电信终端产业协会标准

TAF-WG4-AS0056-V1.0.0:2020

面向消费电子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) Consumer Devices 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 II
引言 III
面向消费电子设备的嵌入式通用集成电路卡（eUICC）安全能力技术要求 1
1 范围 1
2 规范性引用文件 1
3 术语、定义和缩略语 1
3.1 术语定义 2
3.2 缩略语 2
4 eUICC 架构 3
4.1 eUICC 架构概述 3
5 eUICC 安全问题定义 7
5.1 安全资产 7
5.2 用户/主体 11
5.3 安全威胁 12
5.4 组织安全策略 15
5.5 假设 15
6 安全目标 16
6.1 TOE 的安全目标 16
6.2 运行环境的安全目标 18
6.3 安全目标基本原理 21
7 扩展要求 28
7.1 扩展族 28
8 安全要求 30
8.1 安全功能要求 30
8.2 安全保障要求 51
8.3 安全要求基本原理 58
9 LPAe 66
9.1 LPAe 架构 66
9.2 LPAe 安全问题定义 66
9.3 LPAe 安全目标 69
9.4 LPAe 安全要求 74
附 录 A （规范性附录） 86
附 录 B （资料性附录） 87
参考文献 88

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、王海兰、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，eUICC 技术逐渐从物联网领域扩展到消费电子领域，目前主要应用于手机、智能手表和其他可穿戴设备。相对于物联网领域的 eUICC，从形态上看，消费电子的 eUICC 卡不再局限于嵌入式 SMD 卡；技术上，除了遵循 GSMA 规范的消费类电子 eUICC 技术，各种非标准的、厂家私有的消费电子 eUICC 技术也不断涌现，所以同时伴随而来消费类电子 eUICC 相关的安全问题。

本标准主要参考了 GSMA 的《SGP.25 eUICC for Consumer Device 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。

面向消费电子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

本标准规定了消费电子设备嵌入式通用集成电路卡的安全技术要求、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.25: eUICC for Consumer Device Protection Profile Version 1.0

PP-JCS: Java Card™ System - Open Configuration Protection Profile, version 3.0.5

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

GMSA SGP.02: Remote Provisioning Architecture for Embedded UICC Technical Specification Version 3.2

PP-USIM: (U)SIM Java Card Platform Protection Profile Basic and SCWS Configurations version 2.0.2

GP-SecurityGuidelines-BasicApplications: GlobalPlatform Card Composition Model Security Guidelines for Basic Applications, version 2.0

CC1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model version 3.1, Revision 5

CC2: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, Revision 5

CC3: Common Criteria for Information Technology Security Evaluation, Part 2: Security assurance components, version 3.1, Revision 5

GlobalPlatform_Card_Specification: GlobalPlatform Card Specification v2.3

SCP80: ETSI TS 102 225 - Secured packet structure for UICC based applications, version 9.0.0, release 9 ETSI TS 102 226 - Remote APDU structure for UICC based applications, version 12.0.0, release 9

SCP81: GlobalPlatform Card Specification Amendment B – Remote Application Management over HTTP version 1.1.3

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

GSMA SGP.22: Remote SIM Provisioning (RSP) Technical Specification, version 2.1

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 version 12.1.0 release 12

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

嵌入式 UICC 即嵌入式通用集成电路卡，能够支持安全的远程/本地 Profile 配置管理。

3.1.2 预置签约数据文件 Provisioning Profile

允许连接到商业移动网络的 Profile，仅用于提供系统服务，如 Profile 的配置管理。

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
LPA	Local Profile Assistant	Profile 代理
LPAd	Local Profile Assistant in the device	在终端设备上的 LPA
LPAe	Local Profile Assistant in the eUICC	在 eUICC 上的 LPA
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
SSD	Supplementary Security Domains	补充安全域
TOE	Target of Evaluation	评估对象
TSF	TOE Security Functionality	TOE 安全功能
UICC	Universal Integrated Circuit Card	通用集成电路卡

4 eUICC 架构

4.1 eUICC 架构概述

本节描述消费类电子 eUICC 内部的上层架构，其与物联网 eUICC 的架构非常相似。运营商的 Profile 存储在 eUICC 中的安全域中并且用 GlobalPlatform 标准来实现。这样确保任何 Profile 不能够对卡片内其余 Profile 的应用和数据进行访问.同样的机制已经用在 SIM 卡内以确保支付应用的安全.

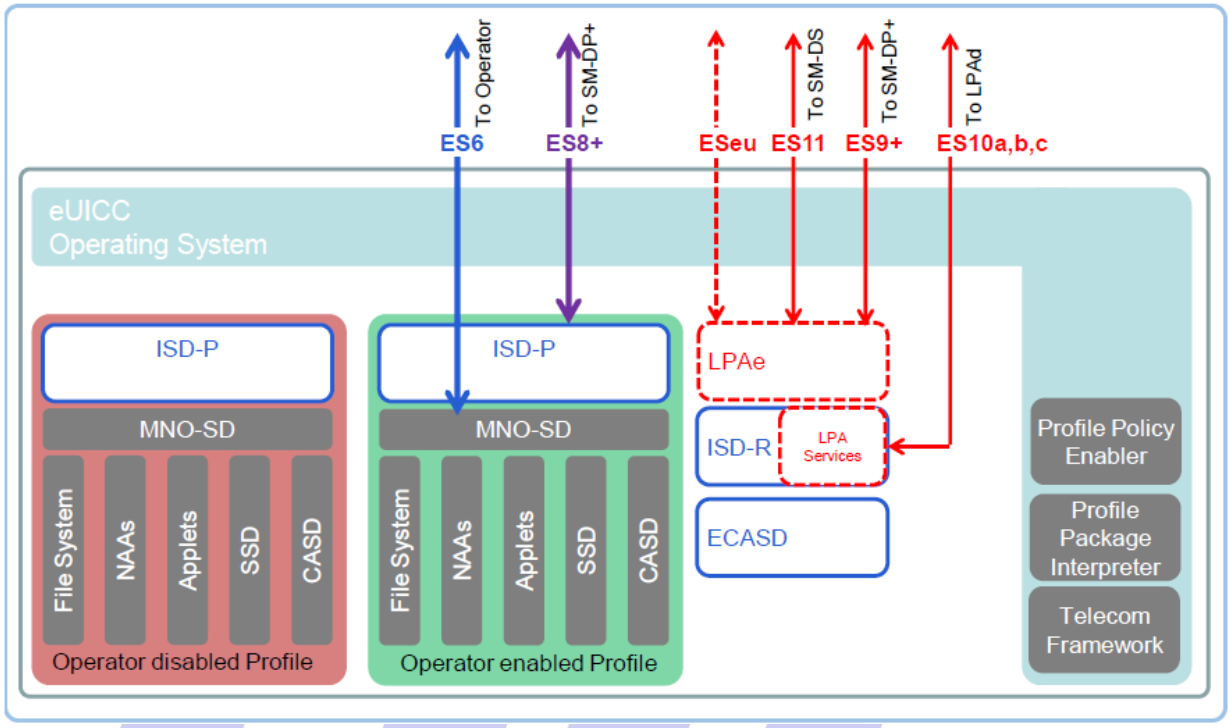

图 1 消费电子设备 eUICC 架构

4.1.1 ECASD

ECASD 负责 eUICC 上支持的所需安全域所需的证书的安全存储。

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。

在 eUICC 制造之后，ECASD 应处于 Global Platform Card Specification 卡规范第 5.3 节中的定义的 PERSONALIZED 状态。

ECASD 的 AID 应遵循 SGP.02 规范.

ECASD 应包含：

- SK.EUICC.ECDSA，eUICC 的私钥，用于生成签名；
- CERT.EUICC.ECDSA(包含 PK.EUICC.ECDSA，即 eUICC 的公钥)，eUICC 证书，用于 eUICC 认证；
- PK.CI.ECDSA，CI 的公钥。ECASD 可以包含属于同一 CI 或不同 CI 的几组公钥。每一个 PK.CI.ECDSA 应该至少与来自于其所属的 CERT.CI.ECDSA 的如下信息一起存储：
  - 证书序列号：用来管理 CRL 对 CI 的回收；
  - 证书发行 ID：CI OID；
  - 使用者密钥标识符：用来验证卡外实体的证书链。

- CERT.EUM.ECDSA，EUM 的证书；
- 更新密钥或者证书的 EUM 密钥对：
  - 更新 eUICC 的私钥和证书
  - 更新 EUM 的证书
  - 更新 CI 的公钥

ECASD 要为 ISD-R 提供以下服务：

- ISD-R 提供数据，ECASD 为 eUICC 生成签名。
- 用 PK.CI.ECDSA 校验 ISD-R 提供的卡外实体证书。

4.1.2 ISD-R

ISD-R 负责新的 ISD-P 的生成和所有 ISD-P 生命周期的管理.

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。ISD-R 应按照附录 B 授予相对应的权限。

ISD-R 不能被删除和禁用。

4.1.3 ISD-P

ISD-P 是 SM-DP+的卡内代表,并且是一个拥有 Profile 的安全容器（安全域）。ISD-P 用于 Profile 的下载和安装,并且通过与 Profile 包解释器的合作对收到的 Profile 包进行解码或者解释。

一个 ISD-P 拥有唯一的 Profile。

除了 ISD-R，ISD-P 外部的组件对任何 Profile 组件不具有可见性或访问权限，ISD-R 具有对 Profile 元数据的访问权限。

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

删除一个 Profile 应当移除包含它的 ISD-P 和所有属于它的 Profile 组件。

4.1.4 Profile

一个 Profile 由以下组件组成：

- 一个 MNO-SD；
- SSD 和一个 CASD；
- 应用；
- 至少一个 NAA；
- 文件系统的其余部分；
- Profile 元数据，包括 PPR。

MNO-SD 是运营商在卡内的代表，它包含了运营商的 OTA 密钥并且提供安全的 OTA 通道。

所有 Profile 内的安全域应当都位于 MNO-SD 的层级之中或者迁移到自身的一个 SD 中。

拥有一个处于激活状态的 Profile 的 eUICC 其行为等同于一个 UICC 卡，这个尤其适用于 Profile 内的 NAA 和应用。

当一个 Profile 被禁用，eUICC 应确保：

- 任何 Profile 组件都不能通过 ES6 接口进行远程管理；
- Profile 内的文件系统不能被设备或者 eUICC 内的任何应用选中。
- Profile 内的应用（包括 NAA 和安全域）不能被选中，触发或者单独的删除。

4.1.4.1 Operational Profile

一个 Operational Profile 要在 Profile 元数据中把 Profile Class 设为“Operational”，指示 LPA 和 eUICC 按照适用于 Operational Profile 的方式处理。

4.1.4.2 Provisioning Profile

一个 Provisioning Profile 要在 Profile 元数据中把 Profile Class 设为“Provisioning”，指示 LPA 和 eUICC 按照适用于 Provisioning Profile 的方式处理。在其他方面，一个 Provisioning Profile 和其他所有 Profile 拥有相同的格式构造。

4.1.4.3 Test Profile

一个 eUICC 可以支持 Test Profile.

一个 Test Profile 要在 Profile 元数据中把 Profile Class 设为“Test”，指示 LPA 和 eUICC 按照适用于 Test Profile 的方式处理。在其他方面，一个 Test Profile 和其他所有 Profile 拥有相同的格式构造。

4.1.5 LPA 服务

LPA 服务对 LPA 功能所需的服务和数据提供必要的访问。这些服务是：

- 将绑定的 Profile 包从 LPAd 传输到 ISD-P；
- 提供已安装的 Profile 列表；
- 获取 EID；
- 提供本地 Profile 管理操作。

即使 eUICC 提供了 LPAe，LPA 服务也是必不可少的。

符合此规范的设备应至少实现以下一项：

- LPAd，或
- 一个可选的 LPAe。

支持不带 LPAe 的嵌入式 eUICC 的设备应提供 LPAd。

符合此规范的 eUICC 应实现 LPA 服务，LPAe 作为可选项。支持 LPAd 和 LPAe 两种方式的设备应实现适当的机制，使 LPA 能够使用。

4.1.6 LPAd(LPA in Device)

在设备端实现的 LPA 服务。

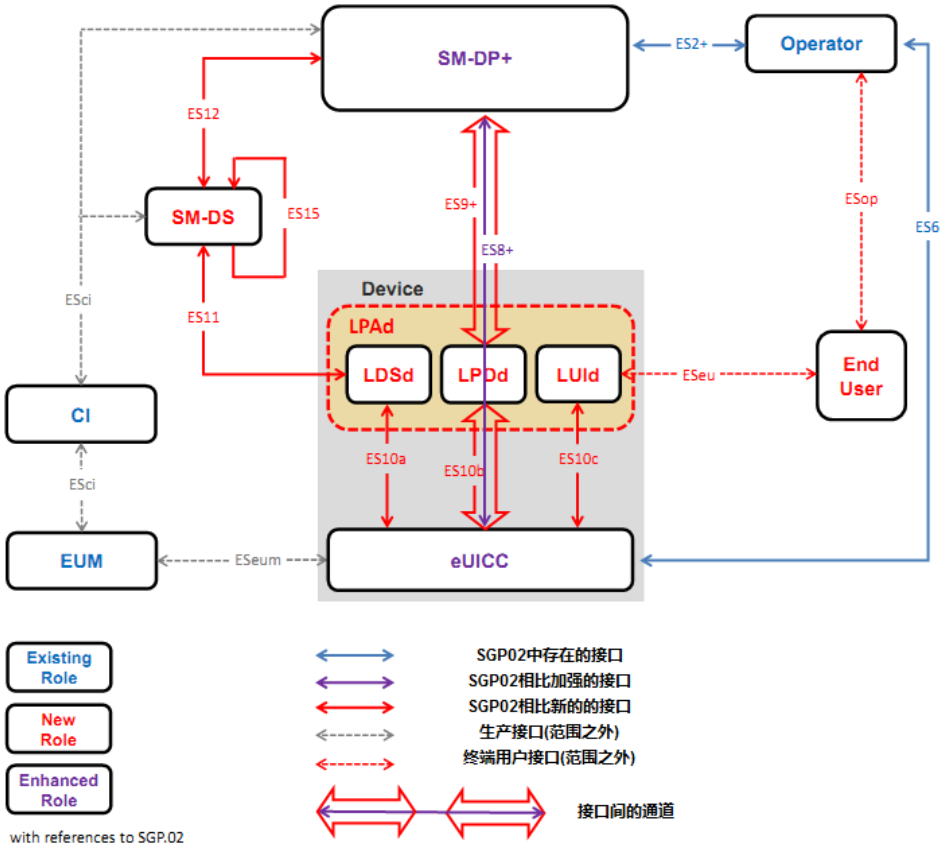

图 2 RSP 系统中 LPAd 结构图

上图提供了 LPA 在设备（LPAd）中时消费类远程 SIM 配置和管理系统的完整描述。

4.1.7 LPAe (LPA in eUICC)

在 eUICC 端实现的 LPA 服务。
该架构如下图所示。

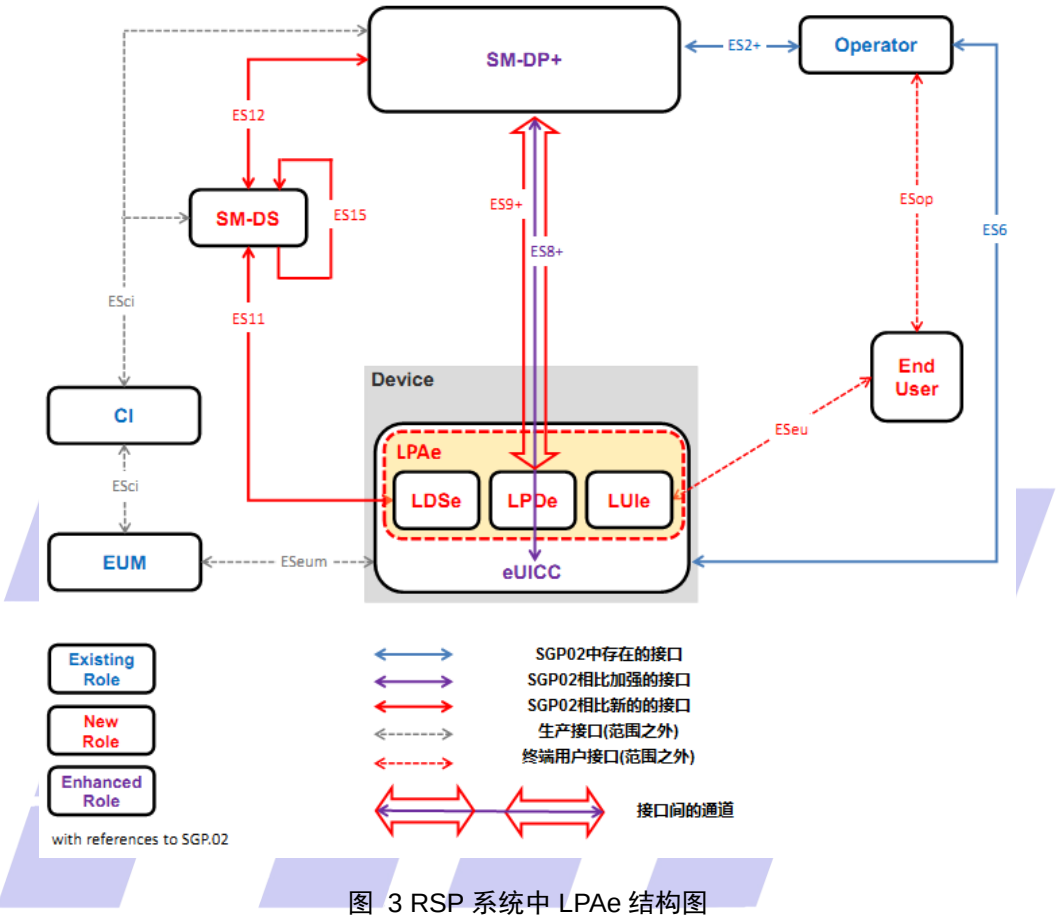

图 3 RSP 系统中 LPAe 结构图

- LPAe 是一个提供 LPDe，LDSe 和 LUIe 特性的功能单元。这些功能类似于 LPAd 的功能。
- LPAe 是可选的。
- LPAe 的技术实现取决于 EUM。例如，LPAe 可以是 ISD-R 的一个功能。

5 eUICC 安全问题定义

5.1 安全资产

安全资产是由安全目标直接保护的安全相关要素。他们被分成两组。第一组包含由用户创建和用于用户的数据（用户数据），第二组包含由 TOE（TSF 数据）创建或使用的数据。对于每个资产，需要指定它们运行的风险种类。

5.1.1 用户数据

用户数据包括：

- ISD-P 控制的用户数据：

- 至少一个网络认证程序（D.PROFILE_CODE 的一部分）及其相关参数（D.Profile_NAA_Params）；
- PPR 策略文件（D.Profile_Policy_Rules）；
- 文件系统（包括在 D.Profile_Code 中）；
- MNO-SD，它可以包括其他应用程序，例如：
  - 与 Profile 相关的身份（D.Profile_Identity），
  - MNO-SD 密钥集（D.MNO_Keys）；
- 与 Profile 下载相关的用户代码（D.Profile_User_Codes）。

此标准旨在保护 Profile 的数据和应用程序，而不考虑格式。因此，在资产描述中，格式将不详细说明。

5.1.1.1 密钥

安全域拥有的密钥。所有密钥都需要被保护，防止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。

5.1.1.2 Profile 数据

应用程序的数据，比如对象中包含的数据、包的静态字段、当前执行的方法的本地变量、或操作数堆栈的位置，包括机密敏感数据。

D.PROFILE_NAA_PARAMS

用于网络身份验证的参数，包括密钥。这些参数可以包括例如椭圆曲线参数。参数在配置期间加载并在 ISD-P 的控制下存储。它们可能被传输到包含身份验证算法的电信框架中。

需要被保护，防止未经授权的泄露和修改。

D.PROFILE_IDENTITY

国际移动用户标识（IMSI）是通过身份验证算法在 MNO 网络上进行身份验证时的用户凭证。IMSI 是用户身份的表示，并且将由 MNO 用作其 HLR 中的用户的索引。在配置期间，每个 IMSI 都在 ISD-P 的控制下存储。

应保护 IMSI 免受未经授权的修改。

D.PROFILE_POLICY_RULES

描述 Profile 的 Profile 策略规则（PPR）的数据。

这些规则在配置期间加载并在 ISD-P 的控制之下存储。它们由 MNO OTA 平台管理。

应保护 PPR，防止未经授权的修改。

D.PROFILE_USER_CODES

该资产包括：

- 最终用户通过本地用户界面（LUId）启动 Profile 下载和安装的可选激活码；
- 最终用户通过本地用户界面（LUId）确认 Profile 下载和安装的可选确认码的散列值（散列确认码）。

请注意，虽然这些代码是由最终用户在 TOE 之外的 LUId 输入的，但是代码被发送到 TOE 以进行签名（例如 euiccSigned2 数据结构）。

需要防止未经授权的修改。

5.1.1.3 Profile 代码

D.PROFILE_CODE

Profile 应用程序包括第一级和第二级应用程序，特别是：

- MNO-SD 以及 MNO-SD 控制下的安全域（CASD，SSD）；
- 可以在 MNO-SD 中配置的其他应用程序（网络访问应用程序等）。

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 的控制之下。

需要保护这些资产免受未经授权的修改。

5.1.2 TSF 数据

TSF 数据包括三类数据：

- TSF 代码，确保对 Profile 数据的保护；
- 管理数据，确保应用程序的管理将执行一组规则（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 代码

D.TSF_CODE

TSF 代码分为：

- ISD-R、多个 ISD-P 和 ECASD；
- 平台代码。

所有这些资产都必须保护免受未经授权的披露和修改。对于该 TSF 代码的熟悉可以使攻击者尝试绕过 TSF。这涉及运行时的逻辑攻击，以便获得对可执行代码的读取访问，通常通过执行试图读取存储一段代码的存储器区域的应用程序来实现。

应用说明：

- 这不包括 MNO-SD 中的应用程序，它们是用户数据的一部分（Profile 中的应用程序）；
- 未经授权的披露和修改的概念与（本文其他定义）相同 。

5.1.2.2 管理数据

D.PLATFORM_DATA

平台环境的数据，例如，

- 包括 SM-DS OID、MNO OID 和 SM-DP+OID 的标识符和权限；
- ISD-P 安全域的 eUICC 生命周期状态。

这些数据可以部分地在 ISD-R 和平台代码的逻辑中实现，而不是“数据”。因此，这一资产与 D.TSF_CODE 紧密相连。

需要保护免受未经授权的修改。

D.DEVICE_INFO

该资产包括设备信息数据的安全敏感元素，例如 LPAd 提供给 eUICC 的设备类型分配代码（TAC）或设备能力（例如，支持更新证书撤销列表（CRL））。

需要保护免受未经授权的修改。

D.PLATFORM_RAT

描述 eUICC 规则授权表（RAT）的数据。

这些规则在 eUICC 制造时或在初始设备设置期间初始化，是在没有安装可操作的 Profile 之前进行的。OEM 或 EUM 负责设置 RAT 的内容。规则授权表储存在 eUICC 中。

必须保护免受未经授权的修改。

5.1.2.3 身份管理数据

身份管理数据被用来保证参与者身份的真实性。它包括：

- EID、eUICC 证书和相关的私钥，用于保证 eUICC 的身份；
- CI 根证书（自签名），用于验证所有参与者的证书；
- EUM 证书；
- 用于生成凭证的共享秘密。

D.SK.EUICC.ECDSA

eUICC 私钥，存储在 ECASD 中，由 eUICC 使用以证明其身份并与远程参与者生成共享密文。

必须保护其免受未经授权的泄露和修改。

D.CERT.EUICC.ECDSA

EUM 为特定的、独立的 eUICC 颁发的证书。证书包含公共密钥 PK.EUICC.ECDSA，并存储在 ECASD 中。可以使用 EUM 证书验证该证书。

eUICC 证书必须被保护以避免未经授权的修改。

D.PK.CI.ECDSA

CI 的公钥（PK.CI.ECDSA）用于验证 eUICC 和远程参与者的认证链。它存储在 ECASD 中。

必须保护免受未经授权的修改。

ECASD 可包含属于同一 CI 或不同 CI 的多个公钥。

每个 PK.CI.ECDSA 应与来自其所属 CERT.CI.ECDSA 的信息一起存储，至少包括：

- 证书序列号：需要通过 CRL 管理 CI 撤销；
- 证书颁发者标识符：CI OID；
- 使用者密钥标识符：验证卡外实体的证书链所需的

D.EID

EID（EUICC ID）唯一标识 eUICC 的标识符。该标识符由 eUICC 制造商设置，并且在 eUICC 的运行期间不改变。它存储在 ECASD 中。EID 被用作 SM-DP+和 SM-DS 的关键字，以识别其数据库中的 eUICCs。

EID 应被保护免受未经授权的修改。

D.SECRETS

此资产包括：

- eUICC 和 SM-DP+的一次性密钥：otSK.EUICC.ECKA，otPK.EUICC.ECKA 和 otPK.DP.ECKA；
- 用于保护 Profile 下载的共享秘密（ShS）；
- 会话密钥（S-ENC 和 S-MAC）和初始 MAC 链值。

应保护这些资产免受未经授权的泄露和修改。

D.CERT.EUM.ECDSA

EUM 证书（CERT.EUM.ECDSA）。

应保护免受未经授权的修改。

D.CRLs

eUICC 中存储的可选证书撤销列表。

需要被保护以防止未经授权的修改。

5.2 用户/主体

本节包含两个部分：

- 用户，TOE 外的实体，可能访问 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-DPplus

准备 Profile 并管理 Profile 的安全下载和安装到 eUICC 上的角色。

U.MNO-OTA

一个远程管理 UICC 和 eUICC 上启用的 MNO Profile 内容的平台。

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 启用后 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 负责创建新的 ISD-P，以及所有 ISD-P 的生命周期管理。

ISD-R 包含 LPA 服务，提供对 LPA 功能所需的服务和数据的必要访问，

S.ISD-P

ISD-P 是 SM-DP+的卡上代表，是拥有一个 Profile 的安全容器（安全域）。

S.ECASD

嵌入式 UICC 授权控制安全域（ECASD）。

S.PPI

Profile 包解释器，一个 eUICC 操作系统服务，使用目标 eUICC 的特定内部格式将 Profile 包数据转换为已安装的 Profile.

S.PPE

Profile 策略激活，包含两个功能：

- 验证一个包含 PPR 的 Profile 是否由 RAT 授权；
- 实施 Profile 中的 PPR

S.TELECOM

电信框架是一种操作系统服务，为 ISD-Ps 中托管的 NAA 提供标准化的网络认证算法。

5.3 安全威胁

5.3.1 未经授权的 Profile 和平台管理

一个卡外参与者或卡内应用可能试图通过以下尝试来破坏 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 中的网络认证参数）；
- 或未经授权的平台管理（通常试图禁用启用的 Profile）。

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 内的应用试图破坏其自身的 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 的 Profile 产生影响。最后一种情况包括修改 ISD-P 的回退属性，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：

- 修改或泄露 ISD-R 或 PPE 的数据;
- 执行或修改 ISD-R 或 PPE 的操作;
- 修改存储在 PPE 中的规则授权表（RAT）。

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

直接受威胁的资产是 D.TSF_CODE，D.PLATFORM_DATA 和 D.PLATFORM_RAT。

通过改变 ISD-R 或 PPE 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+（ES8+）或 eUICC 和 MNO OTA 平台（ES6）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；
- 替换或修改来自 SM-DP+或 MNO OTA 平台的命令内容；
- 在 MNO OTA 平台更新 Profile 元数据时，替换或修改 Profile 元数据（例如 Profile 策略规则（PPR））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.MNO_KEYS，D.TSF_CODE（ISD-P），D.PROFILE_*。

T.PROFILE-MNG-ELIGIBILITY

攻击者改变或窃听 eUICC 和 SM-DP+（ES8+）之间的传输，或者改变 LPAd 提供给 eUICC 的设备信息，以便损害 eUICC 的资格，例如：

- 通过声明符合旧版本规范或缺少加密支持来降低发送给 eUICC 的 Profile 的安全性;
- 通过修改设备信息或 eUICC 标识符来获取未经授权的 Profile。

注意：攻击者可能是卡上的应用程序拦截到安全域的传输，或者是卡外的参与者拦截 OTA 传输或者 eUICC 和设备之间的接口。

直接威胁资产：D.TSF_CODE，D.DEVICE_INFO，D.EID。

5.3.2 身份篡改

T.UNAUTHORIZED-IDENTITY-MNG

恶意卡上应用程序：

- 泄露或修改属于“身份管理数据”或“TSF 代码”资产类别的数据：
  - 泄露或修改 D.SK.EUICC.ECDSA, D.SECRETS，
  - 修改 D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs，
  - 修改用于共享秘密、一次性密钥或会话密钥的生成方法（D.TSF_CODE 的一部分）（即用于生成 D.SECRETS 的方法）；
- 泄露或修改 ECASD 的功能（D.TSF_CODE 的一部分）。

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, D.SK.EUICC.ECDSA, D.SECRETS, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.CERT.EUM.ECDSA, D.CRLs。

T.IDENTITY-INTERCEPTION

攻击者可能试图拦截凭据，无论是在卡外还是在卡上，以便

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

这包括卡上拦截以下信息：

- 在 Profile 下载中使用的共享秘密（D.SECRETS）
- eUICC ID（D.EID）

这不包括：

- 在 Profile 下载期间 SM-DP+凭据的卡外或卡上拦截（由 T.PROFILE-MNG-INTERCEPTION 考虑）

直接威胁资产：D.SECRETS, D.EID。

5.3.3 eUICC 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.SK.EUICC.ECDSA, D.EID, D.SECRETS。

5.3.4 LPAd 模拟

T.LPAd-INTERFACE-EXPLOIT

攻击者利用 LPAd 的接口（接口 ES10a、ES10b 和 ES10c）来：

- 模拟 LPAd（中间人、伪装），或
- 利用接口中的缺陷来修改或泄露敏感资产，或执行代码（特别针对 LPAd 接口的 T.LOGICAL-ATTACK 和 T.PHYSICAL-ATTACK 的扩展）。

因此，攻击者可以执行未经授权的 Profile 和平台管理，例如绕过此类操作所需的最终用户确认。

攻击者还可以通过在下载和安装 Profile 之前破坏通常从 LPA 传递到 eUICC 的设备信息，从而破坏资格检查过程。

与威胁 T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, 和 T.PROFILE-MNG-ELIGIBILITY 的不同之处在于本威胁利用的接口(ES10a，b，c)。

直接威胁资产：D.DEVICE_INFO, D.PLATFORM_DATA.。

5.3.5 未经授权的手机网络访问

T.UNAUTHORIZED-MOBILE-ACCESS

一个卡上或卡外的参与者试图代替合法的 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

5.3.6 其他

T.LOGICAL-ATTACK

卡上恶意应用程序通过逻辑手段绕过平台安全措施，以便在平台处理敏感数据时泄露或修改敏感数据：

- 集成电路和操作系统软件
- 运行环境（例如 JCS 提供的环境）
- Profile 策略使能器
- Profile 包解释程序
- 电信框架（访问网络认证参数）。

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

直接威胁资产：D.TSF_CODE, D.PROFILE_NAA_PARAMS, D.PROFILE_POLICY_RULES, D.PLATFORM_DATA, D.PLATFORM_RAT。

T.PHYSICAL-ATTACK

攻击者通过物理(与逻辑相反)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.LIFE-CYCLE

这个安全目标必须强制执行所定义的 eUICC 生命周期。特别地：

- 一次只能有一个 ISD-P 启用；
- eUICC 必须强制执行 Profile 策略规则（PPR），以防篡改 Profile 的状态改变（安装、禁用或删除 Profile），在存储器复位或测试存储器复位功能期间除外：在这种情况下，eUICC 可以禁用和删除当前启用的 Profile，即使 PPR 声明该 Profile 不能被禁用或删除；
- eUICC 必须在包含 PPR 的 Profile 被授权安装在 eUICC 上之前强制执行规则授权表(RAT)。

5.5 假设

5.5.1 设备假设

A.TRUSTED-PATHS-LPAd

当 LPAd 存在和启用时，假设接口 ES10a、ES10b 和 ES10c 是 eUICC 和 LPAd 之间的可信途径。

5.5.2 其他

A.ACTORS

基础设施的参与者（CI、EUM、SM-DP+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（操作系统）的安全准则文档。这些准则必须对应用程序的编写风格和平台安全机制（如安全域、应用程序防火墙）进行充分描述，以确保应用程序不会损害 TOE。

6 安全目标

6.1 TOE 的安全目标

6.1.1 平台支持功能

O.PPE-PPI

TOE 应提供负责整个 eUICC 和已安装应用程序的生命周期的平台管理功能（加载，安装，启用，禁用和删除应用程序），以及由 Profile 策略使能器（PPE）和 Profile 包解释器（PPI）提供的相应授权控制。

特别是，PPE 确保：

- 一次只启用一个 ISD-P；
- 验证包含 PPR 的 Profile 是否由 RAT 授权；
- 执行 Profile 中的 PPR。

PPI 使用目标 eUICC 的特定内部格式将 Profile 包数据按照 SIMalliance eUICC Profile 包规范中的定义转换为已安装的 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：

实际上，PPE 和 PPI 将与 TOE 的其余部分紧密相关，而 TOE 的其余部分很可能依靠 PPE 和 PPI 来有效执行其某些安全功能。平台确保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 PPR 和 RAT 来完成的。执行操作的参与者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 MNO-SD 密钥。此安全域密钥集的修改仅限于其相应的所有者（MNO OTA 平台）。

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，例如身份管理数据（针对 ECASD）或 D.PROFILE_NAA_PARAMS（针对 ISD-P）。

域分离功能依赖于应用程序的运行环境保护。

O.SECURE-CHANNELS

eUICC 应保持以下两者之间的安全通道

- ISD-R 和 SM-DP+；
- MNO-SD 和 MNO OTA 平台。

TOE 应在任何时候都确保：

- 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泄露、修改和重放。

该保护机制应依赖于运行环境和 PPE/PPI（参见 O.PPE-PPI）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，以防止未经授权的泄露或修改。

该保护机制应依赖于运行环境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 标识，基于 eUICC 的硬件标识。

eUICC 必须提供密码学手段，基于此 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 PPE、PPI 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。为了遵守其他认证计划，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

TOE 在对数据进行存储和操作时，应避免未经授权泄露以下数据：

- D.SK.EUICC.ECDSA；
- D.SECRETS；
- 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：

在 TOE 的组件中，

- PPE、PPI 和电信框架必须保护它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。

该目标包括抵抗侧信道攻击。

O.DATA-INTEGRITY

TOE 对数据进行管理或操作时，应避免未经授权修改以下数据：

- 以下密钥集：
  - D.MNO_KEYS；
- Profile 数据：
  - D.PROFILE_NAA_PARAMS，
  - D.PROFILE_IDENTITY，
  - D.PROFILE_POLICY_RULES，

- D.PROFILE_USER_CODES；
- 管理数据：
  - D.PLATFORM_DATA，
  - D.DEVICE_INFO，
  - D.PLATFORM_RAT；
- 身份管理数据：
  - D.SK.EUICC.ECDSA，
  - D.CERT.EUICC.ECDSA，
  - D.PK.CI.ECDSA，
  - D.EID，
  - D.CERT.EUM.ECDSA，
  - D.CRLs，
  - D.SECRETS。

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 应提供向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-DS 和 SM-DP+提供证书。CI 必须确保自己的私钥的安全性。

OE.SM-DPplus

SM-DP+应是负责数据准备和相关 OTA 服务器的可信赖的参与者。SM-DP+站点必须遵循相关认证规范。

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

- MNO 密钥包括 OTA 密钥（由 SM-DP +或 MNO 生成的电信密钥），
- 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 之前不会受到损害。

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+与个人化设备合作实施。

应用说明：

SM-DP+取代 PP-USIM 规范中定义的 OE.PERSONALIZER。

OE.MNO

MNOs 必须确保在 Profile（ISD-P，MNO SD 和任何其他 SSD）中使用的任何密钥在通过 MNO OTA 平台传输到 eUICC 之前是安全生成的。MNO 必须确保在 Profile（ISD-P，MNO SD 和任何其他 SSD）中使用的任何密钥在通过 MNO OTA 平台传输到 eUICC 上之前不会受到损害。

移动运营商 OTA 服务器的管理员应该是值得信赖的人。他们应接受培训，以使用和管理这些服务器。他们拥有执行任务的方法和设备。他们必须意识到他们管理的资产的敏感性以及与 OTA 服务器管理相关的责任。ES6 上的 OTA 平台通信至少使用了 GSMA SGP.02 第 2.4 节中为 ES5 定义的最低安全设置。

应用说明：

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

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

（2）它为 Profile 策略使能器（PPE）、Profile 包解释器（PPI）和电信框架（S.PPE，S.PPI 和 S.TELECOM）提供安全的底层加密处理。

（3）它允许 S.PPE、S.PPI 和 S.TELECOM 根据需要将数据存储在“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的存储器中）。存储器模型是结构化的，允许底层控制访问（分段故障检测）。

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

应用说明：

注：相当于 PP-JCS 规范的 OE.SCP-SUPPORT。

OE.IC.RECOVERY

如果在操作正在进行时断电，则底层 IC 必须允许 TOE 最终成功完成中断操作，或者恢复到一致且安全的状态。

OE.RE.PPE-PPI

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，
- 应用程序或安全域的权限更新，
- 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 规范的安全目标来转换这一目标：T.DELETION，T.INSTALL。

OE.RE.SECURE-COMM

运行环境应提供方法保护应用程序通信的机密性和完整性。

应用说明：

该目标特别需要运行环境提供：

- 应用程序防火墙；
- 应用程序可用于实际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 规范认证的 Java 卡系统完全符合此目标。ST 作者可以通过重用与以下威胁相关的 PP-JCS 规范的安全目标来转换此目标：T.CONFID-APPLI-DATA 和 T.INTEG-APPLI-DATA。

OE.RE.API

运行环境应确保只能通过 API 调用本地代码。

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.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方法始终保护其处理的 TOE 敏感数据机密性。

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 卡系统完全符合此目标。 ST 作者可以通过以下操作转换这个目标：

- 重用与以下威胁相关的 PP-JCS 规范安全目标：T.CONFID-APPLI-DATA；
- 改进 ADV_ARC“非绕过性”要求，以明确 ST TOE 安全架构对侧信道攻击的覆盖。

OE.RE.DATA-INTEGRITY

运行环境应提供方法始终保护其处理的 TOE 敏感数据的完整性。

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.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执行的应用程序。

OE.RE.CODE-EXE

运行环境应防止应用程序执行未授权的代码。

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。

OE.TRUSTED-PATHS-LPAd

当 LPAd 存在且运行时，接口 ES10a，ES10b 和 ES10c 是 eUICC 和 LPAd 之间的可信路径。

6.2.3 Profile

OE.APPLICATIONS

应用程序应符合所用平台（操作系统）的安全准则文档。这些准则必须充分描述应用程序编写风格和平台安全机制（例如安全域，应用程序防火墙），这些机制将用于确保应用程序不会损害 TOE。

应用说明：

使用这些指南旨在提供合理的保证，即即使在考虑平台提供的安全功能之前，应用程序也不会对本产品上加载的其他应用程序构成安全风险。

该目标意指来自 JCS 保护配置文件（PP-JCS 规范）的目标 OE.VERIFICATION。

在 GlobalPlatform 是使用平台的情况下，应采用 GP-SecurityGuidelines-BasicApplications 规范的准则。

OE.MNO-SD

根据 GSMA SGP.02，安全域 U.MNO-SD 必须使用 TOE 提供的安全通道 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：

- O.PPE-PPI 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）才能访问安全域功能和内容；
- OE.SM-DPplus 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将安全地使用 TOE 提供的 SCP80/81 安全通道（OE.MNO-SD）。

为了确保应用程序防火墙的安全运行，操作环境的以下目标也应满足：

- 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：

- O.PPE-PPI 和 O.eUICC-DOMAIN-RIGHTS 确保只有经过授权和认证的参与者才能访问安全域功能和内容。

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）。

为了确保应用程序防火墙的安全运行，操作环境的以下目标也应满足：

- 遵守应用程序的安全准则（OE.APPLICATIONS）。

T.PROFILE-MNG-INTERCEPTION 命令和 Profile 由 SM-DP+传输到其卡上代表（ISD-P），而 Profile 数据（包括元数据，如 PPR）也由 MNO OTA 平台传输到其卡上代表（MNO-SD）。

因此，TSF 确保：

- 通过要求 SM-DP+和 MNO OTA 平台的认证，以及保护传输免受未经授权的泄露、修改和重放，确保传输到安全域的安全性（O.SECURE-CHANNELS 和 O.INTERNAL-SECURE-CHANNELS）。这些安全通道依赖于底层运行环境，它可以保护应用程序通信（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将安全地使用 TOE 提供的 SCP80/81 安全通道（OE.MNO-SD）。

OE.SM-DPplus 和 OE.MNO 确保在由卡外参与者使用时不会泄露与安全通道相关的凭证。

T.PROFILE-MNG-ELIGIBILITY SM-DP+在允许 Profile 下载到 eUICC 前，使用由 eUICC 发送到 SM-DP+的设备信息和 eUICCInfo2 进行资格审查。

因此，TSF 确保：

- 通过要求 SM-DP+进行身份验证，以及保护传输免受未经授权的泄露、修改和重放，确保传输到安全域的安全性（O.SECURE-CHANNELS 和 O.INTERNAL-SECURE-CHANNELS）。这些安全通道依赖于底层运行环境，它可以保护应用程序通信（OE.RE.SECURE-COMM）。

OE.SM-DPplus 确保在由卡外参与者使用时不会泄露与安全通道相关的凭证。

O.DATA-INTEGRITY 和 OE.RE.DATA-INTEGRITY 确保设备信息和 eUICCInfo2 的完整性在 eUICC 级别受到保护。

6.3.1.2 身份篡改

T.UNAUTHORIZED-IDENTITY-MNG O.PPE-PPI 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这种威胁。卡上访问控制策略依赖于底层的运行环境，它可以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。

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通信（OE.RE.SECURE-COMM）。

OE.CI 确保 CI 根安全地管理其卡外的凭证。

6.3.1.3 eUICC 克隆

T.UNAUTHORIZED-eUICC O.PROOF_OF_IDENTITY 保证可以基于 EID 向卡外参与者提供身份加密证明。

O.PROOF_OF_IDENTITY 基于 eUICC 硬件标识（由于 OE.IC.PROOF_OF_IDENTITY 而唯一）来保证此 EID 唯一性。

6.3.1.4 LPAd 模拟

T.LPAd-INTERFACE-EXPLOIT OE.TRUSTED-PATHS-LPAd 确保接口 ES10a，ES10b 和 ES10c 是 LPAd 的可信路径。

6.3.1.5 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，防止攻击者冒充。

6.3.1.6 其他

T.LOGICAL-ATTACK 此威胁通过控制安全域与 PPE、PPI、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。因此它涵盖：

- 由运行环境提供的 API（OE.RE.API）；
- TSF 的 API（O.API）；电信框架、PPE 和 PPI 的 API 应确保原子事务（OE.IC.SUPPORT）。

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数据的机密性和完整性（OE.RE.DATA-CONFIDENTIALITY，OE.RE.DATA-INTEGRITY）。然而，这些敏感数据也由 PPE、PPI 和电信框架处理，不受这些机制的保护。所以，

- TOE 本身必须确保 PPE、PPI 和电信框架的正确运行（O.OPERATE），
- PPE、PPI 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）。

操作环境的以下目标也应满足：

- 防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）。

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 保护平台的敏感资产免受完整性和机密性的损害，特别是确保 TSF 不被绕过或更改。

特别是，安全目标 OE.IC.SUPPORT 提供功能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。特别是，它明确确保平台数据完整性的独立保护。

由于 TOE 不能仅依赖 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，Java 卡平台安全体系结构必须可以应对侧信道（OE.RE.DATA-CONFIDENTIALITY）。

6.3.2 组织安全策略

6.3.2.1 生命周期

OSP.LIFE-CYCLE O.PPE-PPI 确保一次仅有一个 ISD-P 启用。

Profile 删除功能依赖于 OE.RE.PPE-PPI 提供的安全应用程序删除机制。

O.OPERATE 通过确保始终强制执行平台安全功能来支持此 OSP。

6.3.3 假设

6.3.3.1 设备假设

A.TRUSTED-PATHS-LPAd 这一假设通过 OE.TRUSTED-PATHS-LPAd 支持。

6.3.3.2 其他

A.ACTORS 这一假设通过目标 OE.CI，OE.SM-DPplus 和 OE.MNO 支持，它确保基础设施的每个参与者正确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 1 威胁和安全目标——覆盖范围

威胁	安全目标	基本原理
T.UNAUTHORIZED-PROFILE-MNG	O.eUICC-DOMAIN-RIGHTS, OE.SM-DPplus, OE.MNO, O.PPE-PPI, O.SECURE-CHANNELS, OE.APPLICATIONS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.MNO-SD	6.3.1 小节
T.UNAUTHORIZED-PLATFORM-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.APPLICATIONS, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	6.3.1 小节
T.PROFILE-MNG-INTERCEPTION	OE.SM-DPplus, OE.MNO, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM, OE.MNO-SD	6.3.1 小节
T.PROFILE-MNG-ELIGIBILITY	OE.SM-DPplus, OE.RE.SECURE-COMM, O.SECURE-CHANNELS, O.INTERNAL-SECURE-CHANNELS, OE.RE.DATA-INTEGRITY, O.DATA-INTEGRITY	6.3.1 小节
T.UNAUTHORIZED-IDENTITY-MNG	O.eUICC-DOMAIN-RIGHTS, O.PPE-PPI, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY, OE.RE.IDENTITY	6.3.1 小节
T.IDENTITY-INTERCEPTION	OE.CI, O.INTERNAL-SECURE-CHANNELS, OE.RE.SECURE-COMM	6.3.1 小节
T.UNAUTHORIZED-eUICC	O.PROOF_OF_IDENTITY, OE.IC.PROOF_OF_IDENTITY	6.3.1 小节
T.LPAd-INTERFACE-EXPLOIT	OE.TRUSTED-PATHS-LPAd	6.3.1 小节
T.UNAUTHORIZED-MOBILE-ACCESS	O.ALGORITHMS	6.3.1 小节

威胁	安全目标	基本原理
T.LOGICAL-ATTACK	O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY, O.API, OE.APPLICATIONS, O.OPERATE, OE.RE.API, OE.RE.CODE-EXE, OE.IC.SUPPORT, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	6.3.1 小节
T.PHYSICAL-ATTACK	OE.IC.SUPPORT, OE.IC.RECOVERY, O.DATA-CONFIDENTIALITY, OE.RE.DATA-CONFIDENTIALITY	6.3.1 小节

表 2 安全目标和威胁——覆盖范围

安全目标	威胁
O.PPE-PPI	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.eUICC-DOMAIN-RIGHTS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG
O.SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
O.INTERNAL-SECURE-CHANNELS	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
O.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
O.OPERATE	T.LOGICAL-ATTACK
O.API	T.LOGICAL-ATTACK
O.DATA-CONFIDENTIALITY	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
O.DATA-INTEGRITY	T.PROFILE-MNG-ELIGIBILITY, T.LOGICAL-ATTACK
O.ALGORITHMS	T.UNAUTHORIZED-MOBILE-ACCESS
OE.CI	T.IDENTITY-INTERCEPTION
OE.SM-DPplus	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY
OE.MNO	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION
OE.IC.PROOF_OF_IDENTITY	T.UNAUTHORIZED-eUICC
OE.IC.SUPPORT	T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
OE.IC.RECOVERY	T.PHYSICAL-ATTACK

安全目标	威胁
OE.RE.PPE-PPI	
OE.RE.SECURE-COMM	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION, T.PROFILE-MNG-ELIGIBILITY, T.IDENTITY-INTERCEPTION
OE.RE.API	T.LOGICAL-ATTACK
OE.RE.DATA-CONFIDENTIALITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK, T.PHYSICAL-ATTACK
OE.RE.DATA-INTEGRITY	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.PROFILE-MNG-ELIGIBILITY, T.UNAUTHORIZED-IDENTITY-MNG, T.LOGICAL-ATTACK
OE.RE.IDENTITY	T.UNAUTHORIZED-IDENTITY-MNG
OE.RE.CODE-EXE	T.LOGICAL-ATTACK
OE.TRUSTED-PATHS-LPAd	T.LPAd-INTERFACE-EXPLOIT
OE.APPLICATIONS	T.UNAUTHORIZED-PROFILE-MNG, T.UNAUTHORIZED-PLATFORM-MNG, T.LOGICAL-ATTACK
OE.MNO-SD	T.UNAUTHORIZED-PROFILE-MNG, T.PROFILE-MNG-INTERCEPTION

表 3 OSP 和安全目标——覆盖范围

组织安全策略	安全目标	基本原理
OSP.LIFE-CYCLE	O.PPE-PPI, OE.RE.PPE-PPI, O.OPERATE	6.3.2 小节

表 4 安全目标和 OSP——覆盖范围

安全目标	组织安全策略
O.PPE-PPI	OSP.LIFE-CYCLE
O.eUICC-DOMAIN-RIGHTS	
O.SECURE-CHANNELS	
O.INTERNAL-SECURE-CHANNELS	
O.PROOF_OF_IDENTITY	
O.OPERATE	OSP.LIFE-CYCLE
O.API	
O.DATA-CONFIDENTIALITY	
O.DATA-INTEGRITY	
O.ALGORITHMS	
OE.CI	

安全目标	组织安全策略
OE.SM-DPplus	
OE.MNO	
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PPE-PPI	OSP.LIFE-CYCLE
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd	
OE.APPLICATIONS	
OE.MNO-SD	
OE.SM-DS	

表 5 假设和操作环境安全目标——覆盖范围

假设	操作环境安全目标	基本原理
A.TRUSTED-PATHS-LPAd	OE.TRUSTED-PATHS-LPAd	6.3.3 小节
A.ACTORS	OE.CI, OE.SM-DPplus, OE.MNO	6.3.3 小节
A.APPLICATIONS	OE.APPLICATIONS	6.3.3 小节

表 6 操作环境安全目标和假设——覆盖

操作环境安全目标	假设
OE.CI	A.ACTORS
OE.SM-DPplus	A.ACTORS
OE.MNO	A.ACTORS
OE.IC.PROOF_OF_IDENTITY	
OE.IC.SUPPORT	
OE.IC.RECOVERY	
OE.RE.PPE-PPI	
OE.RE.SECURE-COMM	
OE.RE.API	
OE.RE.DATA-CONFIDENTIALITY	
OE.RE.DATA-INTEGRITY	
OE.RE.IDENTITY	
OE.RE.CODE-EXE	
OE.TRUSTED-PATHS-LPAd	A.TRUSTED-PATHS-LPAd

操作环境安全目标	假设
OE.APPLICATIONS	A.APPLICATIONS
OE.MNO-SD	

7 扩展要求

7.1 扩展族

7.1.1 扩展族 FIA_API-身份验证证明

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 证明所声称身份的功能要求，并允许外部实体进行身份验证。类 FIA 的其他族解决 TOE 对外部实体的身份验证问题。

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

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 内容访问控制 SFP，
- ECASD 访问控制 SFP。

安全策略中使用的所有角色在第 5.2 节中定义为用户或主体。如果角色不属于 TOE，则定义为用户；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-DPplus，U.MNO OTA 平台）或本地（U.MNO-SD，它是 eUICC 上的应用程序）。

8.1.1.1 安全通道协议信息流控制 SFP

图 4 安全通道协议信息流控制 SFP

eUICC 应支持 SCP-SGP22，SCP80，SCP81。

8.1.1.2 平台服务信息流控制 SFP

图 5 平台服务信息流控制 SFP

8.1.1.3 ISD-R 访问控制 SFP

图 6 ISD-R 访问控制 SFP

8.1.1.4 ISD-P 内容访问控制 SFP

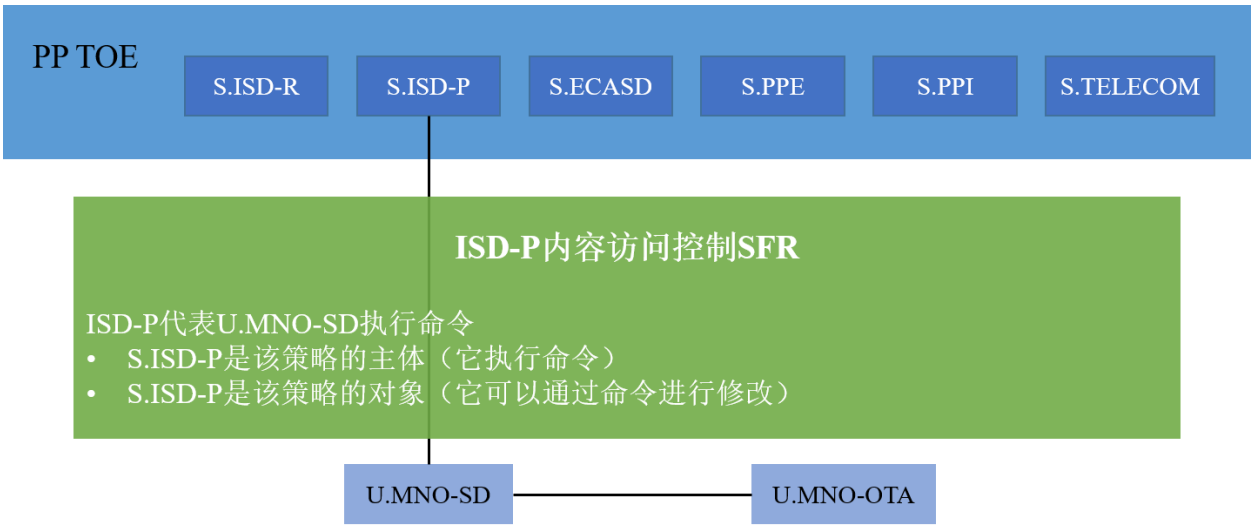

图 7 ISD-P 内容访问控制 SFP

8.1.1.5 ECASD 访问控制 SFP

图 8 ECASD 访问控制 SFP

8.1.1.6 SFR 中使用的安全属性

表 7 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 规范的资产）
S.ISD-P 状态	主体 S.ISD-P 的状态。此状态的可能值为： • 启用 • 禁用 • 已安装 • 可选择	该属性是 D.PLATFORM_DATA 的一部分

安全属性	细节	与资产的关系
PPR	PPR 与给定的 S.ISD-P 相关联，并由 TOE 用于评估是否授权 ISD-P 禁用或删除。PPR 可能包括以下一条或几条规则： • （PPR1）'不允许禁用此配置文件' • （PPR2）'不允许删除此配置文件'	该属性描述为 D.PROFILE_POLICY_RULES
RAT	RAT 在 eUICC 个人化时安装，并由 PPE 和 LPA 用于确定包含 PPR 的 Profile 是否已获得授权并可以安装在 eUICC 上。	
密钥集和会话密钥 (D.MNO_KEYS, D.SECRETS)	TOE 使用的密钥集，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.SECRETS）在 5.1.1.1 密钥中定义
CERT.DPauth.ECDSA CERT.DPpb.ECDSA	TOE 用于验证用户的 U.SM-DPplus 证书。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资产。 CI 根公钥在 5.1.2.3 身份管理数据中被描述为资产 D.PK.CI.ECDSA
SM-DP+ OID MNO OID	SM-DP+ OID 是默认 SM-DP+的标识。该值可以为空，在这种情况下，必须使用 SM-DS 发现过程或激活码中包含的 SM-DP +地址。在 eUICC 的生命周期内，可以修改或删除默认的 SM-DP+地址；存储器复位将 SM-DP+ OID 重置为其初始值。 MNO OID 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.PLATFORM_DATA 中
EID	EID 是实现 TOE 的物理 eUICC 的标识符。	EID 是硬件标识符，不属于此标准的资产。

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 SM-DP+ OID 识别远程用户 U.SM-DPplus
- 通过 MNO OID 识别远程用户 U.MNO-OTA
- 通过 AID 识别卡上用户 U.MNO-SD

TOE 必须：

- 使用 CERT.DPauth.ECDSA 验证 U.SM-DPplus;
- 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-DPplus 下载和安装 Profile 过程中在 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+认证。在 TOE 的使用寿命期间，U.MNO-SD 代表 U.MNO-OTA 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-DPplus 与 S.ISD-R 绑定，

- U.MNO-OTA 绑定到 U.MNO-SD，并且 U.MNO-SD 绑定到管理相应 MNO Profile 的 S.ISD-P。

TOE 最终将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 的以下外部（远程）用户的标识有关：

- U.SM-DPplus，
- U.MNO-OTA。

唯一本地用户（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-DPplus，
- U.MNO-OTA。

由于用于认证的加密机制可能由底层平台提供，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.22 规范所述的要求：

- U.SM-DPplus 必须通过使用其证书（CERT.DPauth.ECDSA 和 CERT.DPpb.ECDSA）中包含的公钥以及 CI 的公钥（D.PK.CI.ECDSA）验证其 ECDSA 签名来进行身份验证。
- 必须根据 SCP80 规范用 GSMA SGP.02 第 2.4.3 章中定义的参数使用 SCP80 安全通道，或根据 SCP81 规范使用 GSMA SGP.02 第 2.4.4（用于此操作的密钥集根据 FCS_CKM.2 / SCP-MNO 分发）章中定义的参数选择 SCP81 来验证 U.MNO-OTA。

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：

- NIST P-256，在数字签名标准中定义（由 NIST 推荐）；
- brainpoolP256r1，在 RFC 5639 中定义（由 BSI 推荐）；
- FRP256V1，在 ANSSI ECC 中定义（由 ANSSI 推荐）。

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：

- **SM-DP+ OID 与代表 U.SM-DPplus 操作的 S.ISD-R 相关联，**
- **MNO OID 与代表 U.MNO-OTA 操作的 U.MNO-SD 相关联。**

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：

- **SM-DP+ OID 和 MNO OID 的初始关联要求通过“CERT.DPauth.ECDSA”对 U.SM-DPplus 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：

- **更改 SM-DP+ OID 要求通过“CERT.DPauth.ECDSA”对 U.SM-DPplus 进行身份验证**
- **不允许更改 MNO OID。**

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-DP+与主体（S.ISD-R）绑定
- U.MNO-OTA 与卡上用户（U.MNO-SD）绑定。

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：

- D.MNO_KEYS 密钥集的初始关联由 ES8+.ConfigureISDP 命令执行。

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-DPplus
- 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-DPplus，
- U.MNO-OTA。

FIA_UID.1/MNO-SD 标识的时机

FIA_UID.1.1/MNO-SD TSF 应允许在识别用户前代表用户执行[赋值：*其他 TSF 调解行动列表*]。

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，U.SM-DPplus 通过主体 S.ISD-R（参见 FDP_ACF.1/ISDR）在 TOE 上安装了 U.MNO-SD，U.SM-DPplus 和 S.ISD-R 之间的绑定需要 U.SM-DP +的认证，如 FIA_USB.1/EXT 中所述。

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 U.SM-DP+通过 CERT.DPauth.ECDSA 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-R 执行，需要 U.SM-DPplus 的认证。

为了执行诸如 PPR 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-R 的认证:S.ISD-R 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：

- **属于 U.SM-DPplus 的 CERT.DPauth.ECDSA，CERT.DPpb.ECDSA 和 SM-DP+ OID;**
- **属于 U.MNO-OTA 的 MNO OID;**
- **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-DPplus 和 S.ISD-R 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 中描述的安全通道协议信息流控制 SFP）建立。该策略特别要求保护传输信息的机密性（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.SECRETS 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-DPplus 和 S.ISD-R**
  - **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-DPplus 和 S.ISD-R，具有安全属性 D.SECRETS**
  - **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：

- **如果未在 SCP-SGP22 安全通道中执行，TOE 应拒绝 U.SM-DPplus 和 S.ISD-R 之间的通信。**

应用说明：

有关安全通道的更多详情，请参阅 GSMA SGP.22 规范

- SM-DP+：第 5.5 章
- MNO-SD：第 5.4 章

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 要求以包括 GSMA SGP.22 规范所述的要求：

- SM-DP+的安全通道必须是 SCP-SGP22 安全通道。根据 GlobalPlatform_Card_Specification 规范修正案 F 使用 AES 和 GSMA SGP.22 规范第 2.6 和 5.5 章中定义的参数来解决端点的识别问题。
- 必须提供 SCP80 以建立到 MNO OTA 平台的安全通道（GSMA SGP.22 规范的第 5.4 章）。TSF 还可以允许使用 SCP81 安全通道执行与 SCP80 安全通道相同的功能。

相关密钥是：

- 在卡上生成（D.SECRETS）;有关详细信息，请参阅 FCS_CKM.1/SCP-SM，
- 或与 Profile（D.MNO_KEYS）一起分发;有关详细信息，请参阅 FCS_CKM.2/SCP-SM-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-DP+打开 SCP-SGP22 安全通道以传输以下操作：
  - ES8+.InitialiseSecureChannel
  - ES8+.ConfigureISDP
  - ES8+.StoreMetadata
  - ES8+.ReplaceSessionKeys
  - ES8+.LoadProfileElements。
- TSF 应允许 LPAd 传输以下操作：
  - ES10a.GetEuiccConfiguredAddresses
  - ES10a.SetDefaultDpAddress
  - ES10b.PrepareDownload
  - ES10b.LoadBoundProfilePackage
  - ES10b.GetEUICCChallenge
  - ES10b.GetEUICCInfo
  - ES10b.ListNotification
  - ES10b.RetrieveNotificationsList
  - ES10b.RemoveNotificationFromList
  - ES10b.AuthenticateServer
  - ES10b.CancelSession
  - ES10c.GetProfilesInfo
  - ES10c.EnableProfile
  - ES10c.DisableProfile
  - ES10c.DeleteProfile
  - ES10c.eUICCMemoryReset
  - ES10c.GetEID
  - ES10c.SetNickname
  - ES10c.GetRAT。
- TSF 应允许远程 OTA 平台打开 SCP80 或 SCP81 安全通道以传输以下操作：
  - ES6.UpdateMetadata。

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-DPplus 和 U.MNO-OTA 的命令**
- **从 U.SM-DPplus 和 U.MNO-OTA 下载的对象**

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_IFF.1/SCP 相关的命令以及与此 SFR FPT_TDC.1/SCP 相关的下载对象：

- SM-DP+命令
  - ES8+.InitialiseSecureChannel
  - ES8+.ConfigureISDP
  - ES8+.StoreMetadata
  - ES8+.ReplaceSessionKeys
  - ES8+.LoadProfileElements
- LPAd 命令
  - ES10a.GetEuiccConfiguredAddresses
  - ES10a.SetDefaultDpAddress
  - ES10b.PrepareDownload
  - ES10b.LoadBoundProfilePackage
  - ES10b.GetEUICCChallenge
  - ES10b.GetEUICCInfo
  - ES10b.ListNotification
  - ES10b.RetrieveNotificationsList
  - ES10b.RemoveNotificationFromList
  - ES10b.AuthenticateServer
  - ES10b.CancelSession
  - ES10c.GetProfilesInfo
  - ES10c.EnableProfile
  - ES10c.DisableProfile
  - ES10c.DeleteProfile

- ES10c.eUICCMemoryReset
- ES10c.GetEID
- ES10c.SetNickname
- ES10c.GetRAT

- 从 SM-DP+下载的对象
  - 会话密钥
  - Profile 元数据（包括 PPR 数据）
- MNO 命令
  - ES6.UpdateMetadata
- 从 MNO OTA 平台下载的对象
  - Profile 元数据（包括 PPR 数据）。

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。

由于用于可信通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.22 规范中所述的要求。

相关密钥是：

- 卡上生成（D.SECRETS）：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;
- 从 SM-DP+和 MNO OTA 平台收到的命令;
- 从 MNO OTA 平台收到的 PPR。

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.22 规范中所述的要求。

相关密钥是：

- 卡上生成（D.SECRETS）：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 U.SM-DPplus 公钥 otPK.DP.ECKA 通过 ES8+.InitialiseSecureChannel 命令生成的 D.SECRETS 密钥集。

用于此密钥协议的椭圆曲线可由底层平台提供。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）。

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 与下述密钥的分发有关

- Profile 下载期间的 D.MNO_KEYS。

注：此 SFR 不适用于 TOE 预先发布加载的私钥（D.SK.EUICC.ECDSA）。

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

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 的安全域的特定要求。特别是它定义：

- S.ISD-R 可以执行其功能的规则（FDP_ACC.1/ISDR 和 FDP_ACF.1/ISDR 中的 ISD-R 访问控制 SFP），
- S.ISD-R 可以执行 ECASD 功能并从这些功能获取输出数据的规则（FDP_ACC.1/ECASD 和 FDP_ACF.1/ECASD 中的 ECASD 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-P**
- **操作：**
  - **创建和配置 Profile**
  - **存储 Profile 元数据**
  - **启用 Profile**
  - **禁用 Profile**
  - **删除 Profile**
  - **执行存储器复位。**

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.22 规范第 5.x 节要求的 ISD-R 对操作的访问。

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"和"PPR"的 S.ISD-P**
- **操作：**
  - **创建和配置 Profile**
  - **存储 Profile 元数据**
  - **启用 Profile**
  - **禁用 Profile**
  - **删除 Profile**
  - **执行存储器复位。**

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**：

- **仅在以下情况才能授权启用一个 S.ISD-P：**
  - **相应的 S.ISD-P 处于"DISABLED"状态并且**
  - **当前启用的 S.ISD-P 的 PPR 数据允许其禁用。**
- **仅在以下情况才能授权禁用一个 S.ISD-P：**
  - **相应的 S.ISD-P 处于"ENABLED"状态并且**
  - **相应的 S.ISD-P 的 PPR 数据允许其禁用。**
- **仅在以下情况才能授权删除一个 S.ISD-P：**
  - **相应的 S.ISD-P 未处于"ENABLED"状态并且**
  - **相应的 S.ISD-P 的 PPR 数据允许其删除。**
- **无论涉及的 S.ISD-P 的状态和 PPR 属性是什么，都可以执行 S.ISD-P 存储器复位。**

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：[赋值：*基于安全属性明确拒绝主体对客体的访问*]。

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.22 规范中第 5.x 节要求的 ISD-R 对以下操作的访问：

- ES8+.ConfigureISDP（创建和配置 Profile）
- ES8+.StoreMetadata（存储 Profile 元数据）
- ES10c.EnableProfile（启用 Profile）
- ES10c.DisableProfile（禁用 Profile）
- ES10c.DeleteProfile（删除 Profile）
- ES10c.eUICCMemoryReset（执行存储器复位）。

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,**
  客体：S.ECASD,
  操作：
  - **执行 ECASD 功能**
  - **访问这些功能的输出数据**
- **[赋值：*SFP 覆盖的主体、客体和主体与客体之间的操作的附加列表*]。**

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，具有安全属性"AID"**
  客体：S.ECASD
  操作：
  - **执行 ECASD 功能**
    - **使用 CI 公钥（PK.CI.ECDSA）验证由 ISD-R 提供的卡外实体证书（SM-DP+，SM-DS）**
    - **在 ISD-R 提供的材料上创建 eUICC 签名**

- 访问这些功能的输出数据。
- **[赋值：*在指定的 SFP 下控制的主体和客体的附加列表，以及每个与 SFP 相关的安全属性或 SFP 相关安全属性的命名组的附加列表*]。**

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 标识的 S.ISD-R 才可被授权执行以下 S.ECASD 功能：**
  - **使用 CI 公钥（PK.CI.ECDSA）验证由 ISD-R 提供的证书 CERT.DPauth.ECDSA，CERT.DPpb.ECDSA，CERT.DP.TLS，CERT.DSauth.ECDSA 或 CERT.DS.TLS**
  - **使用 D.SK.EUICC.ECDSA 在 ISD-R 提供的材料上创建 eUICC 签名。**
- **[赋值：*使用受控客体上的受控操作管理受控主体和受控客体之间访问的附加规则*]。**

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

8.1.5 平台服务

此要求包描述了适用于 Profile 策略使能器、Profile 包解释器和电信框架的特定要求。特别是它定义：

- FDP_IFC.1/Platform_services 和 FDP_IFF.1/Platform_services：为控制安全域与 PPE，PPI 或电信框架之间的信息流动而采取的措施；
- FPT_FLS.1/Platform_services：在 PPE，PPI 或电信框架失败的情况下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.PPE，S.PPI，S.TELECOM）**

信息：

- **D.PROFILE_NAA_PARAMS**
- **D.PROFILE_POLICY_RULES**
- **D.PLATFORM_RAT**

操作：

- **安装 Profile**
- **PPR 和 RAT 执行**
- **网络认证。**

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_POLICY_RULES**
- **D.PLATFORM_RAT**

操作：

- **安装 Profile**
- **PPR 和 RAT 执行**
- **网络认证。**

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 以执行网络认证功能**
  - **由 S.ISD-R 使用 Profile 安装功能传输给 S.PPI**
- **D.PROFILE_POLICY_RULES 只能在以下情况传输：**
  - **由 S.ISD-R 传输给 S.PPE 以执行 PPR 执行功能**
- **D.PLATFORM_RAT 只能在以下情况传输：**
  - **由 S.ISD-R 传输给 S.PPE 以执行 RAT 执行功能。**

FDP_IFF.1.3/Platform_services TSF 应执行[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：*基于安全属性明确拒绝信息流的规则*]。

应用说明：

此 SFR 旨在控制哪个主体能够将 Profile 策略规则、规则授权表或网络身份验证密钥传输到 PPE，PPI 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 实例替换该 SFR，只要它解决了对这些数据的信息流的控制。这种调整的例子可能是由于以下情况：

- D.PROFILE_POLICY_RULES 从 S.ISD-P 传递到 S.ISD-R，然后从 S.ISD-R 传递到 S.PPE；
- D.PROFILE_NAA_PARAMS 从 U.MNO-SD 发送到 S.ISD-P，然后由 S.ISD-P 发送到 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.PPE，S.PPI 或 S.TELECOM API 特定功能期间导致潜在安全违规的故障：**
  - **安装 Profile**
  - **PPR 和 RAT 执行**
  - **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，和
- 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：

- 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，例如平台数据（FMT_MSA.1/PLATFORM_DATA）、PPR（FMT_MSA.1/PPR）、（FMT_MSA.1/RAT）和密钥（FMT_MSA.1/CERT_KEYS）及它们的限制性默认值（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

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.SK.EUICC.ECDSA**

以及**作为以下密钥集一部分的密钥：**

- **D.MNO_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
- Profile 数据
  - D.PROFILE_NAA_PARAMS
  - D.PROFILE_IDENTITY
  - D.PROFILE_POLICY_RULES
  - D.PROFILE_USER_CODES
- 管理数据
  - D.PLATFORM_DATA
  - D.DEVICE_INFO
  - D.PLATFORM_RAT
- 身份管理数据
  - D.SK.EUICC.ECDSA
  - D.CERT.EUICC.ECDSA
  - D.PK.CI.ECDSA
  - D.EID
  - D.SECRETS
  - D.CERT.EUM.ECDSA
  - D.CRLs（如果存在）

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.SK.EUICC.ECDSA;**
- **作为以下密钥集的一部分的密钥：**
  - **D.MNO_KEYS,**
  - **D.PROFILE_NAA_PARAMS.**

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-R 无法安装 Profile**

FMT_MSA.1/PLATFORM_DATA 安全属性管理

FMT_MSA.1.1/PLATFORM_DATA TSF 应强制执行 **ISD-R 访问控制策略**，以限制修改 **D.PLATFORM_DATA 以下部分**的安全属性的能力：

- **ISD-P 状态**

给

- **ISD-R 修改 ISD-P 状态**
  - **从"INSTALLED"到"SELECTABLE"（在 ISD-P 创建期间）**
  - **从"ENABLED"到"DISABLED"（在 Profile 禁用期间）**
- **S.ISD-R 修改 ISD-P 状态**
  - **从"DISABLED"到"ENABLED"（在 Profile 启用期间）。**

应用说明：

如果平台功能的一部分由 GlobalPlatform 包执行，则 S.PPE 的角色可能部分归属于 OPEN。

FMT_MSA.1/PPR 安全属性管理

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

- **D.PROFILE_POLICY_RULE**

给

- **S.ISD -R 通过函数"ES8.ConfigureISDP"修改默认值**
- **S.ISD-R 查询**
- **S.ISD-P 通过函数"ES6.UpdateMetadata"进行修改**
- **S.ISD-R 通过函数"ES10c.DeleteProfile"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**安全通道协议信息流 SFP，ISD-R 访问控制 SFP 和 ECASD 访问控制 SFP**，以限制查询和删除以下安全属性的能力

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

给

- **S.ISD-R：**
  - **查询 D.PK.CI.ECDSA**
  - **通过函数"ES10c.DeleteProfile"删除 D.MNO_KEYS**
- **其他操作没有参与者。**

应用说明：

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

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-DPplus**

- **U.MNO-SD**
- **U.MNO-OTA**

- 主体
  - **S.ISD-R**
  - **S.ISD-P**
  - **S.ECASD**
  - **S.PPI**
  - **S.PPE**
  - **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 小节中定义的用户和主体。

FMT_MSA.1/RAT 安全属性管理

FMT_MSA.1.1/RAT TSF 应强制执行**平台服务信息流 SFP 和 ISD-R 访问控制 SFP**，以限制查询以下安全属性的能力

- **D.PLATFORM_RAT**

给

- **S.ISD-R 查询**
- **S.PPE 查询**

FMT_MSA.3 静态属性初始化

FMT_MSA.3.1 TSF 应强制执行**安全通道协议信息流控制 SFP、ISD-P 内容访问控制 SFP、ISD-R 访问控制 SFP 和 ECASD 访问控制 SFP**，以便为用于执行 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。

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（FCS_CKM.2/Mobile_network 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（请参阅 FCS_CKM.2/Mobile_network），并且必须安全删除（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

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：

为了强制执行域分离，安全架构可能要求在包含 TOE 的 eUICC 上加载的应用程序符合某些规则。但在这种情况下，安全架构不需要比 A.APPLICATIONS 中规定的规则更多的规则。
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 指导性文件

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 安全目的

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。

8.2.5.1 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。

8.2.5.1 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。

8.2.5.2 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 安全目标

平台支持功能

O.PPE-PPI 与安全域相关的所有 SFR（FDP_ACC.1/*和 FDP_ACF.1/*）通过实施符合卡内容管理规则的安全域访问控制策略（规则和限制）来涵盖此安全目标。

FMT_MSA.1/PPR 和 FMT_MSA.1/RAT 通过确保管理 Profile 策略规则（PPR）和规则授权表（RAT）文件来支持这些 SFR，从而确保生命周期修改根据授权策略进行。

FMT_MSA.1/PLATFORM_DATA 限制可应用于 TSF 的其他安全策略(ISD-R 访问控制 SFP 和 ISD-P 内容访问控制 SFP）所用安全属性的平台数据（ISD-P 状态和回退属性）的状态转换。。

该目的还需要 FPT_FLS.1 中描述的安全故障模式。

需要 FCS_RNG.1 来支持 FDP_ACF.1/ECASD。

注：存储器复位也被描述为 FPT_FLS.1 中的安全故障模式。

O.eUICC-DOMAIN-RIGHT 安全要求 FDP_ACC.1/ISDR、FDP_ACF.1/ISDR、FDP_ACC.1/ECASD 和 FDP_ACF.1/ECASD 确保 ISD-R 和 ECASD 的功能和内容只能由相应的经过身份验证的用户访问。

FTP_ITC.1/SCP 为授权用户提供相应的安全通道.

需要 FCS_RNG.1 来支持 FDP_ACF.1/ECASD。

O.SECURE-CHANNELS 所有与 ES6 和 ES8 +接口相关的 SFR（*/SCP，*/SCP-SM 和*/SCP-MNO）通过实施安全通道协议信息流控制 SFP 来确保传输的命令和数据免受未经授权的泄露和修改，从而

覆盖该安全目的。

识别和认证 SFR（FIA_*）通过要求远程 SM-DP +和 MNO OTA 平台进行认证和识别以建立这些安全通道，从而支持此安全目的。

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。

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，不会泄露在 TOE 内存储或传输的秘密数据。尤其包括在 ECASD 和 ISD-R/ISD-P 之间传输的共享秘密。

FDP_SDI.1 确保共享秘密在传输期间不被修改。

FDP_RIP.1 确保不能释放的资源中恢复共享秘密。

eUICC 身份证明

O.PROOF_OF_IDENTITY 此目的由扩展要求 FIA_API.1 覆盖。

平台服务

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

O.API FDP_IFC.1/Platform_services 、 FDP_IFF.1/Platform_services 、 FMT_MSA.3 、 FMT_SMR.1 和 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。

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/ECASD）解决安全域之间的隔离问题。

FPT_EMS.1 确保了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，以及相关密钥的分发和销毁。

O.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 SFR（FDP_ACC.1/ISDR、FDP_ACC.1/ECASD）解决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）。

FPT_TST.1 将有助于完整性保护。

连接性

O.ALGORITHMST 算法在 FCS_COP.1/Mobile_network 中定义。FCS_CKM.2/Mobile_network 描述了密钥在 MNO Profile 中的分发，FCS_CKM.4/Mobile_network 描述了密钥的销毁。

8.3.2 安全目标和 SFR 的基本原理表

表 8 安全目标和 SFR——覆盖范围

安全目标	安全功能要求	基本原理

安全目标	安全功能要求	基本原理
O.PPE-PPI	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/PPR, FMT_MSA.1/RAT, FCS_RNG.1, FPT_FLS.1, FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD	8.3.1 小节
O.eUICC-DOMAIN-RIGHTS	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FTP_ITC.1/SCP, FCS_RNG.1	8.3.1 小节
O.SECURE-CHANNELS	FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FIA_UID.1/EXT, FIA_UAU.4/EXT, FIA_ATD.1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FDP_IFC.1/SCP, FDP_IFF.1/SCP, FIA_UID.1/MNO-SD, FCS_CKM.4/SCP-SM, FCS_CKM.4/SCP-MNO, FIA_USB.1/MNO-SD, FIA_USB.1/EXT, FMT_SMF.1, FMT_SMR.1, FIA_UAU.1/EXT	8.3.1 小节
O.INTERNAL-SECURE-CHANNELS	FDP_RIP.1, FDP_SDI.1, FPT_EMS.1	8.3.1 小节
O.PROOF_OF_IDENTITY	FIA_API.1	8.3.1 小节
O.OPERATE	FPT_FLS.1/Platform_services	8.3.1 小节
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	8.3.1 小节
O.DATA-CONFIDENTIALITY	FDP_RIP.1, FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ECASD, FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network, FPT_EMS.1	8.3.1 小节
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ECASD, FDP_SDI.1	8.3.1 小节
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network	8.3.1 小节

表 9 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

安全功能要求	安全目标
FIA_UID.1/MNO-SD	O.SECURE-CHANNELS
FIA_USB.1/MNO-SD	O.SECURE-CHANNELS
FIA_ATD.1	O.SECURE-CHANNELS
FIA_API.1	O.PROOF_OF_IDENTITY
FDP_IFC.1/SCP	O.SECURE-CHANNELS
FDP_IFF.1/SCP	O.SECURE-CHANNELS
FTP_ITC.1/SCP	O.eUICC-DOMAIN-RIGHTS, O.SECURE-CHANNELS
FDP_ITC.2/SCP	O.SECURE-CHANNELS
FPT_TDC.1/SCP	O.SECURE-CHANNELS
FDP_UCT.1/SCP	O.SECURE-CHANNELS, O.DATA-CONFIDENTIALITY
FDP_UIT.1/SCP	O.SECURE-CHANNELS, O.DATA-INTEGRITY
FCS_CKM.1/SCP-SM	O.SECURE-CHANNELS
FCS_CKM.2/SCP-MNO	O.SECURE-CHANNELS
FCS_CKM.4/SCP-SM	O.SECURE-CHANNELS
FCS_CKM.4/SCP-MNO	O.SECURE-CHANNELS
FDP_ACC.1/ISDR	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ISDR	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS
FDP_ACC.1/ECASD	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS, O.DATA-CONFIDENTIALITY, O.DATA-INTEGRITY
FDP_ACF.1/ECASD	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS
FDP_IFC.1/Platform_services	O.API
FDP_IFF.1/Platform_services	O.API
FPT_FLS.1/Platform_services	O.OPERATE, O.API
FCS_RNG.1	O.PPE-PPI, O.eUICC-DOMAIN-RIGHTS
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.PPE-PPI
FMT_MSA.1/PLATFORM_DATA	O.PPE-PPI
FMT_MSA.1/PPR	O.PPE-PPI
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS
FMT_SMF.1	O.SECURE-CHANNELS, O.API
FMT_SMR.1	O.SECURE-CHANNELS, O.API

安全功能要求	安全目标
FMT_MSA.1/RAT	O.PPE-PPI
FMT_MSA.3	O.SECURE-CHANNELS, O.API
FCS_COP.1/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS
FCS_CKM.2/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS
FCS_CKM.4/Mobile_network	O.DATA-CONFIDENTIALITY, O.ALGORITHMS

8.3.3 依赖关系

8.3.3.1 SFR 依赖关系

排除依赖关系的理由

FCS_CKM.1/SCP-SM 的依赖关系 FCS_CKM.2 或 FCS_COP.1 被丢弃。如果 TOE 使用其底层平台提供的密码库，则不满足对 FCS_COP.1 的依赖性。否则，ST 应包含此依赖项。

表 10 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

要求	CC 依赖关系	满足的依赖关系
FCS_CKM.2/SCP-MNO	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2) 和 (FCS_CKM.4)	FDP_ITC.2/SCP, FCS_CKM.4/SCP-MNO
FCS_CKM.4/SCP-SM	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FCS_CKM.4/SCP-MNO	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.2/SCP, FCS_CKM.1/SCP-SM
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) 和 (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) 和 (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) 和 (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_services	无依赖关系	
FCS_RNG.1	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	
FMT_MSA.1/PLATFORM_DATA	(FDP_ACC.1 or FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/PPR	(FDP_ACC.1 或 FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 或 FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_SMF.1	无依赖关系	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD
FMT_MSA.1/RAT	(FDP_ACC.1 或 FDP_IFC.1) 和 (FMT_SMF.1) 和 (FMT_SMR.1)	FDP_ACC.1/ISDR, FMT_SMF.1, FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1) 和 (FMT_SMR.1)	FMT_MSA.1/PLATFORM_DATA, FMT_MSA.1/PPR, FMT_MSA.1/CERT_KEYS, FMT_SMR.1, FMT_MSA.1/RAT

要求	CC 依赖关系	满足的依赖关系
FCS_COP.1/Mobile_network	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2) 和 (FCS_CKM.4)	FDP_ITC.2/SCP, 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.2/SCP, FCS_CKM.4/SCP-MNO
FCS_CKM.4/Mobile_network	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.2/SCP

8.3.3.2 SAR 依赖关系

表 11 SAR 依赖关系

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

要求	CC 依赖关系	满足的依赖关系
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 安全保障要求的基本原理

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。

9 LPAe

9.1 LPAe 架构

本章节的 TOE 是嵌入式本地 Profile 助理（LPAe），它管理 Profile 下载和最终用户界面。LPAe 是应用层的一部分。

9.1.1 TOE 类型和主要特性

本章节 TOE 的保护类型是软件。
该模块仅包括下图中显示的块（蓝色）。

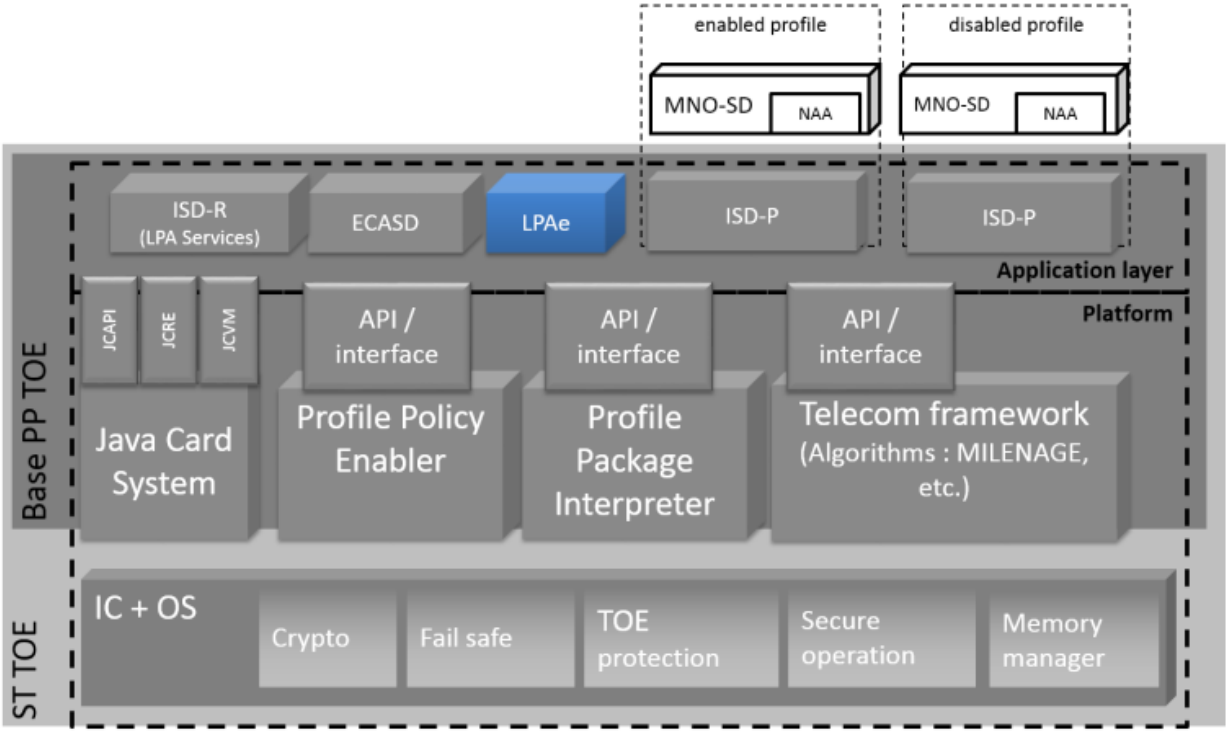

图 9 TOE 范围

LPAe

LPAe 是应用层的一个单元。它具有与设备上（可选）非 TOE 单元 LPAd 相同的功能。特别是，它提供 LPDe（本地 Profile 下载），LDSe（本地发现服务）和 LUIe（本地用户界面）功能。

LPAe 的技术实现取决于 EUM。例如，LPAe 可以是 ISD-R 的一个功能。

LPAe 可以使用 eUICC 规则授权表（RAT）来确定是否授权在 eUICC 上安装包含 Profile 策略规则（PPR）的 Profile。

9.1.2 TOE 生命周期

LPAe 软件单元在 eUICC 生命周期的 C 阶段添加

9.2 LPAe 安全问题定义

9.2.1 安全资产

资产是 TOE 直接保护的与安全相关的元素。他们分为两组。第一组包含由用户创建和为用户创建的数据（用户数据），第二组包含由 TOE 创建和为 TOE 创建的数据（TSF 数据）。对于每个资产，指定它们运行的风险类型。

请注意，虽然底层运行环境中列出的资产未包含在此部分中，但 ST 作者仍应考虑其每个资产。

9.2.1.1 用户数据

LPAe 模块的用户数据包括：

- 用户可以输入的用于 Profile 下载的代码（D.LPAe_PROFILE_USER_CODES）；
- 在用户界面上向用户显示的用于确认平台管理操作的 Profile 元数据（D.LPAe_PROFILE_DISPLAYED_METADATA）。

D.LPAe_PROFILE_USER_CODES

该资产包括：

- 最终用户通过本地用户界面（LUIe）启动 Profile 下载和安装时使用的可选激活码;
- 最终用户通过本地用户界面（LUIe）确认 Profile 下载和安装时的可选确认码。

D.LPAe_PROFILE_DISPLAYED_METADATA

在执行 Profile 管理操作时，本地用户界面（LUIe）向最终用户显示、用于请求确认/信息的 Profile 元数据的部分副本。此资产特别包括 Profile 类（“运营”，“配置”或“测试”）、Profile 策略规则（PPR）和 Profile 状态（“已禁用”或“已启用”）。

需要防止未经授权的修改。

9.2.1.2 TSF 数据

TSF 数据包括：

- LPAe 的 TSF 代码，确保保护 Profile 数据。

TSF 代码

D.LPAe_TSF_CODE

LPAe 代码是一种必须保护的资产，以防止未经授权的披露和修改。了解此代码可能允许绕过 TSF。这涉及运行时的逻辑攻击，以获得对可执行代码的读访问，通常是通过执行应用程序试图读取存储代码段的存储区。

应用说明：

- 这不包括 MNO-SD 中的应用程序，它们是用户数据的一部分（Profile 应用程序）；
- 未经授权的披露和修改的概念与本文其他含义相同。

管理数据

D.LPAe_DEVICE_INFO

此资产包括设备信息数据的安全敏感元素，例如设备类型分配代码（TAC）或设备功能（例如，支持更新证书撤销列表（CRL）），由 eUICC 提供给 LPAe。

需要防止未经授权的修改。

密钥

D.LPAe_KEYS

此资产包含 LPAe 用于执行平台管理功能的密钥（对应于基本要求中的资产 D.SECRETS）：

- 依托接口 ES9 +的 LPDe 到 SM-DP +的 TLS 连接（版本 1.2 或更高版本）的会话密钥;
- 依托接口 ES11 的 LDSe 到 SM-DS 的 TLS 连接（版本 1.2 或更高版本）的会话密钥。

所有这些资产都应受到保护，以免受未经授权的披露和修改。

9.2.2 用户/主体

本节包含两个部分：

- 用户，TOE 外的实体，可能访问 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。

9.2.2.1 用户

U.SM-DS

安全执行发现功能的角色。

9.2.2.2 主体

S.LPAe

LPAe 是 TOE 中的功能元素，提供 LPDe、LDSe 和 LUIe 特性。

9.2.3 安全威胁

9.2.3.1 未经授权的平台管理

T.PLATFORM-MNG-INTERCEPTION-LPDe

攻击者改变或窃听接口 ES9+上 SM-DP+和 LPDe 之间的传输，以破坏平台管理过程：

- eUICC 的 Profile 包的交付和绑定;
- 通知的发送。

注意：攻击者可能是卡上的应用程序拦截到 LPDe 的传输，或者是卡外的参与者拦截 OTA 传输或者 eUICC 和设备之间的接口。

直接受威胁的资产：D.LPAe_KEYS，D.LPAe_PROFILE_*。

T.PLATFORM-MNG-INTERCEPTION-LDSe

攻击者在接口 ES11 上更改或窃听 SM-DS 与 LDSe 之间的传输，以破坏发现过程：

即，LPAe 和 SM-DS（备选 SM-DS 或根 SM-DS）之间的事件检索过程。

注意：攻击者可能是卡上的应用程序拦截到 LDSe 的传输，或者是卡外的参与者拦截 OTA 传输或者 eUICC 和设备之间的接口。

直接受威胁的资产：D.LPAe_KEYS。

T.UNAUTHORIZED-PLATFORM-MNG-LPAe

卡上应用程序可能：

- 修改或披露 LPAe 数据;
- 执行或修改从 LPAe 来的操作。

特别是，可能发生以下情况：

- 在启用或禁用 Profile 期间在 LUIe 显示给最终用户的 Profile 元数据可能会受到损害;
- 激活码或确认码在进入 LUIe 时，可能会被披露或修改;
- 在发送给 eUICC 之前，设备信息可能会被修改，从而导致：

- Profile 的资格检查失败，或
- 安全参数降级，例如指示设备不支持证书撤销列表（CRL）。

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.LPAe_TSF_CODE，D.LPAe_PROFILE_*。

T.PROFILE-MNG-ELIGIBILITY-LPAe

当设备信息从 LPAe 提供给 eUICC 时，攻击者会更改设备信息，以便损害 eUICC 的资格，例如：

- 通过修改设备信息获取未经授权的 Profile。

注意：攻击者可能是卡上的应用程序拦截到安全域的传输。

直接威胁资产：D.LPAe_TSF_CODE，D.LPAe_DEVICE_INFO。

9.2.3.2 其他

T.LOGICAL-ATTACK-LPAe

卡上的恶意应用程序通过逻辑方式绕过平台安全措施，以便在 LPAe 处理敏感数据时泄露或修改敏感数据。

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.LPAe_*。

T.PHYSICAL-ATTACK-LPAe

卡外参与者通过物理（相对于逻辑）篡改手段来泄露或修改 LPAe 的设计、其敏感数据或应用代码。

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

卡外参与者具有很高的攻击潜力。卡外参与者可以是使用 eUICC 的外部接口的任何参与者，无论他们是否打算使用。

直接威胁资产：D.LPAe_*。

9.2.4 假设

A.ACTORS-LPAe

SM-DS 是基础设施的一个参与者，安全地管理自己的证书和其他敏感数据。

这个假设扩展了基础要求里面的假设 A.ACTORS。

9.3 LPAe 安全目标

9.3.1 TOE 的安全目标

9.3.1.1 平台支持的功能

O.SECURE-CHANNELS-LPAe

eUICC 应保持以下角色之间的安全通道

- LPAe 和 SM-DP+
- LPAe 和 SM-DS。

TOE 应随时确保：

- 传入的消息未经替换地正确提供给 LPAe;

- 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 PPE/PPI 提供的通信保护措施（参见 O.PPE-PPI）。

O.INTERNAL-SECURE-CHANNELS-LPAe

TOE 确保从 ECASD 传输到 LPAe 的通信共享秘密受到保护，以防止未经授权的泄露或修改。

该保护机制应依赖于运行环境提供的通信保护措施。

9.3.1.2 数据保护

O.DATA-CONFIDENTIALITY-LPAe

TOE 应避免未经授权泄露作为密钥集 D.LPAe_KEYS 一部分的密钥。

应用说明：

在 TOE 的组件中，

- PPE，PPI 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。

该目标包括抵抗侧信道攻击。

O.DATA-INTEGRITY-LPAe

TOE 管理或操作数据时，TOE 应避免对以下数据的未经授权修改：

- 密钥：
  - D.LPAe_KEYS;
- Profile 数据：
  - D.LPAe_PROFILE_USER_CODES，
  - D.LPAe_PROFILE_DISPLAYED_METADATA;
- 管理数据：
  - D.LPAe_DEVICE_INFO。

应用说明：

在 TOE 的组件中，

- PPE，PPI 和电信框架必须保护他们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。

9.3.2 运行环境的安全目标

9.3.2.1 参与者

OE.SM-DS

SM-DS 应是负责发现服务的值得信赖的参与者。SM-DS 站点必须遵循相关认证。SM-DS 具有与 SM-DP+或其他 SM-DS 的安全通信信道。

SM-DS 必须确保从 SM-DP+或其他 SM-DS 收到的凭证的安全性。

9.3.3 安全目标基本原理

9.3.3.1 威胁

<u>未经授权的平台管理</u>

T.PLATFORM-MNG-INTERCEPTION-LPDe

SM-DP+将 Profile（绑定 Profile 包）发送到 LPAe（LPDe）。

因此，TSF 确保：

- 通通过要求 SM-DP+进行身份验证，以及保护传输免受未经授权的泄露、修改和重放，确保传输到 LPAe（O.SECURE-CHANNELS-LPAe 和 O.INTERNAL-SECURE-CHANNELS-LPAe）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通信（OE.RE.SECURE-COMM）。

OE.SM-DP+确保在由卡外参与者使用时不会泄露与安全通道相关的凭证。

T.PLATFORM-MNG-INTERCEPTION-LDSe

SM-DS 将事件发送到 LPAe（LDSe）。

因此，TSF 确保：

- 通过要求 SM-DS 进行身份验证，以及保护传输免受未经授权的泄露、修改和重放，确保传输到（O.SECURE-CHANNELS-LPAe 和 O.INTERNAL-SECURE-CHANNELS-LPAe）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通信（OE.RE.SECURE-COMM）。

OE.SM-DS 确保在由卡外参与者使用时不会泄露与安全通道相关的凭证。

T.UNAUTHORIZED-PLATFORM-MNG-LPAe

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）。

为了确保应用程序防火墙的安全运行，操作环境的以下目标也应满足：

- 遵守应用程序的安全准则（OE.APPLICATIONS）。

T.PROFILE-MNG-ELIGIBILITY-LPAe

SM-DP+在允许 Profile 下载到 eUICC 前，使用由 LPAe 发送到 SM-DP+的用于签名的设备信息进行资格审查。

因此，TSF 确保：

- 通过保护传输免受未经授权的泄露、修改和重放，保护 LPAe 和 TOE 的其他安全域（O.INTERNAL-SECURE-CHANNELS-LPAe）之间的传输安全性；这些安全通道依赖于底层运行环境，它可以保护应用程序通信（OE.RE.SECURE-COMM）。

OE.SM-DPplus 确保在由卡外参与者使用时不会泄露与安全通道相关的凭证。

O.DATA-INTEGRITY-LPAe 和 OE.RE.DATA-INTEGRITY 确保设备信息和 eUICCInfo2 的完整性在 eUICC 级别受到保护。

其他

T.LOGICAL-ATTACK-LPAe

通过控制 LPAe 安全域与平台层或 TOE 的任何本机/OS 部分之间的信息流来覆盖此威胁。因此它涵盖：

- 由运行环境提供的 API（OE.RE.API）；
- TSF 的 API（O.API）。LPAe 的 API 应确保原子性事务（OE.IC.SUPPORT）。

每当 LPAe 处理 TOE 的敏感数据时，运行环境必须始终保护敏感数据的机密性和完整性（OE.RE.DATA-CONFIDENTIALITY，OE.RE.DATA-INTEGRITY）。但是，这些敏感数据也由 TOE 的平台层处理，不受这些机制的保护。所以，

- TOE 本身必须确保平台层（PPE、PPI 和电信框架（O.OPERATE））的正确运行，以及

- 平台层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）。

运行环境的以下目标也应满足：

- 防止 LPAe 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）。

T.PHYSICAL-ATTACK-LPAe

这种威胁主要受到依赖于基础平台的物理保护的抵制，因此是一个环境问题。

安全目标OE.IC.SUPPORT和OE.IC.RECOVERY保护平台的敏感资产免受完整性和机密性的损失，特别是确保 TSF 不被绕过或更改。

特别是，安全目标 OE.IC.SUPPORT 提供了确保敏感操作的原子性、安全的低级访问控制和防止绕过 TOE 的安全功能的功能。特别是，它明确确保平台数据完整性的独立保护。

由于 TOE 不仅可以依赖 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-LPAe）。出于同样的原因，卡片运行平台安全体系结构必须涵盖辅助通道（OE.RE.DATA-CONFIDENTIALITY）。

9.3.3.2 假设

A.ACTORS-LPAe

这一假设通过目标 OE.SM-DS 支持，它确保基础设施的这个参与者正确管理凭证和其他敏感数据

9.3.3.3 SPD 和安全目标

表 12 威胁和安全目标——覆盖范围

威胁	安全目标	基本原理
T.PLATFORM-MNG-INTERCEPTION-LPDe	OE.RE.SECURE-COMM, OE.SM-DPplus, O.SECURE-CHANNELS-LPAe, O.INTERNAL-SECURE-CHANNELS-LPAe	9.3.3 小节
T.PLATFORM-MNG-INTERCEPTION-LDSe	OE.RE.SECURE-COMM, OE.SM-DS, O.SECURE-CHANNELS-LPAe, O.INTERNAL-SECURE-CHANNELS-LPAe	9.3.3 小节
T.UNAUTHORIZED-PLATFORM-MNG-LPAe	OE.APPLICATIONS, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	9.3.3 小节
T.PROFILE-MNG-ELIGIBILITY-LPAe	OE.RE.SECURE-COMM, O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-INTEGRITY-LPAe, OE.SM-DPplus, OE.RE.DATA-INTEGRITY	9.3.3 小节
T.LOGICAL-ATTACK-LPAe	O.OPERATE, O.API, OE.RE.API, OE.RE.CODE-EXE, OE.APPLICATIONS, O.DATA-CONFIDENTIALITY-LPAe, O.DATA-INTEGRITY-LPAe, OE.IC.SUPPORT, OE.RE.DATA-CONFIDENTIALITY, OE.RE.DATA-INTEGRITY	9.3.3 小节
T.PHYSICAL-ATTACK-LPAe	O.DATA-CONFIDENTIALITY-LPAe, OE.IC.SUPPORT, OE.IC.RECOVERY, OE.RE.DATA-CONFIDENTIALITY	9.3.3 小节

表 13 安全目标和威胁——覆盖范围

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

表 14 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	基本原理
A.ACTORS-LPAe	OE.SM-DS	9.3.3 小节

表 15 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
OE.SM-DS	A.ACTORS-LPAe

9.4 LPAe 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 作者执行的赋值。因此，该文本既是粗体又是斜体（例如参见 FIA_UID.1/LPAe）。

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。

9.4.1 安全功能要求

9.4.1.1 介绍

此技术要求模块定义了一下安全策略：

- LPAe 信息流控制 SFP。

标准中使用的所有角色定义为用户或主体。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。

该技术要求模块仅涉及远程用户（U.SM-DS 和 U.SM-DPplus）。

LPAe 信息流控制 SFP

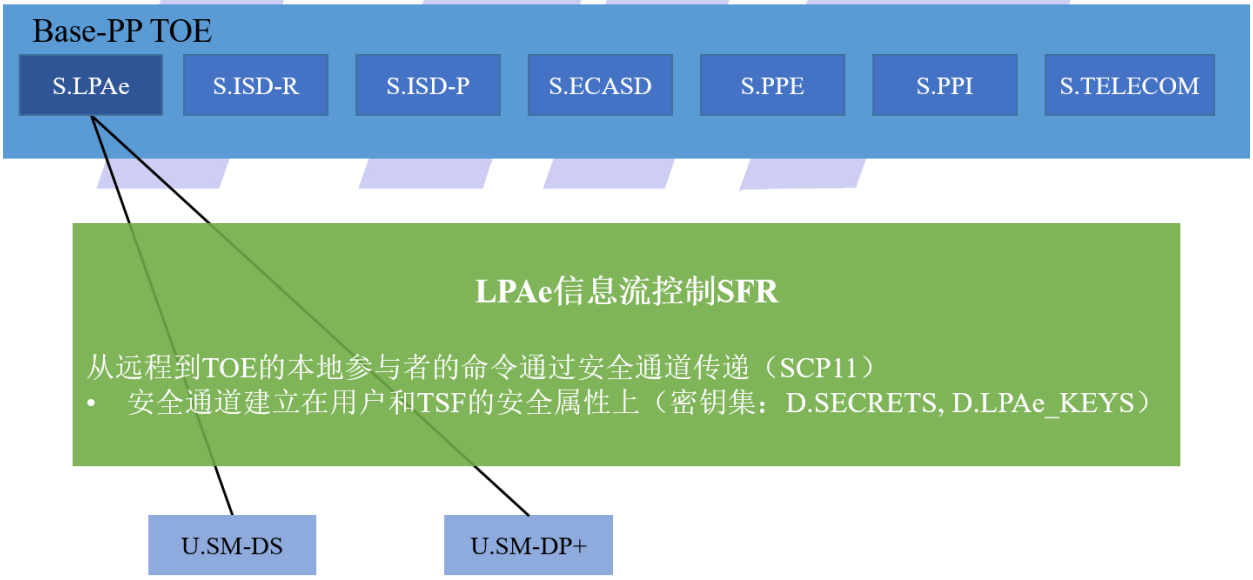

图 10 LPAe 信息流控制 SFP

SFR 中用于 LPAe 模块的安全属性

表 16 LPAe 模块的安全属性定义

安全属性	细节	与资产的关系

LPAe 会话密钥 (D.LPAe_KEYS)	LPAe 与 SM-DP+和 SM-DS 之间的 TLS 连接的会话密钥。	与密钥相关资产
CERT.DSauth.ECDSA CERT.DS.TLS CERT.DP.TLS	TOE 用于对此用户进行身份验证的 U.SM-DS 和 U.SM-DPplus 证书。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资产。CI 根公钥在标识管理数据中被描述为资产 D.PK.CI.ECDSA
SM-DS OID	SM-DS OID 是根 SM-DS 的标识。根 SM-DS 地址是唯一的并且填写在 eUICC 中。根 SM-DS 在设备制造时配置并且是不变的。	这些属性包含在管理数据部分中描述的 D.PLATFORM_DATA 中

9.4.1.2 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 SM-DS OID 识别远程用户 U.SM-DS。

TOE 必须：

- 使用 CERT.DSauth.ECDSA 验证 U.SM-DS。

TOE 应将卡外和卡上用户绑定到内部主体：

- U.SM-DPplus 与 S.LPAe 绑定，
- U.SM-DS 与 S.LPAe 绑定。

TOE 最终将提供一种向卡外用户证明其身份的方法。

FIA_UID.1/LPAe 标识的时机

FIA_UID.1.1/LPAe

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/LPAe

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 的以下外部（远程）用户的标识有关：

- U.SM-DPplus
- U.SM-DS。

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

FIA_UAU.1/LPAe 身份验证的时间

FIA_UAU.1.1/LPAe

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*]。**

在验证用户之前代表用户执行。

FIA_UAU.1.2/LPAe

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-DPplus
- U.SM-DS。

由于用于认证的加密机制可以由底层平台提供，因此本要求不包括相应的 FCS_COP.1 SFR。

ST 作者应添加 FCS_COP.1 要求以包括以下要求：

- U.SM-DPplus 必须通过使用其证书（CERT.DPauth.ECDSA，CERT.DPpb.ECDSA 和 CERT.DP.TLS）中包含的公钥以及 CI 公钥验证其 ECDSA 签名进行身份验证。
- U.SM-DS 必须通过使用其证书中包含的公钥（CERT.DSauth.ECDSA 和 CERT.DS.TLS）以及 CI 的公钥（D.PK.CI.ECDSA）验证其 ECDSA 签名来进行身份验证。

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，在数字签名标准中定义（由 NIST 推荐）
- brangpoolP256r1，在 RFC 5639 中定义（由 BSI 推荐）
- FRS256V1，在 ANSSI ECC 中定义（由 ANSSI 推荐）

FIA_USB.1/LPAe 用户-主体绑定

FIA_USB.1.1/LPAe

TSF 应将以下用户安全属性与代表该用户的主体相关联：

- **SM-DP+ OID 与代表 U.SM-Dpplus 操作的 S.LPAe 相关联**
- **SM-DS OID 与代表 U.SM-DS 操作的 S.LPAe 相关联。**

FIA_USB.1.2/LPAe

TSF 应对用户安全属性与代表用户主体的初始关联强制执行以下规则：

- **SM-DP+ OID 的初始关联要求通过"CERT.DPauth.ECDSA"对 U.SM-DPplus 进行身份验证**
- **SM-DS OID 的初始关联要求通过"CERT.DSauth.ECDSA"对 U.SM-DS 进行身份验证。**

FIA_USB.1.3/LPAe

TSF 应执行以下规则，管理与代表用户行事的主体相关联的用户安全属性的更改：

- **更改 SM-DP+ OID 要求通过"CERT.DPauth.ECDSA"对 U.SM-DPplus 进行身份验证**
- **更改 SM-DS OID 要求通过"CERT.DSauth.ECDSA"对 U.SM-DS 进行身份验证。**

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-DPplus 与主体（S.LPAe）绑定
- U.SM-DS 与主体（S.LPAe）绑定

FIA_UAU.4/LPAe 一次性身份验证机制

FIA_UAU.4.1/LPAe

TSF 应防止重用**用于在 LPAe 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-DPplus**
- **U.SM-DS。**

应用说明：

此 SFR 与 TOE 的外部（远程）用户的身份验证有关：

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

FIA_ATD.1/LPAe 用户属性定义

FIA_ATD.1.1/LPAe

TSF 应维护属于各个用户的以下安全属性列表：

- **属于 U.SM-DPplus 的 CERT.DP.TLS**
- **属于 U.SM-DS 的 CERT.DSauth.ECDSA，CERT.DS.TLS 和 SM-DS OID。**

9.4.1.3 通信

此章节描述了 TSF 如何保护与外部用户的通信。

TSF 应强制实施安全通道（FTP_ITC.1/LPAe 和 FTP_ITC.2/LPAe）：

- U.SM-DPplus 和 S.LPAe 之间
- U.SM-DS 和 S.LPAe 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/LPAe）一致地解释这些命令和对象。

这些安全通道根据安全策略（在 FDP_IFC.1/LPAe 和 FDP_IFF.1/LPAe 中描述的 LPAe 信息流控制 SFP）建立。该策略特别要求保护传输信息的机密性（FDP_UCT.1/LPAe）和完整性（FDP_UIT.1/LPAe）。

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：

- 生成和删除 D.LPAe_KEYS 和证书（FCS_CKM.1/SCP-SM， FCS_CKM.4/SCP-SM，FCS_CKM.2/SCP-MNO，FCS_CKM.4/SCP-MNO，FCS_CKM.1/LPAe 和 FCS_CKM.4/LPAE）。

FDP_IFC.1/LPAe 子集信息流控制

FDP_IFC.1.1/LPAe

TSF 应强制执行 **LPAe 信息流控制 SFP**

- **用户/主体：**
  - **U.SM-DPplus 和 S.LPAe**
  - **U.SM-DS 和 S.LPAe**
- **信息：命令的传输。**

FDP_IFF.1/LPAe 简单的安全属性

FDP_IFF.1.1/LPAe

TSF 应根据以下类型的主体和信息安全属性强制执行 **LPAe 信息流控制 SFP**：

- **用户/主体：**
  - **U.SM-DPplus 和 S.LPAe，具有安全属性 D.LPAe_KEYS**
  - **U.SM-DS 和 S.LPAe，具有安全属性 D.LPAe_KEYS**
- **信息：命令的传输。**

FDP_IFF.1.2/LPAe

如果以下规则满足，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：[赋值：*对于每个操作，主体和信息安全属性之间必须保持基于安全属性的关系*]。

FDP_IFF.1.3/LPAe

TSF 应强制执行[赋值：*附加信息流控制 SFP 规则*]。

FDP_IFF.1.4/LPAe

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/LPAe

TSF 应根据以下规则明确拒绝信息流：

- **如果未在 SCP-SGP22 安全通道中执行，TOE 应拒绝 U.Sm-DPplus 和 S.LPAe 之间的通信;**
- **如果未在 SCP-SGP22 安全通道中执行，TOE 应拒绝 U.Sm-DS 和 S.LPAe 之间的通信。**

FTP_ITC.1/LPAe TSF 间可信通道

FTP_ITC.1.1/LPAe

TSF 应在其自身与另一个可信 IT 产品之间提供通信通道，该通信通道在逻辑上与其他通信通道不同，并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/LPAe

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/LPAe

TSF 应通过可信信道为[赋值：*需要信任信道的功能列表*]发起通信。

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，因此本要求不包括相应的 FCS_COP.1 SFR。ST 作者应添加 FCS_COP.1 要求以包括下述要求：

- SM-DP+和 SM-DS 的安全通道必须是 SCP-SGP22 安全通道

相关密钥在卡上生成（D.LPAe_KEYS）；参见 FCS_CKM.1/LPAe。

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 LPAe 向 SM-DP+打开 SCP-SGP22 安全通道并发送以下操作：
  - ES9+.InitiateAuthentication
  - ES9+.GetBoundProfilePackage
  - ES9+.AuthenticateClient
  - ES9+.HandeNotification
  - ES9+.CancelSession
- TSF 应允许 LPAe 向 SM-DS 打开 SCP-SGP22 安全通道并发送以下操作：
  - ES11.InitiateAuthentication
  - ES11.AuthenticateClient

FDP_ITC.2 / LPAe 使用安全属性导入用户数据

FDP_ITC.2.1/LPAe

当从 TOE 外部导入受 SFP 控制的用户数据时，TSF 应强制执行 **LPAe 信息流控制 SFP**。

FDP_ITC.2.2/LPAe

TSF 应使用与导入的用户数据关联的安全属性。

FDP_ITC.2.3/LPAe

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/LPAe

TSF 应确保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/LPAe

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/LPAe TSF 间基本 TSF 数据一致性

FPT_TDC.1.1/LPAe

TSF 应对下述内容提供一致的解释能力

- **来自 U.SM-DPplus 和 U.SM-DS 的命令**
- **从 U.SM-DPplus 下载的对象**

在 TSF 和另一个可信 IT 产品之间共享时。

FPT_TDC.1.2/LPAe

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/LPAe，FDP_IFC.1/LPAe，FDP_IFF.1/LPAe 以及与此 SFR FPT_TDC.1/LPAe 相关的下载对象相关的命令：

SM-DP+命令

- ES9+.InitiateAuthentication
- ES9+.GetBoundProfilePackage
- ES9+.AuthenticateClient
- ES9+.HandeNotification
- ES9+.CancelSession

从 SM-DP+下载的对象

- 会话密钥
- 绑定 profile 包

SM-DS 命令

- ES11.InitiateAuthentication
- ES11.AuthenticateClient

FDP_UCT.1/LPAe 基本数据交换机密性

FDP_UCT.1.1/LPAe

TSF 应强制执行 **LPAe 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+下载的绑定 Profile 包。

由于用于可信信道的加密机制可以由底层平台提供，因此本要求不包括相应的 FCS_COP.1 SFR。ST 作者应添加 FCS_COP.1 要求：通信的机密性必须通过使用 AES 的 CBC 模式（NIST 800-38A）来解决，最小密钥大小为 128 位。

相关密钥在卡上生成（D.LPAe_KEYS）；有关详细信息，请参阅 FCS_CKM.1/LPAe。

FDP_UIT.1/LPAe 数据交换完整性

FDP_UIT.1.1/LPAe

TSF 应强制 **LPAe 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 / LPAe

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+下载的绑定 Profile 包;
- 从 SM-DP+和 SM-DS 收到的命令。

由于用于可信信道的加密机制可以由底层平台提供，因此本要求不包括相应的 FCS_COP.1 SFR。ST 作者应添加 FCS_COP.1 要求：通信的完整性必须通过使用 AES 的 CMAC 模式（NIST SP 800-38B）来解决，最小密钥大小为 128 位并且 MAC 长度为 64 位。

相关密钥在卡上生成（D.LPAe_KEYS）；有关详细信息，请参阅 FCS_CKM.1/LPAe。

FCS_CKM.1/LPAe 密钥生成

FCS_CKM.1.1/LPAe

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：

- D.LPAe_KEYS 键。

用于此密钥协议的椭圆曲线加密可由底层平台提供。因此，本要求不包括相应的 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）

FCS_CKM.4/LPAe 密钥销毁

FCS_CKM.4.1/LPAe

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.LPAe_KEYS。

9.4.1.4 安全管理

本章节包括几个支持的安全功能：

用户数据和 TSF 自我保护措施：

- TOE 发散（FPT_EMS.1/LPAe）
- 完整性监视（FDP_SDI.1 / LPAe）
- 残留数据保护（FDP_RIP.1 / LPAe）

安全管理措施：

- 角色管理（FMT_SMR.1/LPAe）和功能（FMT_SMF.1/LPAe）

FPT_EMS.1/LPAe TOE 发散

FPT_EMS.1.1/LPAe

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.LPAe_KEYS**

和[赋值：*用户数据类型列表*]。

FPT_EMS.1.2/LPAe

TSF 应确保[赋值：*用户类型*]无法使用接口[赋值：连接类型]来访问以下资源

- **D.LPAe_KEYS**

和[赋值：*用户数据类型列表*]。

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/LPAe 存储数据完整性监控

FDP_SDI.1.1/LPAe

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以下需要防止未经授权的修改的资产：

- 个人资料数据
  - D.LPAe_PROFILE_USER_CODES
  - D.LPAe_PROFILE_DISPLAYED_METADATA
- 管理数据
  - D.LPAe_DEVICE_INFO
- 密钥

- LPAe_KEYS

FDP_RIP.1/LPAe 子集残余信息保护

FDP_RIP.1.1/LPAe

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.LPAe_KEYS**。

FMT_SMF.1/LPAe 管理职能规范

FMT_SMF.1.1/LPAe

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/LPAe 安全角色

FMT_SMR.1.1/LPAe

TSF 应保持角色

- **外部用户：**
  - **U.SM-DS**
- **密钥：**
  - **S.LPAe。**

FMT_SMR.1.2/LPAe

TSF 应能够将用户与角色相关联。

9.4.2 安全保障要求

无额外要求

9.4.3 安全要求基本原理

9.4.3.1 目标

平台支持功能

O.SECURE-CHANNELS-LPAe

所有相对于 ES9+和 ES11 接口的 SFR（FDP_IFC.1/LPAe，FDP_IFF.1/LPAe，FTP_ITC.1/LPAe，FDP_ITC.2/LPAe，FPT_TDC.1/LPAe，FDP_UCT.1/LPAe，FDP_UIT.1/LPAe，FCS_CKM.1/LPAe，FCS_CKM.4/LPAe）通过强制执行 LPAe 信息流控制 SFP 来覆盖此安全目标，该 SFP 确保传输的命令和数据免受未经授权的泄露和修改。

识别和认证 SFR 通过要求远程 SM-DP+和 SM-DS 的识别和认证（FIA_UID.1/LPAe，FIA_UAU.1/LPAe，FIA_USB.1/LPAe，FIA_UAU.4/LPAe）来建立安全通道，从而支持该安全目的。

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

O.INTERNAL-SECURE-CHANNELS-LPAe

FPT_EMS.1/LPAe 确保在侧信道攻击的情况下不泄露在 TOE 内存储或传输的秘密数据。尤其包括在 ECASD 和 LPAe 之间传输的秘密（资产 D.SECRETS）。

FDP_SDI.1/LPAe 确保秘密在此传输期间不被修改。

FDP_RIP.1/LPAe 确保无法从释放的资源中恢复秘密。

数据保护

O.DATA-CONFIDENTIALITY-LPAe

FDP_UCT.1/LPAe 处理来自卡外参与者的数据接收。

FPT_EMS.1/LPAe 确保在侧信道攻击的情况下不泄露在 TOE 内存储或传输的秘密数据。

FDP_RIP.1/LPAe 确保没有剩余的机密数据可用。

O.DATA-INTEGRITY-LPAe

FDP_UIT.1 LPAe 解决了从卡外参与者接收数据的问题。

FDP_SDI.1/LPAe 指定在完整性破坏的情况下监视的数据

9.4.3.2 安全目标和 SFR 的基本原理表

表 17 安全目标和 SFR——覆盖范围

安全目标	安全功能要求	基本原理
O.SECURE-CHANNELS-LPAe	FMT_MSA.1/CERT_KEYS, FMT_SMF.1/LPAe,FMT_SMR.1/LPAe, FIA_UID.1/LPAe,FIA_UAU.1/LPAe, FIA_USB.1/LPAe,FIA_UAU.4/LPAe, FIA_ATD.1/LPAe,FDP_IFF.1/LPAe, FTP_ITC.1/LPAe,FDP_ITC.2/LPAe, FPT_TDC.1/LPAe,FDP_UIT.1/LPAe, FCS_CKM.1/LPAe,FCS_CKM.4/LPAe, FDP_IFC.1/LPAe,FDP_UCT.1/LPAe, FIA_ATD.1, FMT_MSA.3	9.4.3.1 小节
O.INTERNAL-SECURE-CHANNELS-LPAe	FPT_EMS.1/LPAe, FDP_SDI.1/LPAe, FDP_RIP.1/LPAe	9.4.3.1 小节
O.DATA-CONFIDENTIALITY-LPAe	FPT_EMS.1/LPAe, FDP_RIP.1/LPAe, FDP_UCT.1/LPAe	9.4.3.1 小节
O.DATA-INTEGRITY-LPAe	FDP_SDI.1/LPAe, FDP_UIT.1/LPAe	9.4.3.1 小节

表 18 SFR 和安全目标

安全功能要求	安全目标
FIA_ATD.1	O.SECURE-CHANNELS-LPAe
FMT_MSA.1/CERT_KEYS	O.SECURE-CHANNELS-LPAe
FMT_SMF.1/LPAe	O.SECURE-CHANNELS-LPAe
FMT_MSA.3	O.SECURE-CHANNELS-LPAe

安全功能要求	安全目标
FIA_UID.1/LPAe	O.SECURE-CHANNELS-LPAe
FIA_UAU.1/LPAe	O.SECURE-CHANNELS-LPAe
FIA_USB.1/LPAe	O.SECURE-CHANNELS-LPAe
FIA_UAU.4/LPAe	O.SECURE-CHANNELS-LPAe
FIA_ATD.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_IFC.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_IFF.1/LPAe	O.SECURE-CHANNELS-LPAe
FTP_ITC.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_ITC.2/LPAe	O.SECURE-CHANNELS-LPAe
FPT_TDC.1/LPAe	O.SECURE-CHANNELS-LPAe
FDP_UCT.1/LPAe	O.SECURE-CHANNELS-LPAe, O.DATA CONFIDENTIALITY-LPAe
FDP_UIT.1/LPAe	O.SECURE-CHANNELS-LPAe, O.DATA INTEGRITY-LPAe
FCS_CKM.1/LPAe	O.SECURE-CHANNELS-LPAe
FCS_CKM.4/LPAe	O.SECURE-CHANNELS-LPAe
FPT_EMS.1/LPAe	O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-CONFIDENTIALITY-LPAe
FDP_SDI.1/LPAe	O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-INTEGRITY-LPAe
FDP_RIP.1/LPAe	O.INTERNAL-SECURE-CHANNELS-LPAe, O.DATA-CONFIDENTIALITY-LPAe
FMT_SMR.1/LPAe	O.SECURE-CHANNELS-LPAe

9.4.3.3 依赖关系表

表 19 SFR 依赖关系

要求	CC 依赖关系	满足的依赖关系
FIA_UID.1/LPAe	无依赖关系	
FIA_UAU.1/LPAe	(FIA_UID.1)	FIA_UID.1/LPAe
FIA_USB.1/LPAe	(FIA_ATD.1)	FIA_ATD.1/LPAe
FIA_UAU.4/LPAe	无依赖关系	
FIA_ATD.1/LPAe	无依赖关系	
FDP_IFC.1/LPAe	(FDP_IFF.1)	FDP_IFF.1/LPAe
FDP_IFF.1/LPAe	(FDP_IFC.1) 和 (FMT_MSA.3)	FMT_MSA.3, FDP_IFC.1/LPAe
FTP_ITC.1/LPAe	无依赖关系	

要求	CC 依赖关系	满足的依赖关系
FDP_ITC.2/LPAe	(FDP_ACC.1 或 FDP_IFC.1) 和 (FPT_TDC.1) 和 (FTP_ITC.1 或 FTP_TRP.1)	FDP_IFC.1/LPAe, FTP_ITC.1/LPAe, FPT_TDC.1/LPAe
FPT_TDC.1/LPAe	无依赖关系	
FDP_UCT.1/LPAe	(FDP_ACC.1 或 FDP_IFC.1) 和 (FTP_ITC.1 或 FTP_TRP.1)	FDP_IFC.1/LPAe, FTP_ITC.1/LPAe
FDP_UIT.1/LPAe	(FDP_ACC.1 或 FDP_IFC.1) 和 (FTP_ITC.1 或 FTP_TRP.1)	FDP_IFC.1/LPAe, FTP_ITC.1/LPAe
FCS_CKM.1/LPAe	(FCS_CKM.2 或 FCS_COP.1) 和 (FCS_CKM.4)	FCS_CKM.4/LPAe
FCS_CKM.4/LPAe	(FCS_CKM.1 或 FDP_ITC.1 或 FDP_ITC.2)	FDP_ITC.2/LPAe, FCS_CKM.1/LPAe
FPT_EMS.1/LPAe	无依赖关系	
FDP_SDI.1/LPAe	无依赖关系	
FDP_RIP.1/LPAe	无依赖关系	
FMT_SMF.1/LPAe	无依赖关系	
FMT_SMR.1/LPAe	(FIA_UID.1)	FIA_UID.1/LPAe

9.4.3.4 排除依赖关系的理由

FCS_CKM.1/LPAe 的依赖关系 FCS_CKM.2 或 FCS_COP.1 被丢弃。如果 TOE 使用其底层平台提供的密码库，则不满足对 FCS_COP.1 的依赖性。否则，ST 应包含此依赖项。

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