PP Module for Application Isolation in the eUICC

Version 1.0

17th July 2026

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

1 Introduction

This PP Module introduces enhancements to support implementations with defensive virtual machine capabilities and risk-based verification approaches. These enhancements aim to preserve the high level of security assurance expected from Common Criteria evaluations, while enabling greater flexibility in how eUICC platforms are deployed and managed across diverse operational environments.

Current Protection Profile [SGP.25] relies on application verification through environmental objectives that ensure complete application verification and code integrity. The relevant environmental objectives include:

- OE.APPLICATIONS: Ensures applications comply with security guidelines.

In case Java Card is used, this will also imply using the following environmental objectives:

- OE.CODE-EVIDENCE (from PP0099 [JC-PP] via Java Card layer): Ensures digital evidence exists that application code has been verified.
- OE.VERIFICATION (from PP0099 [JC-PP] via Java Card layer): Ensures bytecode verification of all applications.
- OE.CAP-FILE (from PP0099 [JC-PP] via Java Card layer): Ensures that post issuance applications do not contain native methods.

If not using Java Card, equivalent environmental objectives SHALL be required, unless these are covered by the TOE.

This approach provides strong security guarantees but may impose operational constraints in certain deployment scenarios where:

- Real-time Profile/application loading is required with minimal latency
- Network connectivity for complete verification services is limited
- Risk-based security approaches are preferred based on application criticality
- Differentiated security requirements exist for different types of eUICC applications

All the requirements related to CAP files and applications contained in PP0100 [SGP.25] and PP0099 [JC-PP] shall also apply when IJC or any other format instead of CAP is used for loading applications, either in or outside a Profile (e.g. RAM).

1.1 Scope

The proposal introduces:

1. Enhanced TOE capability through new objective O.ISOLATION for defensive runtime protection
2. Maintained environmental objectives - no changes to existing OE.APPLICATIONS, OE.CODE-EVIDENCE, OE.CAP-FILE or OE.VERIFICATION requirements
3. Supporting Security Functional Requirements to implement defensive isolation mechanisms

These changes enable TOE implementations to provide equivalent security through enhanced defensive runtime mechanisms while maintaining existing verification requirements in the operational environment.

1.2 Definitions

Term	Description
Application	An executable software program running on top of the TOE Runtime Environment.
eSIM Functional Realm	Any Application, Security Domain or Runtime Environment related to eSIM. This includes eUICC architecture elements and their contents. This is the PP TOE.
Functional Realm	A set of functionally related Applications, security domains, and environment with managed access to resources and that preserves confidentiality and integrity.
Interoperable Javacard CAP	A file that is a serialization of the different CAP file components that should be loaded on the card. The CAP file components that are not required to be loaded on the card are removed from this file.
Issuer Security Domain - Profile	Security Domain for the hosting of a Profile [3].
Non-eSIM Functional Realm	Any Application, Security Domain or Runtime Environment not related to eSIM which are not covered by the PP TOE. This definition includes Self-Managed Security Domain.
Operator	A Mobile Network Operator or Mobile Virtual Network Operator; a company providing wireless cellular network services [3].
Operational Profile	An Operator-Owned Profile in support of a Subscription with the relevant Operator and that allows connectivity to a mobile network. Applications may be included to provide non-telecommunication services [3].
Profile	A combination of data and Applications to be provisioned on an eUICC for the purpose of providing services by the Profile Owner, as defined in [3]. A Profile is either an Operational Profile, a Provisioning Profile or a Test Profile.
Profile Owner	The entity that controls the operations that can be performed upon its Profile. With the exception of Test Profile, this is always an Operator.
Self-Managed Security Domain	A Security Domain that is extradited to itself from a Profile with Authorized Management (AM) rights, allowing it to be independently managed and operated with little reliance on the Profile Owner.

1.3 Abbreviations

Term	Description
CC	Common Criteria
IJC	Interoperable Javacard CAP
ISD-P	Issuer Security Domain – Profile
SD	Security Domain

Term	Description
SSD	Supplementary Security Domain
TRE	Tamper Resistant Element

1.4 References

Ref	DocNumber	Title	
[1]	[JC-PP]	Java Card System – Open Configuration Protection Profile	
[2]	[SGP.25]	eUICC for Consumer and IoT Device Protection Profile	
[3]	[SGP.21]	RSP Architecture	
[4]	[GPCS]	GlobalPlatform Card Specification v2.4	

2 Related Security Problem Definition and Security Objectives

2.1 Assets

The existing asset model will be enhanced with D.PROFILE_APPLICATIONS to cover all user data contained in the Profiles. All existing assets (D.TSF_CODE, D.PLATFORM_DATA, etc.) remain protected under the enhanced security framework.

D.PROFILE_APPLICATIONS general Profile applications data and code stored in Profiles and used by Profile Applications**.**

This asset has to be protected from unauthorised modification and unauthorised disclosure.

2.2 Threats

2.2.1 T.UNVERIFIED_APPLICATION

An unverified on-card Application performs unauthorised code execution, modifies or discloses any asset in the TOE per Note 1.

Note 1:

An unverified malicious on-card Application performs unauthorised operations:

- modifies or discloses Profile data belonging to the ISD-P or MNO-SD;
- executes or modifies operations from Profile Applications (ISD-P, MNO-SD and Applications controlled by MNO-SD).
- modifies or discloses the ISD-P or MNO-SD Application;
- modifies or discloses data of the ISD-R or PRE;
- executes or modifies operations from ISD-R or PRE;
- modifies the rules authorisation table (RAT) stored in the PRE;
- modifies or discloses data belonging to the ECASD;
- executes or modifies operations from ECASD;
- unauthorised disclosure or modification of TSF Data or Code

Such threats are described in T.LOGICAL-ATTACK within [SGP.25].

This threat does not address the following cases

- An Application within a Profile tries to compromise its own MNO-SD;

- An Application within a Profile tries to compromise another Application under the control of its own MNO-SD or ISD-P.

These cases are considered the responsibility of the Profile Owner, since they only compromise their own Profile, without any side-effects on other Profiles.

This threat addresses the following cases:

- An Application within a Profile represented by an ISD-P (including an Application in a Self-Managed Security Domains) tries to compromise another Profile MNO-SD or ISD-P or an Application under the control of another MNO-SD or ISD-P; any data or Applications residing in any other SD in the TOE containing TOE assets (e.g., ISD-R or ECASD).
- An Application outside of any Profile represented by an ISD-P (for example, in the ISD-R, ECASD inside a Non-eSIM Functional Realm) tries to compromise another Profile MNO-SD or ISD-P; an Application under the control of an MNO-SD or ISD-P; any data or Application residing in any other SD in the TOE containing TOE assets.
- An Application within a Self-Managed Security Domains tries to compromise MNO-SD or ISD-P or an Application under the control of another MNO-SD or ISD-P; any data or Applications residing in any other SD in the TOE containing TOE assets (e.g., ISD-R or ECASD).

Directly threatens assets: All assets (D.MNO_KEYS, D-PROFILE_NAA_PARAMS, D.PROFILE_IDENTITY, D.PROFILE_RULES, D.PROFILE_USER_CODES (SGP.22), D.PROFILE_CODE, D.TSF_CODE, D.PLATFORM_DATA, D.DEVICE_INFO, D.PLATFORM_RAT, D.SK.EUICC.ECDSA, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.PK.EIM.ECDSA (SGP.32), D.EID, D.CERT.EUM.ECDSA, D.SECRETS, D.CRLs, D.PROFILE_APPLICATIONS).

Application Note 1: An unverified Application is an Application that does not follow the verification rules required through the defined environmental objectives regarding Application isolation and it is loaded after TOE delivery by the dedicated Application loading mechanism(s) available. In case the verification rules are fully or partially enforced by the TOE itself before the on-card Application reach the installed state, then that mechanism can be considered as part of the isolation mechanism. The unverified on-card Application may reside in any Security Domain or storage area within the TRE, regardless of whether it is located inside or outside a specific Profile. This threat persists independently of the specific platform architecture layered upon the TRE and shall guarantee the isolation from Non-eSIM Functional Realms (including native Applications in case they exist).

In case of a complex architecture, in which multiple Functional Realms are present (e.g. eSIM Functional Realm and eSE Functional Realm), Applications from different Functional Realms are also considered a threat.

The ST physical and logical scope of the TOE shall reflect the complexity of the platform and describe the additional Functional Realms and the isolation mechanisms.

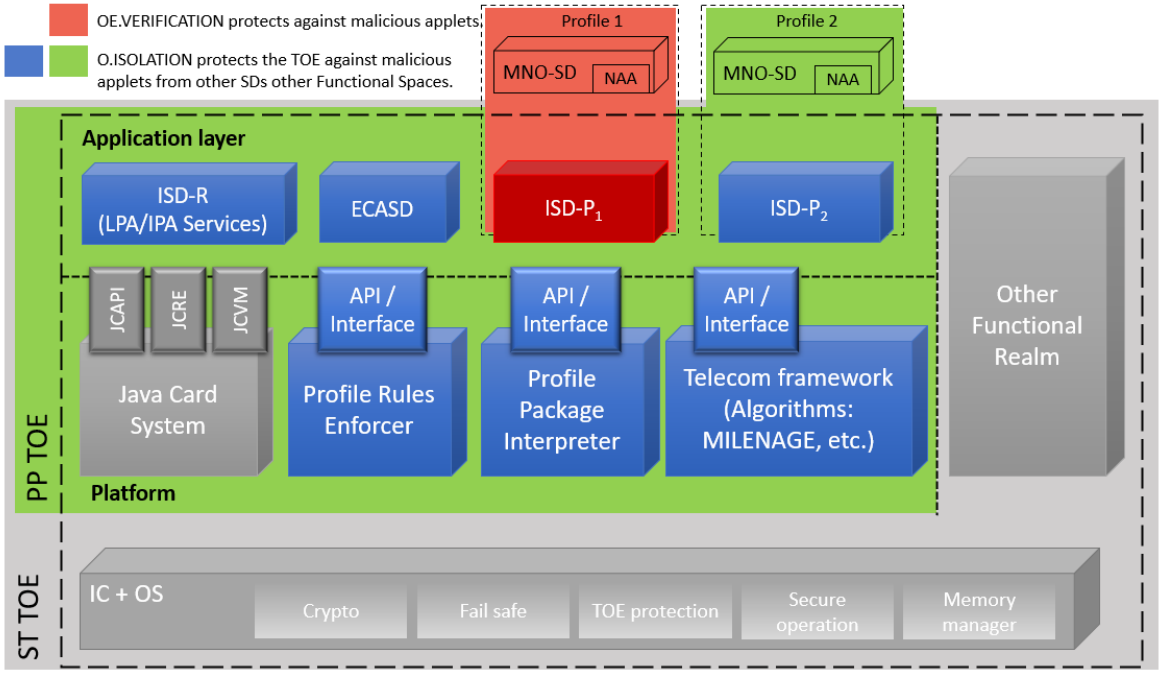

Figure 1: Example of a complex architecture including an eSIM Functional Realm and a Non-eSIM Functional Realm

2.3 Assumptions

A.PROFILE-APPLICATIONS: It is assumed that a Profile Owner ensures that Applications within their Profile do not present a threat to any other Applications within the Profile. This assumption does not cover Self-Managed Security Domains.

2.4 Organizational Security Policies

OSP.APPLICATIONS: All Applications shall comply with the security guidelines document for the used platform on top of the TRE. These guidelines 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. This OSP replaces the assumption A.APPLICATIONS defined within [SGP.25].

Note 3: The term "all Applications" encompasses every Application residing within the TRE boundary. This includes, but is not limited to, Applications located inside a Profile, those residing in any Security Domain (SD), and Applications belonging to different Functional Realms.

2.5 Security Objectives Rationale

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).
- by enhanced isolation provided by O.ISOLATION.

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.DATACONFIDENTIALITY, 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 (O.DATA-CONFIDENTIALITY, O.DATAINTEGRITY).

The following objectives for the operational environment are also required:

- prevention of unauthorized code execution by Applications (OE.RE.CODE-EXE),

T.UNVERIFIED_APPLICATION: This threat is covered by the security objective O.ISOLATION which ensures that any Application inside a Profile cannot threaten any asset outside that Profile and any Application outside a Profile cannot threaten any TOE asset including assets inside a Profile.

Other security objectives are also expected from the TOE and the environment related to this threat but are not considered as sufficient to cover the threat. Therefore, O.ISOLATION shall be evaluated independently from those objectives:

- OE.RE.PRE-PPI and O.eUICC-DOMAIN-RIGHTS ensure that only authorized and authenticated actors will access the Security Domain functions and content;
- OE.SM-DP+, OE.MNO-SD and OE.EIM protect the corresponding credentials when used off-card;
- OE.RE.DATA-CONFIDENTIALITY and OE.RE.DATA-INTEGRITY ensure the integrity and confidentiality of Application data;
- O.SECURE-CHANNELS and O.INTERNAL-SECURE-CHANNELS provide a secure channel for communication either with the SM-DP+ or the MNO OTA Platform. These secure channels rely upon the underlying Runtime Environment, which protects the Applications communications (OE.RE.SECURE-COMM);
- The secure operation of the Application Firewall requires the compliance to security guidelines for Applications (OE.PROFILE_APPLICATIONS and OE.APPLICATIONS)

Note 2: The unverified on-card Application may reside in any Functional Realm within the TRE, regardless of whether it is located inside or outside a specific Profile. This threat persists independently of the specific platform architecture layered upon the TRE.

OSP.LIFE-CYCLE: O.PRE-PPI ensures that there is a single ISD-P enabled at a time if the eUICC supports only SEP (Single Enabled Profile). 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.

OSP.APPLICATIONS: This OSP is enforced by the security objective for the operational environment OE.APPLICATIONS.

A.PROFILE_APPLICATIONS: This assumption is directly upheld by objective OE.PROFILE_APPLICATIONS.

3 Additional Security Objectives

3.1 New Security Objectives

O.ISOLATION: O.ISOLATION ensures that Profile boundaries, eUICC platform boundaries (which includes ISD-R, ECASD, PRE, PPI, and Telecom framework and the RE), and eSIM Functional Realm boundaries are not crossed when any Application attempts to exploit implementation vulnerabilities.

The TOE mitigates logical attacks from Applications including but not limited to control flow manipulation, unauthorized code fragment execution, type confusion, buffer underflow/overflow, and improper access to native code or system components. The logical attacks may come from Applications that do not follow the security guidelines.

The isolation provided by this objective of the TOE allows inter-Application communication within a Profile or with the eUICC platform as long as the target Application explicitly provides an interface to share services or data.

O.ISOLATION complements the existing RE objectives OE.RE.SECURE-COMM, OE.RE.API and OE.RE.CODE-EXE by providing enhanced isolation mechanisms specifically designed to limit the impact of potentially harmful Applications.

OE.PROFILE_APPLICATIONS: It is the responsibility of the Profile Owner to ensure that applications within their Profile do not present a threat to any other Applications within the Profile (for example, by ensuring that the security guidelines are followed). This objective does not cover Self-Managed Security Domains.

3.2 Clarification of Application Note 23 of OE.APPLICATIONS

A modification of the Application note 23 of OE.APPLICATIONS from [SGP.25] is proposed to acknowledge the practical reality of multi-purpose eUICC deployments where different actors may have different verification approaches, making it necessary for the TOE to provide defensive isolation capabilities to maintain security even when environmental verification cannot be uniformly guaranteed across all Profiles or Functional Realms.

OE.APPLICATIONS: All Applications residing in any Functional Realm as defined in Note 3 shall comply with the security guidelines document for the platform (operating system) used. These guidelines 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 from [SGP.25]:

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]). However, while OE.VERIFICATION is expected to be enforced for Applications within each Profile, in eUICC implementations with multiple Profiles from different Operators or multiple purposes, Profile Owners cannot enforce verification requirements on Applications belonging to other Profiles owned by different MNOs or other Security Domains residing outside Profiles, e.g., the ISD-R, or in different Functional Realms. Therefore, the TOE shall enforce isolation as described by O.ISOLATION.

3.3 New Security Functional Requirements

New SFRs implementing defensive isolation mechanisms to support O.ISOLATION could be defined by:

- Isolation Access Control SFP (FDP_ACC.2 and FDP_ACF.1):
    - An Application may access data objects only if the objects pertain to its Profile (Applications are confined to their own Profile boundaries)
    - An Application may access system resources or data only if the resources are explicitly designated as publicly available (System resources are protected unless specifically shared)

3.4 Profile Isolation access control SFP

This section proposes a definition of the Isolation access control security policy using FDP_ACC.2 and FDP:ACF.1 and including dependencies FMT_MSA.1 and FMT_MSA.3.

The SFP guarantees isolation in three respects:

- the platform is isolated from any Operator Profile, any Self-Managed Security Domain, any Functional Realm and any applications in general
- any profile is mutually isolated from one another. For example, Profile 1 is isolated from Profile 2 and 3, Profile 2 is isolated from Profile 1 and 3, the platform is isolated from both Profile 1, Profile 2 and Profile 3 including cases where a Profile contains unverified Applications.
- a Profile within an eSIM Functional Realm is isolated from Application within any other Functional Realm such as Self-Managed Security Domain.

The following figures depict what access could be explicitly allowed (green full arrows) and what accesses are denied (red dash-dotted arrows)

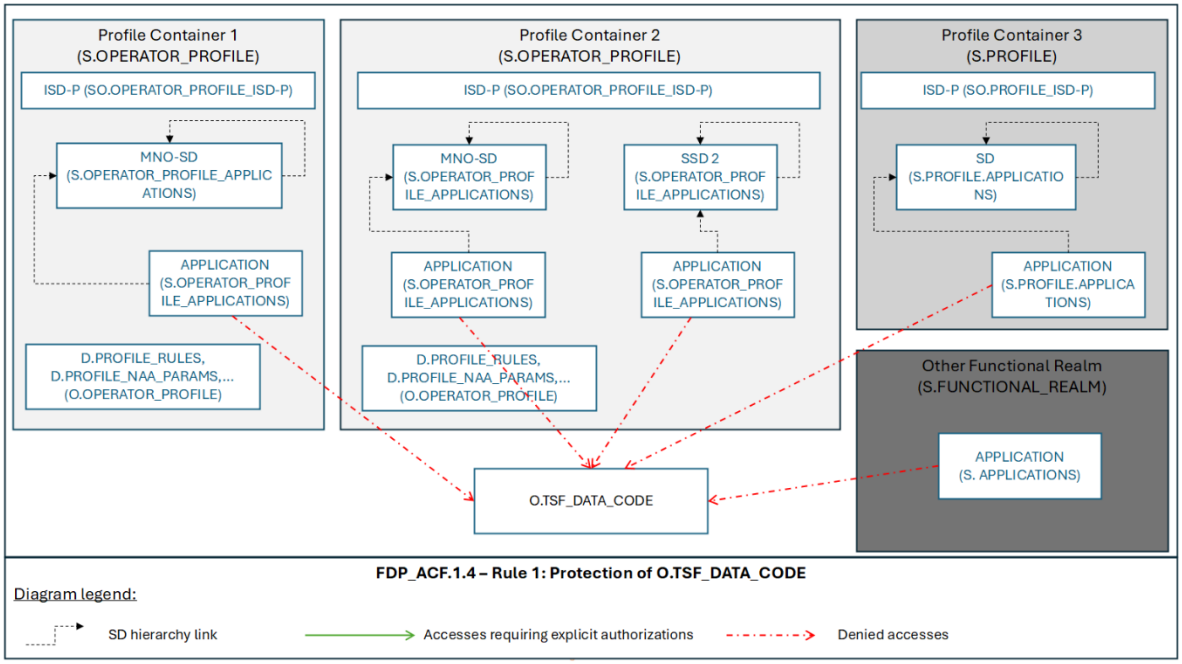

Figure 2: Example of O.TSF_DATA_CODE protection from all Applications

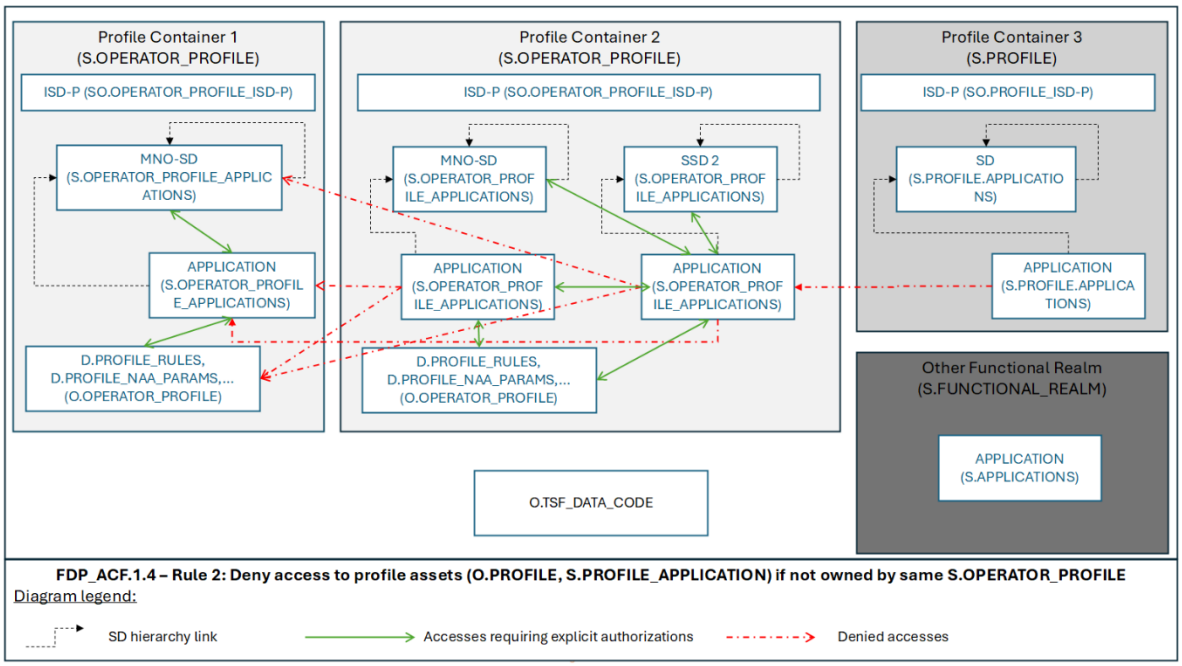

Figure 3: Example of Intra Profile Data and Application allowed, but protection from outside Functional Realms

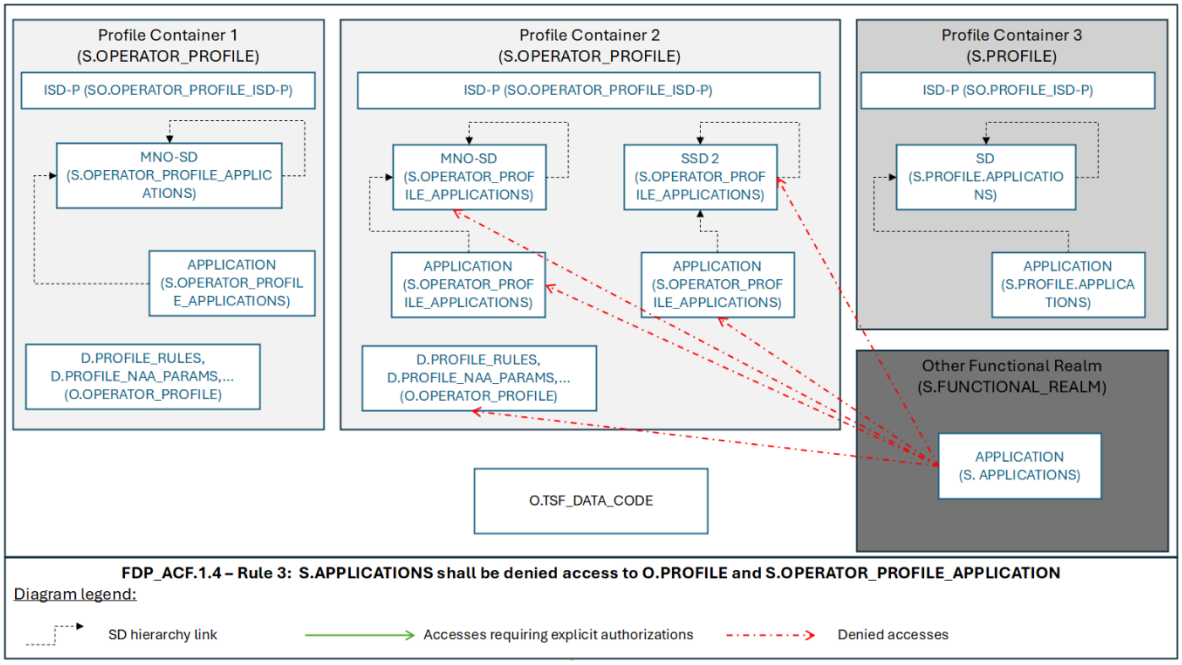

Figure 4: Example of Profile Data and Applications protection from S.APPLICATIONS

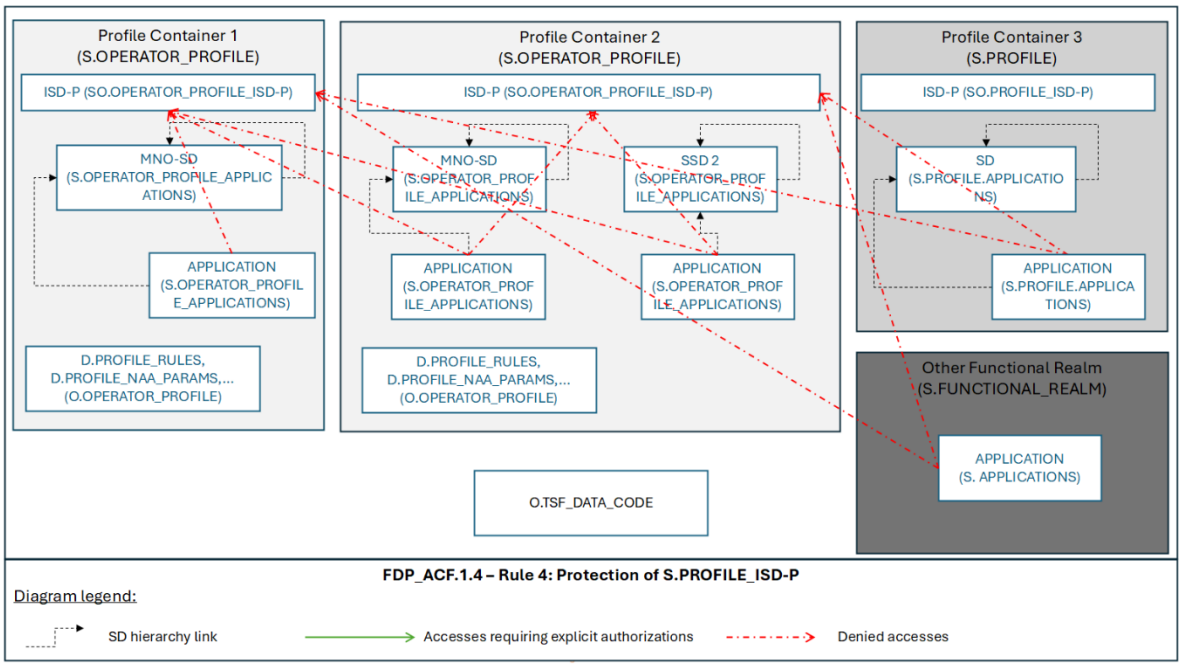

Figure 5: Example of ISD-P protection from S.APPLICATIONS

Subject/Object	Description
S.OPERATOR_PROFILE_APPLICATIONS	Applications within Operator Profiles, either Provisioning or Subscription (including Network

	Access Applications, mobile Applications, and other executable components).
SO.OPERATOR_PROFILE_ISD-P	ISD-P within Operator Profiles
S.OPERATOR_PROFILE	Operator-owned containers representing individual commercial subscriptions and containing all Operator-specific Applications, data, and credentials for network access included in a SO.ISD-P.
S.PROFILE_APPLICATIONS	Applications within subscription Profiles (including Network Access Applications, mobile Applications, and other executable components).
S.APPLICATIONS	On-card Applications not contained inside any Operator Profile (for example, in the ISD-R, ECASD , test Profile or inside a Non-eSIM Functional Realm).
S.PROFILE	Containers not owned by an MNO (e.g., Test Profile).
S.FUNCTIONAL_REALM	Functional Realm which is not a Profile.
SO.PROFILE_ISD-P	ISD-P within Profiles now owned by an MNO.
O.OPERATOR.PROFILE	Operator-owned Profile data and code including D.MNO_KEYS, D.PROFILE_NAA_PARAMS, D.PROFILE_IDENTITY D.PROFILE_RULES, D.PROFILE_USER_CODES (SGP.22), D.PROFILE_CODE and D.PROFILE_APPLICATIONS.
O.TSF_DATA_CODE	Platform protected data and code including D.PLATFORM_DATA, D.DEVICE_INFO, D.PLATFORM_RAT, D.SK.EUICC.ECDSA, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.PK.EIM.ECDSA (SGP.32), D.EID, D.SECRETS, D.CERT.EUM.ECDSA, D.CRLs and D.TSF_CODE (the TSF Code distinguishes between the ISD-R, ISD-Ps, ECASD, and the Platform code).

3.4.1 FDP_ACC.2/ISOLATION Complete access control

FDP_ACC.2.1/ISOLATION The TSF shall enforce the [assignment: **Profile Isolation SFP**] on [assignment:

- **Subject:**
  - **S.OPERATOR_PROFILE_APPLICATIONS**
  - **S.OPERATOR_PROFILE**
  - **S.PROFILE**
  - **S.APPLICATIONS**

- **SO.OPERATOR_PROFILE_ISD-P**
- **SO.PROFILE_ISD-P**

- **Objects:**

  - **O.OPERATOR_PROFILE**
  - **O.TSF_DATA_CODE**
  - **SO.OPERATOR_PROFILE_ISD-P**
  - **SO.PROFILE_ISD-P**

] and all operations among subjects and objects covered by the SFP.

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

3.4.2 FDP_ACF.1/ISOLATION Security attribute-based access control

FDP_ACF.1.1/ISOLATION The TSF shall enforce the [assignment: **Profile Isolation SFP**] to objects based on the following: [assignment:

Subject/Object	Security attributes
O.OPERATOR_PROFILE	Ownership by a S.OPERATOR_PROFILE

]

FDP_ACF.1.2/ISOLATION The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: **None**].

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

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

1. **S.OPERATOR_PROFILE_APPLICATION and S.APPLICATIONS shall be denied access to O.TSF_DATA_CODE regardless of Profile ownership**.
2. **S.OPERATOR_PROFILE_APPLICATION shall be denied access to O. OPERATOR_PROFILE and other S.OPERATOR_PROFILE_APPLICATION if they are not owned by the same S.OPERATOR_PROFILE**. **Furthermore, an S.OPERATOR_PROFILE_APPLICATION shall be denied access to the MNO-SD assets and other Application within the same Profile unless an explicit, shareable interface object is defined.**
3. **S.APPLICATIONS shall be denied access to O.OPERATOR_PROFILE and S.OPERATOR_PROFILE_APPLICATION.**
4. **Any type of Application (S.PROFILE_APPLICATION, S.APPLICATIONS or S.OPERATOR_PROFILE_APPLICATION) shall be denied access to SO.OPERATOR_PROFILE_ISD-P regardless of Profile ownership as well as O.TSF_DATA_CODE**
5.

].

3.4.3 FMT_MSA.1/ISOLATION Management of security attributes

FMT_MSA.1.1/ISOLATION The TSF shall enforce the [assignment: **Profile Isolation SFP**] to restrict the ability to [selection: **change_default, modify and delete**] the security attributes [assignment: **ownership of O.OPERATOR_PROFILE**] to [assignment: **no role (nobody)**].

3.4.4 FMT_MSA.3/ISOLATION Static attribute initialisation

FMT_MSA.3.1/ISOLATION The TSF shall enforce the [assignment: **Profile Isolation SFP**] to provide [selection, **restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/ISOLATION The TSF shall allow the [assignment: **no role (nobody)**] to specify alternative initial values to override the default values when an object or information is created.

4 Security Assurance Rationale Refinements

4.1 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 rules included in A.APPLICATIONS and OSP.APPLICATIONS must be sufficient to maintain the security for all Applications loaded on the eUICC containing the TOE. In addition, the TOE shall provide additional isolation mechanisms to guarantee O.ISOLATION independently from the defined objectives for the environment.

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.

4.2 Refinements of Vulnerability Analysis (AVA_VAN.5)

Refinement:

The vulnerability analysis covers the resistance against logical attacks related to the threat T.UNVERIFIED_APPLICATION. This is covered with independence from the rules derived from the objectives for the environment OE.APPLICATIONS (in case of Java Card also OE.VERIFICATION, OE.CAP-FILE and OE.CODE-EVIDENCE).

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
V1.0	17th July 2026	CR0001R01 - Application Definition CR0002R01 - Addition of OE.CAP-FILE CR0003R04 - Assumptions, Organisation Security Policies and Security Objectives Rationale CR0004R06 - New Security Objectives and Clarification of application note 23 of OE.APPLICATIONS CR0005R01 - Modify the diagram for section 3.4 to address feedback and add a description CR0008R01 - Addition of IJC file format CR0007R01 - PP_Module_on_Security Enhacements_Plus_Clarifcations_Threat CR0010R00 – PP Module Refinement Clarification CR0011R00 – Functional Real Images CR0009R04 - Refinement of T.UNVERIFIED_APPLICATION CR0012R01 - Editorial CR to create refinement section CR0013R01 - Editorial CR to add Application Note numbering CR0014R02 -Zero trust environment approach CR0014R04 -Zero trust environment approach	ISAG	Gloria Trujillo, GSMA