电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0055-V1.0.0:2020

面向物联网设备的嵌入式通用集成电路卡（eUICC）安全能力技术要求

Embedded Universal Integrated Circuit Card (eUICC) M2M Security Requirements Specification

2020- 04-09 发布　　2020- 04-09 实施

电信终端产业协会　　发 布

目次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、中国电信集团有限公司、中国联合网络通信股份有限公司、华为技术有限公司、北京中广瑞波科技股份有限公司、上海果通通信科技股份有限公司、捷德（中国）信息科技有限公司。

本标准主要起草人：路晔绵、国炜、魏凡星、李煜光、贾聿庸、杨剑、耿炎、刘煜、仇剑书、常新苗、范姝男、朱旭东、邹俊伟、吴俊、彭成、孙亨博、李明。

引　　言

随着移动通信技术的发展及广泛应用，物联网业务也向移动性、易于连接和远程管理的方向迅速发展，因此，推动物联网终端接入移动网络的关键模块智能卡产生了新的技术需求：一种新的智能卡形态eUICC(Embedded UICC，嵌入式通用集成电路卡)出现，eUICC 是物联网终端接入网络的安全工具，同样是承载各种应用、数据的安全载体，然而新的智能卡形态的诞生也伴随而来相关的安全问题。

本标准主要参考了 GSMA 的《SGP.05 Embedded eUICC Protection Profile》等规范规定的安全框架，并结合行业的实际情况和需求编写而成。

面向物联网设备的嵌入式通用集成电路卡（eUICC）安全能力技术要求

1 范围

本标准规定了物联网嵌入式通用集成电路卡的安全技术要求,包括安全问题定义、安全目标、安全功能和安全保障要求等内容。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GSMA SGP.05: eUICC Protection Profile Version 1.1

PP-JCS: Common Criteria Protection Profile Java Card™ System Open Configuration，Version 3.0

PP0084: Security IC Platform Protection Profile with Augmentation Packages Version 1.0

GSMA: SGP.02: Remote Provisioning Architecture for Embedded UICC Technical Specification version 3.0

GP-SecurityGuidelines-BasicApplications: GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications - Version 1.0

GPC_GUI_010: GlobalPlatform Card Specification v2.2.1 UICC Configuration v1.0.1

GlobalPlatform_Card_Specification: GlobalPlatform Card Specification v2.2.1

SCP80: ETSI TS 102 225 [Secured packet structure for UICC based applications; Release 9] ETSI TS 102 226 [Remote APDU structure for UICC based applications; Release 9]

SCP81: GlobalPlatform Card Specification v.2.2 Amendment B: Remote Application Management over HTTP v1.1.1

MILENAGE: 3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 11)

Tuak: 3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233 (Release 12)

KS2011: W. Killmann, W. Schindler, A proposal for: Functionality classes for random number generators, Version 2.0

3 术语、定义和缩略语

下列术语和定义适用于本文件。

3.1 术语定义

3.1.1 嵌入式 UICC Embedded UICC

不容易接触或替换的 UICC，在终端中不能被删除或替换，并可安全的进行 Profile 变更。

3.1.2 用户信息 Profile

配置在或出现在 eUICC 上的文件结构、数据和应用程序的集合。

3.1.3 预置用户信息 Provisioning Profile

一个包含 NAA 参数且有能力访问通信网络的 Profile，为 eUICC 管理和 Profile 管理提供 eUICC 和远程签约管理平台之间的传输能力。

3.1.4 用户信息激活 Enabled Profile

Profile 的一种状态，它的文件和/或应用程序（例如 NAA）可通过 UICC-终端接口选择。

3.1.5 Profile 策略授权规则 Profile Policy Authorisation Rule(PPAR)

可以管理 Profile 所有者使用 Profile 策略规则的能力的一组数据。

3.1.6 Profile 策略启动器 Profile Policy Enabler

Profile 管理系统内的一个功能原件，用于解释以及执行 Profile 策略规则。

3.2 缩略语

下列缩略语适用于本文件。

CASD	Controlling Authority Security Domain	授权控制安全域
CI	Certificate Issuer	证书发行方
ECASD	eUICC Controlling Authority Security Domain	eUICC 授权控制安全域
EUM	eUICC Manufacturer	eUICC 卡制造商
EID	eUICC-ID	eUICC 标识
eUICC	Embedded UICC	嵌入式 UICC
ISD	Issuer Security Domain	主安全域
ISD-P	Issuer Security Domain Profile	Profile 集主安全域
ISD-R	Issuer Security Domain Root	根主安全域
MNO	Mobile Network Operator	移动网络运营商
NAA	Network Access Application	网络接入应用
PPAR	Profile Policy Authorisation Rule	Profile 策略授权规则
PPE	Profile Policy Enabler	Profile 策略规则使能器
PPR	Profile Policy Rules	Profile 策略规则
RAT	Rules Authorisation Table	规则授权表
SM	Subscription Manager	签约管理
SM-DP+	Subscription Manager Data Preparation	签约管理数据准备
UICC	Universal Integrated Circuit Card	通用集成电路卡

4 eUICC 架构

4.1 eUICC 架构概述

本节主要描述当前广泛被使用的基于 eUICC 架构的电信标准，以及非常适合建立角色分离和数据隔离的 GlobalPlatform 标准。尤其是，每个实体都拥有一个具有不同权限和配置的专用安全域。

eUICC 体系结构包含以下安全域，用于平台和 Profile 管理：

- ISD-R 是卡外实体 SM-SR 的代表；
- ECASD 是卡外实体 CI 的代表；
- ISD-P 是卡外实体 SM-DP 的代表，一个 eUICC 可以包含多个 ISD-P。

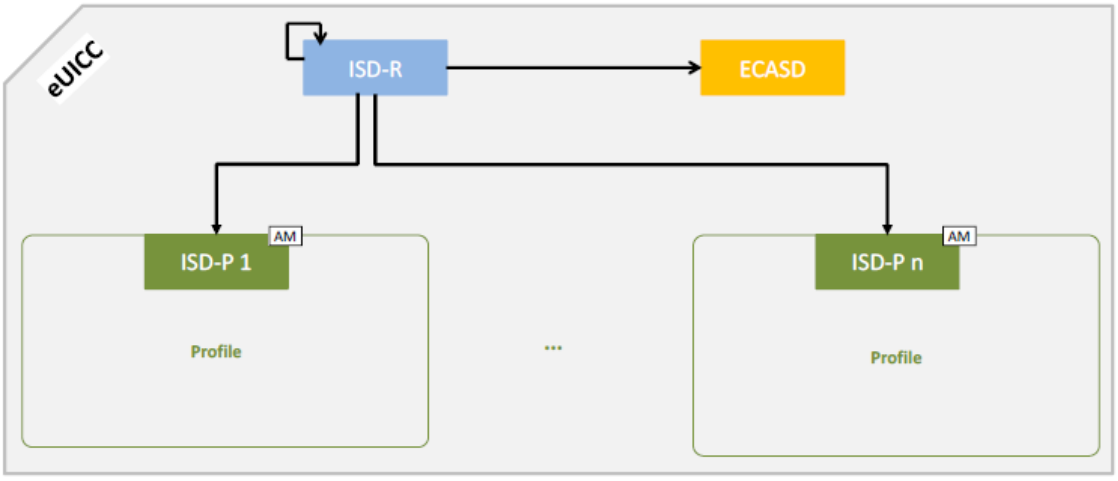

图 1 安全域架构概述

在 GlobalPlatform 卡规范中定义的 ISD 在 eUICC 的体系结构中不存在。

4.1.1 ISD-R

一个 eUICC 上只能有一个 ISD-R。

ISD-R 应当在 eUICC 的制造期间由 EUM 进行安装和个人化。ISD-R 应与自身相关联。

在 eUICC 制造完成之后，ISD-R 应处于 GlobalPlatform 卡规范第 5.3 节中所定义的生命周期中的 PERSONALIZED 状态。ISD-R 不支持 LOCKED 状态。

ISD-R 的权限应根据附录 B 授予。

ISD-R 只能在 ISD-P 上执行平台管理功能。

4.1.2 ECASD

一个 eUICC 上只有一个 ECASD。

ECASD 应在 eUICC 制造期间由 EUM 安装和个人化。ECASD 应与 ISD-R 相关联。

在 eUICC 制造完毕之后，ECASD 应处于 Global Platform 卡规范第 5.3 节中的定义的 PERSONALIZED 状态。

ECASD 包含以下功能：

- 为 Profile 下载和安装建立 SM-DP 密钥集；
- 为 SM-SR 变更建立 SM-SR 密钥集。

ECASD 应在 eUICC 制造期间由 EUM 进行个人化，需要安装以下数据：

- PK.CI.ECDSA；

- SK.ECASD.ECKA；
- CERT.ECASD.ECKA 用来进行 eUICC 认证并建立密钥；
- EUM key set 用来更新密钥；
- EID。

ECASD 应符合在 GlobalPlatform 卡规范 UICC 配置中 CASD 的要求，除了以下几点：

- AID 和 TAR 应按 SGP.02 规范 2.2.3 节的规定进行分配；
- 不需要支持 SCP02；
- 只有 ISD-R 和 ISD-P 才能使用 ECASD 服务。

4.1.3 ISD-P

一个 ISD-P 拥有唯一的 Profile。

在任何时间点，eUICC 上只有一个 ISD-P 处于启用状态。

ISD-P 应由 ISD-R 安装，然后由其相关的 SM-DP 进行个人化。在 eUICC 制造期间，至少应安装一个带有 Profile 的 ISD-P，并由 EUM 进行首次个人化，用于后面的 eUICC 连接。

除了 ISD-R，ISD-P 外部的任何组件都不具有对其 Profile 的可见性或访问权限，ISD-R 应具有对 POL1 的读访问权限。

一个 Profile 组件不得对 ISD-P 之外的任何组件具有可见性或访问权限。一个 ISD-P 不得对任何其他 ISD-P 具有可见性或访问权限。

在不同的 Profile 中可以分配相同的 AID。Profile 组件不得使用保留的 ISD-R、ISD-P 和 ECASD 的 AID。

在不同的 Profile 中可以分配相同的 TAR。Profile 组件不得使用保留的 ISD-R、ISD-P 和 ECASD 的 TAR。

ISD-P 在其生命周期中应始终与 ISD-R 相关联，以便 ISD-R 能够执行平台管理功能：

- ISD-P 创建：在创建的时候建立 ISD-R 和 ISD-P 之间的关联；
- ISD-P 删除和 Master 删除；
- Profile 的启用和禁用；
- 回滚属性设置；
- 数据传输功能：允许在 SM-DP 和 ISD-P 之间建立 SCP03/SCP03t 连接。

ISD-P 应基于 GlobalPlatform 卡规范第 5.3 节中定义的安全域生命周期遵循图 2 所示的生命周期。

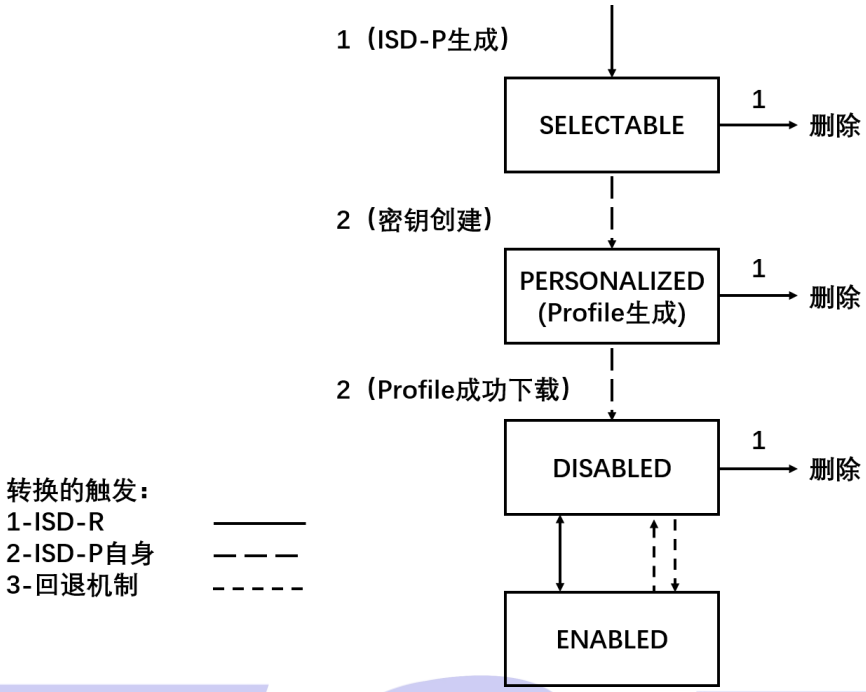

图 2 ISD-P 生命周期转换

ISD-P 生成后处于 SELECTABLE 状态，在密钥对建立后处于 PERSONALIZED 状态。

注意：ISD-P 创建命令跳过了 GlobalPlatform 卡规范中定义的安全域的 INSTALLED 状态。

在 Profile 下载和安装，或者执行了 Profile 禁用的流程之后，ISD-P 应处于禁用状态。如果另一个 ISD-P 被启用，或者启动了回滚机制，ISD-P 也可能转换到禁用状态。

执行 Profile 启用的过程后，ISD-P 应处于启用状态。如果回滚机制被激活，ISD-P 也可能转换到启用状态。

删除 ISD-P 会从 eUICC 中删除 ISD-P 及其 Profile。

ISD-P 不支持 LOCKED 状态。

对于状态编码，本标准对 Global Platform 卡规范的表 11-5 修改如下：

表 1 ISD-P 状态编码

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	1	1	(INSTALLED)
0	0	0	0	0	1	1	1	SELECTABLE
0	0	0	0	1	1	1	1	PERSONALIZED (Profile creation)
0	0	0	1	1	1	1	1	DISABLED
0	0	1	1	1	1	1	1	ENABLED

这些状态可以映射到 SGP.01 中定义的体系结构状态，如下所示：

表 2 ISD-P 状态映射

State (as defined in [1])	State (as defined above)
Created	(INSTALLED)
	SELECTABLE
	PERSONALIZED
Disabled	DISABLED
Enabled	ENABLED
Deleted	No explicit mapping; ISD-P no longer exists on the eUICC

ISD-P 权限应根据附录 B 授予。

所有 Profile 组件，特别是 MNO-SD，应保持与 ISD-P 的关联，以便实现以下目标：

- Profile 下载和安装：生成从属于 ISD-P 的 Profile 组件；
- ISD-P 删除和 Master 删除：Profile 组件应当被删除；
- Profile 启用和禁用：启用和禁用对所有 Profile 组件的访问；
- 更新 POL1；
- 在平台管理功能需要时提供对 POL1 的读访问权限。

分配给一个 Profile 组件的应用权限（在 GlobalPlatform 卡规范中定义）应按照附录 B 适用。

由 ISD-P 创建的所有 Profile 组件应始终保持与该 ISD-P 的从属关系，任何 Profile 组件与 ISD-P 的从属关系一旦确立不能够被更改。

当 ISD-P 未处于启用状态时，eUICC 应确保：

- 无法通过 ES6 接口远程管理任何 Profile 组件；
- 任何设备或应用都无法在 eUICC 上选择 Profile 组件中的文件系统；
- 无法选择、触发或删除 Profile 中的应用（包括安全域和具有网络访问权限的应用）。

4.1.4 Profile

Profile 的结构由一组 Profile 组件组成，该结构由 MNO 定义并且完全处于 MNO 的控制下。整体的 Profile 结构应包含在唯一的 ISD-P 中。

Profile 结构应包含一个名为 MNO-SD 的 Profile 组件，它与 UICC 的 ISD 处于相同的角色（参见 GlobalPlatform 卡规范）。MNO-SD 代表 MNO 拥有该 Profile，它包含了 MNO 的 OTA 密钥集。

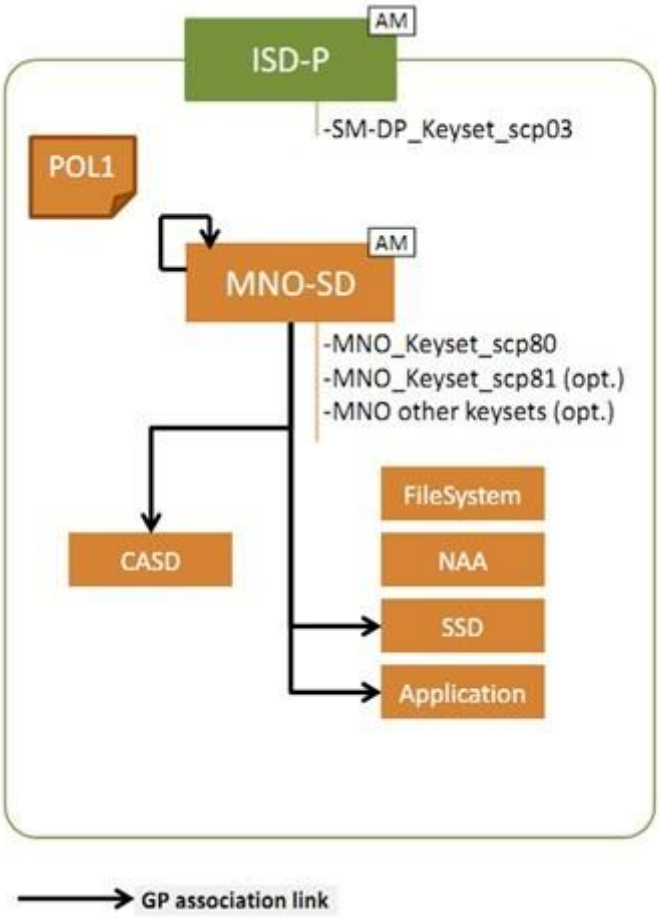

图 3 Profile 的结构概述

图 3 中的 Profile 提供了 Profile 结构的示例。

Profile 结构应包括：

- MNO-SD；
- 至少一个 NAA；
- POL1，即使不被使用；
- 文件系统；
- Profile 的连接参数。

Profile 结构可能包含：

- 除 MNO-SD 外，还有多个应用（如 GlobalPlatform 卡规范中所定义）；
- 一个 CASD（在 Global Platform 卡规范 UICC 配置中定义）。

MNO 应按照 ETSI TS 102 225 和 ETSI TS 102 226 中所规定的，在 MNO OTA 平台和 Profile 的安全域之间建立安全通道。

4.1.5 MNO-SD

MNO-SD 是 Profile 的一个必要组件，MNO 拥有其所有权。MNO-SD 提供 eUICC 与 MNO 的 OTA 平台之间的安全通道，用来管理处于启用状态的 Profile。

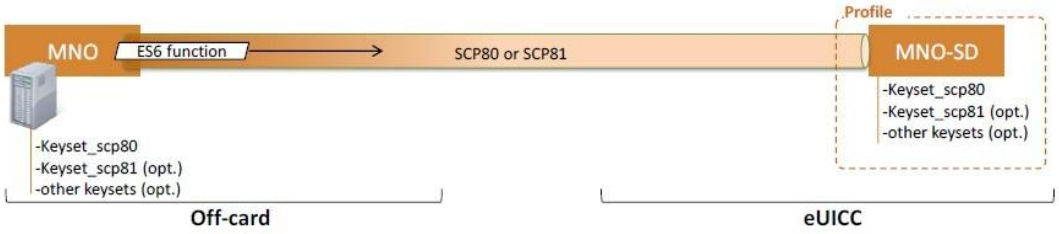

图 4 MNO 与 MNO-SD 之间的安全通道

MNO-SD 的 AID 和 TAR 由 MNO 在定义 Profile 时自由分配。

MNO-SD 的权限分配应遵循附录 B。

5 eUICC 安全问题定义

5.1 安全资产

资产是受 TOE 直接保护的、与安全相关的要素。资产可分成两类。第一类包含由用户创建并使用的数据（用户数据），第二类包含由 TOE 创建并使用的数据（TSF 数据）。对于每类资产，需要详述它们面临的风险类别。

备注：

虽然底层的运行时环境中列出的资产不包括在此标准中，但安全目标编写者仍应考虑的所有资产。

5.1.1 用户数据

用户数据包括：

由 ISD-R 控制的用户数据:

- ISD-R 密钥组 (D.ISDR_KEYS)

由 ISD-P 控制的用户数据:

- ISD-P 密钥组 (D. ISDP_KEYS)
- 至少一个网络鉴权应用（D.PROFILE-CODE 的一部分）及其相关参数（D.PROFILE_NAA_PARAMS）
- POL1 策略文件（D.PROFILE_POL1）
- 文件系统（包含在 D.PROFILE-CODE）
- MNO-SD（D.MNO_SD），其中可包括其他应用，以及
    - 与 Profile 关联的身份信息（D.PROFILE_IDENTITY）
    - MNO-SD 密钥组（D.MNO_KEYS）

此标准旨在保护 Profile 的数据和应用，与其格式无关。因此，在资产描述中，格式将不作详细说明。

5.1.1.1 密钥

安全域拥有的密钥。所有密钥都应受到保护以免受未经授权的泄露和修改。

D.MNO_KEYS

MNO OTA 平台用于从 ISD-P 请求管理操作的密钥。密钥在配置过程中加载，并在 MNO SD 的控制下存储。

D.ISDR_KEYS

SM-SR 使用此平台管理密钥集，通过其卡上代表 ISD-R 执行平台管理功能。

D.ISDP_KEYS

SM-DP 使用此 Profile 管理密钥集，通过其卡上代表 ISD-P 执行 Profile 管理功能。

5.1.1.2 Profile 数据

应用程序的机密敏感数据，如对象中包含的数据、包的静态字段、当前执行方法的局部变量或操作堆栈的位置。

这些数据需要保护免受未经授权的披露和修改。

D.PROFILE_NAA_PARAMS

用于网络鉴权的参数，包括密钥。这些参数可能包括例如 Opc、Ri、Ci 等。参数在配置过程中加载并在 ISD-P 的控制下存储。它们可以传输到包含鉴权算法的电信框架。

D.PROFILE_IDENTITY

移动用户标识（IMSI）是用于 MNO 的网络鉴权算法中的用户身份标识。IMSI 是用户的身份标识，MNO 将使用其作为其 HLR 中用户的索引。用户身份标识在配置过程中在 ISD-P 的控制下存储。

IMSI 应受到保护，避免未经授权的修改。

D.PROFILE_POL1

Profile 中策略控制规则的数据。这些规则在配置过程中加载，并在 ISD-P 的控制下存储。它们由 MNO OTA 平台管理。

应保护 POL1，防止未经授权的修改。

5.1.1.3 Profile 代码

D.PROFILE_CODE

Profile 中应用包括一级和二级应用，特别是：

- MNO-SD 和在 MNO-SD 控制下的安全域（如 CASD / SSD）
- 在 MNO-SD 内配置其他应用（网络接入应用等）

按照惯例，此资产还包括 Profile 的文件系统。

所有这些应用都在 MNO SD 的控制下。

必须保护这些资产，防止未经授权的修改。

5.1.2 TSF 数据

TSF 数据包括三类数据:

- TSF 代码，确保 Profile 数据的保护
- 管理数据，确保应用的管理将强制执行一组规则（例如权限、生命周期等）
- 身份管理数据，保证 eUICC 和远程参与者的身份。

5.1.2.1 TSF_CODE

D.TSF_CODE

TSF 代码包含：

- ISD-R、多个 ISD-P、ECASD
- 平台代码

所有这些资产都必须得到保护，以免受未经授权的披露和修改。对此代码的了解可能允许绕过 TSF。这涉及到运行时的逻辑攻击，以获得对可执行代码的读取访问权限，通常是通过执行试图尝试读取存储一段代码的内存区域的应程序用来执行的。

应用说明：

- 这不包括 MNO-SD 中的应用程序，这些应用是用户数据的一部分(Profile 应用)
- 未经授权的披露和修改的要求与本规范中的要求相同。

5.1.2.2 管理数据

D.PSF_DATA

PSF 环境的数据，例如，

- 标识符和权限，包括 smsr-id, mno-id 和 smdp-id
- eUICC 生命周期状态
- eUICC 的配置状态或“ISD-P 状态”（INSTALLED, SELECTABLE, PERSONALIZED, DISABLED, ENABLED）
- 回滚属性（当仅有一个 Profile 时，该属性必须为"true"）

“配置状态”是一组在 ISD-P 的配置周期中定义的数据，它与 eUICC 生命周期完全不同。

这些数据可以部分实现在 ISD-R 和 PSF 代码逻辑中，而不是笼统地说是“数据”。因此，该资产与 D.TSP_CODE 密切相关。

必须保护这些资产，防止未经授权的修改。

5.1.2.3 身份管理数据

身份管理数据用于保证参与者身份的真实性。这包括：

- EID，eUICC 证书和相关私钥，用于保证 eUICC 的身份
- CI 的根公钥，用于验证所有参与者的证书
- 用于生成凭据的共享秘密

注意：在当前版本的标准中不考虑用于密钥/证书续订的 EUM 密钥集，因为没有为密钥续订定义的场景。

D.eUICC_PRIVKEY

eUICC 私钥由 eUICC 用于证明其身份并与远程参与者生成共享秘密，存储在 ECASD 中。

必须保护它免受未经授权的披露和修改。

D.eUICC_CERT

EUM 为特定的个人 eUICC 颁发的证书。可以使用 EUM 证书验证此证书。存储在 ECASD 中。

必须保护 eUICC 证书免受未经授权的修改。

备注：

为了验证 eUICC 的认证链，需要 EUM 证书和 CI 的根证书。但是，此标准尚未考虑 EUM 证书，因为没有针对其在 eUICC 中的生命周期定义用例。

D.CI_ROOT_PUBKEY

CI 的根公钥用于验证 eUICC 和远程参与者的认证链。它存储在 ECASD 中。

必须保护 CI 的根公钥免受未经授权的修改。

D.EID

EID（eUICC-ID）唯一标识 eUICC。该标识符由 eUICC 制造商设置，并且在 eUICC 的运行期间不会改变。它存储在 ECASD 中。EID 被 SM-SR 用作关键字，以识别其数据库中的 eUICC。

应保护 EID 免受未经授权的修改。

D.SECRETS

该资产包括：

- 用于保护 Profile 下载的共享密钥
- 用于在切换期间保护新 SM-SR 凭证的共享秘密。当 ISD-R 或 ISD-P 请求时，ECASD 生成共享秘密，然后将其发送到请求密钥的安全域。

应保护共享秘密免受未经授权的披露和修改。

5.2 用户/主体

本节包含两个部分：

- 用户，TOE 外的实体，可访问 TOE 的服务或接口；
- 主体，TOE 的特定部分，执行特定操作。主体是资产 D.TSF_CODE 的子部分。

所有的用户和主体都是角色。

5.2.1 用户

U.SM-SR

安全执行平台管理命令以及 Profile 管理命令的传输功能的角色。

U.SM-DP

准备 Profile 和管理 Profile 在 eUICC 上的安全下载和安装的角色。

U.MNO-OTA

远程管理 UICC 和 eUICC 上激活的 MNO Profile 内容的 MNO 平台。

U.MNO-SD

MNO-SD 是 Profile 的一个安全域部分，归 MNO 所有，提供与 MNO OTA 平台（U.MNO-OTA）的安全通道。用于 Profile 激活后 Profile 内容的管理。

一个 eUICC 可以包含多于一个 MNO-SD。

5.2.2 主体

S.ISD-R

ISD-R 是卡外实体 U.SM-SR 的代表。

S.ISD-P

ISD-P 是卡外实体 U.SM-DP 的代表。

S.ECASD

ECASD 是卡外实体 CI 的代表。

S.PSF

PSF 是具有特定权限的（一组）应用程序，负责管理 eUICC，在 D.TSF_CODE 中描述。

S.TELECOM

网络访问应用程序用于在移动网络上验证 eUICC 的一组算法。电信框架在 D.TSF_CODE 中描述。

5.3 安全威胁

5.3.1 未经授权的 profile 和平台管理

卡外参与者或卡上应用程序可能会尝试执行以下操作来破坏 eUICC：

- 未经授权的 Profile 管理（通常访问或修改 Profile 的内容，例如在安装之前更改下载的 Profile，或泄漏存储在 Profile 中的网络身份验证参数）；
- 或未经授权的平台管理（通常尝试禁用已启用的 Profile）。

这两个通用类别分为四种特定威胁：

- T.UNAUTHORIZED-PROFILE-MNG：试图在未经授权的情况下披露/修改 ISD-P 或 MNO-SD 的功能内容;
- T.UNAUTHORIZED-PLATFORM-MNG：试图在未经授权的情况下披露/修改 ISD-R 的内容或功能;
- T.PROFILE-MNG-INTERCEPTION：尝试伪造/拦截/修改/重放由 SM-DP 或 MNO-SD 发送的命令或 Profile（在传输期间或在 eUICC 上加载期间）；
- T.PLATFORM-MNG-INTERCEPTION：尝试伪造/拦截/修改/重放由 SM-SR 发送的命令或凭证（在传输期间或在 eUICC 上加载期间）。

T.UNAUTHORIZED-PROFILE-MNG

恶意的卡上应用程序：

- 修改或泄露属于 ISD-P 或 MNO-SD 的 Profile 数据;
- 执行或修改 Profile 应用程序（ISD-P，MNO-SD 和 MNO-SD 控制的应用程序）的操作
- 修改或泄露 ISD-P 或 MNO-SD 应用程序。

此类威胁通常包括例如：

- 直接访问 Java 对象的字段或方法
- 利用 APDU 缓冲区和全局字节数组

本标准没有解决以下情况：

- ISD-P 中的应用程序试图破坏其自己的 MNO-SD
- ISD-P 中的应用程序试图破坏在其自己的 MNO-SD 或 ISD-P 的控制下的另一个应用程序。

这些案例被认为是 MNO 的责任，因为它们只会损害自己的 Profile，而不会对其他 MNO 的 Profile 产生任何副作用。

本标准解决了以下情况：

- ISD-P 内的应用试图破坏另一个 MNO-SD 或 ISD-P
- ISD-P 内的应用程序试图破坏在另一个 MNO-SD 或 ISD-P 的控制下的应用程序
- ISD-P 中的应用程序试图破坏其自身的 ISD-P。前两个案例会对其他 MNO Profile 产生影响。最后一种情况包括修改 ISD-P 的回滚属性，从而对整个平台管理行为产生影响。

直接威胁资产：D.ISDP_KEYS，D.MNO_KEYS，D.TSF_CODE（ISD-P），D.PROFILE_*

T.UNAUTHORIZED-PLATFORM-MNG

卡上应用程序：

- 修改或披露 ISD-R 数据;
- 执行或修改 ISD-R 的操作。

这种威胁通常包括例如：

- 直接访问 Java 对象的字段或方法
- 利用 APDU 缓冲区和全局字节数组

直接威胁资产：D.ISDR_KEYS，D.TSF_CODE（ISD-R）

注意：通过改变 ISD-R 的行为，攻击者间接地威胁到 eUICC 的初始配置状态，因此也威胁到 D.PSF_DATA 和与 T.UNAUTHORIZED-PROFILE-MNG 相同的资产。

T.PROFILE-MNG-INTERCEPTION

攻击者改变或窃听 eUICC 和 SM-DP 或 MNO OTA 平台之间的传输，以便：

- 在下载到 eUICC 期间，泄露、替换或修改 Profile 的内容；
- 未经授权在 eUICC 上下载 Profile；
- 替换或修改 SM-DP 或 MNO OTA 平台的命令内容；
- 由 MNO OTA 平台更新时，替换或修改 POL1 数据的内容。

注意：攻击者可能是拦截到安全域的传输的卡上应用程序，或者是拦截 OTA 传输或者 eUICC 和设备之间接口的卡外参与者。

直接威胁资产：D.ISDP_KEYS，D.MNO_KEYS，D.TSF_CODE（ISD-P），D.PROFILE_*

T.PLATFORM-MNG-INTERCEPTION

攻击者改变或窃听 eUICC 和 SM-SR 之间的传输，以便：

- 泄露、替换或修改在 SM-SR 切换期间发送的 SM-SR 凭证;
- 替换或修改 SM-SR 中的命令内容。

注意：攻击者可能是拦截到安全域的传输的卡上应用程序，或者是拦截 OTA 传输或者 eUICC 和设备之间接口的卡外参与者。

直接威胁资产：D.ISDR_KEYS，D.TSF_CODE（ISD-R）

注意：通过改变 ISD-R 的行为，攻击者间接地威胁到 eUICC 的配置状态，因此也威胁到 D.PSF_DATA 和与 T.UNAUTHORIZED-PROFILE-MNG 相同的资产。

5.3.2 身份篡改

T.UNAUTHORIZED-IDENTITY-MNG

恶意的卡上应用程序：

- 泄露或修改在 ECASD 的控制下的数据：
  - 泄露或修改 D.eUICC_PRIVKEY
  - 修改 D.EID、D.eUICC_PUBKEY 或 D.CI_ROOT_PUBKEY
  - 修改共享秘密生成方法
- 泄露或修改 ECASD 的功能

这种威胁通常包括例如：

- 直接访问 Java 对象的字段或方法
- 利用 APDU 缓冲区和全局字节数组
- 模拟应用程序、运行环境或修改应用程序的权限

直接威胁资产：D.TSF_CODE（ECASD），D.eUICC_PRIVKEY，D.eUICC_CERT，D.CI_ROOT_PUBKEY，D.EID，D.SECRETS

T.IDENTITY-INTERCEPTION

攻击者可能会尝试拦截凭证，无论是在卡上还是在卡外，以便

- 在另一个 eUICC 或模拟器上使用它们
- 修改它们/用其他凭证替换它们。

这包括：

- 在 SM-SR 切换或 Profile 下载中使用的共享秘密的卡上拦截

这不包括：

- Profile 下载期间的 SM-DP 凭证的卡外或卡上拦截（由 T.PROFILE-MNG-INTERCEPTION 考虑）
- SM-SR 切换期间的 SM-SR 凭证的卡外或卡上拦截（T.PLATFORM-MNG-INTERCEPTION 考虑）

直接威胁资产：D.SECRETS

5.3.3 profile 克隆

T.UNAUTHORIZED-eUICC

攻击者在未经授权的 eUICC 或任何其他未经授权的环境(例如模拟器或软 SIM)上使用合法 Profile。

直接威胁资产：D.TSF_CODE（ECASD），D.eUICC_PRIVKEY，D.eUICC_CERT，D.CI_ROOT_PUBKEY，D.EID，D.SECRETS

5.3.4 未经授权的手机网络访问

T.UNAUTHORIZED-MOBILE-ACCESS

卡上或卡外的攻击者尝试代替合法的 Profile 在 MNO 的移动网络上进行身份验证。

直接威胁资产：D.PROFILE_NAA_PARAMS

5.3.5 其他

T.LOGICAL-ATTACK

卡上的恶意应用程序通过逻辑方式绕过 PSF 措施，以便在平台处理敏感数据时泄露或修改敏感数据：

- IC 和 OS 软件
- 运行环境（例如由 JCS 提供）
- 平台支持功能：
  - 扩展的 GP OPEN
  - 策略执行功能（访问 POL1）
- 电信框架（访问网络验证参数）。

这种威胁的一个例子包括使用缓冲区溢出来访问由本地库操纵的机密数据。此威胁还包括应用程序执行未经授权代码的情况。

直接威胁资产：D.TSF_CODE，D.PROFILE_NAA_PARAMS，D.PROFILE_POL1，D.PSF_DATA

T.PHYSICAL-ATTACK

攻击者通过物理（相对于逻辑）篡改手段泄露或修改 TOE 设计、其敏感数据或应用程序代码。

这种威胁包括环境压力、IC 失效分析、电子探针、意外拆解和侧信道。这还包括通过物理篡改技术更改（一组）指令的预期执行顺序来修改 TOE 运行时执行。

直接威胁：所有资产。

5.4 组织安全策略

5.4.1 生命周期

OSP.LIFECYCLE

TOE 必须强制执行 GSMA SGP.02 规范中定义的 eUICC 生命周期。特别是：

- 一次只启用一个 ISD-P;
- 在禁用或删除 Profile 的情况下，eUICC 必须强制执行 POL1 规则，除非在主删除期间：在这种情况下，即使 POL1 声明无法禁用或删除 Profile，eUICC 也可以禁用和删除当前启用的 Profile。

应用说明：

GSMA SGP.02 规范还包括一个回滚功能，确保 eUICC 能够检测到连接丢失，然后回滚到安全 Profile 并通知 SM-SR。此 PP 未解决此功能。

5.5 假设

A.ACTORS

基础设施的参与者（CI、SM-DP、SM-SR 和 MNO）安全地管理自己的证书和其他敏感数据。特别是为了 3GPP TS 33.102 中定义的整体移动认证机制的安全，某些属性需要保持在 eUICC 范围之外。特别的，用户密钥的生成应具备一定的强度，且密钥应被安全管理。因此陈述以下假设：

- 密钥 K 在 Profile 准备期间随机生成，并被安全地传输到属于 MNO 的认证中心；
- 随机挑战数 RAND 在属于 MNO 的认证中心生成，且应具备足够的熵值；
- 属于 MNO 的认证中心生成唯一序列号 SQN，因此每一个五元组只能使用一次；
- 三元组/五元组在 MNO 之间安全通信以进行漫游。

A.APPLICATIONS

应用程序应符合所用平台的安全准则文档。

6 安全目标

6.1 TOE 的安全目标

6.1.1 平台支持功能

O.PSF

TOE 应提供 PSF 的功能（加载、安装、启用、禁用、删除应用程序和 GP 注册表更新），负责整个 eUICC 和已安装应用程序的生命周期，以及相应的授权控制。特别地，PSF 确保：

- 一次只启用一个 ISD-P;
- 在禁用或删除 Profile 的情况下，必须强制执行规则，除非在主删除期间：在这种情况下，即使 POL1 声明无法禁用或删除 Profile，eUICC 也可以禁用和删除当前启用的 Profile。

此功能应依赖于运行环境安全服务来进行包加载、应用程序的安装和删除。

应用说明：

在实践中，PSF 将与 TOE 的其余部分紧密连接，反过来 TOE 的其余部分可能需要依靠 PSF 来有效执行它的某些安全功能。平台保证只有拥有具有适当权限的安全域的 ISD-R 或服务提供商（SM-DP，MNO）才能管理与其安全域相关联的卡上的应用程序。这是通过政策 POL1 来完成的。执行操作的人员必须事先使用安全域进行身份验证。

O.eUICC-DOMAIN-RIGHTS

TOE 应确保未经授权的参与者不得访问或更改个人化的 ISD-R、ISD-P 或 MNO-SD 密钥。这些安全域密钥集仅限其相应的所有者（SM-SR、SM-DP、MNO OTA 平台）修改。

TOE 不允许在个人化后更改 ECASD 密钥集。

以同样的方式，TOE 应确保只有每个安全域的合法所有者才能访问或更改其机密或完整性敏感数据，例如身份数据（用于 ECASD）或 D.PROFILE_NAA_PARAMS（用于 ISD-P）。

此域的分离功能依赖于应用程序的运行环境保护。

O.SECURE-CHANNELS

eUICC 应保持以下每组之间的安全通道

- ISD-P 和 SM-DP
- ISD-R 和 SM-SR
- MNO-SD 和 MNO OTA 平台。

TOE 应随时确保：

- 传入的消息被未修改地正确地提供给相应的安全域；
- 任何响应消息都正确地返回到卡外实体

应保护通信免受未经授权的披露、修改和重放。

该保护机制应依赖于运行环境和 PSF（参见 O.PSF）提供的通信保护措施。

O.INTERNAL-SECURE-CHANNELS

TOE 确保从 ECASD 传送到 ISD-R 或 ISD-P 的通信共享秘密受到保护，以防止它被泄露或修改。

该保护机制应依赖于运行环境所提供的通信保护措施。

6.1.2 eUICC 身份证明

O.PROOF_OF_IDENTITY

TOE 确保 eUICC 由唯一的 EID 所标识，这是基于 eUICC 的硬件标识。

eUICC 必须提供一种加密手段，以便根据此 EID 向卡外参与者证明其身份。

应用说明：

例如，可以通过在 eUICC 证书中包含 EID 值来获得该证明，该证书由 eUICC 制造商签署。

6.1.3 平台服务

O.OPERATE

属于 TOE 的 PSF 和电信框架应确保其安全功能的正确运行。

应用说明：

FPT_TST.1 可以涵盖 TOE 的启动（TSF 测试）。与 PP-JCS 规范中一样，此 SFR 组件不是必需的。测试也可以随机进行。为了符合其他认证计划，自检可能成为强制性要求。

O.API

属于 TOE 的平台代码应提供 API

- 为其服务提供原子事务，以及
- 控制对其服务的访问。TOE 必须防止未经授权使用命令。

6.1.4 数据保护

O.DATA-CONFIDENTIALITY

在 TOE 对数据进行存储和操作时，TOE 应避免未经授权泄露以下数据：

- D.SECRETS;
- D.eUICC_PRIVKEY;

- 作为下列密钥集的一部分的密钥：
  - D.MNO_KEYS，
  - D.ISDR_KEYS，
  - D.ISDP_KEYS，
  - D.PROFILE_NAA_PARAMS。

应用说明：

在 TOE 的组件中，

- 平台支持功能和电信框架必须保护他们处理的敏感数据的机密性
- 应用程序必须使用运行环境提供的保护机制。

该目标包括抵抗侧通道攻击。

O.DATA-INTEGRITY

TOE 对数据进行管理或操作时，TOE 应避免未经授权修改以下数据：

- 身份管理数据
  - D.eUICC_PRIVKEY;
  - D.eUICC_CERT;
  - D.CI_ROOT_PUBKEY;
  - D.EID
  - D.SECRETS;
- 下列密钥集：
  - D.MNO_KEYS，
  - D.ISDR_KEYS，
  - D.ISDP_KEYS
- Profile 数据
  - D.PROFILE_NAA_PARAMS。
  - D.PROFILE_IDENTITY。
  - D.PROFILE_POL1。

应用说明：

在 TOE 的组件中，

- 平台支持功能和电信框架必须保护其处理的敏感数据的完整性
- 应用程序必须使用运行环境提供的完整性保护机制。

6.1.5 连通性

O.ALGORITHMS

eUICC 应提供对移动网络进行身份验证的机制。

6.2 运行环境的安全目标

6.2.1 参与者

OE.CI

证书颁发者是受信任的第三方，用于验证系统中的实体。CI 为 EUM，SM-SR 和 SM-DP 提供证书。CI 必须确保其自身凭据的安全性。

应用说明：

这种假设的一种可能的实现是执行安全指导文件中定义的安全规则，并定期进行现场检查以检查规则的适用性。

OE.SM-SR

SM-SR 应是负责安全路由和相关 OTA 服务器的可信赖的参与者。SM-SR 站点必须遵循相关规范。SM-SR 具有与 MNO 和 SM-DP 的安全通信信道。

SM-SR 必须确保从 EUM 或其他 SM-SR 收到的平台管理证书的安全性。

应用说明：

根据相关规范进行了认证，从而证明了安全规则的实施。

OE.SM-DP

SM-DP 应是负责数据准备工作和相关 OTA 服务器的可信赖的参与者。SM-DP 站点必须遵循相关规范。

它必须确保其管理和加载到 eUICC 上的 Profile 的安全性，包括但不仅限于：

- MNO 密钥包括 OTA 密钥（由 SM-DP 或 MNO 生成的电信密钥），
- ISD-P 密钥，
- 应用程序提供商安全域密钥（APSD 密钥），
- 控制授权安全域密钥（CASD 密钥）。

SM-DP 必须确保 ISD-P 中使用的任何密钥在传输到 eUICC 之前都是安全生成的。SM-DP 必须确保 ISD-P 中使用的任何密钥在传输到 eUICC 之前没有受到损害。

必须通过明确定义的安全策略来确保 ISD-P 令牌验证密钥的安全性，该策略涵盖生成、存储、分发、销毁和恢复。该策略由 SM-DP 与个人化设备一起实施。

应用说明：

安全规则的实现应通过相关规范的认证来证明。

6.2.2 平台

OE.IC.PROOF_OF_IDENTITY

TOE 使用的底层 IC 是唯一标识的

OE.IC.SUPPORT

IC 嵌入式软件应支持以下功能：

（1）它不允许绕过或者更改 TSF，也不允许访问除 API 程序包提供的功能之外的底层功能。这包括对其私有数据和代码的保护（防止泄露或修改）。

（2）它为平台支持功能和电信框架（S.PSF 和 S.TELECOM）提供安全的底层加密处理。

（3）它允许 S.PSF 和 S.TELECOM 根据需求将数据存储在“持久性技术存储器”或易失性存储器中（例如，瞬态对象不得存储在非易失性存储器中）。内存模型是结构化的，允许底层控制访问（分段故障检测）

（4）它提供了一种为 S.PSF 和 S.TELECOM 原子地执行存储器操作的方法。

应用说明：

该目标相当于 PP-JCS 规范中的 OE.SCP-SUPPORT。

OE.IC.RECOVERY

如果当操作正在进行时断电，则底层 IC 必须允许 TOE 最终成功地完成中断操作，或者是恢复到一致且安全的状态。

OE.RE.PSF

运行环境应为卡管理活动提供安全的手段，包括：

- 加载包文件
- 安装包文件
- 引用包文件或应用程序
- 个人化应用程序或安全域
- 删除包文件或应用程序
- 应用程序或安全域权限更新
- 以超出预期可用性的方式访问应用程序

应用说明：

此标准不需要完全符合 PP-JCS 规范，但 PP-JCS 规范认证的 Java 卡系统必须完全符合此目标。ST 作者可以通过重用与以下威胁相关的 PP-JCS 规范安全目标来转换这一目标：T.DELETION，T.INSTALL。

OE.RE.SECURE-COMM

运行环境应提供保护应用程序通信的机密性和完整性的方法。

应用说明：

该目标特别要求运行环境提供

- 应用程序防火墙
- 应用程序可用于保护交换信息的加密功能

此标准不需要完全符合 PP-JCS 规范，但 PP-JCS 规范下认证的 Java 卡系统需完全满足此目标。ST 作者可以通过重用与以下威胁相关的 PP-JCS 规范安全目标来转换这一目标：T.CONFID-APPLI-DATA 和 T.INTEG-APPLI-DATA。

OE.RE.API

运行环境应确保只能通过 API 调用本机代码。

应用说明：

此标准不需要完全符合 PP-JCS 规范，但 PP-JCS 规范认证的 Java 卡系统需完全满足此目标。 ST 编写者可以通过重新使用与以下威胁相关的 PP-JCS 规范的安全目标来转换这一目标：T.CONFID-JCS-CODE，T.INTEG-JCS-CODE，T.CONFID-JCS-DATA，T.INTEG-JCS-DATA。

OE.RE.DATA-CONFIDENTIALITY

运行环境应提供一种始终保护其处理的 TOE 敏感数据的机密性的方法。

应用说明：

此标准不需要完全符合 PP-JCS 规范，但 PP-JCS 规范认证的 Java 卡系统需完全满足此目标。 ST 作者可以通过以下操作转换这个目标：

重用 PP-JCS 规范中与以下威胁相关的安全目标：T.CONFID-APPLI-DATA

OE.RE.DATA-INTEGRITY

运行环境应提供一种始终保护其处理的 TOE 敏感数据的完整性的方法。

应用说明：

此标准不需要完全符合 PP-JCS 规范，但 PP-JCS 规范认证的 Java 卡系统需完全满足此目标。 ST 作者可以通过重用与以下威胁相关的 PP-JCS 规范的安全目标来转换这一目标：T.INTEG-APPLI-DATA，T.INTEG-APPLI-DATA.LOAD，T.INTEG-APPLI-CODE，T.INTEG-APPLI-CODE.LOAD

OE.RE.IDENTITY

运行环境应确保安全地识别它所执行的应用程序。

OE.RE.CODE-EXE

运行环境应阻止应用程序执行未经授权的代码。

应用说明：

此标准不需要完全符合 PP-JCS 规范，但 PP-JCS 规范认证的 Java 卡系统需完全满足此目标。 ST 作者可以通过重用与以下威胁相关的 PP-JCS 规范的安全目标来转换这一目标：T.EXE-CODE.1，T.EXE-CODE.2，T.EXE-CODE-REMOTE 和 T.NATIVE。

6.2.3 Profile

OE.APPLICATIONS

应用程序应符合 GP-SecurityGuidelines-BasicApplications 规范要求。

OE.MNOSD

根据 GSMA SGP.02 规范，安全域 U.MNO-SD 必须使用 TOE 提供的安全信道 SCP80/81。

6.3 安全目标基本原理

6.3.1 威胁

6.3.1.1 未经授权的 Profile 和平台管理

T.UNAUTHORIZED-PROFILE-MNG

此威胁通过要求合法参与者的身份验证和授权来应对：

- PSF 和 O.eUICC-DOMAIN-RIGHTS 确保只有经过授权和认证的参与者（SM-DP 和 MNO OTA 平台）才能访问安全域的功能和内容。
- OE.SM-DP 和 OE.MNO 在卡外使用时保护相应的凭证

卡上访问控制策略依赖于底层运行环境，该环境确保应用程序数据的机密性和完整性（OE.RE.DATA-CONFIDENTIALITY 和 OE.RE.DATA-INTEGRITY）。

身份验证通过相应的安全通道支持：

- O.SECURE-CHANNELS 和 O.INTERNAL-SECURE-CHANNELS 提供与 SM-DP 通信的安全通道以及与 MNO OTA 平台通信的安全通道。这些安全通道依赖于底层运行环境，它可以保护应用程序之间的通信（OE.RE.SECURE-COMM）。

由于 MNO-SD 安全域不是 TOE 的一部分，因此操作环境必须保证它能够安全地使用 TOE 提供的 SCP80/81 安全信道（OE.MNOSD）。

为了确保应用程序防火墙的安全运行，针对操作环境的以下目标也需要满足：

- 遵守应用程序的安全准则（OE.APPLICATIONS）

T.UNAUTHORIZED-PLATFORM-MNG

此威胁通过要求合法参与者的身份验证和授权来应对：

- PSF 和 O.eUICC-DOMAIN-RIGHTS 确保只有经过授权和认证的参与者（SM-SR）才能访问安全域的功能和内容。
- 当 OE.SM-SR 在卡外使用时保护相应的凭据

卡上访问控制策略依赖于底层运行环境，该环境确保应用程序数据的机密性和完整性（OE.RE.DATA-CONFIDENTIALITY 和 OE.RE.DATA-INTEGRITY）。

身份验证通过相应的安全通道支持：

- O.SECURE-CHANNELS 和 O.INTERNAL-SECURE-CHANNELS 提供与 SM-SR 通信的安全通道。这些安全通道依赖于底层运行环境，它可以保护应用程序之间的通信（OE.RE.SECURE-COMM）。

为了确保应用程序防火墙的安全运行，针对操作环境的以下目标也需要满足：

- 遵守应用程序的安全准则（OE.APPLICATIONS）

T.PROFILE-MNG-INTERCEPTION

命令和 Profile 由 SM-DP 发送到其卡上代表（ISD-P），而 POL1 由 MNO OTA 平台发送到其卡上代表（MNO-SD）。

因此，TSF 确保：

- 通过要求 SM-DP 和 MNO OTA 平台进行身份验证，防止在传输过程中受到未经授权的泄露、修改和重放，确保传输到安全域（O.SECURE-CHANNELS 和 O.INTERNAL-SECURE-CHANNELS）的安全性；这些安全通道依赖于底层运行环境，它可以保护应用程序之间的通信（OE.RE.SECURE-COMM）。

为了确保应用程序防火墙的安全运行，针对操作环境的以下目标也需要满足：

- 遵守应用程序的安全准则（OE.APPLICATIONS）

由于 MNO-SD 安全域不是 TOE 的一部分，因此操作环境必须保证它能够安全地使用 TOE（OE.MNOSD）提供的 SCP80/81 安全信道。

OE.SM-DP 和 OE.MNO 确保在由卡外人员使用时不会泄露与安全通道相关的凭证。

T.PLATFORM-MNG-INTERCEPTION

命令和 Profile 由 SM-SR 发送给其卡上代表（ISD-R）。

因此，TSF 确保：

- 通过要求 SM-SR 进行认证，防止在传输过程中受到未经授权的泄露、修改和重放，确保了向 ISD-R（O.SECURE-CHANNELS 和 O.INTERNAL-SECURE-CHANNELS）传输的安全性；这些安全通道依赖于底层运行环境，它可以保护应用程序之间的通信（OE.RE.SECURE-COMM）。

为了确保应用程序防火墙的安全运行，针对操作环境的以下目标也需要满足：

- 遵守应用程序的安全准则（OE.APPLICATIONS）

OE.SM-SR 确保在由卡外人员使用时不会泄露与安全通道相关的凭证。

6.3.1.2 身份篡改

T.UNAUTHORIZED-IDENTITY-MNG

O.PSF 和 O.eUICC-DOMAIN-RIGHTS 通过为 ECASD 内容和功能提供访问控制策略来应对此威胁。

卡上访问控制策略依赖于底层运行环境，该环境确保应用程序数据的机密性和完整性（OE.RE.DATA-CONFIDENTIALITY 和 OE.RE.DATA-INTEGRITY）。

OE.RE.IDENTITY 确保在 Java 卡级别，应用程序无法模拟其他参与者或修改其权限。

注意：在此标准中，无法为 ECASD 建立安全通道，因为尚未考虑 eUICC 密钥集更新。因此，没有远程角色被授权访问 ECASD 的功能内容。

T.IDENTITY-INTERCEPTION

O.INTERNAL-SECURE-CHANNELS 确保从 ECASD 到 ISD-R 和 ISD-P 的共享秘密的安全传输。这些安全通道依赖于底层运行环境，它可以保护应用程序之间的通信（OE.RE.SECURE-COMM）。

注意：在此标准中，无法为 ECASD 建立安全通道，因为尚未考虑 eUICC 密钥集更新。因此，没有远程角色被授权访问 ECASD 的功能内容。

OE.CI 确保 CI 根目录安全地管理其卡外凭证。

6.3.1.3 profile 克隆

T.UNAUTHORIZED-eUICC

O.PROOF_OF_IDENTITY 保证可以基于 EID 向卡外参与者提供加密身份证明。

O.PROOF_OF_IDENTITY 还可以基于 eUICC 硬件标识（由 OE.IC.PROOF_OF_IDENTITY 来确保其唯一）来保证此 EID 唯一性。

6.3.1.4 未经授权访问移动网络

T.UNAUTHORIZED-MOBILE-ACCESS

目标 O.ALGORITHMS 确保 Profile 只能使用安全身份验证方法访问移动网络，这样可以防止攻击者冒充。

6.3.1.5 其他

T.LOGICAL-ATTACK

通过控制安全域与平台支持功能、电信框架或 TOE 的任何本机/操作系统部分之间的信息流来应对此威胁。因此它包括：

- 由运行环境提供的 APIs（OE.RE.API）
- 通过 TSF 的 API（O.API）。电信框架和平台支持功能的 API 应确保原子事务。

每当应用程序处理 TOE 的敏感数据时，运行环境必须始终保护其机密性和完整性（OE.RE.DATA-CONFIDENTIALITY，OE.RE.DATA-INTEGRITY）。这些敏感数据也可由平台支持功能和电信框架处理，但是，其功能不受运行环境的保护。因此，

- TOE 本身必须确保平台支持功能和电信框架的正确运行（O.OPERATE）
- 平台支持功能和电信框架必须保护其处理的敏感数据的机密性和完整性，而应用程序必须使用运行环境提供的保护机制（O.DATA-CONFIDENTIALITY，O.DATA-INTEGRITY）

还需要满足以下操作环境目标：

- 阻止应用程序执行未经授权的代码（OE.RE.CODE-EXE）
- 遵守应用程序的安全准则（OE.APPLICATIONS）

IC 嵌入式软件通过目标 OE.IC.SUPPORT 来支持这些目标。特别地，IC 嵌入式软件：

- 为平台支持功能和电信框架（S.PSF 和 S.TELECOM）提供安全的底层加密处理。
- 允许 S.PSF 和 S.TELECOM 将数据存储在“持久性技术存储器”或易失性存储器中，具体取决于其需求（例如，瞬态对象必须不存储在非易失性存储器中）。内存模型是结构化的，允许底

层控制访问（分段故障检测）

- 提供了一种为 S.PSF 和 S.TELECOM 原子地执行内存操作的方法。

T.PHYSICAL-ATTACK

这种威胁主要受到依赖于底层平台的物理保护的影响，因此也是一个环境问题。

安全目标 OE.IC.SUPPORT 和 OE.IC.RECOVERY 保护平台的敏感数据的完整性和机密性，特别是确保 TSF 不能绕过或更改。

特别是，安全目标 OE.IC.SUPPORT 能够确保敏感操作的原子性，安全的底层访问控制和防止绕过 TOE 的安全功能等。特别是，它确保了对平台数据完整性的独立保护。

由于 TOE 不仅仅依赖 IC 保护措施，因此 TOE 应强制执行任何必要的机制以确保对侧信道的抵抗（O.DATA-CONFIDENTIALITY）。出于同样的原因，运行环境安全体系结构必须涵盖侧通道（OE.RE.DATA-CONFIDENTIALITY）。

O.OPERATE 通过确保始终强制执行这些安全功能来帮助应对这一威胁。

6.3.2 组织安全政策

6.3.2.1 生命周期

OSP.LIFECYCLE

O.PSF 确保 SM-SR 可以删除阻塞的孤立 Profile，并且只能由 SM-SR 删除。此删除功能依赖于 OE.RE.PSF 提供的安全应用程序删除机制。O.PSF 确保每时每刻都仅启用一个 ISD-P。

O.OPERATE 通过确保始终强制执行 PSF 安全功能来为此 OSP 服务。

6.3.3 假设

A.ACTORS

目标 OE.CI，OE.SM-SR，OE.SM-DP 和 OE.MNO 支持这一假设，它确保了基础设施的每个参与者正确地管理凭证和其他敏感数据。

A.APPLICATIONS

这一假设由目标 OE.APPLICATIONS 直接支持。

6.3.4 SPD 和安全目标

表 3 威胁和安全目标——覆盖范围

威胁	安全目标
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DP, OE.MNO, O.PSF, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.MNOSD
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PSF, O.SECURE-CHANNELS, OE.SM-SR, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY

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

表 4 安全目标和威胁——覆盖范围

安全目标	威胁
O.PSF	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.IDENTITY-INTERCEPTION

安全目标	威胁
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-SR	T.UNAUTHORIZED-PLATFORM-MNG, T.PLATFORM-MNG-INTERCEPTION
OE.SM-DP	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
OE.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
OE.IC.RECOVERY	T.PHYSICAL-ATTACK
OE.RE.PSF	
OE.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.IDENTITY-INTERCEPTION
OE.RE.API	T.LOGICAL-ATTACK
OE.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.PHYSICAL-ATTACK
OE.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
OE.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
OE.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-INTERCEPTION, T.PLATFORM-MNG-INTERCEPTION, T.LOGICAL-ATTACK
OE.MNOSD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION

表 5 OSP 和安全目标——覆盖范围

组织安全策略	安全目标

OSP.LIFECYCLE	O.PSF, OE.RE.PSF, O.OPERATE

表 6 安全目标和 OSP——覆盖范围

安全目标	组织安全策略
O.PSF	OSP.LIFECYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFECYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	
OE.SM-SR	
OE.SM-DP	
OE.MNO	
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PSF	OSP.LIFECYCLE
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.APPLICATIONS	
OE.MNOSD	

表 7 假设和运行环境安全目标——覆盖范围

假设	运行环境安全目标
A.ACTORS	OE.CI, OE.SM-SR, OE.SM-DP, OE.MNO
A.APPLICATIONS	OE.APPLICATIONS

表 8 运行环境安全目标和假设——覆盖范围

运行环境安全目标	假设

运行环境安全目标	假设
OE.CI	A.ACTORS
OE.SM-SR	A.ACTORS
OE.SM-DP	A.ACTORS
OE.MNO	A.ACTORS
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PSF	
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.APPLICATIONS	A.APPLICATIONS
OE.MNOSD	

7 扩展要求

7.1 扩展族

7.1.1 扩展族 FIA_API – 身份验证

7.1.1.1 描述

为了描述 TOE 的 IT 安全功能要求，此处定义了类 FIA（标识和认证）的功能族 FIA_API（身份认证证明）。该族描述了 TOE 证明其身份的功能要求，并允许外部实体进行身份验证。类 FIA 的其他成员通过 TOE 解决外部实体的身份验证问题。

类 FIA 的其他族仅描述 TOE 所执行的用户身份认证，并未描述用户证明其身份的功能。类 FIA 的其他族仅描述 TOE 执行的用户身份的认证验证，并未描述用户证明其身份的功能。以下段落采用了 CC 第 2 部分的风格，从 TOE 的角度定义了族 FIA_API。

族行为：

该族定义了 TOE 提供的证明其身份、并由 TOE IT 环境中的外部实体进行验证的功能。

组件层次：

FIA_API.1 身份验证证明，向外部实体提供 TOE、对象、授权用户或角色的身份证明。

管理：

FIA_API.1 FMT 中的管理功能可以考虑以下行动：用于证明所声称身份的认证信息的管理。

审计：

FIA_API.1 没有可审计的行为定义。

7.1.1.2 扩展组件

扩展组件 FIA_API.1

FIA_API.1 身份验证证明

FIA_API.1.1 TSF 应提供[赋值：*认证机制*]以向外部实体证明[选择：*TOE，[赋值：对象、授权用户或角色]*]的身份。

依赖关系：没有依赖关系

7.1.2 扩展族 FPT_EMS - TOE 发散

7.1.2.1 描述

为了描述 TOE 的 IT 安全功能要求，此处定义了类 FPT（TSF 保护）的功能族 FPT_EMS（TOE 发散）。TOE 应防止基于 TOE 的外部可观察物理现象而针对 TOE 秘密数据实施的攻击。这种攻击的例子是 TOE 的电磁辐射评估、简单功耗分析（SPA）、差分功耗分析（DPA）、时间攻击、无线电放射等。该族描述了限制可理解发散的功能要求。

FPT_EMS 族属于 FPT 类，因为它是 TSF 保护的类。FPT 类中的其他族无法涵盖 TOE 发散。

族行为：

该族定义了减轻可理解发散的要求。

组件层次：

FPT_EMS.1 TOE 发散有两个组成部分：

FPT_EMS.1.1 发散限制要求不能发出能够访问 TSF 数据或用户数据的可识别的发散。

FPT_EMS.1.2 接口发散要求不发出能够访问 TSF 数据或用户数据的接口发散。

管理：

FPT_EMS.1

没有可预见的管理活动。

审计：

FPT_EMS.1

如果 FAU_GEN（安全审计数据生成）包含在使用 FPT_EMS.1 的 PP 或 ST 中，则没有可识别的审计行为。

7.1.2.2 扩展组件

扩展组件 FPT_EMS.1

PT_EMS.1 TOE 发散

FPT_EMS.1.1 TOE 不应发出超过[赋值：*指定限制*]的[赋值：*发散类型*]，以便能够访问[赋值：*TSF 数据类型列表*]和[赋值：*用户数据类型列表*]。

FPT_EMS.1.2 TSF 应确保[赋值：*用户类型*]无法使用以下接口[赋值：*连接类型*]来访问[赋值：*TSF 数据类型列表*]和[赋值：*用户数据类型列表*]。

依赖关系：没有依赖关系

7.1.3 扩展族 FCS_RNG – 随机数生成

7.1.3.1 描述

FCS_RNG – 随机数生成

随机数的生成要求随机数满足定义的质量度量。

族行为：

该族定义了生成随机数的要求，其中随机数旨在用于加密目的。这些要求涉及 AIS 20/31 中定义的随机数发生器的类型和随机数的质量。该族中使用的随机数发生器类（DRG 和 PTG）在文献 KS2011 中描述。

FCS_RNG.1 不包括对 FPT_TST.1 的依赖性，因为 ST 作者可能选择不需要自检的 RNG（通常是确定性 RNG）。应用说明解决了 FPT_TST.1 的附加问题。

组件层次：

FCS_RNG 随机数生成有两个组成部分：

FCS_RNG.1.1 要求提供随机数生成。

FCS_RNG.1.2 需要定义质量指标。

管理：

FCS_RNG.1

没有可预见的管理活动。

审计：

FCS_RNG.1

没有可审计的行为定义。

7.1.3.2 扩展组件

扩展组件 FCS_RNG.1

FCS_RNG.1 随机数生成

FCS_RNG.1.1 TSF 应提供[选择：*确定性*、*混合确定性*、*物理*、*混合物理*]随机数发生器[选择：*DRG.2*，*DRG.3*，*DRG.4*，*PTG.2*，*PTG.3*]实现：[赋值：所选 RNG 类的安全功能列表]。

FCS_RNG.1.2 TSF 应提供满足[赋值：*所选 RNG 类的已定义质量度量*]的随机数。

依赖关系：没有依赖关系。

8 安全要求

为了定义安全功能要求，使用了 CC 的第 2 部分。

一些安全功能要求进行了细化。在相关 SFR 下面描述了细化的地方。细化操作用于向需求添加细节，因此进一步限制了需求。这些细化是解释细化，并被描述为一个额外的段落，从“细化”一词开始。

选择操作用来选择 CC 提供的一个或多个选项来说明要求。由 PP 作者做出的选择表示为带下划线的文本。ST 作者要填写的选择出现在方括号中，表示要进行选择[选择：]并用斜体表示。

赋值操作用来将特定值分配给未指定的参数，例如口令的长度。由 PP 作者作出的赋值通过用粗体文字来表示。由 ST 作者填写的赋值显示在方括号中，表示要进行赋值[赋值：]并用斜体表示。

在某些情况下，PP 作者的赋值定义了应由 ST 作者执行的选择。因此，该文本既是粗体又是斜体（参见例如 FCS_COP.1/Mobile_network）。

在某些情况下，PP 作者的赋值定义了应由 ST 作者执行的赋值。因此，该文本既是粗体又是斜体（例如参见 FIA_UID.1/EXT）。

当需要重复操作同一组件时，使用迭代操作。迭代通过斜杠"/"和组件标识符之后的迭代指示符来表示。

8.1 安全功能要求

8.1.1 简介

此标准定义以下安全策略：

- 安全通道协议信息流控制 SFP
- 平台服务信息流控制 SFP
- ISD-R 访问控制 SFP
- ISD-P 访问控制 SFP
- ECASD 内容访问控制 SFP

安全策略中使用的所有角色在 5.2 节中定义为用户或主体。如果角色不属于 TOE，则角色定义为用户；如果是 TOE 的一部分，则角色定义为主体。

用户可以是远程（U.SM-SR，U.SM-DP，U.MNO OTA 平台）或本地（U.MNO-SD，它是 eUICC 上的应用程序）。

8.1.1.1 安全信道协议信息流控制 SFP

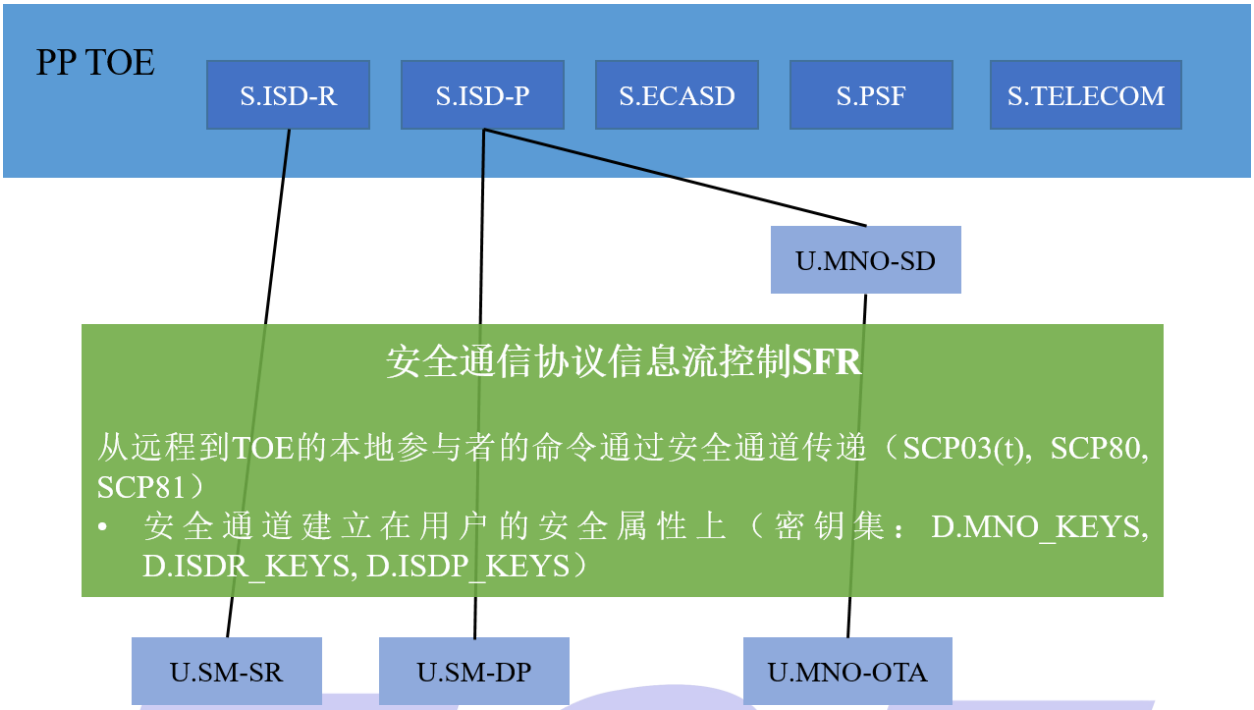

图 5 安全通道协议信息流控制 SFP

eUICC 应支持 SCP03（t），SCP80，SCP81。

8.1.1.2 平台服务信息流控制 SFP

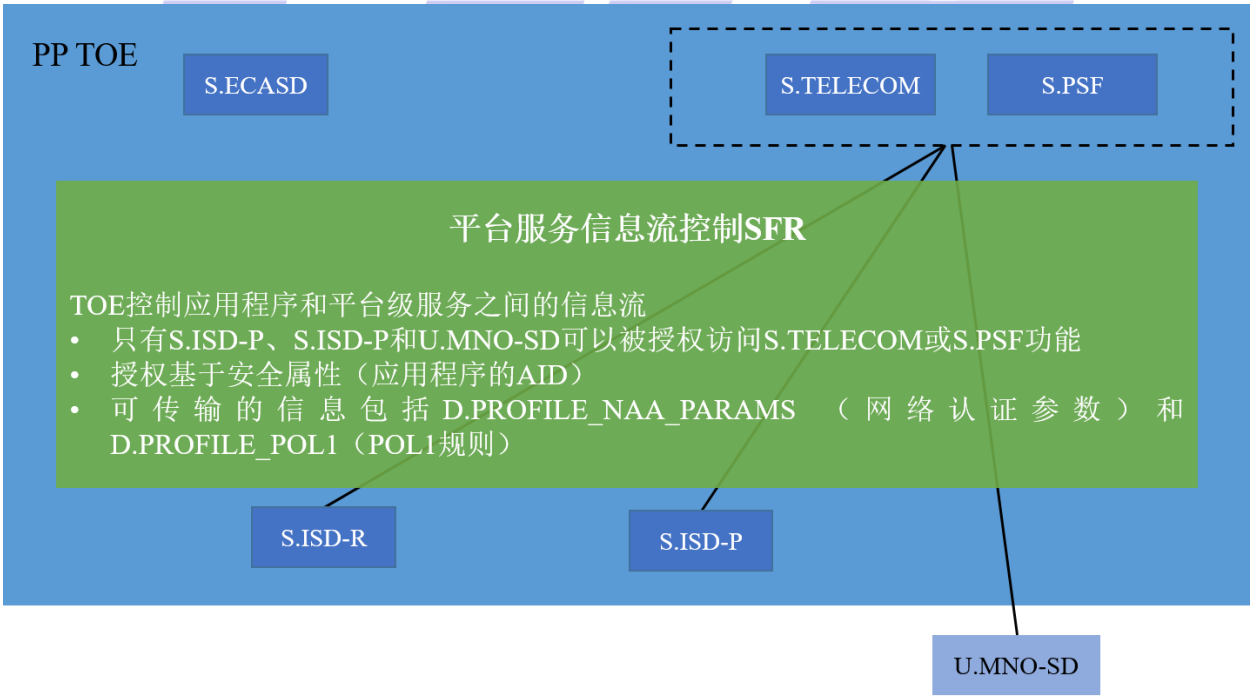

图 6 平台服务信息流控制 SFP

8.1.1.3 ISD-R 访问控制 SFP

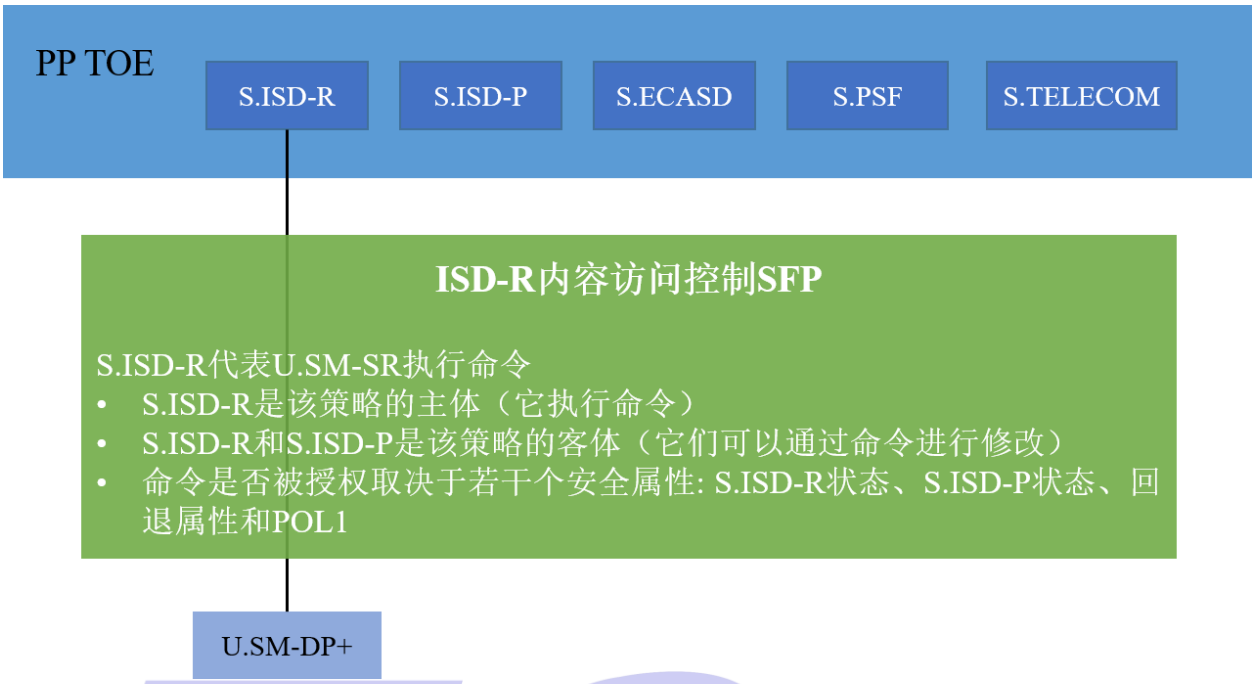

图 7 ISD-R 访问控制 SFP

8.1.1.4 ISD-P 访问控制 SFP

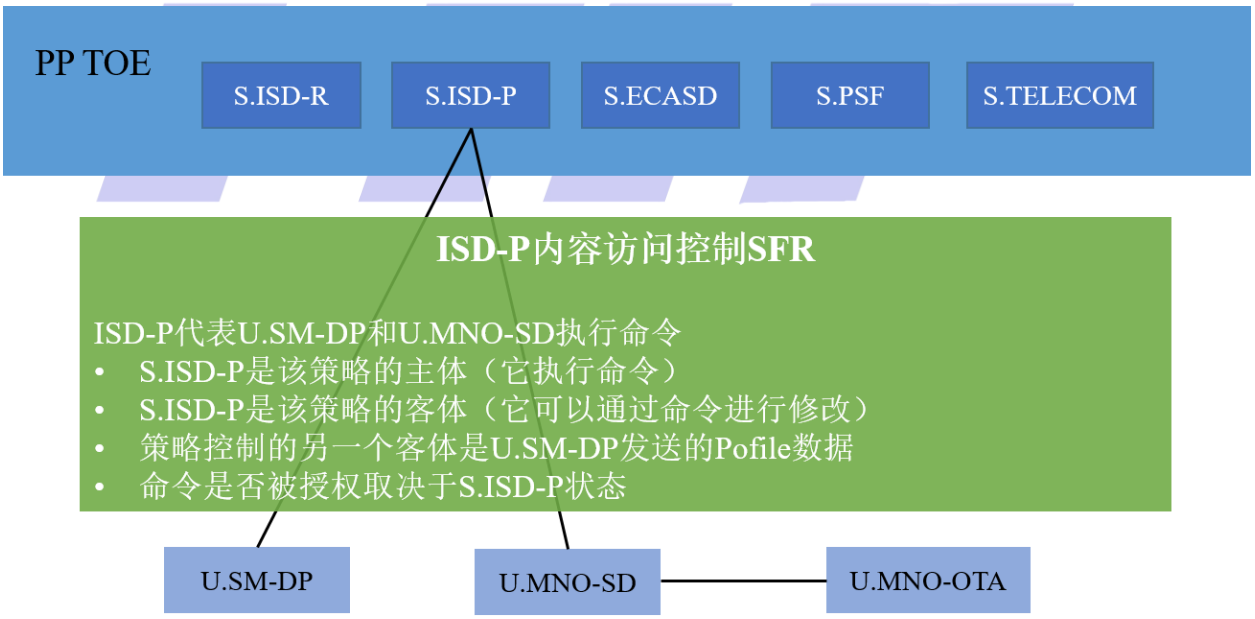

图 8 ISD-P 内容访问控制 SFP

8.1.1.5 ECASD 内容访问控制 SFP

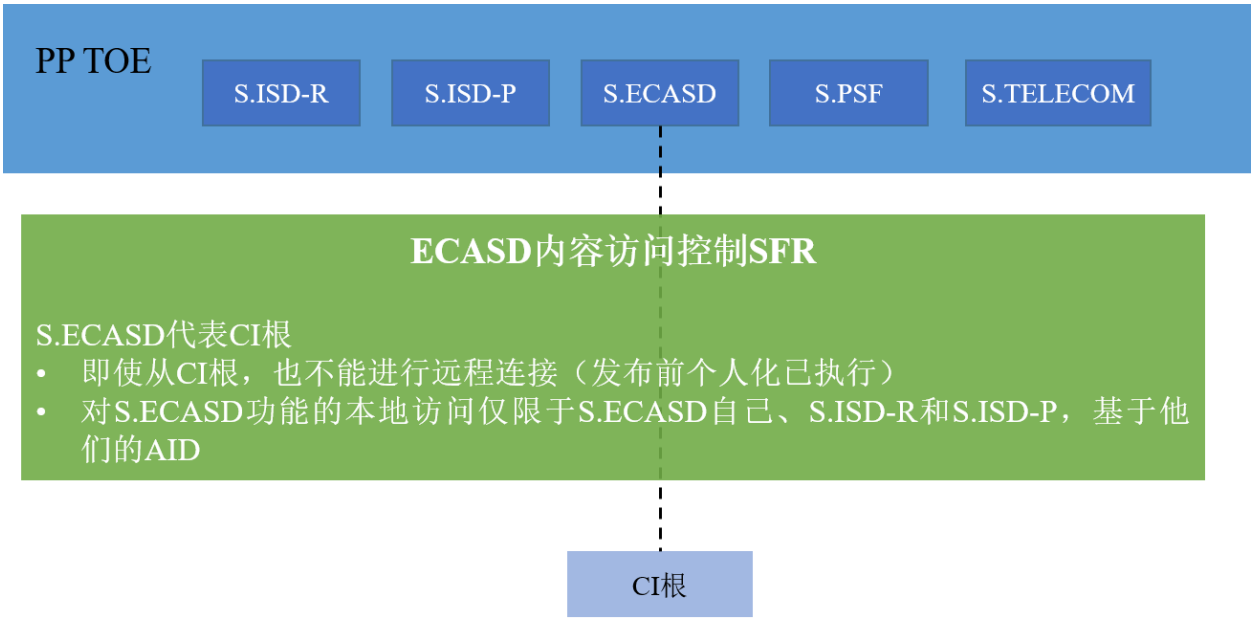

图 9 ECASD 内容访问控制 SFP

8.1.1.6 SFR 中使用的安全属性

表 9 安全属性定义

安全属性	细节	与资产的关系
AID	AID 是 JCS 运行环境中应用程序的标识符。由于此标准不强制要求 JCS，因此 ST 作者可以使用另一个等效的方法来标识应用程序。	AID 属于运行环境（是 PP-JCS 规范的一部分）
S.ISD-R 状态	主体 S.ISD-R 的状态。 此状态的可能值为： • 生成 • 可选择 • 个人化	该属性是 D.PSF_DATA 的一部分
S.ISD-P 状态	主体 S.ISD-P 的状态。 此状态的可能值为： • 生成 • 选择 • 个人化 • 启用 • 禁用	该属性是 D.PSF_DATA 的一部分
回滚属性	对于一个且仅有一个 S.ISD-P，回滚属性为 "true"。 这意味着，如果 TOE 执行回滚操作，则必须启用此特定 S.ISD-P，而同时其他的必须禁用。	该属性是 D.PSF_DATA 的一部分

安全属性	细节	与资产的关系
POL1	POL1 规则与给定的 S.ISD-P 相关联，并且由 TOE 用于评估 ISD-P 禁用或删除是否被授权。POL1 可能包括以下一条或几条规则： • 不允许禁用此 Profile • 不允许删除此 Profile • 当 Profile 状态更改为禁用时，必须删除 Profile	该属性描述为 D.PROFILE_POL1
密钥集 (D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS)	TOE 使用密钥集在远程参与者与 eUICC 上的本地对等方之间建立安全通道。	这些属性（D.MNO_KEYS, D.ISDR_KEYS, D.ISDP_KEYS）在 5.1.1.1 密钥中定义
CERT.DP.ECDSA CERT.SR.ECDSA	TOE 用 U.SM-SR 和 U.SM-DP 证书来对这些用户进行身份验证。这些证书由 CI 根签名。TOE 可以使用 CI 根公钥验证此签名。	这些属性不是此标准的一部分。CI 根公钥在 5.1.2.3 身份管理数据中被描述为资产 D.CI_ROOT_PUBKEY
smsr-id smdp-id mno-id	smsr-id 是当前负责 eUICC 管理的 SM-SR 的标识。 smsr-id 可能会在 eUICC 的生命周期内发生变化。 smdp-id 是最初下载并安装了 Profile 的 SM-DP 的标识。如果在发布 eUICC 期间加载了 Profile，则该值可以为空，否则该值是必需的。 一旦此信息与 Profile 关联，它将在 Profile 的生命周期内保持不变。 mno-id 是 Profile 的 MNO 所有者的标识。 一旦此信息与 Profile 关联，它将在 Profile 的生命周期内保持不变。	这些属性包含在 D.PSF_DATA 中
EID	EID 是实现 TOE 的物理 eUICC 的标识符。	EID 是硬件标识符，不属于此标准的部分。

8.1.2 识别和认证

该要求包描述了 TOE 的识别和认证措施：

TOE 必须：

- 通过 smsr-id 识别远程用户 U.SM-SR
- 通过 smdp-id 识别远程用户 U.SM-DP
- 通过 mno-id 识别远程用户 U.MNO-OTA
- 通过 AID 识别卡上用户 U.MNO-SD

TOE 必须：

- 验证 U.Sm-SR：
  - 使用 CERT.SR.ECDSA（对于 U.SM-SR 第一次连接，以创建共享的 SCP80 / 81 密钥集）；
  - 通过 SCP80/81，一旦密钥集初始化完成；

- 验证 U.Sm-DP：
  - 使用 CERT.DP.ECDSA（对于 U.SM-DP 第一次连接，以便创建共享的 SCP03（t）密钥集）；
  - 通过 SCP03(t)，一旦密钥集初始化完成;
- 使用 MNO Profile 中加载的密钥集通过 SCP80/81 验证 U.MNO-OTA。

U.MNO-SD 未经 TOE 认证。它是在 U.SM-DP 下载和安装 Profile 时在 eUICC 上创建的。因此，U.MNO-SD 与内部主体 S.ISD-P 绑定，并且此绑定需要 USM-DP 身份验证。在 TOE 的使用寿命期间，U.MNO-SD 代表 U.MNO-OTA 执行操作，因此需要 U.MNO-OTA 认证。

TOE 应将卡外和卡上用户绑定到内部主体：

- U.SM-SR 与 S.ISD-R 绑定，
- U.SM-DP 与 S.ISD-P 绑定，
- U.MNO-OTA 与 U.MNO-SD 绑定，并且 U.MNO-SD 与管理相应 MNO Profile 的 S.ISD-P 绑定。

最后，TOE 应提供一种向卡外用户证明其身份的方法。

FIA_UID.1/EXT 标识的时机

FIA_UID.1.1/EXT TSF 应允许

- **应用选择**
- **请求标识 eUICC 的数据**
- **[赋值：*其他 TSF 调解行动清单*]。**

在识别用户之前代表用户执行。

FIA_UID.1.2/EXT 在允许代表该用户执行任何其他 TSF 介导的操作之前，TSF 应要求成功识别每个用户。

应用说明：

此 SFR 与 TOE 的外部（远程）用户的标识有关：

- U.SM-SR
- U.SM-DP
- U.MNO-OTA 唯一的本地用户（U.MNO-SD）的标识由 FIA_UID.1/MNO-SD SFR 处理

应用程序选择在识别之前授权，因为可能需要向远程用户提供 eUICC 的标识。

FIA_UAU.1/EXT 鉴别的时机

FIA_UAU.1.1/EXT TSF 应允许

- **应用选择**
- **请求标识 eUICC 的数据**
- **用户识别**
- **[赋值：*其他 TSF 调解行动清单*]**

在用户通过身份验证之前代表用户执行。

FIA_UAU.1.2/EXT 在允许代表该用户进行任何其他 TSF 介导的操作之前，TSF 应要求每个用户成功通过身份验证。

应用说明：

此 SFR 与 TOE 的以下外部（远程）用户的身份验证有关：

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

由于用于认证的加密机制可以由底层平台提供，因此该标准不包括相应的 FCS_COP.1 SFR。

ST 作者应添加 FCS_COP.1 要求来包括 GSMA SGP.02 规范以下要求：

- 新的 U.SM-SR 必须通过使用其 CERT.SR.ECDSA 证书中包含的公钥验证其 ECDSA 签名来验证(这使新的 SM-SR 能够根据 FCS_CKM.1/SCP-SM 创建 D.ISDR_KEYS 密钥集来构建 SCP80 或 SCP81 安全通道)。
- 创建 D.ISDR_KEYS 密钥集后,必须根据 SCP80 安全通道或可选 SCP81 对 USM-SR 进行身份验证。
- 新的 U.SM-DP 必须通过使用其 CERT.DP.ECDSA 证书中包含的公钥验证其 ECDSA 签名来验证(这使新的SM-DP 能够根据FCS_CKM.1/SCP-SM 创建D.ISDP_KEYS 密钥集来构建SCP03(t)安全通道。
- 创建 D.ISDP_KEYS 密钥集后，必须使用 SCP03(t)安全通道对 U.S.M-DP 进行身份验证。
- U.MNO-OTA 必须使用 SCP80 或 SCP81（用于此操作的密钥集根据 FCS_CKM.2/SCP-MNO 分发）进行身份验证

关于 ECDSA 签名验证的使用，底层椭圆曲线加密必须符合以下之一：

- NISTP-256（FIPS PUB 186-3 数字签名标准）
- brainpoolP256r1（BSI TR-03111，版本 1.11，RFC 5639）
- FRP256V1（ANSSI ECC FRP256V1)。

FIA_USB.1/EXT 用户主体绑定

FIA_USB.1.1/EXT TSF 应将以下用户安全属性与代表该用户的主体相关联：

- **smsr-id 与 S.ISD-R 相关联，代表 U.SM-SR**
- **smdp-id 与 S.ISD-P 相关联，代表 U.SM-DP**
- **mno-id 与 U.MNO-SD 相关联，代表 U.MNO-OTA。**

FIA_USB.1.2/EXT TSF 应对用户安全属性与代表用户的主体的初始关联强制执行以下规则：

- **smsr-id 的初始关联要求通过"CERT.SR.ECDSA"对 U.SM-SR 进行身份验证**
- **smdp-id 和 mno-id 的初始关联要求通过"CERT.DP.ECDSA"对 USM-DP 进行身份验证。**

FIA_USB.1.3/EXT TSF 应执行以下规则，管理与代表用户操作的主体相关的用户安全属性的更改：

- **smsr-id 的更改要求通过"CERT.SR.ECDSA"对 U.SM-SR 进行身份验证**
- **不允许更改 smdp-id 和 mno-id。**

应用说明：

此 SFR 与外部（远程）用户与 TOE 的本地主体或用户的绑定有关：

- U.SM-SR 与主体（S.ISD-R）绑定
- U.SM-DP 与主体（S.ISD-P）绑定
- U.MNO-OTA 绑定到卡上用户（U.MNO-SD）

ST 作者必须知道 U.MNO-SD 不是 TOE 的主体，而是代表 U.MNO-OTA 的外部卡上用户，U.MNO-OTA 是外部的卡外用户。

此 SFR 与以下命令相关：

- ES8.EstablishISDPKeySet 命令执行 D.ISDP_KEYS 密钥集的初始关联和更改
- ES5.EstablishISDRKeySet 命令执行 D.ISDR_KEYS 密钥集的初始关联和更改
- ES8.DownloadAndInstallation 命令执行 D.MNO_KEYS 密钥集的初始关联

FIA_UAU.4/EXT 一次性身份验证机制

FIA_UAU.4.1/EXT TSF 应防止重用**用于在 eUICC 和下述用户之间打开安全通信信道的认证机制**相关的认证数据：

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

应用说明：

此 SFR 与 TOE 的外部（远程）用户的身份验证有关：

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

FIA_UID.1/MNO-SD 标识的时机

FIA_UID.1.1/MNO-SD TSF 应允许

- **申请选择**

在识别用户之前代表用户执行。

FIA_UID.1.2/MNO-SD 在允许代表该用户进行任何其他 TSF 介导的操作之前，TSF 应要求成功识别每个用户。

应用说明：

该 SFR 仅与本地用户 U.MNO-SD 的标识有关。远程用户的识别问题由 FIA_UID.1/EXT SFR 解决。

应该注意，U.MNO-SD 被识别但未被认证。但是，USM-DP 通过主体 S.ISD-P（见 FDP_ACF.1/ISDP 中的“下载和安装”）在 TOE 上安装了 U.MNO-SD。USM-DP 与 S.ISD-P 之间的绑定要求对 USM-DP 进行认证，如 FIA_USB.1/EXT 中所述。

应用程序选择在识别之前授权，因为可能需要向远程用户提供 eUICC 的标识。

FIA_USB.1/MNO-SD 用户主体绑定

FIA_USB.1.1/MNO-SD TSF 应将以下用户安全属性与代表该用户的主体相关联：**U.MNO-SD AID 与代表 U.MNO-SD 的 S.ISD-P 相关联**。

FIA_USB.1.2 / MNO-SD TSF 应对用户安全属性与代表用户的主体的初始关联强制执行以下规则：**AID 的初始关联要求通过 CERT.DP.ECDSA 对 USM-DP 进行身份验证**。

FIA_USB.1.3/MNO-SD TSF 应强制执行以下规则，以管理与代表用户操作的主体相关联的用户安全属性的更改：**不允许更改 AID**。

应用说明：

该 SFR 与本地用户 U.MNO-SD 的识别有关。

作为 TOE 的本地但是外部用户，U.MNO-SD 绑定到 S.ISD-R，负责在“Profile 下载和安装”期间安

装它。Profile 安装由 FDP_ACC.1/ISDR SFP 控制。由 S.ISD-P 执行，需要 USM-DP 的认证。

为了执行诸如 POL1 更新和连接参数更新的操作，U.MNO-OTA 进行认证，然后向 U.MNO-SD 发送命令，该命令将其发送到 S.ISD-P；该操作最终由 S.ISD-P 根据 FDP_ACC.1/ISDP SFP 执行。

该标识不依赖于 MNO OTA 平台的直接认证，而是依赖于 S.ISD-P 的认证：S.ISD-P 安装包括 U.MNO-SD 和相关密钥集的 Profile。

FIA_ATD.1 用户属性定义

FIA_ATD.1.1 TSF 应维护属于各个用户的以下安全属性列表：

- **CERT.SR.ECDSA 和属于 U.SM-SR 的 smsr-id**
- **CERT.DP.ECDSA 和属于 U.SM-DP 的 smdp-id**
- **属于 U.MNO-OTA 的 mno-id**
- **属于 U.MNO-SD 的 AID。**

FIA_API.1 身份验证证明

FIA_API.1.1 TSF 应**根据 eUICC 的 EID 提供加密认证机制**，以向外部实体证明 TOE 的身份。

应用说明：

该证明是通过在 eUICC 证书中包含 EID 值获得的，该证书由 eUICC 制造商签署。

8.1.3 通信

该要求包描述了 TSF 如何保护与外部用户的通信。

TSF 应强制执行安全通道（FTP_ITC.1/SCP 和 FTP_ITC.2/SCP）：

- U.SM-SR 和 S.ISD-R 之间
- U.SM-DP 和 S.ISD-P 之间
- U.MNO-OTA 和 U.MNO-SD 之间

这些安全通道用于导入命令和对象，因此要求 TSF（FPT_TDC.1/SCP）一致地解释这些命令和对象。

这些安全通道根据安全策略（FDP_IFC.1/SCP 和 FDP_IFF.1/SCP 中描述的安全信道协议信息流控制 SFP）建立。该政策特别要求保护所传输信息的机密性（FDP_UCT.1/SCP）和完整性（FDP_UIT.1/SCP）。

TSF 必须使用加密方法来强制执行此保护，并安全地管理相关的密钥集：

- D.ISDP_KEYS 和 D.ISDR_KEYS 的生成和删除（FCS_CKM.1/SCP-SM 和 FCS_CKM.4/SCP-SM）
- D.MNO_KEYS 的分发和删除（FCS_CKM.2/SCP-MNO 和 FCS_CKM.4/SCP-MNO）

FDP_IFC.1/SCP 子集信息流控制

FDP_IFC.1.1/SCP TSF 应在下述场景强制执行**安全通道协议信息流控制 SFP**

- **用户/主体：**
  - **U.SM-SR 和 S.ISD-R**
  - **U.SM-DP 和 S.ISD-P**
  - **U.MNO_OTA 和 U.MNO-SD**
- **信息：命令的传输。**

FDP_IFF.1/SCP 简单的安全属性

FDP_IFF.1.1/SCP TSF 应根据以下类型的主体和信息安全属性强制执行**安全通道协议信息流控制 SFP**：

- **用户/主体：**
  - **U.SM-SR 和 S.ISD-R，具有安全属性 D.ISDR_KEYS**
  - **U.SM-DP 和 S.ISD-P，具有安全属性 D.ISDP_KEYS**
  - **U.MNO_OTA 和 U.MNO-SD，具有安全属性 D.MNO_KEYS**
- **信息：命令的传输。**

FDP_IFF.1.2/SCP 如果遵守以下规则，TSF 应允许通过受控操作在受控主体和受控信息之间传递信息：

- **TOE 应允许 U.MNO-OTA 和 U.MNO-SD 之间在 SCP80 或 SCP81 安全通道中进行通信**。

FDP_IFF.1.3/SCP TSF 应强制执行[赋值：*附加信息流控制 SFP 规则*]。

FDP_IFF.1.4/SCP TSF 应根据以下规则明确授权信息流：[赋值：*基于安全属性明确授权信息流的规则*]。

FDP_IFF.1.5/SCP TSF 应根据以下规则明确拒绝信息流：

- **如果未通过 SMS、CAT_TP 或 HTTPS 在 SCP80 或 SCP81 安全通道中执行，则 TOE 应拒绝 U.SM-SR 与 S.ISD-R 之间的通信**
- **如果未通过 U.SM-SR 和 S.ISD-R 之间创建的隧道在 SCP03(t)安全信道中执行，TOE 将拒绝 USM-DP 与 S.ISD-P 之间的通信。**

应用说明：

有关安全通道的更多详细信息，请参见 GSMA SGP.02 规范

- SM-SR：第 2.2.5.1 节和第 2.4 节
- SM-DP：第 2.2.5.2 节和第 2.5 节
- MNO-SD：第 2.2.5.3 节和第 2.7 节

FTP_ITC.1/SCP TSF 间可信信道

FTP_ITC.1.1/SCP TSF 应在其自身与另一个可信的 IT 产品之间提供一个通信通道，该产品在逻辑上与其他通信通道不同，提供对其端点的确定识别以及保护通道数据不被修改或泄露。

FTP_ITC.1.2/SCP TSF 应允许其他可信 IT 产品通过可信通道发起通信。

FTP_ITC.1.3/SCP TSF 应通过可信信道发起[赋值：*需要可信通道的功能列表*]的通信。

应用说明：

由于用于可信信道的加密机制可以由底层平台提供，因此该标准不包括相应的 FCS_COP.1 SFR。 ST 作者应添加 FCS_COP.1 要求，用来包括 GSMA SGP.02 规范第 2.2.5 节中规定的要求：

- SM-DP 的安全通道必须是 SCP03(t)安全通道。根据 GlobalPlatform 卡规范修正案 D 中在 GSMA SGP.02 规范第 2.5 章中定义的参数使用 AES 来解决端点识别问题。
- 必须提供 SCP80，以便为 SM-SR 和 MNO OTA 平台建立安全通道。 TSF 还可以允许使用 SCP81 安全信道执行与 SCP80 安全信道相同的功能。端点的识别通过以下方式解决
  - 对于 SCP80：根据 GSMA SGP.02 规范第 2.4.3 章中定义的参数使用 AES。
  - 对于 SCP81：根据 SCP81 规范使用 TLS V1.2（RFC 5246），使用 GSMA SGP.02 规范第 2.4.4 章中定义的参数。

相关密钥是：

- 在 Profile 下载或 SM-SR 切换期间在卡上生成（D.ISDP_KEYS，D.ISDR_KEYS）；有关详细信息，

请参阅 FCS_CKM.1/SCP-SM

- 或与 Profile 一起分发（D.MNO_KEYS）；有关详细信息，请参阅 FCS_CKM.2/SCP-MNO

在命令方面，TSF 应允许远程参与者在以下情况下通过可信信道发起通信：

TSF 应允许 SM-SR 打开 SCP80 安全通道以执行 Profile 下载和安装，分为以下步骤：

- TSF 应允许 SM-SR 发送 ES5.CreateISDP 命令；
- 然后，TSF 应允许 SM-DP 打开 SCP03（t）安全信道进行传输
  - ES8.EstablishISDPKeySet 命令，后跟
  - ES8.DownloadAndInstallation 命令；
- TSF 应允许 SM-SR 发送 ES5.EnableProfile 命令（可选）

TSF 应允许 SM-SR 打开 SCP80 安全信道以发送以下平台管理命令：

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

TSF 应允许 SM-SR 打开 SCP80 安全信道，以发送以下 eUICC 管理命令：

- ES5.EstablishISDRKeySet
- ES5.FinaliseISDRhandover
- ES5.UpdateSMSRAddressingParameters

TSF 应允许 SM-SR 打开 SCP80 安全信道以修改 SM-DP 的连接参数：

- TSF 应允许 SM-DP 打开 SCP03（t）安全信道以发送 ES8.UpdateConnectivityParameters SCP03 命令

TSF 应允许远程 OTA 平台打开 SCP80 安全通道，以传输以下 Profile 管理操作：

- ES6.UpdatePOL1byMNO
- ES6.UpdateConnectivityParametersByMNO

在命令方面，TSF 应通过可信信道发起通信：

- ES5.HandleDefaultNotification

FDP_ITC.2/SCP 使用安全属性导入用户数据

FDP_ITC.2.1/SCP 当从 TOE 外部导入受 SFP 控制的用户数据时，TSF 应强制执行**安全通道协议信息流控制 SFP**。

FDP_ITC.2.2/SCP TSF 应使用与导入的用户数据关联的安全属性。

FDP_ITC.2.3/SCP TSF 应确保所使用的协议提供安全属性与接收的用户数据之间的明确关联。

FDP_ITC.2.4/SCP TSF 应确保对导入的用户数据的安全属性的解释符合用户数据源的预期。

FDP_ITC.2.5/SCP 当从 TOE 外部导入受 SFP 控制的用户数据时，TSF 应执行以下规则：[赋值：*附加输入控制规则*]。

FPT_TDC.1/SCP TSF 间基本 TSF 数据一致性

FPT_TDC.1.1/SCP TSF 应对下述内容提供一致的解释能力

- **来自 U.SM-SR，U.SM-DP 和 U.MNO-OTA 的命令**
- **从 U.SM-SR，U.SM-DP 和 U.MNO-OTA 下载的对象**

当在 TSF 和另一个可信 IT 产品之间共享时。

FPT_TDC.1.2/SCP 在解释来自另一个可信 IT 产品的 TSF 数据时，TSF 应使用[赋值：*TSF 应用的解释规则列表*]。

应用说明：

下面列出了与 SFR FPT_TDC.1/SCP，FDP_IFC.1/SCP，FDP_IFC.1/SCP 相关的命令和与此 SFR FPT_TDC.1/SCP 相关的下载对象：

- SM-SR 命令
  - ES5.CreateISDP
  - ES5.EnableProfile
  - ES5.DisableProfile
  - ES5.DeleteProfile
  - ES5.eUICCCapabilityAudit
  - ES5.MasterDelete
  - ES5.SetFallbackAttribute
  - ES5.EstablishISDRKeySet
  - ES5.FinaliseISDRhandover
  - ES5.UpdateSMSRAddressingParameters
- 从 SM-SR 下载的对象
  - 平台管理密钥集
- SM-DP 命令
  - ES8.EstablishISDPKeySet
  - ES8.DownloadAndInstallation
  - ES8.UpdateConnectivityParameters SCP03
- 从 SM-DP 下载的对象
  - Profile 管理密钥集
  - MNO Profile
- MNO 命令
  - ES6.UpdatePOL1byMNO
  - ES6.UpdateConnectivityParametersByMNO
- 从 MNO OTA 平台下载的对象
  - POL1 数据
  - 连接参数

FDP_UCT.1/SCP 基本数据交换机密性

FDP_UCT.1.1/SCP TSF 应强制执行**安全通道协议信息流控制 SFP**，以受保护的方式接收用户数据，防止未经授权的泄露。

应用说明：

此 SFR 与以下保护有关：

- 从 SM-DP 下载的 Profile
- 在切换期间从 SM-SR 收到的 SM-SR 凭证

由于用于可信信道的加密机制可以由底层平台提供，因此该标准不包括相应的 FCS_COP.1 SFR。 ST 作者应添加 FCS_COP.1 要求以包括 GSMA SGP.02 规范下述的要求：通信的机密性必须通过在 CBC 模式（NIST 800-38A）中使用 AES 来解决，最小密钥大小为 128 位。

相关密钥是：

- 在 Profile 下载或 SM-SR 切换期间在卡上生成（D.ISDP_KEYS，D.ISDR_KEYS）；有关详细信息，请参阅 FCS_CKM.1/SCP-SM
- 或与 Profile 一起分发（D.MNO_KEYS）；有关详细信息，请参阅 FCS_CKM.2/SCP-MNO

FDP_UIT.1/SCP 数据交换完整性

FDP_UIT.1.1/SCP TSF 应强制执行**安全通道协议信息流控制 SFP**，以保护其免受修改、删除、插入和重放错误的方式接收用户数据。

FDP_UIT.1.2/SCP TSF 应能够在收到用户数据时确定是否发生了修改、删除、插入和重放。

应用说明：

此 SFR 与以下保护有关：

- 从 SM-DP 下载的 Profile;
- 在切换期间从 SM-SR 收到的 SM-SR 凭证;
- 从 SM-SR、SM-DP 和 MNO OTA 平台接收到的命令;
- 从 MNO OTA 平台收到的 POL1。

由于用于可信信道的加密机制可以由底层平台提供，因此该标准不包括相应的 FCS_COP.1 SFR。 ST 作者应添加 FCS_COP.1 要求以包括 GSMA SGP.02 规范下述的要求：通信的完整性必须通过在 CMAC 模式（NIST SP 800-38B）中使用 AES 来解决，最小密钥大小为 128 位并且 MAC 长度为 64 位。

相关密钥是：

- 在 Profile 下载或 SM-SR 切换期间在卡上生成（D.ISDP_KEYS，D.ISDR_KEYS）；有关详细信息，请参阅 FCS_CKM.1/SCP-SM
- 或与 Profile 一起分发（D.MNO_KEYS）；有关详细信息，请参阅 FCS_CKM.2/SCP-MNO

FCS_CKM.1/SCP-SM 密钥生成

FCS_CKM.1.1/SCP-SM TSF 应根据指定的加密密钥生成算法 **ElGamal 椭圆曲线密钥协商（ECKA）**和指定的加密密钥大小 **256** 生成加密密钥，且符合以下条件：**ECKA-EG 使用以下标准之一：**

- **NIST P-256（FIPS PUB 186-3 数字签名标准）**
- **brainpoolP256r1（BSI TR-03111，版本 1.11，RFC 5639）**
- **FRP256V1（ANSSI ECC FRP256V1）。**

应用说明：

此密钥生成机制用于生成

- 使用 CERT.DP.ECDSA 中包含的 U.SM-DP 公钥通过 ES8.EstablishISDPKeySet 命令生成的

D.ISDP_KEYS 密钥集

- 使用 CERT.SR.ECDSA 中包含的 U.SM-SR 公钥通过 ES5.EstablishISDRKeySet 命令生成的 D.ISDR_KEYS 密钥集

用于此密钥协议的椭圆曲线加密可由底层平台提供。因此，该标准不包括相应的 FCS_COP.1 SFR。ST 作者应添加 FCS_COP.1 要求以包括以下要求:此密钥协议的基础加密是 ECKA-EG,符合以下条件之一：

- NIST P-256（FIPS PUB 186-3 数字签名标准）
- brainpoolP256r1（BSI TR-03111，版本 1.11，RFC 5639）
- FRP256V1（ANSSI ECC FRP256V1）

FCS_CKM.2/SCP-MNO 密钥分发

FCS_CKM.2.1/SCP-MNO TSF 应根据符合以下条件的指定密钥分发方法[赋值：*密钥分发方法*]分发密钥：[赋值：*标准清单*]。。

应用说明：

该 SFR 与下述密钥分发有关

- Profile 下载期间的 D.MNO_KEYS
- 公钥分发在用户证书（CERT.SR.ECDSA 和 CERT.DP.ECDSA）中或加载预先发布的 TOE（D.eUICC_CERT，D.CI_ROOT_PUBKEY）

应用说明：

此 SFR 不适用于加载 TOE 预发行的私钥（D.eUICC_PRIVKEY）。

FCS_CKM.4/SCP-SM 密钥销毁

FCS_CKM.4.1/SCP-SM TSF 应根据符合以下条件的指定密钥销毁方法[赋值：*密钥销毁方法*]销毁密钥：[赋值：*标准列表*]。

应用说明：

此 SFR 与以下密钥的销毁有关：

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

FCS_CKM.4/SCP-MNO 密钥销毁

FCS_CKM.4.1/SCP-MNO TSF 应根据符合以下条件的指定密钥销毁方法[赋值：*密钥销毁方法*]销毁密钥：[赋值：*标准列表*]。

应用说明：

此 SFR 与以下密钥的销毁有关：

- D.MNO_KEYS

8.1.4 安全域

此要求包描述了适用于属于 TOE 安全域的特定要求。它特别定义：

- S.ISD-R 可以执行其功能时的规则(I（FDP_ACC.1/ISDP 和 FDP_ACF.1/ISDP 中 ISD-R 访问控制 SFP），
- S.ISD-P 可以执行其功能时的规则（在 FDP-ACC.1/ISDP 和 FDP-ACF.1/ISDP 中 ISD-P 访问控制 SFP），
- S.ISD-R 和 S.ISD-P 可以执行 ECASD 功能并从这些功能获得输出数据时规则（FDP_ACC.1/ECASD 和 FDP_ACF.1/ECASD 时 ECASD 内容访问控制 SFP）。

FDP_ACC.1/ISDR 子集访问控制

FDP_ACC.1.1/ISDR TSF 应对以下主体、客体和操作强制执行 **ISD-R 访问控制 SFP**

- **主体：S.ISD-R**
- **客体：S.ISD-R 和 S.ISD-P**
- **操作：**
  - **创建（S.ISD-P）**
  - **启用（S.ISD-P）**
  - **禁用（S.ISD-P）**
  - **删除（S.ISD-P）**
  - **设置备用属性（S.ISD-P）**
  - **执行功能审核（S.ISD-P）**
  - **执行主删除（S.ISD-P）**
  - **更新 SM-SR 寻址参数（S.ISD-R）**
  - **完成 SM-SR 切换（S.ISD-R）。**

应用说明：

- 此策略描述了应用于访问平台管理操作的规则。它涵盖了 GSMA SGP.02 规范中第 3.x 节要求的 ISD-R 对所有操作的访问。
- 应该注意的是，ISD-R 是该 SFP 的主体和客体，因为 SFP 控制 S.ISD-R 对 S.ISD-P 和 S.ISD-R 的修改。

FDP_ACF.1/ISDR 基于安全属性的访问控制

FDP_ACF.1.1/ISDR TSF 应根据以下内容对客体强制执行 **ISD-R 访问控制 SFP**：

- **主体：S.ISD-R**
- **客体：**
  - **具有安全属性" state "的 S.ISD-R**
  - **具有安全属性"state"，"fallback"和"POL1"的 S.ISD-P**
- **操作：**
  - **创建（S.ISD-P）**
  - **启用（S.ISD-P）**
  - **禁用（S.ISD-P）**

- **删除（S.ISD-P）**
- **设置备用属性（S.ISD-P）**
- **执行功能审核（S.ISD-P）**
- **执行主删除（S.ISD-P）**
- **更新 SM-SR 寻址参数（S.ISD-R）**
- **完成 SM-SR 切换（S.ISD-R）。**

FDP_ACF.1.2/ISDR TSF 应执行以下规则以确定是否允许受控主体和受控客体之间的操作：**授权状态**：

- **仅在以下情况下授权启用 S.ISD-P：**
  - **相应 S.ISD-P 处于"DISABLED"状态下并且**
  - **先前启用的 S.ISD-P 处于"DISABLED"状态**
- **仅在以下情况下授权禁用 S.ISD-P：**
  - **相应的 S.ISD-P 处于"ENABLED"或"PERSONALIZED"状态并且**
  - **相应的 S.ISD-P 的 POL1 数据允许其禁用并且**
  - **未设置相应的 S.ISD-P 的 fallback 属性**
- **仅在以下情况下授权删除 S.ISD-P：**
  - **相应的 S.ISD-P 不在状态"ENABLED"下并且**
  - **相应的 S.ISD-P 的 POL1 数据允许其删除并且**
  - **未设置相应的 S.ISD-P 的 fallback 属性**
- **仅在以下情况下授权执行主删除：**
  - **相应的 S.ISD-P 在状态"ENABLED"下并且**
  - **未设置相应的 S.ISD-P 的 fallback 属性并且**
  - **相应的 S.ISD-P 已成功验证了该命令发送的 USM-DP 令牌;**

FDP_ACF.1.3/ISDR TSF 应根据以下附加规则明确授权主体对客体的访问：[赋值：*基于安全属性明确授权主体访问客体的规则*]。

FDP_ACF.1.4/ISDR TSF 应根据以下附加规则明确拒绝主体对客体的访问：

- **如果 S.ISD-R 不在"PERSONALIZED"状态下以下任何操作都不能执行：**
  - **创建一个 ISD-P**
  - **在 S.ISD-P 上进行功能审核**
  - **设置一个 S.ISD-P 的 fallback 属性**
  - **在 S.ISD-R 上更新 SM-SR 寻址参数**
  - **在 S.ISD-R 上完成 SM-SR 切换**
- **对于除 S.ISD-R 之外的其他主体，禁止对 S.ISD-R 进行任何操作。**

应用说明：

此策略描述了应用于访问平台管理或 eUICC 管理操作的规则。它涵盖了 GSMA SGP.02 规范中第 3.x 节要求的 ISD-R 对所有操作的访问，包括：

- CreateISDP（创建一个 ISD-P）
- EnableProfile（启用一个 Profile）
- DisableProfile（禁用一个 Profile）
- DeleteProfile（删除一个 Profile）
- eUICCCapabilityAudit（执行功能审核）

- MasterDelete（执行主删除）
- SetFallbackAttribute（设置 fallback 属性）
- UpdateSMSRAddressingParameters（更新 SM-SR 寻址参数）
- FinaliseISDRhandover（完成 SM-SR 切换）

标识和身份验证 SFR（FIA_*/EXT）要求这些操作仅在经过身份验证后才能用于合法用户 U.SM-SR。

FDP ACC.1/ISDP 子集访问控制

FDP_ACC.1.1/ISDP TSF 应强制执行 **ISD-P 访问控制 SFP**：

主体：S.ISD-P

客体：

- **Profile（从 U.SM-DP 上获取）**
- **S.ISD-P**

操作：

- **下载并安装（Profile）**
- **建立密钥集（S.ISD-P）**
- **更新 POL1 数据（S.ISD-P）**
- **采用 FDP_IFF.1.1/SCP (S.ISD-P)中定义的 SCP03(t)安全频道更新 ISD-P 连接参数**
- **通过 MNO（S.ISD-P）更新 ISD-P 连接参数。**

应用说明：

此策略描述了在平台管理操作期间应用的规则。它涵盖了 GSMA SGP.02 规范中第 3.x 节所要求的 ISD-P 的所有操作。注意：这包括 Profile 安装。

基于 FDP_ACF.1/ISDP 安全属性的访问控制

FDP_ACF.1.1/ISDP TSF 应根据以下内容强制执行 **ISD-P 访问控制 SFP**:

主体：

- **S.ISD-P**

客体：

- **Profile（从 U.SM-DP 上获取）**
- **带有"state"安全属性的 S.ISD-P**

操作：

- **下载并安装（Profile）**
- **建立密钥集（S.ISD-P）**
- **更新 POL1 数据（S.ISD-P）**
- **采用 SCP03(t)更新 ISD-P 连接参数**
- **通过 MNO（S.ISD-P）更新 ISD-P 连接参数。**

FDP_ACF.1.2/ISDP TSF 应执行以下规则以确定是否允许受控主体和受控客体之间的操作：

- **仅当 S.ISD-P 的属性"state"为"PERSONALIZED"时，才会授权下载和安装配置 Profile**
- **如果 S.ISD-P 的属性"state"至少是"SELECTABLE"，则授权建立 D.ISDP_KEYS 密钥集**

- **仅当 S.ISD-P 的属性"state"为"ENABLED"时才授权更新 POL1**
- **仅当 S.ISD-P 的属性"state"为"ENABLED"时，才允许通过 SCP03（t）更新 ISD-P 连接参数**
- **仅当 S.ISD-P 的属性"state"为"PERSONALIZED"时，才授权 MNO 更新 ISD-P 连接参数。**

FDP_ACF.1.3/ISDP TSF 应根据以下附加规则明确授予主体对客体的访问权限：[赋值：*基于安全属性明确授权主体访问客体的规则*]

FDP_ACF.1.4/ISDP TSF 应根据以下附加规则明确拒绝授予主体对客体的访问权限：

- **对于除 S.ISD-P 之外的其他主体，禁止对 Profile 或 S.ISD-P 进行任何操作。**

应用说明：

此策略描述了在 Profile 管理操作期间应用的规则。它涵盖了 GSMA SGP.02 规范中描述的 SM-DP 操作：

- DownloadAndInstallation（下载并安装一个 Profile）
- EstablishISDPKeySet（建立一个 D.ISP_KEYS 密钥集）
- UpdateConnectivityParameters SCP03（采用 SCP03(t)更新 ISD-P 连接参数）

标识和身份验证 SFR（FIA_*/EXT）要求这些操作仅在经过身份验证后才能用于合法用户 U.SM-DP。

它还涵盖了 GSMA SGP.02 规范中描述的 MNO 操作：

- POL1update（更新 POL1 数据）
- UpdateConnectivityParametersByMNO（MNO 的连接参数更新）

标识和认证 SFR（FIA_*/EXT 和 FIA_*/MNO-SD）要求这些操作仅在经过身份验证后通过本地用户 U.MNO-SD 可供合法用户 U.MNO-OTA 使用。

FDP_ACC.1/ECASD 子集访问控制

FDP_ACC.1.1/ECASD TSF 应对于以下内容强制执行 **ECASD 访问控制 SFP**：

主体:S.ISD-R 和 S.ISD-P

客体：S.ECASED

操作：

- **执行 ECASD 功能**
- **访问这些功能的输出数据。**

FDP_ACF.1/ECASD 基于安全属性的访问控制

FDP_ACF.1.1/ECASD TSF 应根据以下内容对客体强制执行 **ECASD 访问控制 SFP**：

主体：S.ISD-R 和 S.ISD-P，具有安全属性"AID"

客体：S.ECASD

操作：

- **执行 ECASD 功能：**
  - **验证证书**
  - **生成随机挑战（以及对生成的随机挑战的访问）**
  - **使用公钥验证签名的随机挑战**
  - **生成共享密钥（以及访问生成的共享密钥）**

- **访问这些功能的输出数据。**

FDP_ACF.1.2/ECASD TSF 应执行以下规则以确定是否允许受控主体和受控客体之间的操作：

- **授权用户：只有通过其 AID 识别的 S.ISD-P（相应的 S.ISD-R）才有权执行以下 S.ECASD 功能：**
  - **验证证书 CERT.DP.ECDSA（分别为 CERT.SR.ECDSA）**
  - **生成随机挑战（以及对生成的随机挑战的访问）**
  - **使用 PK.DP.ECDSA（相应的 PK.SR.ECDSA）验证签名的随机挑战**
  - **生成共享密钥（以及访问生成的共享密钥）。**

FDP_ACF.1.3/ECASD TSF 应根据以下附加规则明确授予主体访问客体的权限：

- **EID、PK.CI.ECDSA 和 CERT.ECASD.ECKA 的值可由任何卡上主体检索而无需身份验证。**

FDP_ACF.1.4/ECASD TSF 应根据以下附加规则明确拒绝授予主体对客体的访问权限：

- **由 S.ECASD 控制的其他数据不能被除 S.ECASD 之外的任何其他主体访问。**

8.1.5 平台服务

该要求包描述了适用于平台支持功能和电信框架的特定要求。它特别定义：

- FDP_IFC.1/Platform_services 和 FDP_IFF.1/Platform_services：为控制安全域和平台支持功能（或电信框架）之间的信息流而采取的措施；
- FPT_FLS.1/Platform_Services：在平台支持功能（或电信框架）出现故障时强制实施安全状态的措施。

FDP_IFC.1/Platform_services 子集信息流控制

FDP_IFC.1.1/Platform_services TSF 应对以下内容强制执行**平台服务信息流控制 SFP：**

用户/主体：

- **S.ISD-R, S.ISD-P, U.MNO-SD**
- **平台代码（S.PSF，S.TELECOM）**

信息：

- **D.PROFILE_NAA_PARAMS**
- **D.PROFILE_POL1**

操作：

- **安装 Profile**
- **强制执行 POL1**
- **网络身份验证。**

FDP_IFF.1/Platform_services 简单的安全属性

FDP_IFF.1.1/Platform_services TSF 应根据以下类型的主体和信息安全属性强制执行**平台服务信息流控制 SFP：**

用户/主体：

- **S.ISD-R，S.ISD-P，U.MNO-SD，具有安全属性“应用程序标识符（AID）”**

信息：

- **D.PROFILE_NAA_PARAMS**
- **D.PROFILE_POL1**

操作：

- **安装 Profile**
- **强制执行 POL1**
- **网络身份验证。**

FDP_IFF.1.2/Platform_services 如果以下规则成立，TSF 应允许受控主体和受控信息之间的信息流通过受控操作：

- **D.PROFILE-NAA-PARAMS 只能在以下情况传输**
  - **由 U.MNO-SD 传输给 S.TELECOM 以执行“网络认证”API 功能**
  - **由 S.ISD-P 使用“安装”API 功能传输给 S.PSF**
- **D.PROFILE-POL1 只能在以下情况传输**
  - **由 S.ISD-P 传输给 S.PSF 以执行“强制执行 POL1”功能。**

FDP_IFF.1.3/Platform_services TSF 应强制执行[赋值：*附加信息流控制 SFP 规则*]。

FDP_IFF.1.4/Platform_services TSF 应根据以下规则明确授权信息流：[赋值：*基于安全属性明确授权信息流的规则*]。

FDP_IFF.1.5/Platform_services TSF 应根据以下规则明确拒绝信息流：[赋值：*基于安全属性明确授权信息流的规则*]

应用说明：

该 SFR 旨在控制哪个主体能够将 POL1 或网络认证密钥传输到 PSF 和电信框架。允许实现差异，因为该标准需要可证明的一致性。因此，ST 作者可以用另一个 FDP_IFF.1 实例替换此 SFR，只要它解决这些数据的信息流控制问题。这种调整的例子可能是由于诸如此类的情况：

- D.PROFILE-POL1 从 S.ISD-P 传输到 S.ISD-R，然后从 S.ISD-R 传输到 S.PSF
- D.PROFILE-NAA-PARAMS 从 U.MNO-SD 传输到 S.ISD-P，然后由 ISD-P 传输到 S.TELECOM

FPT_FLS.1/Platform_services 失效即保持安全状态

FPT_FLS.1.1/Platform_services 发生以下类型的故障时，TSF 应保持安全状态：

- **在处理 S.PSF 或 S.TELECOM API 特定功能期间导致潜在安全违规的故障：**
  - **安装 Profile**
  - **强制执行 POL1**
  - **网络认证**
- **[赋值：*其他类型的失败*]**

应用说明：

ST 作者应包括：

- 此 FPT_FLS.1 SFR，以及
- PP-JCS 规范的安全目标所要求的 FPT_FLS.1 SFR。两个 SFR 可以合并为一个，但 ST 作者必须确保合并的 SFR 包含该标准的特定故障情景和 PP-JCS 规范中的特定故障情景。

8.1.6 安全管理

该要求包包括几个支持的安全功能：

- ECASD 将使用的随机数生成（FCS_RNG.1）

- 用户数据和 TSF 自我保护措施：
  - TOE 发散（FPT_EMS.1）
  - 完整性监视（FDP_SDI.1）
  - 残留数据保护（FDP_RIP.1）
  - 保护安全状态（FPT_FLS.1）
- 安全管理措施：
  - 管理安全属性，如 PSF 数据（FMT_MSA.1/PSF_DATA）、POL1（FMT_MSA.1/POL1）和密钥（FMT_MSA.1/CERT_KEYS）及他们的限制性默认值（FMT_MSA.3）
  - 角色和安全功能的管理（FMT_SMR.1 和 FMT_SMF.1）

FCS_RNG.1 随机数生成

FCS_RNG.1.1 TSF 应提供[选择：*确定性，混合确定性，物理，混合物理*]随机数发生器[选择：*DRG.2，DRG.3，DRG.4，PTG.2，PTG.3*]，其实现：[赋值：*所选 RNG 类的安全功能列表*]。

FCS_RNG.1.2 TSF 应提供满足[赋值：*所选 RNG 类的已定义质量度量*]的随机数

应用说明：

如果 ST 作者选择需要自检的 RNG 类，则还必须包含专用的 FPT_TST.1 SFR 来描述此自测试。

FPT_EMS.1 TOE 发射

FPT_EMS.1.1 TOE 不得发出超过[赋值：*指定限制*]以能够访问以下资源的[赋值：*排放类型*]

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

以及作为以下键集的一部分的密钥：

- **D.MNO_KEYS,**
- **D.ISDR_KEYS,**
- **D.ISDP_KEYS,**
- **D.PROFILE_NAA_PARAMS**

FPT_EMS.1.2 TSF 应确保[赋值：*用户类型*]无法使用接口[赋值：*连接类型*]来获取对下述资源的访问

- **D.SECRETS;**
- **D.SK.EUICC.ECDSA**

以及**作为以下密钥集的一部分的密钥：**

- **D.MNO_KEYS,**
- **D.PROFILE_NAA_PARAMS.**

应用说明：

TOE 应防止攻击 TOE 的秘密数据，其中攻击基于 TOE 的外部可观察物理现象。这种攻击可以在 TOE 的接口处观察到，或者可以源自 TOE 的内部操作，或者可以源自改变 TOE 操作的物理环境的攻击者。可测量的物理现象集受到用于实现 TOE 的技术的影响。

可测量现象的示例是功耗的变化，内部状态的转变时序，由内部操作引起的电磁辐射，无线电放射。由于可能导致此类发散的技术具有异构性，因此假设应对适用于 TOE 所采用技术的最新攻击进行评估。此类攻击的示例包括但不限于 TOE 的电磁辐射评估，简单功耗分析（SPA），差分功耗分析（DPA），时序攻击等。

FDP_SDI.1 存储数据完整性监控

FDP_SDI.1.1 TSF 应根据以下属性监视所有对象存储在由 TSF 控制的容器中的用户数据的**完整性错误：完整性敏感数据**。

细化：

完整性敏感数据的概念涵盖了需要保护免受未经授权的修改的安全目标 TOE 的资产，包括但不限于此标准中需要保护免受未经授权修改的资产：

- D.MNO_KEYS,
- D.ISDR_KEYS,
- D.ISDP_KEYS,
- Profile 数据
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE_POL1
- 身份管理数据
  - D.eUICC_PRIVKEY
  - D.eUICC_CERT
  - D.CI_ROOT_PUBKEY
  - D.EID
  - D.SECRETS

FDP_RIP.1 子集残余信息保护

FDP_RIP.1.1 TSF 应确保为以下对象进行资源的释放和分配时，资源的任何先前信息内容都不可用：

- **D.SECRETS;**
- **D.eUICC_PRIVKEY;**
- **作为以下密钥集的一部分的密钥：**
  - **D.MNO_KEYS,**
  - **D.ISDR_KEYS,**
  - **D.ISDP_KEYS,**
  - **D.PROFILE_NAA_PARAMS.**
  - **FPT_FLS.1 保持安全状态失败**

FPT_FLS.1 失效即保持安全状态

FPT_FLS.1.1 发生以下类型的故障时，TSF 应保持安全状态：

- **ISD-R 未能创建新的 ISD-P**
- **ISD-P 无法创建 Profile**
- **由于存在孤立 Profile 而导致安装失败。**

FMT_MSA.1/PSF_DATA 安全属性的管理

FMT_MSA.1.1/PSF_DATA TSF 应强制执行 **ISD-R 访问控制策略和 ISD-P 访问控制策略**，以限制其修改安全属性的能力：

- **D.PSF_DATA 的以下部分：**

- **ISD-P 状态**
- **回滚属性**

到

- **S.ISD-R 修改 ISD-P 状态**
  - **从"INSTALLED"到"SELECTABLE"（在 ISD-P 创建期间）**
  - **从"DSIABLED"到"ENABLED"（在 Profile 启用期间）**
  - **从"ENABLED"到"DISABLED"（在 Profile 禁用期间）**
- **S.ISD-P 修改 ISD-R 状态**
  - **从"SELECTABLE"到"PERSONALIZED"（在 Profile 个人化期间）**
  - **从"PERSONALIZED"到"DISABLED"（在 Profile 个人化期间）**
- **S.PSF 修改 ISD-P 状态**
  从"ENABLED"到"DISABLED"（在回滚期间）
  - **S.ISD-R 修改回滚属性（设置回滚属性时）。**

应用说明：

- 如果部分 PSF 功能由 GlobalPlatform 包执行，则 S.PSF 的角色可能部分归因于 OPEN。
- GSMA SGP.02 规范中包括一个回滚功能，确保 eUICC 能够检测到连接丢失，然后回滚到安全 Profile 并通知 SM-SR。此标准未解决此功能。但是，仍然包含回滚元素，因为它会影响生命周期策略以及禁用/删除给定 Profile 的能力（请参阅 FDP_ACF.1/ISDR）

FMT_MSA.1/POL1 安全属性管理

FMT_MSA.1.1/POL1 TSF 应强制执行**安全信道协议信息流 SFP、ISD-P 访问控制 SFP 和 ISD-R 访问控制 SFP**，以限制修改默认值、查询、修改和删除安全属性的能力

- **D.PROFILE_POL1**

到

- **S.ISD-P 根据"ES8.DownloadAndInstallation"通过 U.SM-DP 的请求改变默认值**
- **S.ISD-R，S.ISD-P 查询**
- **S.ISD-P 根据 U.MNO-SD 的要求通过"ES6.UpdatePOL1byMNO"进行修改**
- **S.ISD-R 根据"ES5.DeleteProfile"的 U.SM-SR 要求删除。**

FMT_MSA.1/CERT_KEYS 安全属性管理

FMT_MSA.1.1/CERT_KEYS TSF 应强制执行**安全信道协议信息流 SFP、ISD-P 访问控制 SFP、ISD-R 访问控制 SFP 和 ECASD 内容访问控制 SFP**，以限制修改默认值，查询，修改和删除安全属性的能力

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

到

- **使用 S.ISD-P：**
  - **查询 CERT.DP.ECDSA**
  - **根据 U.SM-DP 的要求通过"ES8.EstablishISDPKeySet"修改默认值 D.ISDP_KEYS**

- **根据 U.SM-DP 的要求通过"ES8.DownloadAndInstallation"修改默认值 D.MNO_KEYS**
- **查询 D.ISDP_KEYS**

- **使用 S.ISD-R：**
  - **查询 CERT.SR.ECDSA**
  - **根据 U.SM-DP 的要求通过"ES8.EstablishISDRKeySet"修改默认值 D.ISDR_KEYS**
  - **查询 D.ISDR_KEYS**
  - **根据 U.SM-DP 的要求通过"ES5.FinaliseISDRhandover"删除 D.ISDR_KEYS**
  - **删除 D.ISDP_KEYS 和 D.MNO_KEYS，根据"ES5.DeleteProfile"的 USM-SR 请求**
- **其他操作没有参与者**

应用说明：

禁止修改 D.ISDP_KEYS 和 D.MNO_KEYS 密钥集。要修改密钥集，必须删除该 Profile 并加载另一个 Profile。

FMT_MSA.3 静态属性初始化

FMT_MSA.3.1 TSF 应强制执行**安全信道协议信息流 SFP、ISD-P 访问控制 SFP、ISD-R 访问控制 SFP 和 ECASD 访问控制 SFP**，以便为用于强制执行 SFP 的安全属性提供限制性默认值。

FMT_MSA.3.2 TSF **不允许任何参与者**指定备用初始值，以在创建对象或信息时覆盖默认值。

FMT_SMF.1 管理职能规范

FMT_SMF.1.1 TSF 应能够执行以下管理功能：[赋值：*由 TSF 提供的管理功能列表*]。

FMT_SMR.1 安全角色

FMT_SMR.1.1 TSF 应保持以下角色

- **外部用户**
  - **U.SM-DP**
  - **U.SM-SR**
  - **U.MNO-SD**
  - **U.MNO-OTA**
- **主体：**
  - **S.ISD-R**
  - **S.ISD-P**
  - **S.ECASD**
  - **S.PSF**
  - **S.TELECOM**

FMT_SMR.1.2 TSF 应能够将用户与角色相关联

应用说明：

此处定义的角色对应于 5.2 节中定义的用户和主体。

8.1.7 移动网络认证

该要求包定义了与 MNO 网络上的 eUICC 认证相关的要求

TSF 必须在 MNO 网络上实施加密机制（FCS_COP.1/Mobile_network）并安全地管理密钥（FDP_ITC.1/SCP 和 FCS_CKM.4/Mobile_network）。

FCS_COP.1/Mobile_network 密码运算

FCS_COP.1.1/Mobile_network TSF 应根据指定的加密算法 **MILENAGE，Tuak，[选择：*其他算法，无其他算法*]**和加密密钥大小，根据符合以下条件的**相应标准**执行**网络身份验证**：

- **符合 MILENAGE 规范的 MILENAGE 具有以下限制：**
  - **仅使用 128 位 AES 作为内核函数，不支持其他选择**
  - **允许常量 OP 的任何值**
  - **允许常数 C1-C5 和 R1-R5 的任何值，但须遵守标准 MILENAGE 规范第 5.3 节中的规则和建议**
- **符合 Tuak 规范的 Tuak，有以下限制：**
  - **允许任何 TOP 值**
  - **允许 Keccak 多次迭代**
  - **支持 256 位和 128 位 K**
  - **将 RES，MAC，CK 和 IK 的支持大小限制为 3GPP 标准中当前支持的大小。**

应用说明：

ST 作者必须列出 TOE 电信框架支持的完整算法列表（例如 Milenage 等）

这些算法使用的密钥在配置期间在 Profile 中分发（FDP_ITC.1/SCP），必须安全删除（FCS_CKM.4/Mobile_network）。

FCS_CKM.2/Mobile_network 密钥分发

FCS_CKM.2.1/Mobile_network TSF 应根据符合以下条件的指定密钥分发方法[赋值：*密钥分发方法*]分发密钥：[赋值：*标准列表*]。

应用说明：

此 SFR 中的密钥是资产 D.PROFILE_NAA_PARAMS 中包含的移动网络身份验证密钥。在 Profile 下载期间，这些密钥作为 MNO Profile 的一部分分发。

FCS_CKM.4/Mobile_network 密钥销毁

FCS_CKM.4.1/Mobile_network TSF 应使用满足[赋值：*标准列表*]的特定的密钥销毁方法[赋值：*密钥销毁方法*]销毁密钥。

8.2 安全保障要求

评估保障级别为 EAL4，增加了 AVA_VAN.5 和 ALC_DVS.2.ADV_ARC。

8.2.1 ADV 开发

8.2.1.1 ADV_ARC 安全架构

ADV_ARC.1 安全架构描述

ADV_ARC.1.1D 开发者应设计并实现 TOE，确保 TSF 的安全特性不可绕过。
ADV_ARC.1.2D 开发者应设计并实现 TSF，以防止不可信主体的篡改。

ADV_ARC.1.3D 开发者应提供 TSF 的安全架构描述。
ADV_ARC.1.1C 安全架构描述的详细程度应与 TOE 设计文档中描述的 SFR-执行的抽象描述相当。
ADV_ARC.1.2C 安全架构描述应描述由 TSF 维护的与 SFR 一致的安全域。
细化：

特别是，在不需要比 GP-SecurityGuidelines-BasicApplications 规范更多的 applet 验证规则的情况下，TOE 应保持 applet 隔离。

ADV_ARC.1.3C 安全架构描述应描述 TSF 初始化过程为何是安全的。
ADV_ARC.1.4C 安全架构描述应证明 TSF 可保护自己免受篡改。
ADV_ARC.1.5C 安全架构描述应证明 TSF 可防止 SFR-执行功能被绕过。
ADV_ARC.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.1.2 ADV_FSP 功能规范

ADV_FSP.4 完整的功能规范

ADV_FSP.4.1D 开发者应提供功能规范。
ADV_FSP.4.2D 开发者应提供从功能规范到 SFR 的追溯。
ADV_FSP.4.1C 功能规范应完全描述 TSF。
ADV_FSP.4.2C 功能规范应描述所有 TSFI 的使用目的和方法。
ADV_FSP.4.3C 功能规范应识别和描述每个与 TSFI 相关的所有参数。
ADV_FSP.4.4C 功能规范应描述与每个 TSFI 相关的所有动作。
ADV_FSP.4.5C 功能规范应描述可能由每个 TFSI 调用而引起的所有直接错误消息。
ADV_FSP.4.6C 功能规范应证明 SFR 到 TSFI 的追溯。
ADV_FSP.4.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ADV_FSP.4.2E 评估者应确定功能规范是 SFR 的一个准确且完整的实例。

8.2.1.3 ADV_IMP 实现表示

ADV_IMP.1 TSF 的实现表示

ADV_IMP.1.1D 开发者应提供整个 TSF 的实现表示。
ADV_IMP.1.2D 开发者应提供 TOE 设计描述与实现表示实例之间的映射。
ADV_IMP.1.1C 实现表示应按详细级别定义 TSF，以达到无需进一步设计决策即可生成 TSF。
ADV_IMP.1.2C 实现表示应以开发人员使用的形式提供。
ADV_IMP.1.3C TOE 设计描述与实施表示实例之间的映射应证明它们的一致性。
ADV_IMP.1.1E 对于所选择的实现表示实例，评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.1.4 ADV_TDS TOE 设计

ADV_TDS.3 基础模块设计

ADV_TDS.3.1D 开发者应提供 TOE 的设计。
ADV_TDS.3.2D 开发者应提供从功能规范的 TSFI 到 TOE 设计中获取到的最低层分解的映射。
ADV_TDS.3.1C 设计应根据子系统描述 TOE 的结构。
ADV_TDS.3.2C 设计应根据模块描述 TSF。
ADV_TDS.3.3C 设计应标识 TSF 的所有子系统。
ADV_TDS.3.4C 设计应提供 TSF 的每个子系统的描述。

ADV_TDS.3.5C 设计应描述 TSF 所有子系统之间的相互作用。
ADV_TDS.3.6C 设计应提供从 TSF 的子系统到 TSF 的模块的映射。
ADV_TDS.3.7C 设计应描述每个 SFR-执行模块，包括其目的和与其他模块间的相互作用。
ADV_TDS.3.8C 设计应描述每个 SFR-执行模块，包括 SFR 相关的接口、这些接口的返回值、与其他模块的交互以及调用接口。
ADV_TDS.3.9C 设计应描述每个 SFR-支撑或 SFR-无关模块，包括其目的和与其他模块的相互作用。
ADV_TDS.3.10C 映射关系应论证 TOE 设计中描述的所有行为能映射到调用它的 TSFI。
ADV_TDS.3.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ADV_TDS.3.2E 评估者应确定该设计是所有安全功能要求的准确和完整的实例。

8.2.2 AGD 指导文件

8.2.2.1 AGD_OPE 操作用户指南

AGD_OPE.1 操作用户指南

AGD_OPE.1.1D 开发者应提供操作用户指导。
AGD_OPE.1.1C 操作用户指南应对每个用户角色描述应在安全处理环境中控制的用户可访问的功能和特权，包括适当的警告。
AGD_OPE.1.2C 操作用户指南应为每个用户角色描述如何以安全的方式使用 TOE 提供的可用接口。
AGD_OPE.1.3C 操作用户指南应为每个用户角色描述可用的功能和接口，特别是用户控制下的所有安全参数，适当时应指明安全值。
AGD_OPE.1.4C 对于每个用户角色，操作用户指南应清楚地说明与需要执行的用户可访问功能相关的每一种的安全相关事件，包括改变 TSF 控制下的实体的安全特性。
AGD_OPE.1.5C 操作用户指南应标识 TOE 运行的所有可能状态（包括操作导致的失败或者操作性错误），它们与维持安全运行之间的因果关系和联系。
AGD_OPE.1.6C 对于每个用户角色，操作用户指南应描述为了充分实现 ST 中描述的操作环境安全目的所必须执行的安全策略。
AGD_OPE.1.7C 操作用户指南应清晰合理。
AGD_OPE.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.2.2 AGD_PRE 准备程序

AGD_PRE.1 准备程序

AGD_PRE.1.1D 开发者应提供 TOE，包括其准备程序。
AGD_PRE.1.1C 准备程序应描述与开发者交付程序相一致的安全接受所交付的 TOE 所需的所有步骤。
AGD_PRE.1.2C 准备程序应描述安全安装 TOE 以及安全准备与 ST 中描述的运行环境安全目的一致的运行环境必须的所有步骤。
AGD_PRE.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
AGD_PRE.1.2E 评估者应运用准备程序确认 TOE 运行能被安全的准备。

8.2.3 ALC 生命周期支持

8.2.3.1 ALC_CMC CM 能力

ALC_CMC.4 生产支持和接受程序及其自动化

ALC_CMC.4.1D 开发者应提供 TOE 和 TOE 的参照号。
ALC_CMC.4.2D 开发者应提供 CM 文档。
ALC_CMC.4.3D 开发者应使用 CM 系统。
ALC_CMC.4.1C 应给 TOE 标记唯一参照号。
ALC_CMC.4.2C CM 文档应描述用于唯一标识配置项的方法。
ALC_CMC.4.3C CM 系统应唯一标识所有配置项。
ALC_CMC.4.4C CM 系统应提供自动化措施，以便仅对配置项进行授权更改。
ALC_CMC.4.5C CM 系统应通过自动化方式支持 TOE 的生产。
ALC_CMC.4.6C CM 文档应包括 CM 计划。
ALC_CMC.4.7C CM 计划应描述 CM 系统如何用于 TOE 的开发。
ALC_CMC.4.8C CM 计划应描述用于接受修改或新创建的配置项作为 TOE 一部分的程序。
ALC_CMC.4.9C 证据应证明所有配置项都在 CM 系统下维护。
ALC_CMC.4.10C 证据应证明 CM 系统正在按照 CM 计划运行。
ALC_CMC.4.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.3.2 ALC_CMS CM 范围

ALC_CMS.4 问题跟踪 CM 覆盖

ALC_CMS.4.1D 开发者应提供 TOE 的配置列表。
ALC_CMS.4.1C 配置列表应包括以下内容：TOE 本身；SAR 所要求的评估证据；TOE 的组成部分；实现表示和安全缺陷报告及其解决状态。
ALC_CMS.4.2C 配置列表应唯一标识配置项。
ALC_CMS.4.3C 对于每个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。
ALC_CMS.4.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.3.3 ALC_DEL 交付

ALC_DEL.1 交付程序

ALC_DEL.1.1D 开发者应将把 TOE 或其部分交付给消费者的程序文档化。
ALC_DEL.1.2D 开发者应使用交付程序。
ALC_DEL.1.1C 交付文档应描述，在向消费类分发 TOE 版本时，用以维护安全性所必需的所有程序。
ALC_DEL.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.3.4 ALC_DVS 开发安全

ALC_DVS.2 充分的安全措施

ALC_DVS.2.1D 开发者应提供开发安全文档。
ALC_DVS.2.1C 开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的及其它方面的安全措施。
ALC_DVS.2.2C 开发安全文档应论证安全措施提供了必需的保护级别以维护 TOE 的保密性和完整性。
ALC_DVS.2.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ALC_DVS.2.2E 评估者应确认安全措施正在被使用。

8.2.3.5 ALC_LCD 生命周期定义

ALC_LCD.1 开发者定义的生命周期模型

ALC_LCD.1.1D 开发者应建立一个生命周期模型，用于 TOE 的开发和维护。
ALC_LCD.1.2D 开发人员应提供生命周期定义文档。
ALC_LCD.1.1C 生命周期定义文档应描述用于开发和维护 TOE 的模型。
ALC_LCD.1.2C 生命周期模型应对 TOE 的开发和维护提供必要的控制。
ALC_LCD.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.3.6 ALC_TAT 工具和技术

ALC_TAT.1 明确定义的开发工具

ALC_TAT.1.1D 开发者应标识用于开发 TOE 的每个工具。
ALC_TAT.1.2D 开发者应在文档中描述每个开发工具所选取的实现依赖选项。
ALC_TAT.1.1C 用于实现的每个开发工具都应是明确定义的。
ALC_TAT.1.2C 每个开发工具的文档应无歧义地定义所有语句和实现用到的所有协定与命令的含义。
ALC_TAT.1.3C 每个开发工具的文档应无歧义地定义所有实现依赖选项的含义。
ALC_TAT.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.4 ASE 安全目标评估

8.2.4.1 ASE_CCL 符合性声明

ASE_CCL.1 符合性声明

ASE_CCL.1.1D 开发者应提供符合性声明。
ASE_CCL.1.2D 开发者应提供符合性声明的基本原理。
ASE_CCL.1.1C 符合性声明应包含 CC 符合性声明，该声明标识 ST 和 TOE 声明符合的 CC 的版本。
ASE_CCL.1.2C CC 符合性声明应描述 ST 与 CC 第 2 部分的符合性，无论 CC 第 2 部分符合或 CC 第 2 部分扩展。
ASE_CCL.1.3C CC 符合性声明应描述 ST 与 CC 第 3 部分的符合性，无论 CC 第 3 部分符合或 CC 第 3 部分扩展。
ASE_CCL.1.4C CC 符合性声明应与扩展组件定义一致。
ASE_CCL.1.5C 符合性声明应标识 ST 声称符合的所有 PP 和安全要求包。
ASE_CCL.1.6C 符合性声明应描述 ST 与包的任何符合性，包括符合包的符合或包扩展。
ASE_CCL.1.7C 符合性声明的基本原理应证明 TOE 类型与声明符合的 PP 中的 TOE 类型一致。
ASE_CCL.1.8C 符合性声明的基本原理应证明安全问题定义的陈述与声明符合的 PP 中的安全问题定义的陈述一致。
ASE_CCL.1.9C 符合性声明的基本原理应证明安全目的陈述与声明符合的 PP 中的安全目的陈述一致。
ASE_CCL.1.10C 符合性声明的基本原理应证明安全要求陈述与声明符合的 PP 中的安全要求陈述一致。
ASE_CCL.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.4.2 ASE_ECD 扩展组件定义

ASE_ECD.1 扩展组件定义

ASE_ECD.1.1D 开发者应提供安全要求的陈述。

ASE_ECD.1.2D 开发者应提供扩展组件的定义。
ASE_ECD.1.1C 安全要求陈述应标识所有扩展的安全要求。
ASE_ECD.1.2C 扩展组件定义应为每一个扩展的安全要求定义一个扩展的组件。
ASE_ECD.1.3C 扩展组件定义应描述每个扩展的组件与已有组件、族和类的关联性。
ASE_ECD.1.4C 扩展组件定义应使用已有的组件、族、类和方法学作为陈述的模型。
ASE_ECD.1.5C 扩展组件应由可测量的和客观的元素组成，以便于证实这些元素之间的符合性或不符合性。
ASE_ECD.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ASE_ECD.1.2E 评估者应确认扩展组件不能利用已经存在的组件明确的表达。

8.2.4.3 ASE_INT ST 引言

ASE_INT.1 ST 引言

ASE_INT.1.1D 开发者应提供 ST 引言。
ASE_INT.1.1C ST 引言应包含 ST 参照号，TOE 参照号，TOE 概述和 TOE 描述。
ASE_INT.1.2C ST 参照号应唯一标识 ST。
ASE_INT.1.3C TOE 参照号应标识 TOE。
ASE_INT.1.4C TOE 概述应概括 TOE 的用法和主要安全特性。
ASE_INT.1.5C TOE 概述应标识 TOE 类型。
ASE_INT.1.6C TOE 概述应标识 TOE 要求的任何非 TOE 范围内的硬件/软件/固件。
ASE_INT.1.7C TOE 描述应描述 TOE 的物理范围。
ASE_INT.1.8C TOE 描述应描述 TOE 的逻辑范围。
ASE_INT.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ASE_INT.1.2E 评估者应确认 TOE 参考，TOE 概述和 TOE 描述是否相互一致。

8.2.4.4 ASE_OBJ 安全目标

ASE_OBJ.2 安全目的

ASE_OBJ.2.1D 开发者应提供安全目的陈述。
ASE_OBJ.2.2D 开发者应提供安全目的基本原理。
ASE_OBJ.2.1C 安全目的陈述应描述 TOE 的安全目的和运行环境的安全目的。
ASE_OBJ.2.2C 安全目的基本原理应追溯到 TOE 的每一个安全目的，以便能追溯到安全目的所对抗的威胁及安全目的实施的组织安全策略。
ASE_OBJ.2.3C 安全目的基本原理应追溯到运行环境的每一个安全目的，以便能追溯到安全目的所对抗的威胁、安全目的实施的组织安全策略和安全目的支持的假设。
ASE_OBJ.2.4C 安全目的基本原理应证明安全目的可抵御所有威胁。
ASE_OBJ.2.5C 安全目的基本原理应证明安全目的执行所有 OSP。
ASE_OBJ.2.6C 安全目的基本原理应证明运行环境安全目的支持所有假设。
ASE_OBJ.2.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.4.5 ASE_REQ 安全要求

ASE_REQ.2 推导出的安全要求

ASE_REQ.2.1D 开发者应提供安全要求的陈述。

ASE_REQ.2.2D 开发者应提供安全要求基本原理。
ASE_REQ.2.1C 安全要求的陈述应描述 SFR 和 SAR。
ASE_REQ.2.2C 应对 SFR 和 SAR 中使用的所有主体、客体、操作、安全属性、外部实体和其他术语进行定义。
ASE_REQ.2.3C 安全要求的陈述应标识有关安全要求的所有操作。
ASE_REQ.2.4C 所有操作都应正确执行。
ASE_REQ.2.5C 应满足安全要求间的依赖关系，或者安全要求的基本原理应论证不需要满足某个依赖关系。
ASE_REQ.2.6C 安全要求的基本原理应将每个 SFR 追溯到 TOE 的安全目的。
ASE_REQ.2.7C 安全要求的基本原理应证明 SFR 可满足所有的 TOE 安全目的。
ASE_REQ.2.8C 安全要求的基本原理应解释选择 SAR 的理由。
ASE_REQ.2.9C 安全要求的陈述应是内在一致的。
ASE_REQ.2.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.4.6 ASE_SPD 安全问题定义

ASE_SPD.1 安全问题定义

ASE_APD.1.1D 开发者应提供安全问题定义。
ASE_SPD.1.1C 安全问题定义应描述威胁。
ASE_SPD.1.2C 所有威胁都应根据威胁主体、资产和敌对行为进行描述。
ASE_SPD.1.3C 安全问题定义应描述 OSP。
ASE_SPD.1.4C 安全问题定义应描述 TOE 运行环境的相关假设。
ASE_SPD.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.4.7 ASE_TSS TOE 概要规范

ASE_TSS.1 TOE 概要规范

ASE_TSS.1.1D 开发者应提供 TOE 概要规范。
ASE_TSS.1.1C TOE 概要规范应描述 TOE 如何满足每个 SFR 的。
ASE_TSS.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ASE_TSS.1.2E 评估者应确认 TOE 概要规范与 TOE 概述和 TOE 描述一致。

8.2.5 ATE 测试

8.2.5.1 ATE_COV 覆盖

ATE_COV.2 覆盖分析

ATE_COV.2.1D 开发者应提供对测试覆盖的分析。
ATE_COV.2.1C 测试覆盖分析应证明测试文档中的测试与功能规范中的 TSFI 之间的对应关系。
ATE_COV.2.2C 测试覆盖分析应证明功能规范中的所有 TSFI 都已经过测试。
ATE_COV.2.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.5.2 ATE_DPT 深度

ATE_DPT.2 测试：安全执行模块

ATE_DPT.2.1D 开发者应提供测试深度的分析。
ATE_DPT.2.1C 测试深度分析应证明测试文档中的测试与 TOE 设计中的 TSF 子系统、SFR-执行模块之间的一致性。
ATE_DPT.2.2C 测试深度分析应证明 TOE 设计中的所有 TSF 子系统都已经过测试。
ATE_DPT.2.3C 测试深度分析应证明 TOE 设计中的 SFR-执行模块都已经过测试。
ATE_DPT.2.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.5.3 ATE_FUN 功能测试

ATE_FUN.1 功能测试

ATE_FUN.1.1D 开发者应当测试 TSF 并文档化测试结果。
ATE_FUN.1.2D 开发者应提供测试文档。
ATE_FUN.1.1C 测试文档应包括测试计划、预期测试结果和实际测试结果。
ATE_FUN.1.2C 测试计划应标识要执行的测试并描述执行每个测试的方案，这些方案应包括对于其它测试结果的任何顺序依赖性。
ATE_FUN.1.3C 预期的测试结果应指出测试成功执行后的预期输出。
ATE_FUN.1.4C 实际的测试结果应与预期的测试结果一致。
ATE_FUN.1.1E 评估者应确认所提供的信息符合证据的内容和形式要求。

8.2.5.4 ATE_IND 独立测试

ATE_IND.2 独立测试——抽样

ATE_IND.2.1D 开发者应提供用于测试的 TOE。
ATE_IND.2.1C TOE 应适合测试。
ATE_IND.2.2C 开发者应提供一组与开发者 TSF 功能测试中同等的一系列资源。
ATE_IND.2.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
ATE_IND.2.2E 评估者应执行测试文档中的测试样本，以验证开发者的测试结果。
ATE_IND.2.3E 评估者应测试 TSF 的一个子集，以确认 TSF 按规定运行。

8.2.6 AVA 脆弱性评定

8.2.6.1 AVA_VAN 脆弱性分析

AVA_VAN.5 高级的系统的脆弱性分析

AVA_VAN.5.1D 开发者应提供用于测试的 TOE。
AVA_VAN.5.1C TOE 应适合于测试。
AVA_VAN.5.1E 评估者应确认所提供的信息符合证据的内容和形式要求。
AVA_VAN.5.2E 评估者应执行公共领域的调查以标识 TOE 的潜在脆弱性。
AVA_VAN.5.3E 评估者应针对 TOE 执行独立的、系统的脆弱性分析去标识 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范、 TOE 设计、安全结构描述和实现表示。
AVA_VAN.5.4E 评估者应基于已标识的潜在脆弱性实施穿透性测试，确认 TOE 能抵抗具有高等攻击潜力的攻击者的攻击。

8.3 安全要求基本原理

8.3.1 目标

8.3.1.1 TOE 的安全目标

平台支持功能

O.PSF

与安全域相关的 SFR（FDP_ACC.1/ISDR，FDP_ACF.1/ISDR，FDP_ACC.1/ISDP，FDP_ACF.1/ISDP，FDP_ACC.1/ECASD 和 FDP_ACF.1/ECASD）通过执行符合卡内容管理规则的安全域访问控制策略（规则和限制）涵盖此安全目标

FMT_MSA.1/POL1 通过确保管理 POL1 策略文件来支持这些 SFR，从而确保根据授权策略进行生命周期修改。

FMT_MSA.1/PSF_DATA 限制可应用于 PSF 数据（ISD-P 状态和回滚属性）的状态转换，这些转换被 TSF 的其他安全策略用作安全属性（ISD-R 访问控制 SFP 和 ISD-P 访问控制 SFP）。

目标还要求 FPT_FLS.1 中描述的安全故障模式。

FCS_RNG.1 需要支持 FDP_ACF.1/ECASD。

O.eUICC-DOMAIN-RIGHT

要求 FDP_ACC.1/ISDR、FDP_ACF.1/ISDR、FDP_ACC.1/ISDP、FDP_ACF.1/ISDP、FDP_ACC.1/ECASD 和 FDP_ACF.1/ECAS 确保 ISD-R、ISD-P、MNO-SD 和 ECASD 功能和内容仅可被相应的授权用户访问。FTP_ITC.1/SCP 为授权用户提供相应的安全通道。

FMT_MSA.1/POL1、FMT_MSA.1/PSF_DATA、FMT_MSA.1/CERT_KEYS 和 FMT_MSA.3 用于管理 SFP 使用的安全属性。

FDP_ACF.1/ECASD 要求 FCS_RNG.1 支持。

注意：没有安全通道可以访问 ECASD，因为其服务可以由卡上的参与者访问，但其内容在 eUICC 的生命周期内无法修改。

O.SECURE-CHANNEL

要求 FTP_ITC.1/SCP，FPT_TDC.1/SCP，FDP_UCT.1/SCP，FDP_UIT.1/SCP，FDP_ITC.2/SCP，FDP_IFC.1/SCP，FDP_IFF.1/SCP，通过执行安全通道协议信息流控制 SFP 涵盖此安全目标，确保传输的命令和数据免受未经授权的泄露和修改。它们依赖于 FCS_CKM.1/SCP-SM，FCS_CKM.2/SCP-MNO，FCS_CKM.4/SCP-SM 和 FCS_CKM.4/SCP-MNO 进行密钥管理。

识别和认证 SFR（FIA_UID.1/EXT，FIA_UAU.1/EXT，FIA_UAU.4/EXT，FIA_UID.1/MNO-SD，FIA_USB.1/MNO-SD，FIA_USB.1/EXT）通过要求远程 SM-DP、SM-SR 和 MNO OTA 平台的身份验证和识别以建立这些安全通道来支持这一安全目标。

FIA_ATD.1，FMT_MSA.1/CERT_KEYS 和 FMT_MSA.3 解决了 SFP 使用的安全属性的管理问题。

FMT_SMF.1 和 FMT_SMR.1 通过提供角色管理和功能管理来支持这些 SFR。

O.INTERNAL-SECURE-CHANNELS

FPT_EMS.1 确保在侧信道攻击的情况下不应泄露在 TOE 内存储或传输的秘密数据。这尤其包括在 ECASD 和 ISD-R/ISD-P.FDP_SDI.1 之间传输的共享秘密。

FDP_SDI.1 确保在此传输期间共享秘密不会被修改。

FDP_RIP.1 确保无法从释放的资源中恢复共享秘密。

eUICC 身份证明

O.PROOF_OF_IDENTITY

该目标由扩展要求 FIA_API.1 涵盖。

平台服务

O.OPERATE

FPT_FLS.1/Platform_services 要求故障不会影响 TOE 的安全性。

O.API

FDP_IFC.1/Platform_services、FDP_IFF.1/Platform_services、FMT_MSA.3 和 FMT_SMR.1 以及 FMT_SMF.1 说明了用于控制应用程序层对 TOE 服务和资源的访问的策略（“API 信息流控制策略”）。

原子性由 FPT_FLS.1/Platform_services 要求提供

数据保护

O.DATA-CONFIDENTIALITY

FDP_UCT.1/SCP 处理来自卡外参与者的数据接收，而访问控制 SFR（FDP_ACC.1/ISDR、FDP_ACC.1/ISDP、FDP_ACC.1/ECASD）解决安全域之间的隔离问题。

FPT_EMS.1 在侧信道攻击的情况下，不应泄露在 TOE 内存储或传输的秘密数据。

FDP_RIP.1 确保没有剩余的机密数据可用。

FCS_COP.1/Mobile_network、FCS_CKM.2/Mobile_network 和 FCS_CKM.4/Mobile_network 处理电信框架中存在的加密算法、相关密钥的分发和销毁。

P.DATA-INTEGRITY

FDP_UIT.1/SCP 处理来自卡外参与者的数据接收，而访问控制 SFP（FDP_ACC.1/ISDR、FDP_ACC.1/ISDP、FDP_ACC.1/ECASD）解决了安全域之间的隔离问题。

FDP_SDI.1 指定了进行监视的 Profile 数据，以防止完整性破坏（例如，在安装操作期间修改接收的 Profile）。

连接性

O.ALGORITHMS

算法在 FCS_COP.1/Mobile_network 中定义。FCS_CKM.2/Mobile_network 描述了如何在 MNO Profile 中分发密钥，FCS_CKM.4/Mobile_network 描述了密钥的销毁。

8.3.2 安全目标和 SFR 基本原理

表 10 安全目标和 SFR——覆盖范围

安全目标	安全功能要求
O.PSF	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FPT_FLS.1, FCS_RNG.1

安全目标	安全功能要求
O.eUICC-DOMAIN-RIGHTS	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FTP_ITC.1/SCP, FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FCS_RNG.1
O.SECURE-CHANNELS	FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP, FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.4/SCP-SM, FCS_CKM.4/SCP-MNO, FIA_UID.1/EXT, FIA_UAU.1/EXT, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD, FIA_USB.1/MNO-SD, FIA_USB.1/EXT, FIA_ATD.1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
O.INTERNAL-SECURE-CHANNELS	FDP_RIP.1, FDP_SDI.1, FPT_EMS.1
O.PROOF_OF_IDENTITY	FIA_API.1
O.OPERATE	FPT_FLS.1/Platform_Services
O.API	FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FPT_FLS.1/Platform_Services, FMT_SMR.1, FMT_SMF.1, FMT_MSA.3
O.DATA-CONFIDENTIALITY	FDP_RIP.1, FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network, FPT_EMS.1
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FDP_SDI.1
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network

表 11 SFR 和安全目标

安全功能要求	安全目标
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

安全功能要求	安全目标
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
FCS_RNG.1	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ISDR	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ISDR	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ISDP	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ISDP	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ECASD	O.PSF, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ECASD	O.PSF, O.eUICC-DOMAIN-RIGHTS
FDP_IFC.1/Platform_services	O.API
FDP_IFF.1/Platform_services	O.API
FPT_FLS.1/Platform_Services	O.OPERATE, O.API
FPT_EMS.1	O.INTERNAL-SECURE-CHANNELS, O.DATA-CONFIDENTIALITY
FDP_SDI.1	O.INTERNAL-SECURE-CHANNELS, O.DATA-INTEGRITY
FDP_RIP.1	O.INTERNAL-SECURE-CHANNELS, O.DATA-CONFIDENTIALITY
FPT_FLS.1	O.PSF
FMT_MSA.1/PSF_DATA	O.PSF, O.eUICC-DOMAIN-RIGHTS
FMT_MSA.1/POL1	O.PSF, O.eUICC-DOMAIN-RIGHTS
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS, O.eUICC-DOMAIN-RIGHTS
FMT_MSA.3	O.SECURE-CHANNELS, O.API, O.eUICC-DOMAIN-RIGHTS
FMT_SMF.1	O.SECURE-CHANNELS, O.API
FMT_SMR.1	O.SECURE-CHANNELS, O.API
FCS_COP.1/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS
FCS_CKM.2/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS
FCS_CKM.4/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS

8.3.3 依赖关系

8.3.3.1 SFR 依赖关系

表 12 SFR 依赖关系

要求	CC 依赖关系	满足的依赖关系
FIA_UID.1/EXT	无依赖关系	
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	无依赖关系	
FIA_UID.1/MNO-SD	无依赖关系	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1	无依赖关系	
FIA_API.1	无依赖关系	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) 和 (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	无依赖关系	
FDP_ITC.2/SCP	(FDP_ACC.1 或 FDP_IFC.1) 和 (FPT_TDC.1) 和 (FTP_ITC.1 或 FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP, FPT_TDC.1/SCP
FPT_TDC.1/SCP	无依赖关系	
FDP_UCT.1/SCP	(FDP_ACC.1 或 FDP_IFC.1) 和 (FTP_ITC.1 或 FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 或 FDP_IFC.1) 和 (FTP_ITC.1 或 FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 或 FCS_COP.1) 和 (FCS_CKM.4)	FCS_CKM.4/SCP-SM
FCS_CKM.2/SCP-MNO	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2) 和 (FCS_CKM.4)	FDP_ITC.1/SCP, FCS_CKM.4/SCP-MNO 基本原理：此 SFR 与以下资源的分布相关： ● Profile 下载期间的 D.MNO_KEYS ● 公钥分发在用户证书（CERT.SR.ECDSA 和 CERT.DP.ECDSA）中或在预先发布的 TOE 中加载（D.eUICC_CERT，D.CI_ROOT_PUBKEY） 因此，分发需要依赖于 FDP_ITC.1/SCP 和安全销毁（FCS_CKM.4/SCP-MNO）

要求	CC 依赖关系	满足的依赖关系
FCS_CKM.4/SCP-SM	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.1/SCP, FCS_CKM.1/SCP-SM 基本原理：FCS_CKM.4/SCP-SM 与以下密钥的销毁有关 ： ● 由 FCS_CKM.1/SCP-SM 生成的密钥： ■ D.ISDP_KEYS ■ D.ISDR_KEYS ● 由 FDP_ITC.1/SCP 分发的密钥： ■ CERT.SR.ECDSA ■ CERT.DP.ECDSA ■ D.eUICC_CERT ■ D.eUICC_PRIVKEY ■ D.CI_ROOT_PUBKEY
FCS_CKM.4/SCP-MNO	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.1/SCP, FCS_CKM.1/SCP-SM
FCS_RNG.1	无依赖关系	
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) 和 (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ISDP	(FDP_ACF.1)	FDP_ACF.1/ISDP
FDP_ACF.1/ISDP	(FDP_ACC.1) 和 (FMT_MSA.3)	FDP_ACC.1/ISDP, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) 和 (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3, FCS_RNG.1
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) 和 (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_Services	无依赖关系	
FPT_EMS.1	无依赖关系	
FDP_SDI.1	无依赖关系	
FDP_RIP.1	无依赖关系	
FPT_FLS.1	无依赖关系	

要求	CC 依赖关系	满足的依赖关系
FMT_MSA.1/PSF_DATA	(FDP_ACC.1 或 FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FMT_SMF.1, FMT_SMR.1 基本原理：此 SFR 与安全属性 D.PSF_DATA 相关，其管理必须强制执行 ISD-R 访问控制策略以及 ISD-P 访问控制策略。因此，依赖性通过相应的 SFR（FDP_ACC.1/ISDR 和 FDP_ACC.1/ISDP）满足。
FMT_MSA.1/POL1	(FDP_ACC.1 或 FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_IFC.1/SCP, FMT_SMF.1, FMT_SMR.1 基本原理：此 SFR 与安全属性 D.PROFILE_POL1 相关，其管理必须强制执行安全通道协议信息流 SFP、ISD-P 访问控制 SFP 和 ISD-R 访问控制 SFP。因此，依赖性通过相应的 SFR（FDP_ACC.1/ISDR，FDP_ACC.1/ISDP 和 FDP_IFC.1/SCP）满足。
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 或 FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_IFC.1/SCP, FDP_ACC.1/ECASD, FMT_SMF.1, FMT_SMR.1 基本原理：此 SFR 与以下安全属性有关： ● CERT.DP.ECDSA ● CERT.SR.ECDSA ● D.ISDP_KEYS ● D.ISDR_KEYS ● D.MNO_KEYST 管理必须强制执行安全通道协议信息流 SFP、ISD-P 访问控制 SFP、ISD-R 访问控制 SFP 和 ECASD 内容访问控制 SFP。因此，依赖性通过相应的 SFR（FDP_ACC.1/ISDR，FDP_ACC.1/ISDP，FDP_ACC.1/ECASD 和 FDP_IFC.1/SCP）满足。
FMT_MSA.3	(FMT_MSA.1) 和 (FMT_SMR.1)	FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FMT_MSA.1/CERT_KEYS, FMT_SMR.1 基本原理：此 SFR 要求上述安全属性的限制性默认值。因此，所有 FMT_MSA.1 迭代都满足依赖性。
FMT_SMF.1	无依赖关系	

要求	CC 依赖关系	满足的依赖关系
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD 理由：此 SFR 与管理功能有关，需要识别它们是由外部参与者还是由 MNO-SD 访问。因此，FIA_UID.1/EXT 和 FIA_UID.1/MNO-SD 都满足依赖性
FCS_COP.1/Mobile_network	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2) 和 (FCS_CKM.4)	FDP_ITC.1/SCP, FCS_CKM.4/Mobile_network 基本原理：此 SFR 使用的密钥在配置期间在 Profile 中分发（FDP_ITC.1/SCP），必须安全删除（FCS_CKM.4/Mobile_network）
FCS_CKM.2/Mobile_network	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2) 和 (FCS_CKM.4)	FDP_ITC.1/SCP, FCS_CKM.4/SCP-MNO 基本原理：此 SFR 中的密钥是资产 D.PROFILE_NAA_PARAMS 中包含的移动网络身份验证密钥。这些密钥在 Profile 下载（FDP_ITC.1/SCP）期间作为 MNO Profile 的一部分分发，必须安全删除（FCS_CKM.4/Mobile_network）
FCS_CKM.4/Mobile_network	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.1/SCP 基本原理：此 SFR 中的密钥是资产 D.PROFILE_NAA_PARAMS 中包含的移动网络身份验证密钥。这些密钥在 Profile 下载期间作为 MNO Profile 的一部分分发（FDP_ITC.1/SCP）

排除依赖关系的基本原理

FCS_CKM.1/SCP-SM 的依赖关系 FCS_CKM.2 或 FCS_COP.1 被丢弃。由于 TOE 使用其底层平台提供的加密库，因此不满足对 FCS_COP.1 的依赖性

8.3.3.2 SAR 依赖关系

表 13 SAR 依赖关系

要求	CC 依赖	满足的依赖
ADV_ARC.1	(ADV_FSP.1) 和 (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) 和 (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	无依赖关系	

要求	CC 依赖	满足的依赖
ALC_CMC.4	(ALC_CMS.1) 和 (ALC_DVS.1) 和 (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	无依赖关系	
ALC_DEL.1	无依赖关系	
ALC_DVS.2	无依赖关系	
ALC_LCD.1	无依赖关系	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) 和 (ASE_INT.1) 和 (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	无依赖关系	
ASE_INT.1	无依赖关系	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) 和 (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	无依赖关系	
ASE_TSS.1	(ADV_FSP.1) 和 (ASE_INT.1) 和 (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) 和 (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) 和 (ADV_TDS.2) 和 (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) 和 (AGD_OPE.1) 和 (AGD_PRE.1) 和 (ATE_COV.1) 和 (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) 和 (ADV_FSP.4) 和 (ADV_IMP.1) 和 (ADV_TDS.3) 和 (AGD_OPE.1) 和 (AGD_PRE.1) 和 (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

8.3.4 安全保证要求的基本原理

这种类型的 TOE 和产品要求 EAL4，因为它旨在抵御复杂的攻击。此评估保障级别允许开发人员根据良好实践从表现良好的安全工程中获得最大的保证。EAL4 代表商业级产品的最高实际保证水平。为了提供有意义的保障，TOE 及其嵌入产品可以提供足够的防御来抵御此类攻击：评估者应该可以访问底层设计和源代码。需要此类访问权限的最低要求是 EAL4。

8.3.4.1 ALC_DVS.2 充分的安全措施

开发安全性涉及可用于开发环境以保护 TOE 和嵌入式产品的物理、程序、人员和其他技术措施。EAL4 规定的标准 ALC_DVS.1 要求是不够的。由于 TOE 和嵌入式产品的性质，有必要证明这些程序的充分性，以保护其机密性和完整性。ALC_DVS.2 没有依赖关系。

8.3.4.2 AVA_VAN.5 高级的系统的脆弱性分析

TOE 预期在恶劣的环境中运行。AVA_VAN.5“高级的系统的脆弱性分析”被认为是拥有敏感应用程序的基于 Java 卡技术的产品的期望级别。AVA_VAN.5 依赖于 ADV_ARC.1，ADV_FSP.1，ADV_TDS.3，ADV_IMP.1，AGD_PRE.1 和 AGD_OPE.1。所有这些 EAL4 都满足。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容

附 录 B
（资料性附录）
安全域的权限分配

eUICC 安全域权限的定义、分配以及管理参见 Global Platform 卡规范的 6.6 章节，如下几个权限在 eUICC 端有特殊处理：

- Card Lock

  Card Lock 不适用于 eUICC，不应该分配给任何安全域与应用，可以通过禁用 Profile 来实现同样的目的。

- Card Terminate

  Card Terminate 不适用于 eUICC，不应该分配给任何安全域与应用，可以通过删除 Profile 来实现同样的目的。

- Card Reset

  Card Reset 只有对于已启用的 Profile 有意义，因此，在一个 eUICC 卡中可以有多个应用同时具备此权限，但在一个 Profile 里，必须是唯一的。

  如果在一个 Profile 中具有 Card Reset 权限的应用被删除，此权限应被自动分配给 MNO-SD。

- CVM Management

  CVM Management 只有对于已启用的 Profile 有意义，因此，在一个 eUICC 卡中可以有多个应用同时具备此权限，但在一个 Profile 里，必须是唯一的。

- Mandated DAP Verification

  Mandated DAP Verification 只有对于已启用的 Profile 有意义，因此，在一个 eUICC 卡中可以有多个应用同时具备此权限，但在一个 Profile 里，必须是唯一的。

  DAP 验证只有在 Profile 内下载应用时是强制的。

- Global Delete

  具备此权限的 MNO-SD 或者应用仅能够删除相对应的 Profile 内应用。

- Global Lock

  具备此权限的 MNO-SD 或者应用仅能够锁定相对应的 Profile 内应用。

- Global Registry

  具备此权限的 ISD-P 或者应用仅允许查找相对应的 Profile 内应用。

- Final Application

  Final Application 不适用于 eUICC，不应该分配给任何安全域与应用。

- Global Service

  具备此权限的 MNO-SD 或者应用只有当其所在的 Profile 是启用状态时才能提供服务。因此，一个 eUICC 内可以有多个应用同时注册相同的服务。

- Contactless Activation

  具有此权限的应用只有在其所在的 Profile 是启用状态才有意义。一个 eUICC 内可能有多个应用同时拥有这个权限，但在一个 Profile 内部必须是唯一的。

- Contactless Self-Activation

  具有此权限的应用只有在其所在的 Profile 是启用状态才有意义。

参 考 文 献