 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/IPAe and FMT_SMR.1/IPAe support these SFRs by providing management of roles and management of functions.

O.INTERNAL-SECURE-CHANNELS-IPAe FPT_EMS.1/IPAe ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks. This includes in particular secrets (asset D.SECRETS) if transmitted between ECASD and IPAe.

FDP_SDI.1/IPAe ensures that the secrets cannot be modified during this transmission.

FDP_RIP.1/IPAe ensures that the secrets cannot be recovered from deallocated resources.

9.7.3.2 Data protection

O.DATA-CONFIDENTIALITY-IPAe FDP_UCT.1/IPAe addresses the reception of data from off-card actor.

FPT_EMS.1/IPAe ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks.

FDP_RIP.1/IPAe ensures that no residual confidential data is available.

O.DATA-INTEGRITY-IPAe FDP_UIT.1/IPAe addresses the reception of data from off-card actors.

FDP_SDI.1/IPAe specifies the data that is monitored in case of an integrity breach.

9.7.3.3 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.SECURE-CHANNELS- IPAe	FMT_MSA.1/CERT_KEYS, FMT_SMF.1/IPAe, FMT_SMR.1/IPAe, FIA_UID.1/IPAe, FIA_UAU.1/IPAe, FIA_USB.1/IPAe, FIA_UAU.4/IPAe, FIA_ATD.1/IPAe, FDP_IFF.1/IPAe, FTP_ITC.1/IPAe, FDP_ITC.2/IPAe, FPT_TDC.1/IPAe, FDP_UIT.1/IPAe, FCS_CKM.1/IPAe, FCS_CKM.4/IPAe, FDP_IFC.1/IPAe, FDP_UCT.1/IPAe, FIA_ATD.1, FMT_MSA.3	section 9.7.3.1
O.INTERNAL-SECURE-CHANNELS-IPAe	FPT_EMS.1/IPAe, FDP_SDI.1/IPAe, FDP_RIP.1/IPAe	section 9.7.3.1
O.DATA-CONFIDENTIALITY-IPAe	FPT_EMS.1/IPAe, FDP_RIP.1/IPAe, FDP_UCT.1/IPAe	section 9.7.3.1
O.DATA-INTEGRITY-IPAe	FDP_SDI.1/IPAe, FDP_UIT.1/IPAe	section 9.7.3.1

Table 25 Security Objectives and SFRs – Coverage

Security Functional Requirements	Security Objectives

FIA_ATD.1	O.SECURE-CHANNELS-IPAe
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS-IPAe
FMT_SMF.1/IPAe	O.SECURE-CHANNELS-IPAe
FMT_MSA.3	O.SECURE-CHANNELS-IPAe
FIA_UID.1/IPAe	O.SECURE-CHANNELS-IPAe
FIA_UAU.1/IPAe	O.SECURE-CHANNELS-IPAe
FIA_USB.1/IPAe	O.SECURE-CHANNELS-IPAe
FIA_UAU.4/IPAe	O.SECURE-CHANNELS-IPAe
FIA_ATD.1/IPAe	O.SECURE-CHANNELS-IPAe
FDP_IFC.1/IPAe	O.SECURE-CHANNELS-IPAe
FDP_IFF.1/IPAe	O.SECURE-CHANNELS-IPAe
FTP_ITC.1/IPAe	O.SECURE-CHANNELS-IPAe
FDP_ITC.2/IPAe	O.SECURE-CHANNELS-IPAe
FPT_TDC.1/IPAe	O.SECURE-CHANNELS-IPAe
FDP_UCT.1/IPAe	O.SECURE-CHANNELS-IPAe, O.DATA- CONFIDENTIALITY-IPAe
FDP_UIT.1/IPAe	O.SECURE-CHANNELS-IPAe, O.DATA- INTEGRITY-IPAe
FCS_CKM.1/IPAe	O.SECURE-CHANNELS-IPAe
FCS_CKM.4/IPAe	O.SECURE-CHANNELS-IPAe
FPT_EMS.1/IPAe	O.INTERNAL-SECURE-CHANNELS-IPAe, O.DATA-CONFIDENTIALITY-IPAe
FDP_SDI.1/IPAe	O.INTERNAL-SECURE-CHANNELS-IPAe, O.DATA-INTEGRITY-IPAe
FDP_RIP.1/IPAe	O.INTERNAL-SECURE-CHANNELS-IPAe, O.DATA-CONFIDENTIALITY-IPAe
FMT_SMR.1/IPAe	O.SECURE-CHANNELS-IPAe

Table 26 SFRs and Security Objectives

9.7.3.4 Dependencies

9.7.3.4.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FIA_UID.1/IPAe	No Dependencies	
FIA_UAU.1/IPAe	(FIA_UID.1)	FIA_UID.1/IPAe
FIA_USB.1/IPAe	(FIA_ATD.1)	FIA_ATD.1/IPAe
FIA_UAU.4/IPAe	No Dependencies	
FIA_ATD.1/IPAe	No Dependencies	
FDP_IFC.1/IPAe	(FDP_IFF.1)	FDP_IFF.1/IPAe

FDP_IFF.1/IPAe	(FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/IPAe
FTP_ITC.1/IPAe	No Dependencies	
FDP_ITC.2/IPAe	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/IPAe, FTP_ITC.1/IPAe, FPT_TDC.1/IPAe
FPT_TDC.1/IPAe	No Dependencies	
FDP_UCT.1/IPAe	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/IPAe, FTP_ITC.1/IPAe
FDP_UIT.1/IPAe	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/IPAe, FTP_ITC.1/IPAe
FCS_CKM.1/IPAe	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_CKM.3) and (FCS_RBG.1 or FCS_RNG.1) and (FCS_CKM.6)	FCS_COP.1 {Either by composition or claim in ST} {*Discarded – No Key Access Interface exists}* FCS_CKM.6/IPAe FCS_RNG.1
FCS_CKM.6/IPAe	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.2/IPAe
FPT_EMS.1/IPAe	No Dependencies	
FDP_SDI.1/IPAe	No Dependencies	
FDP_RIP.1/IPAe	No Dependencies	
FMT_SMF.1/IPAe	No Dependencies	
FMT_SMR.1/IPAe	(FIA_UID.1)	FIA_UID.1/IPAe

Table 27 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FCS_CKM.2 or FCS_COP.1 of FCS_CKM.1/IPAe may be discarded. The dependency to FCS_COP.1 may be discarded if the TOE uses the cryptographic libraries provided by its underlying Platform. Otherwise, the TOE must implement FCS_COP and the ST satisfy this dependency.

10 IPAe PP-configuration

10.1 Reference

Title:	IPAe Configuration for eUICC for IoT Devices Protection Profile
Author:	GSMA
Editor:	GSMA
Reference:	SGP.25.Base+IPAe
Version:	3.0
CC Version:	CC:2022 release 1
Assurance Level:	EAL4 augmented with ALC_DVS.2 and AVA_VAN.5
General Status:	Complete
Keywords:	eUICC, IoT Devices, Remote SIM Provisioning

10.2 Components statement

This PP-Configuration is identified as: *IPAe Configuration for eUICC for IoT Devices Protection Profile*, version 3.0 and defined in the current section 10.

This configuration has one single Base-PP: *eUICC for Consumer and IoT Devices Protection Profile*, version 3.0 and defined in the current document's sections 1 to 6. This configuration consists of the Base-PP together with the PP-Module *IPAe Module for eUICC for IoT Devices Protection Profile*, version 3.0 and defined in the current document's section 9.

10.3 Conformance statement

This Protection Profile requires demonstrable conformance (as defined in [37]) of any ST or PP claiming conformance to this PP Configuration.

10.4 SAR statement

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

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

ADV_ARC.1 is refined to add a particular set of verifications on top of the existing requirement.

Annex A PP Module OS Update

A.1 Scope

This PP-Module addresses the security requirements related to the eUICC OS Update capability

A.2 Security Problem Definition (SPD)

A.2.1 Assets

D.UPDATE_IMAGE	Can be an update for the OS, as a patch or a complete OS replacement, or separate bootloader It is sent to the TOE. It possibly includes executable code, configuration data and/or image type information. It has to be protected from unauthorized disclosure and modification. Is also referred to as Additional Code
D.TOE_IDENTIFIER	Identification data to identify the TOE. To be protected from unauthorized modification.
D.OS-UPDATE_KEY(S)	Key(s) used for OS Update. To be protected from unauthorized disclosure and modification.

Application Note 88:

The Update Image should follow the rules defined in SGP.24 [29] in respect to compliance and certification.

A.2.2 Security Aspects

SA.CONFID-UPDATE-IMAGE	**Confidentiality of Update Image** The update image must be kept confidential. This concerns the non disclosure of the update image in the transit to the eUICC.
SA.INTEG-UPDATE-IMAGE	**Integrity of Update Image** The update image must be protected against unauthorized modification. This concerns the modification of the image in transit to the eUICC.

A.2.3 Threats

T.CONFID-UPDATE-IMAGE.LOAD	Confidentiality of Update Image – Load The attacker discloses (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the eUICC for installation. See SA.CONFID-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, TSF_Data
T.INTEG-UPDATE-IMAGE.LOAD	Integrity of update Image -Load The attacker modifies (part of) the image used to update the TOE in the field while the image (Additional Code) is transmitted to the card for installation. See SA.INTEG-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, TSF_Data
T.UNAUTH-UPDATE-IMAGE.LOAD	Load an unauthorized update

	The attacker tries to upload an unauthorized update image. See SA.INTEG-UPDATEIMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, TSF_Data
T.INTERRUPT_OSU	OS Update procedure interrupted The attacker tries to interrupt the OS update procedure (Load Phase through activation of Additional Code) leaving the TOE in a partially functional state. Directly threatened asset(s): D.TOE_IDENTIFIER, D.UPDATE_IMAGE, TSF_Data

A.2.4 Subjects

S.OSU	OS Update provides secure functionality to update the TOE operating system with an image created by a trusted off-card entity (S.UpdateImageCreator)
S.UpdateImageCreator	The off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

A.3 Security Objectives

This section describes the security objectives for the TOE for the OS Update module.

A.3.1 Security Objectives for the TOE

The following security objectives for the TOE are taken from [27].

O.SECURE_LOAD_ACODE	**Secure loading of the Additional Code** The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure.
O.SECURE_AC_ACTIVATION	**Secure activation of the Additional Code** Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE such as tearing, integrity violation, error

	case…), the Initial TOE shall remain in its initial state or fail secure.
O.TOE_IDENTIFICATION	**Secure identification of the TOE by the user** The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.

In addition, the following security objectives for the TOE are defined:

O.CONFID-UPDATE-IMAGE.LOAD	The TOE shall ensure that the D.UPDATE_IMAGE transferred to the device is not disclosed during the installation.
O.AUTH-LOAD-UPDATE-IMAGE	The TOE shall ensure that it is only possible to load an authorized image.

A.3.2 Security Objectives for the Operational Environment

This section describes the security objectives for the Operatinal Environment for the OS Update module.

OE.CONFID_UPDATE_IMAGE.CREATE	Confidentiality of Update Image – CREATE The off-card Update Image Creator ensures that the confidentiality and integrity requirements are met.

A.3.3 Security Objectives Rationale

For each of the defined threats, a rationale is given mapping the Security Objectives to the threat

T.CONFID-UPDATE-IMAGE.LOAD

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

T.INTEG-UPDATE-IMAGE.LOAD

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

T.UNAUTH-UPDATE-IMAGE.LOAD

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

T.INTERRUPT_OSU

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

Security Requirements

The ST author should select an appropriate set of SFRs to meet the specified security objectives. Examples of how this can be achieved may be referenced in the OS Update Addendum of GlobalPlatform Secure Element Protection Profile [28] or PP0084 [2] Package Loader.

Annex B Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	5th June 2018	First release of PRD	PSMC	Gloria Trujillo, GSMA
2.0	19 December 2023	CR0035R00 - SGP.25 AppNote OE RE IDENTITY CR0037R01 – OS update CR0038R03 - SGP25 Update due to Security Impact CR0039R01 SGP25_RemoteProfileManagement CR0040R01 – Alignement of Test Profile definition CR0042R01 – SGP.25_References Updates CR0043R01 - SGP.25 Addressing different types of eUICC CR0045R00 - Correction of OE.RE.PPE-PPI CR0039R03 - SGP.25 Remote Profile management CR0041R05 - Supporting multiple enabled profiles CR0044R01 - Device Change CR0046R01 - CR on SGP.25 v3-ES8_ES10a-ES10b-ES10c Interfaces CR0047R1 - PPR1 clarification CR0048R03 - SGP.22 V3.0 CR0050R03 - Introduction of Root CA and multiple Root DS CR0051R02 – Enterprise profiles inclusion in SGP25 CR0052R01 – OE.Applications CR0053R00 - Clarify the statement in section 9 CR0055R00 - Enterprise Rules optionality in SFRs CR0056R01 - SGP.25 PP identification CR0057R00 - OE.Applications Revert CR0058R01 - Add IoT Architecture to SGP.25	ISAG	Gloria Trujillo, GSMA

		CR0059R01 - Add eSIM for IoT definitions CR0060R01 - Add of the eIM user to the PP CR0062R00 - Add of SGP.32 functions to the Protection Profile CR0061R05 – Add IPAe PP module to SGP.25 CR0063R02 – Update of TOE overview to include IoT CR0064R01 – Update of Security Requirements to include IoT CR0065R01 – ALC_FLR CR0066R00 – Device Change Update CR0067R01 – Remove section 9 CR0068R01 – Update Security Objectives for the Operational Environment to include IoT CR0069R01 – Update Security objectives for the TOE to include IoT CR0070R01 – Precise consumer and IoT threats CR0071R01 – Assets review CR0072R01 – Add definition of Device and Consumer Device CR0073R01 – PP title change and removal of Consumer Device term CR0074R03 – Replace specific ECC curve references with reference to SGP.22 CR0075R01 – Change chapter to section everywhere in SGP.25 CR0076R00 – Add PSMO and eCO abbreviations CR0077R01 - IPAe Configuration CR0078R03 - SFR and SAR dependencies for switch to CC 2022 CR0079R01 - Review of the threats related to IoT CR0080R00 - PP modules/configurations titles corrections CR0081R01 - FIA_API-FPT_EMS-FCS_RNG updates for PP switch to CC 2022 CR0083R00 – Updates for PP related to CC2022 changes on APE_OBJ.1 and APE_OBJ.2		

		CR0084R00 - Correction of reference 19 CR0085R02_Updates for PP related to CC2022 changes on APE_REQ.1 and APE_REQ.2 CR0086R01 FCS_CKM CR0087R01 Review of threats related to Profile and Platform management CR0088R01 Review objective for the environment CR0089R01 Updates for PP related to CC2022 changes on APE_CCL CR0090R02 Updates for PP related to CC2022 changes on APE_CCL and SARs CR0091R00 Updates for PP related to CC2022 changes on FCS_CKM SFRs to cover CC 2022 for IPA CR0092R01 EXT_COMP CR0093R01 - Deletion of eSA notes in SGP.25		

B.2 Other Information

Type	Description
Document Owner	eSIMG
Editor / Company	Gloria Trujillo, GSMA

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.