

ICS 31.200  
CCS L56

# 团体标准

T/TAF 356—2026



Convergence eUICC chip concurrency and security isolation test  
specification

2026-06-17 发布

2026-06-17 实施

电信终端产业协会 发布

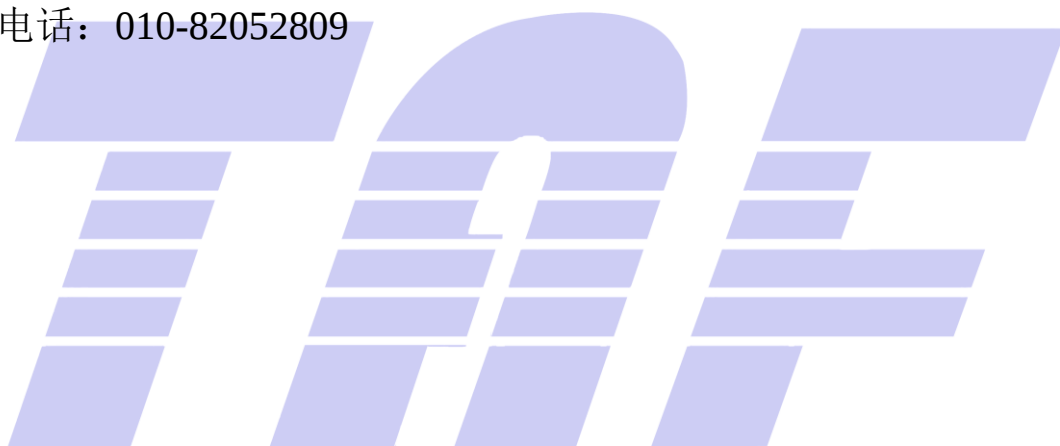


## 版权声明

本文件的版权属于电信终端产业协会，任何单位和个人未经许可，不得进行技术文件的纸质和电子等任何形式的复制、印刷、出版、翻译、传播、发行、合订和宣贯等，也不得未经允许采用其具体内容编制本团体以外各类标准和技术文件。如有以上需要请与本团体联系。

邮箱：tafrb@taf.org.cn

电话：010-82052809





# 目 次

|                              |    |
|------------------------------|----|
| 前言 .....                     | II |
| 1 范围 .....                   | 1  |
| 2 规范性引用文件 .....              | 1  |
| 3 术语和定义 .....                | 1  |
| 4 缩略语 .....                  | 1  |
| 5 测试环境及测试工具 .....            | 2  |
| 5.1 测试样品接口要求 .....           | 2  |
| 5.2 测试样品参数要求 .....           | 2  |
| 5.3 测试样品数量要求 .....           | 3  |
| 6 性能及并发要求（eUICC 部分） .....    | 3  |
| 6.1 概述 .....                 | 3  |
| 6.2 通讯层并发 .....              | 3  |
| 6.3 应用层并发 .....              | 6  |
| 6.4 性能并发测试 .....             | 9  |
| 7 eUICC 隔离安全要求 .....         | 10 |
| 7.1 安全保障 .....               | 10 |
| 7.2 安全功能测试 .....             | 11 |
| 7.3 安全渗透测试 .....             | 20 |
| 8 eUICC NFC 功能通用测试要求 .....   | 20 |
| 附录 A（规范性） 各域和接口测试业务 .....    | 21 |
| 附录 B（规范性） 测试环境配置 .....       | 22 |
| 附录 C（资料性） 脆弱性分析及渗透测试方案 ..... | 23 |

## 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

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专利的责任。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：博鼎实华（北京）技术有限公司、中国信息通信研究院、恩智浦（中国）管理有限公司、北京紫光青藤微系统股份有限公司、北京银联金卡科技有限公司、深圳市汇顶科技股份有限公司、维沃移动通信有限公司、OPPO广东移动通信有限公司、高通无线通信技术（中国）有限公司、华为终端有限公司、荣耀终端股份有限公司、小米通讯技术有限公司、北京三星通信技术研究有限公司、上海泰雷兹智能卡技术有限公司、北京中电华大电子设计有限责任公司、英飞凌科技（中国）有限公司、紫光展锐（上海）科技有限公司、北京握奇数据股份有限公司、北京华弘集成电路设计有限责任公司、梵利特科技（北京）有限公司、捷德（江西）技术有限公司、联发博动科技（北京）有限公司、楚天龙股份有限公司、恒宝股份有限公司、翱捷科技股份有限公司、紫光同芯微电子有限公司、上海优味网络科技有限公司、无锡融卡科技有限公司、东信和平科技股份有限公司、四川科道芯国智能技术股份有限公司、武汉天喻信息产业股份有限公司、深圳信息通信研究院、星汉智能科技股份有限公司、北京兴奥德泰科技有限公司、北京中广瑞波科技股份有限公司、意法半导体（中国）投资有限公司、芯昇科技有限公司。

本文件主要起草人：董霖、邓建国、马凡、刘加、袁琦、田琛、郑琛、杨继堂、张睿杰、张城、张一成、谷有才、陈恒键、施伟周、林国民、王治钦、郑超、张跃、孙金龙、姬闻起、张元、秦冲、张俊、杜志敏、范姝男、赵晓娜、吴越、田鹰、王彬、陈海耘、郝玮琳、赵辉、黄显明、郑煜、李丛蓉、张宇、李中敏、王卫东、帅兰兰、樊妮娜、郭雨鑫、陈宏、刘睿、王韵淇、赵文秀、苏昆、张蕾、肖灵、李维成、龙迪、孙亨博、常志刚、李勋宏、史习阳、余彦飞、魏平姣、郑士超、冯盈盈、黄秋钦、李宇晖、王朋、陈松、梁弋、朱旭东、连莉华、李竞、谢火明、张春辉、陈建辉。

# 多合一 eUICC 芯片并发和安全隔离测试方法

## 1 范围

本文件规定了如何测试验证面向消费电子类产品的多合一eUICC芯片的并发功能要求，以及如何评估其隔离特性的安全保障等级。

本文件适用于多合一eUICC芯片的设计、生产活动，也适用于厂家和第三方评估机构等组织对多合一eUICC芯片的并发和安全隔离测试和评估。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

T/TAF 355—2026 多合一eUICC芯片并发和安全隔离技术要求

GSMA SGP.23 RSP测试方法（Test Specification）V1.16

GSMA SGP.26 RSP测试证书（RSP Test Certificates）V1.5

GSMA SGP.22 RSP技术规范（RSP Technical Specification）V2.5

## 3 术语和定义

下列术语和定义适用于本文件。

### 3.1

**多合一eUICC** Convergence eUICC

eUICC多合一方案，即eUICC物理芯片上除eUICC域外，还支持其他域，如eSE，NFC等等。

### 3.2

**域控制器** Domin Controller

域控制器为多合一eUICC方案中执行域运行时调度，执行安全声明中域隔离访问控制策略，确保域之间安全资产隔离的主体。

### 3.3

**保护轮廓** Protection Profile (PP)

信息技术安全评估准则定义下，用于描述某类信息技术产品所需安全功能和保障要求的标准化、安全性评估规范文件。

### 3.4

**高级系统性脆弱性分析** AVA\_VAN. 5

信息技术安全评估准则中对脆弱性分析的最高安全保障要求。若评估产品存在任何残留攻击，其攻击分值应不小于31分。

## 4 缩略语

下列缩略语适用于本文件。

APDU：应用协议数据单元（Application Protocol Data Unit）

CC: 通用准则 (Common Criteria)

CCRC: 中国网络安全审查技术与认证中心 (China Cybersecurity Review Technology and Certification Center)

COS: 芯片操作系统 (Chip Operating System)

EAL: 评估保障级别 (Evaluation Assurance Level)

eSE: 嵌入式安全元件 (Embedded Secure Element)

eSIM: 嵌入式SIM (Embedded SIM)

eUICC: 嵌入式UICC (Embedded UICC)

I2C: 集成电路总线 (Inter-Integrated Circuit)

ISCCC: 中国信息安全认证中心 (China Information Security Certification Center)

NFC: 近场通信 (Near Field Communication)

OTA: 无线 (Over The Air)

RSP: 远程SIM配置 (Remote Subscription Provisioning)

RAT: 规则授权表 (Rules Authorisation Table)

SAR: 安全保障组件 (Security Assurance Requirement)

SFR: 安全功能组件 (Security Functional Requirement)

SPI: 串行外设接口 (Serial Peripheral Interface)

SUCI: 订阅隐藏标识符 (Subscription Concealed Identifier)

SWP: 单线协议 (Single Wire Protocol)

TOE: 评估目标 (Target of Evaluation)

TSF: TOE安全功能 (TOE Security Functionality)

USIM: 通用用户识别模块 (Universal Subscriber Identity Module)

## 5 测试环境及测试工具

### 5.1 测试样品接口要求

测试样品接口要求如下。

- a) 测试样品应提供支持eUICC操作的ISO/IEC 7816-3接口。
- b) 测试样品应提供支持其他域 (如eSE域) 操作的物理接口, 用于模拟上位机 (如手机、手表) 与该域进行接触或非接触式交互。
  - 对于eSE域, 测试样品应提供支持接触操作的物理接口, 例如OMAPI (Open Mobile API)。
  - 对于eSE域, 测试样品还应提供支持NFC Contactless (CL) 操作的物理接口。

### 5.2 测试样品参数要求

测试样品参数要求如下。

- a) 测试样品的eUICC部分应按如下参数进行配置:
  - ISD-R: 测试样品 eUICC 部分的 ISDR 配置见表 1。

表 1 ISDR 配置

| 内容        | 值                                                  |
|-----------|----------------------------------------------------|
| ISD_R_AID | A0000005591010FFFFFFF8900000100                    |
| 默认 RAT    | A017301580020560A10B30098003EEEEEE8100820082020780 |

- ECASD: 测试样品应参考 GSMA SGP.26 规范, 预置相关密钥及 CI 证书、EUM 证书、eSIM 证书。
  - RAT: RAT 测试需要单独准备 2 个测试样品, 要求标注“RAT 测试”, 并按照 GSMA SGP.23 规范的附录 G 2.1-2.5 章节要求进行参数预置。
  - 其他不需要预置 ISD-P、Profile、MNO-SD。
- b) 测试样品的eSE部分应按如下参数进行配置:
- ISD:
    - ISD AID 为 “A0000001510000”。
    - 应至少支持 SCP02, i=15, security level=0x00, 默认密钥值为 “404142434445464748494A4B4C4D4E4F”。

### 5.3 测试样品数量要求

多合一 eUICC 厂商应提供不少于 10 个测试样品。

## 6 性能及并发要求 (eUICC 部分)

### 6.1 概述

本测试部分的目的是验证eSE域与eUICC域之间的并发通信, 具体目标如下:

- 验证在不同支持的物理通信接口组合下, eSE域与eUICC域之间的并发通信是否正常;
- 并发通信应确保: 分配给eSE域的通信接口上的通信 (无论成功或失败) 不应影响eUICC域上的通信。

注意事项:

在执行本节所描述的并发性测试时, 应对主机计算机模拟器进行校准, 即:

- 能够在特定物理接口上设置APDU间隔的最小值和最大值;
- 并且能够在eSE域业务已发送的APDU达到指定百分比时, 在eUICC域中发起指定的并发操作。

本节所描述的并发测试项目应根据附录B定义的测试环境配置执行, 多合一eUICC厂商应根据自身产品各域接口支持情况适配执行。

### 6.2 通讯层并发

#### 6.2.1 概述

本章节所列测试项的目的是验证eSE侧不同通信接口的指令收发过程 (成功或失败), 不影响eUICC侧的通信接口的指令收发过程。

#### 6.2.2 eUICC ISO7816 接口和 eSE SPI 接口并发测试

在eSE侧, 上位机模拟应用处理器 (AP), 通过SPI接口发送和接收APDU。在eUICC侧, 上位机模拟调制解调器 (Modem), 通过ISO7816接口发送和接收指令。

测试环境配置:

- Test Configuration #1 (参考附录 B);
- 上位机应能够向 eSE 和 eUICC 发送正常有效的 APDU 或错误的 APDU;
- 上位机应能够通过通信接口执行热复位或接口复位。

该测试用例要求如表 2 所示。

表 2 eUICC ISO7816 和 eSE SPI 接口并发测试用例

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_01                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 测试名称 | TC Concurrent Communication over SPI and ISO-7816                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 测试目标 | 在 eSE 和 eUICC 并发通信进行时，eSE SPI 上的业务不应影响 eUICC 的 ISO7816 通信。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 测试条件 | eSE 侧：安装测试 Loopback 应用用于 SPI 接口上重复性操作（支持 short APDU 和 extended APDU）。<br>eUICC 侧：安装并激活含有 Loopback 应用的电信测试 profile（支持 short APDU 和 extended APDU）。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 测试步骤 | 1) 在 eSE 侧：通过 OMAPI/SPI 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 SPI 通信进行中时，在 eUICC 侧通过 ISO7816 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。<br>2) 在 eSE 侧：通过 OMAPI/SPI 接口向 loopback applet 发送扩展 APDU（长度：32767 字节，循环次数：100）或发送短 APDU（长度：255 字节，循环次数：100）。当 SPI 通信进行中时，在 eUICC 侧通过 ISO7816 接口向 loopback applet 发送短 APDU 长度：255 字节，循环次数：100）。<br>3) 在 eUICC 侧：通过 ISO7816 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 eUICC 接口通信进行中时，在 eSE 侧通过 SPI 接口发送错误 APDU（例如：长度错误，循环次数：100）。<br>4) 在 eSE 侧：通过 OMAPI/SPI 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 SPI 通信进行中时，在 eUICC 侧通过 ISO7816 接口执行 Warm Reset（循环次数：100）。<br>5) 在 eUICC 侧：通过 ISO7816 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 eUICC 接口通信进行中时，在 eSE 侧通过 SPI 接口执行接口复位（Interface Reset，循环次数：100）。 |
| 测试结果 | APDU 可在两个域中并发成功收发；<br>eSE OMAPI SPI 接口上的业务错误不应该影响 eUICC ISO7816 接口上的通信；<br>一个接口上的操作不应因另一个接口复位或热复位而受影响。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

6.2.3 eUICC ISO7816 接口和 eSE HCI 接口并发测试

在eSE侧，上位机模拟应用处理器（AP），通过HCI接口发送和接收ETSI HCI指令/事件；在eUICC侧，上位机模拟调制解调器（Modem），通过ISO7816接口发送和接收指令。

测试环境配置：

- Test Configuration #2（参考附录B）；
- 上位机应能够向eSE和eUICC发送正常有效的APDU或错误的APDU；
- 上位机应能够通过通信接口执行热复位或接口复位。

该测试用例要求如表 3 所示。

表 3 eUICC ISO7816 和 eSE HCI 接口并发测试用例

|      |           |
|------|-----------|
| 测试编号 | ISL_CO_02 |
|------|-----------|

表3 eUICC ISO7816 和 eSE HCI 接口并发测试用例 (续)

|      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试名称 | TC Concurrent Communication over HCI and ISO-7816                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 测试目标 | 在 eSE 和 eUICC 并发通信进行时, eSE HCI 通道上的业务不应影响 eUICC 的 ISO7816 通信。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 测试条件 | eSE 侧: 安装测试 Loopback 应用用于 HCI 接口上重复性操作(支持 short APDU 和 extended APDU)。<br>eUICC 侧: 安装并激活含有 Loopback 应用的电信测试 profile(支持 short APDU 和 extended APDU)。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 测试步骤 | <ol style="list-style-type: none"> <li>1) 在 eSE 侧: 通过 HCI 接口向 loopback applet 发送短 APDU (长度: 255 字节, 循环次数: 100)。当 HCI 通信进行中时, 在 eUICC 侧通过 ISO7816 接口向 loopback applet 发送短 APDU (长度: 255 字节, 循环次数: 100)。</li> <li>2) 在 eSE 侧: 通过 HCI 接口向 loopback applet 发送扩展 APDU (长度: 32767 字节, 循环次数: 100) 或发送短 APDU (长度: 255 字节, 循环次数: 100)。当 HCI 通信进行中时, 在 eUICC 侧通过 ISO7816 接口向 loopback applet 发送短 APDU 长度: 255 字节, 循环次数: 100)。</li> <li>3) 或发送短 APDU (长度: 255 字节, 循环次数: 100) eUICC 接口通信进行中时, 在 eSE 侧通过 HCI 接口发送错误 APDU (例如: 长度错误, 循环次数: 100)。</li> <li>4) 在 eSE 侧: 通过 HCI 接口向 loopback applet 发送短 APDU (长度: 255 字节, 循环次数: 100)。当 HCI 通信进行中时, 在 eUICC 侧通过 ISO7816 接口执行 Warm Reset (循环次数: 100)。</li> <li>5) 在 eUICC 侧: 通过 ISO7816 接口向 loopback applet 发送短 APDU (长度: 255 字节, 循环次数: 100)。当 eUICC 接口通信进行中时, 在 eSE 侧通过 HCI 接口执行 Warm Reset (循环次数: 100)。</li> </ol> |
| 测试结果 | APDU 可在两个域中并发成功收发;<br>eSE HCI 接口上的业务错误不应该影响 eUICC ISO7816 接口上的通信;<br>一个接口上的操作不应因另一个接口的复位或热复位而受影响。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

#### 6.2.4 eUICC ISO7816 接口和 NFC 非接接口并发测试

在 eSE 侧, 上位机模拟 NFC 读卡器, 通过 NFC CL 接口发送和接收 ETSI HCI 指令/事件; 在 eUICC 侧, 上位机模拟调制解调器 (Modem), 通过 ISO7816 接口发送和接收指令。

测试环境配置:

- Test Configuration #4 (参考附录 B);
- 上位机应能够向 eSE 和 eUICC 发送正常有效的 APDU 或错误的 APDU;
- 上位机应能够通过通信接口执行热复位或接口复位。

该测试用例要求如表 4 所示。

表4 eUICC ISO7816 和 NFC 非接接口并发测试用例

|      |                                                      |
|------|------------------------------------------------------|
| 测试编号 | ISL_CO_03                                            |
| 测试名称 | TC Concurrent Communication over NFC CL and ISO-7816 |

表 4 eUICC ISO7816 和 NFC 非接接口并发测试用例（续）

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 标准引文  | T/TAF 355—2026 第六章                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 测试目标  | 在 eSE 和 eUICC 并发通信进行时，eSE 通过 NFC 非接通道上的业务不应影响 eUICC 的 ISO7816 通信。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 测试条件  | eSE 侧：安装测试 Loopback 应用用于 NFC 非接接口上重复性操作（支持 short APDU 和 extended APDU）。<br>eUICC 侧：安装并激活含有 Loopback 应用的电信测试 profile（支持 short APDU 和 extended APDU）。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 测试步骤  | <ol style="list-style-type: none"> <li>1) 在 eSE 侧：通过 NFC 非接接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 NFC 通信进行中时，在 eUICC 侧通过 ISO7816 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。</li> <li>2) 在 eSE 侧：通过 NFC 非接接口向 loopback applet 发送扩展 APDU（长度：1024 字节，循环次数：100）或发送短 APDU（长度：255 字节，循环次数：100）。当 NFC 通信进行中时，在 eUICC 侧通过 ISO7816 接口向 loopback applet 发送短 APDU 长度：255 字节，循环次数：100）。</li> <li>3) 在 eUICC 侧：通过 ISO7816 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 eUICC 接口通信进行中时，在 eSE 侧通过 NFC 非接接口发送错误 APDU（例如：长度错误，循环次数：100）。</li> <li>4) 在 eSE 侧：通过 NFC 非接接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 NFC 通信进行中时，在 eUICC 侧通过 ISO7816 接口执行 Warm Reset（循环次数：100）。</li> <li>5) 在 eUICC 侧：通过 ISO7816 接口向 loopback applet 发送短 APDU（长度：255 字节，循环次数：100）。当 eUICC 接口通信进行中时，在 eSE 侧通过非接读卡器对 NFC 非接接口执行 RF 场开关（循环次数：100）。</li> </ol> |
| 测试结果： | APDU 可在两个域中并发成功收发；<br>eSE/NFC 非接接口上的业务错误不应该影响 eUICC ISO7816 接口上的通信；<br>一个接口上的操作不应因另一个接口的复位或热复位而受影响。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## 6.3 应用层并发

### 6.3.1 概述

本章节所列测试项的目的是验证 eSE 侧不同业务的处理过程（成功或失败），不影响 eUICC 侧各项业务的处理过程。

### 6.3.2 ISO7816 接口上 eUICC 应用和 SPI 接口上 eSE 应用并发测试

在 eSE 侧，上位机模拟应用处理器（AP），通过 SPI 接口发送和接收 OMAPI APDU。在 eUICC 侧，上位机模拟调制解调器（Modem），通过 ISO7816 接口发送和接收指令。

测试环境配置：

- Test Configuration #1（参考附录 B）；
- eSE 通过 SPI 接口连接上位机；
- eUICC 通过 ISO7816 接口连接上位机模拟 modem。

该测试用例要求如表 5、表 6 所示。

表 5 ISO7816 接口上 eUICC 应用和 SPI 接口上 eSE 应用并发测试用例-1

|       |                                                                                                                                                                                                                                                                                  |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号: | ISL_CO_04-1                                                                                                                                                                                                                                                                      |
| 测试名称: | TC eUICC-application concurrency with eSE application operations over SPI                                                                                                                                                                                                        |
| 标准引文: | T/TAF 355—2026 第六章                                                                                                                                                                                                                                                               |
| 测试目标: | 在 eSE 和 eUICC 业务同时进行, eSE SPI 上的业务不应影响 eUICC 的 ISO7816 上的业务。                                                                                                                                                                                                                     |
| 测试条件  | eSE 侧: 安装测试 Loopback 应用用于 SPI 接口上重复性操作(支持 short APDU 和 extended APDU)。<br>eUICC 侧: 下载含指定电信功能的 profile。                                                                                                                                                                           |
| 测试步骤: | 1) eSE 侧: 在 SPI 接口上选 loopback applet, 然后持续发送多条 loopback APDUs。<br>2) eUICC 侧: 当 eSE 侧 30%的 APDUs 已发送和接收时, 在 ISO7816 接口上开启业务(详见附录 A 表 A.2)。<br>3) 在 eSE 侧继续执行到 50%时, 在 eUICC 侧在 ISO7816 接口上开启业务(详见附录 A 表 A.2)。<br>4) 在 eSE 侧继续执行到 80%时, 在 eUICC 侧在 ISO7816 接口上开启业务(详见附录 A 表 A.2)。 |
| 测试结果: | 从步骤 2 开始检测 eUICC 在并发场景下所执行的所有业务都能执行成功或者延迟执行成功。                                                                                                                                                                                                                                   |

表 6 ISO7816 接口上 eUICC 应用和 SPI 接口上 eSE 应用并发测试项-2

|      |                                                                                                                                         |
|------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_04-2                                                                                                                             |
| 测试名称 | TC eUICC-application concurrency with eSE application operations over SPI                                                               |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                      |
| 测试目标 | 在 eSE 和 eUICC 业务同时进行, eSE SPI 上的业务不应影响 eUICC 的 ISO7816 上的业务。                                                                            |
| 测试条件 | eSE 侧: 在 SPI 接口上选 ISD。<br>eUICC 侧: 下载含指定电信功能的 profile。                                                                                  |
| 测试步骤 | 1) eSE 侧: 执行 GlobalPlatform 内容管理和应用相关操作(附详见附录 A 表 A.1), 循环次数为 10。<br>2) eUICC 侧: 当 eSE 侧的步骤 1 业务正在进行时, 在 ISO7816 接口上开启业务(详见附录 A 表 A.2)。 |
| 测试结果 | 从步骤 2 开始检测 eUICC 在并发场景下所执行的所有业务都能执行成功或者延迟执行成功。                                                                                          |

6.3.3 ISO7816 接口上 eUICC 应用和 HCI 接口上 eSE 应用并发测试

在eSE侧, 上位机模拟应用处理器 (AP), 通过HCI接口发送和接收ETSI HCI APDU。在eUICC侧, 上位机模拟调制解调器 (Modem), 通过ISO7816接口发送和接收指令。

测试环境配置：

- Test Configuration #2（参考附录B）；
  - eSE通过HCI接口连接上位机；
  - eUICC通过ISO7816接口连接上位机模拟modem。
- 该测试用例要求如表 7、表 8 所示。

表 7 ISO7816 接口上 eUICC 应用和 HCI 接口上 eSE 应用并发测试用例-1

|      |                                                                                                                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_05-1                                                                                                                                                                                                                                                                         |
| 测试名称 | TC eUICC-application concurrency with eSE application operations over HCI                                                                                                                                                                                                           |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                                                                                                                                                                  |
| 测试目标 | 在 eSE 和 eUICC 业务同时进行，eSE HCI 上的业务不应影响 eUICC 的 ISO7816 上的业务。                                                                                                                                                                                                                         |
| 测试条件 | eSE 侧：安装测试 Loopback 应用用于 HCI 接口上重复性操作（需要定义应用的 short/extended APDUs）。<br>eUICC 侧：下载含指定电信功能的 profile。                                                                                                                                                                                 |
| 测试步骤 | 1) eSE 侧：在 HCI 接口上选 loopback applet，然后持续发送多条 loopback APDUs。<br>2) eUICC 侧：当 eSE 侧 30%的 APDUs 已发送和接收时，在 ISO7816 T0 接口上开启业务（详见附录 A 表 A.2）。<br>3) 在 eSE 侧继续执行到 50%时，在 eUICC 侧在 ISO7816 T0 接口上开启业务（详见附录 A 表 A.2）。<br>4) 在 eSE 侧继续执行到 80%时，在 eUICC 侧在 ISO7816 T0 接口上开启业务（详见附录 A 表 A.2）。 |
| 测试结果 | 从步骤 2 开始检测 eUICC 在并发场景下所执行的所有业务都能执行成功或者延迟执行成功。                                                                                                                                                                                                                                      |

表 8 ISO7816 接口上 eUICC 应用和 HCI 接口上 eSE 应用并发测试用例-2

|      |                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_05-2                                                                                                                         |
| 测试名称 | TC eUICC-application concurrency with eSE application operations over HCI                                                           |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                  |
| 测试目标 | 在 eSE 和 eUICC 业务同时进行，eSE HCI 上的业务不应影响 eUICC 的 ISO7816 上的业务。                                                                         |
| 测试条件 | eSE 侧：在 HCI 接口上选 ISD。<br>eUICC 侧：下载含指定电信功能的 profile。                                                                                |
| 测试步骤 | 1) eSE 侧：执行 GlobalPlatform 内容管理和应用相关操作（附详见附录 A 表 A.1），循环次数为 10。<br>2) eUICC 侧：当 eSE 侧的步骤 1 业务正在进行时，在 ISO7816 接口上开启业务（详见附录 A 表 A.2）。 |
| 测试结果 | 从步骤 2 开始检测 eUICC 在并发场景下所执行的所有业务都能执行成功或者延迟执行成功。                                                                                      |

### 6.3.4 ISO7816 接口上 eUICC 应用和 NFC 非接业务并发测试

在eSE侧，上位机模拟应用处理器（AP），通过NFC非接口执行业务。在eUICC侧，上位机模拟调制解调器（Modem），通过ISO7816接口发送和接收指令。

测试环境配置：Test Configuration #3（参考附录B）。

该测试用例要求如表 9 所示。

表 9 ISO7816 接口上 eUICC 应用和 NFC 非接业务并发测试用例

|      |                                                                                                                                                                            |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_06                                                                                                                                                                  |
| 测试名称 | TC eUICC-application concurrency with NFC Services                                                                                                                         |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                                                         |
| 测试目标 | 在 eSE 非接业务和 eUICC 业务同时进行，eSE NFC 非接上的业务不应影响 eUICC 的 ISO7816 上的业务。                                                                                                          |
| 测试条件 | eUICC 侧：在 ISO7816 接口上开启业务（详见附录 A 表 A.2），同时 eSE 侧：在 NFC 接口上开启非接业务（详见附录 A 表 A.3）。                                                                                            |
| 测试步骤 | 1) eUICC 侧：当 eSE/NFC 侧 30%的 APDUs 已发送和接收时，在 ISO7816 接口上开启业务（详见附录 A 表 A.2）。<br>2) 在 eSE 侧继续执行到 50%时，在 eUICC 侧继续执行步骤 2 上述操作。<br>3) 在 eSE 侧继续执行到 80%时，在 eUICC 侧继续执行步骤 2 上述操作。 |
| 测试结果 | 从步骤 1 开始检测 eUICC 在并发场景下所执行的所有操作都能执行成功或者延迟执行成功。                                                                                                                             |

## 6.4 性能并发测试

本章节所列测试项的目的，是验证在以下两种条件下，eUICC侧各项业务的处理时序性能：

- 条件 1：eSE 空闲，即eSE没有任何操作正在进行；
- 条件 2：eSE 繁忙，即eSE正在进行通信操作。

注意事项：由于一体化eUICC的处理时间可能与独立式eUICC不同，因此测试结果仅可用于验证是否满足运营商对最大处理时间的要求。

测试环境配置：

- Test Configuration #1（参考附录B）；
- eSE通过SPI接口连接上位机；
- eUICC通过ISO7816接口连接上位机模拟modem。

该测试用例要求如表 10、表 11 所示。

表 10 eSE 应用并发下 ISO7816 接口上 eUICC 应用性能测试用例-1

|      |                                                                                            |
|------|--------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_07                                                                                  |
| 测试名称 | TC eUICC-performance in concurrency mode with eSE application operations over SPI          |
| 标准引文 | T/TAF 355—2026 第六章                                                                         |
| 测试目标 | 在 eSE 和 eUICC 业务同时进行，检测 eUICC 在 ISO7816 上的业务性能相较于 eUICC 单独执行业务时的性能，不应受 eSE 在 SPI 接口上的业务影响。 |

表 10 eSE 应用并发下 ISO7816 接口上 eUICC 应用性能测试用例-1（续）

|      |                                                                                                                                                                                                                                                  |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试条件 | eSE 侧: 安装测试 Loopback 应用用于 SPI 接口上重复性操作(需要定义应用的 short/extended APDUs)。<br>eUICC 侧: 下载含指定电信功能的 profile。                                                                                                                                            |
| 测试步骤 | 1) eUICC 侧: 在 ISO7816 接口开启业务（详见附录 A 表 A.2），运行 100 次循环，并测量业务的时间性能。<br>2) eSE 侧: 通过 SPI 接口向 loopback applet 连续发送短 APDU（长度: 128 字节）。<br>3) 在步骤 2 进行过程中: 在 eUICC 侧再次运行 100 次循环测试，测量 eUICC 业务的时间性能（附录 A 表 A.2）。<br>4) 比较步骤 1 和步骤 3 中测得的 eUICC 业务时间性能。 |
| 测试结果 | 测量 eUICC 业务在独立模式和并发模式下的性能，且确保性能偏差不得超过 20%。                                                                                                                                                                                                       |

表 11 eSE 应用并发下 ISO7816 接口上 eUICC 应用性能测试用例-2

|      |                                                                                                                                                                                                           |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ISL_CO_08                                                                                                                                                                                                 |
| 测试名称 | TC eUICC-Algorithm-performance in concurrency mode with eSE application operations over SPI                                                                                                               |
| 标准引文 | T/TAF 355—2026 第六章                                                                                                                                                                                        |
| 测试目标 | 在 eSE 和 eUICC 业务同时进行，检测 eUICC 在 ISO7816 上的业务性能相较于 eUICC 单独执行业务时的性能，不应受 eSE 在 SPI 接口上的业务影响。                                                                                                                |
| 测试条件 | eSE 侧: 安装测试 Loopback 应用用于 SPI 接口上重复性操作(需要定义应用的 short/extended APDUs)。<br>eUICC 侧: 下载含指定电信功能的 profile。                                                                                                     |
| 测试步骤 | 1) eSE 侧: 通过 SPI 接口向 loopback applet 连续发送短 APDU（长度: 128 字节）。<br>2) eUICC 侧: 在 ISO7816 接口开启各算法测试业务（详见附录 A 表 A.2），运行 3000 次循环，对 3000 次的总时间计算算术平均值，得出各算法相应的性能计算结果。<br>3) 比较步骤 2 和标准引文附录 A 对 eUICC 并行业务的时间性能。 |
| 测试结果 | 测量 eUICC 业务在并发模式下的性能，且确保性能宜符合标准引文参考要求。                                                                                                                                                                    |

7 eUICC 隔离安全要求

7.1 安全保障

本部分主要是对eUICC TSF开发人员提供的保障类文档进行评估，评估者应对文档内的内容和形式是否满足eUICC隔离安全要求进行充分的评估。

开发人员应提供至少下述文档，且文档保障组件中针对域隔离安全具有相应描述，安全保障类组件和保障类文档之间的关系满足见表12。

表 12 安全保障类、组件和文档对应关系

| 要求的安全保障类 | 要求的安全保障组件 | 保障类文档  |
|----------|-----------|--------|
| ASE      | ASE_INT.1 | 《安全目标》 |
|          | ASE_CCL.1 | 《安全目标》 |

表 12 安全保障类、组件和文档对应关系（续）

| 要求的安全保障类                                                                                | 要求的安全保障组件                                                                                     | 保障类文档    |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|----------|
| ASE                                                                                     | ASE_SPD.1                                                                                     | 《安全目标》   |
|                                                                                         | ASE_OBJ.2                                                                                     | 《安全目标》   |
|                                                                                         | ASE_ECD.1                                                                                     | 《安全目标》   |
|                                                                                         | ASE_REQ.2                                                                                     | 《安全目标》   |
|                                                                                         | ASE_TSS.1                                                                                     | 《安全目标》   |
| ADV                                                                                     | ADV_FSP.4<br>应用说明：此组件不适用。域隔离是 TSF 内部的特性。但是，如果 OE.DOMAINS 所选为选项二时除外，此时开放给第三方开发者的域的接口，也属于 TSFI。 | 《功能规范》   |
|                                                                                         | ADV_IMP.1                                                                                     | 《实现表示》   |
|                                                                                         | ADV_ARC.1                                                                                     | 《安全架构》   |
|                                                                                         | ADV_TDS.3                                                                                     | 《模块设计》   |
| AGD<br>应用说明：此组件不适用。域隔离是 TSF 内部的特性。但是，如果 OE.DOMAINS 所选为选项二时除外，此时开放给第三方开发者的域的接口，也属于 TSFI。 | —                                                                                             | —        |
| ALC<br>应用说明：域隔离从属于 eUICC 评估范围内，因此其声明周期已在 eUICC 产品评估时覆盖。无需额外工作。                          | —                                                                                             | —        |
| ATE                                                                                     | ATE_COV.2                                                                                     | 《测试覆盖分析》 |
|                                                                                         | ATE_DPT.2                                                                                     | 《测试深度分析》 |
|                                                                                         | ATE_FUN.1                                                                                     | 《功能测试》   |
|                                                                                         | ATE_IND.2                                                                                     | 《功能测试》   |
| AVA                                                                                     | AVA_VAN.5                                                                                     | —        |

高级的系统的脆弱性攻击，见附录 C。

## 7.2 安全功能测试

### 7.2.1 概述

在通用安全评估准则中，安全功能测试类（ATE）规定了为验证产品是否达到所宣称的安全要求，供应商应提供的材料以及测试实验室应做的分析。为更好的规范本文档对测试的要求，本文档针对多合一 eUICC 域隔离，提出具体测试用例建议。供应商所准备 ATE 评估材料，应在具体测试项中覆盖定义于章节 7.2.2 中的测试用例。

应用说明：本章节中所建议的测试用例，供应商应根据实际产品情况，定义一个或多个实际测试用例共同佐证。

## 7.2.2 安全功能测试用例

本章节的安全测试用例，定义了功能安全测试用例标识，明确了功能安全测试用例目标，大致步骤，以及预期结果。在供应商具体提供的测试报告中，供应商应基于自身产品技术，细化相应测试步骤描述及实际测试结果。

该安全功能测试用例要求如下列表 13～表 28 所示。

表 13 eUICC 配置文件隔离-1

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_01                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 测试名称   | eUICC 配置文件（PROFILE_DATA-用户内存对象）隔离                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 测试目标   | eUICC 用户数据资产（Profile Data-用户内存对象），在 T/TAF 355—2026 中定义，只能分配或取消分配在属于 eUICC 域的内存中，不能被其他域访问。也就是说，任何在 eSE 域上的操作（如内存分配、释放、加密）都不得“更改”这些数据。                                                                                                                                                                                                                                                                                                                               |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。创建一个 2KB 的字节数组，并填充定义的数据（0xFFFF...）。</li> </ol> </li> <li>2. eUICC 域： <ol style="list-style-type: none"> <li>a. 通过 ISO7816 T0/T1 接口个性化 ISDR，安装并启用配置文件。</li> <li>b. 在接触接口上安装并选择类似的基于 Java 的小程序（“B”）。创建一个 2KB 的字节数组，并填充定义的数据（0xABABAB...）。</li> </ol> </li> <li>3. eSE 域：将字节数组更新为（0x1212121212）</li> <li>4. eUICC 域：读取字节数组——应保持不变。</li> </ol> |
| 预期测试结果 | 当在 eSE 域访问内存对象时，不得访问 eUICC 域中的内存对象。                                                                                                                                                                                                                                                                                                                                                                                                                                |

表 14 eUICC 配置文件隔离-2

|        |                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_02                                                                                                                                                                                                                                                                                                                                                                      |
| 测试名称   | eUICC 配置文件（PROFILE_DATA-用户数据 PIN 对象）隔离                                                                                                                                                                                                                                                                                                                                               |
| 测试目标   | eUICC 用户数据资产（Profile Data - 用户数据 PIN 对象），在 T/TAF 355—2026 中定义，只能分配或取消分配在属于 eUICC 域的内存中，不能被其他域访问。也就是说，任何在 eSE 域上的操作（如内存分配、释放、Global Platform/JavaCard 操作或加密操作）都不得“更改”这些数据。                                                                                                                                                                                                            |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eSE 域： <ol style="list-style-type: none"> <li>a. 安装基于 Java 的小程序（“A”），创建 PIN 并设置 PIN。</li> </ol> </li> <li>2. eUICC 域： <ol style="list-style-type: none"> <li>a. 通过 ISO7816 T0/T1 接口个性化 ISDR。安装基于 Java 的小程序（“B”），创建 PIN 并设置 PIN。</li> </ol> </li> <li>3. eSE 域：输入错误 PIN（3 次）；PIN 应被锁定。</li> <li>4. eUICC 域：使用正确的 PIN 验证；PIN 应被接受</li> </ol> |
| 预期测试结果 | 当在 eSE 域访问 PIN 对象时，不能访问 eUICC 域中的内存对象。                                                                                                                                                                                                                                                                                                                                               |

表 15 eUICC 配置文件隔离-3

|        |                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_03                                                                                                                                                                                                                                                                                            |
| 测试名称   | eUICC 配置文件（PROFILE_DATA-用户数据 Applet 加密对象）隔离                                                                                                                                                                                                                                                                |
| 测试目标   | eUICC TSF 数据资产（Profile Data-用户加密对象），在 T/TAF 355—2026 中定义，只能分配或取消分配在属于 eUICC 域的内存中，不能被其他域访问。也就是说，任何在 eSE 域上的操作（如内存分配、释放、Global Platform/JavaCard 操作或加密操作）都不得“更改”这些数据。                                                                                                                                       |
| 测试步骤   | <p>1. eSE 域：</p> <p>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。</p> <p>b. 创建 AES 密钥（128 字节）并完成初始化。</p> <p>2. eUICC 域：</p> <p>a. 通过 ISO7816 T0/T1 接口个性化 ISDR，安装并启用配置文件。</p> <p>b. 在接触接口上安装并选择基于 Java 的小程序（“B”）。</p> <p>c. 创建 AES 密钥（256 字节）并完成初始化。</p> <p>3. eSE 域：删除 AES 密钥。</p> <p>4. eUICC 域：AES 密钥应可用于加密/解密操作。</p> |
| 预期测试结果 | eUICC 域：AES 密钥应可用于加密/解密，并且不得被 eSE 域更改。                                                                                                                                                                                                                                                                     |

表 16 eUICC 配置文件隔离-4

|        |                                                                                                                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_04                                                                                                                                                                                                                                                                     |
| 测试名称   | eUICC 配置文件（运行时代码和数据）隔离                                                                                                                                                                                                                                                              |
| 测试目标   | eUICC TSF 数据资产（运行时操作），在 T/TAF 355—2026 中定义，只能分配或取消分配在属于 eUICC 域的内存中，不能被其他域访问。也就是说，任何在 eSE 域上的操作（如内存分配、释放、Global Platform/JavaCard 操作或加密操作）都不得“更改”这些数据。                                                                                                                              |
| 测试步骤   | <p>1. eUICC 域：</p> <p>a. 在循环中执行 RSP 操作（包括各种配置文件下载和配置文件删除操作）。循环次数为 10。注意：上述操作将触发 eUICC TSF 代码的运行时代码执行，包括针对运行时数据（如 Global Platform 注册表数据）的垃圾回收，以及 eUICC 域内存访问（分配和访问）。</p> <p>2. eSE 域：在 1.a eUICC 操作循环中，执行 eSE 小程序的加载和删除操作。注意：上述操作将触发 eSE 域代码的运行时代码执行，包括垃圾回收，以及 eSE 域内存访问（分配和访问）。</p> |
| 预期测试结果 | eSE 和 eUICC 域的运行时代码和数据应独立处理，且不得影响其他域。                                                                                                                                                                                                                                               |

表 17 eUICC 配置文件隔离-5

|      |                                                                                                                                                                                                                   |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ATE_TestCase_05                                                                                                                                                                                                   |
| 测试名称 | eUICC 配置文件（PROFILE_DATA-NAA 参数）隔离                                                                                                                                                                                 |
| 测试目标 | 通过配置文件数据在配置文件下载后（无论处于启用或禁用状态）存储的 NAA 参数不得因 eSE 域上的任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或 Java 加密操作）而被“更改”，并且依赖于 NAA 参数的 eUICC 注网操作（即 Tuak128 位、Tuak256 位、Milenage-2G、Milenage-3G、5G SUCI-Identity（A/B））应能够无缝工作。 |

表 17 eUICC 配置文件隔离-5（续）

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。</li> <li>b. 创建 AES 密钥（128 字节）并初始化。</li> </ol> </li> <li>2. eUICC 域： <ol style="list-style-type: none"> <li>a. 通过 ISO7816 T0/T1 接口个性化 ISDR。安装并启用支持不同 eUICC 注网操作的配置文件（即 Tuak 128 位、Tuak 256 位、Milenage-2G、Milenage-3G、5G-SUCI 配置文件（A/B））。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 基于 Tuak-128 位算法执行 eUICC 注网，循环次数为 10。</li> <li>b. 当（3.a）在 eUICC 域进行时，在 eSE 域创建 AES 密钥（128 字节）、初始化并删除密钥。</li> </ol> </li> <li>4. <ol style="list-style-type: none"> <li>a. eUICC 域：基于 Tuak-256 位算法执行 eUICC 注网，循环次数为 10。</li> <li>b. eSE 域：当（4.a）在进行时，创建 AES 密钥（128 字节）、初始化并删除密钥。</li> </ol> </li> <li>5. <ol style="list-style-type: none"> <li>a. eUICC 域：基于 Milenage-2G 算法执行 eUICC 注网，循环次数为 10。</li> <li>b. eSE 域：当（5.a）在进行时，创建 AES 密钥（128 字节）、初始化并删除密钥。</li> </ol> </li> <li>6. <ol style="list-style-type: none"> <li>a. eUICC 域：基于 Milenage-3G 算法执行 eUICC 注网，循环次数为 10。</li> <li>b. eSE 域：当（6.a）在进行时，创建 AES 密钥（128 字节）、初始化并删除密钥。</li> </ol> </li> <li>7. <ol style="list-style-type: none"> <li>a. eUICC 域：基于 5G SUCI-Profile A 算法执行 eUICC 注网，循环次数为 10。</li> <li>b. eSE 域：当（7.a）在进行时，创建 AES 密钥（128 字节）、初始化并删除密钥。</li> </ol> </li> <li>8. <ol style="list-style-type: none"> <li>a. eUICC 域：基于 5G SUCI-Profile B 算法执行 eUICC 注网，循环次数为 10。</li> <li>b. eSE 域：当（8.a）在进行时，创建 AES 密钥（128 字节）、初始化并删除密钥。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，基于 NAA 参数的 eUICC 注网操作应成功执行，并且不应因在 eSE 域中进行的加密操作而受到影响                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

表 18 eUICC 配置文件隔离-6

|      |                                                                                                                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ATE_TestCase_06                                                                                                                                                                                                                                                                                                                                               |
| 测试名称 | eUICC 配置文件（PROFILE DATA 配置文件标识）隔离                                                                                                                                                                                                                                                                                                                             |
| 测试目标 | 在配置文件下载后（无论处于启用或禁用状态），eSIM 配置文件标识 IMSI（国际移动用户识别码）不得因 eSE 域上的任何操作（内存分配、释放、加密）而被“更改”。                                                                                                                                                                                                                                                                           |
| 测试步骤 | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 下载 3 个 GSMA TS.48 eUICC（eSIM）测试配置文件（P1、P2、P3），每个配置文件具有不同的 ICCD 和 IMSI 值。</li> <li>b. 启用配置文件 P1。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。创建一个 2KB 的字节数组，并填充定义的数据（0xFFFF...）。</li> </ol> </li> </ol> |

表 18 eUICC 配置文件隔离-6（续）

|        |                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试步骤   | <p>3. eUICC 域:</p> <p>a. 检查配置文件 P1 是否已启用。</p> <p>b. 执行配置文件切换, 从配置文件 P1→配置文件 P2。</p> <p>c. 检查配置文件 P2 是否已启用。</p> <p>4. eSE 域:</p> <p>a. 安装并选择另一个基于 Java 的小程序 (“B”)。</p> <p>b. 创建 AES 密钥 (256 字节) 并初始化。</p> <p>5. eUICC 域:</p> <p>a. 检查配置文件 P2 是否已启用。</p> <p>b. 执行配置文件切换, 从配置文件 P2→配置文件 P3。</p> <p>6. eSE 域:</p> <p>a. 删除基于 Java 的小程序 (“A”) 和 (“B”)。</p> <p>7. eUICC 域:</p> <p>a. 检查配置文件 P3 是否已启用。</p> |
| 预期测试结果 | 在 eUICC 域中, 配置文件的 P3 值不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                            |

表 19 eUICC 配置文件隔离-7

|        |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_07                                                                                                                                                                                                                                                                                                                                                                                                          |
| 测试名称   | eUICC 配置文件 (Profile Data-配置文件策略规则 (PPR)) 隔离                                                                                                                                                                                                                                                                                                                                                                              |
| 测试目标   | 配置文件策略规则 (Profiles Policy Rules), 在配置文件下载过程中应用或通过 OTA 操作更新后, 不得被 eSE 域上的任何操作 (如内存分配、释放、Global Platform/JavaCard 操作或加密操作) “更改”, 并且依赖 PPR 的 eUICC 功能 (例如配置文件的启用/禁用/删除) 应能无缝工作。                                                                                                                                                                                                                                             |
| 测试步骤   | <p>1. eUICC 域:</p> <p>a. 下载带有配置文件策略规则 (PPR) 的 GSMA TS.48 eUICC (eSIM) 测试配置文件 (规则存储在配置文件的元数据中)。</p> <p>b. 启用配置文件。</p> <p>2. eSE 域:</p> <p>a. 在接触接口上安装并选择基于 Java 的小程序 (“A”)。</p> <p>b. 创建 AES 密钥 (256 字节) 并初始化。</p> <p>3. eUICC 域:</p> <p>a. 通过 SCP81 OTA 操作, 使用 StoreMetadata 或 Update Meta Data 命令更新配置文件的 PPR。</p> <p>4. eSE 域:</p> <p>a. 删除基于 Java 的小程序 (“A”) 和 (“B”)。</p> <p>5. eUICC 域:</p> <p>a. 检查配置文件的 PPR 数据。</p> |
| 预期测试结果 | 在 eUICC 域中, 配置文件的 PPR 值不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                                                |

表 20 eUICC 配置文件数据隔离

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_08                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 测试名称   | eUICC（配置文件数据 - D.profile.code）隔离                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 测试目标   | MNO-SD/CASD/SSD/任何配置文件特定应用及其配置文件文件系统不得因 eSE 域上的任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）而被“更改”，并且 eUICC 功能应能够无缝工作。                                                                                                                                                                                                                                                                                                                                   |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 下载 GSMA TS.48 eUICC（eSIM）测试配置文件。</li> <li>b. 启用配置文件。</li> <li>c. 安装并个性化 CASD。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。</li> <li>b. 创建 AES 密钥（256 字节）并初始化。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 在 MNO SD/CASD 上执行 Amendment A 场景。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，MNO SD/CASD 的状态和数据不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                                                                          |

表 21 eUICC 管理数据隔离-1

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_09                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 测试名称   | eUICC（管理数据-D.PLATFORM_DATA）隔离                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 测试目标   | 平台标识符（如 SM-DS OID、MNO OID、SM-DP+OID、ISDP 安全域生命周期）不得因任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）在 eSE 域上被“更改”，并且 eUICC 功能应无缝运行。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 下载 GSMA TS.48 eUICC（eSIM）测试配置文件。</li> <li>b. 启用配置文件 P1。</li> <li>c. MNO SD 已个性化。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 安装基于 Java 的小程序（“A”），并创建 PIN 并设置该 PIN。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 检查 MNO-SD 状态是否为已个性化。</li> <li>b. 将 MNO-SD 状态更改为终止状态。</li> </ol> </li> <li>4. eSE 域： <ol style="list-style-type: none"> <li>a. 设置不同的 PIN 值。</li> </ol> </li> <li>5. eUICC 域： <ol style="list-style-type: none"> <li>a. 检查 MNO-SD 状态，应为终止状态。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，MNO SD 的状态和数据不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

表 22 eUICC 管理数据隔离-2

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_10                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 测试名称   | eUICC（管理数据-Device Info）隔离                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 测试目标   | 设备信息数据中的安全敏感元素，例如设备类型分配码（TAC）或设备能力（如支持更新证书吊销列表（CRLs）等），这些由 LPA 共享给 eUICC 的数据不得因 eSE 域上的任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）而被“更改”，并且 eUICC 功能应能够无缝工作。                                                                                                                                                                                                                                                                             |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 下载 GSMA TS.48 eUICC（eSIM）测试配置文件（下载中 LPA 提供 IMEI 数据中的类型分配码（TAC））。</li> <li>b. 启用配置文件 P1。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 安装基于 Java 的小程序（“A”），并创建 PIN 并设置该 PIN。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 检查在 AuthenticateServer 响应中返回的 TAC 值。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，TAC 的值不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                                                                        |

表 23 eUICC 管理数据隔离-3

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号：  | ATE_TestCase_11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 测试名称   | eUICC（管理数据-Platform RAT）隔离                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 测试目标   | eUICC 的规则授权表（RAT）不得因任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）在 eSE 域上被“更改”，并且 eUICC 功能（用于在配置文件下载、启用、禁用、删除、内存重置操作中强制执行配置文件策略规则）应无缝运行。                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. eUICC 在初始内部构建 RAT，通过 ISDR 读取 RAT 值。</li> <li>b. 发送 PrepareDownload 以下载 GSMA TS.48 eUICC（eSIM）测试配置文件，配置文件元数据包含配置文件策略规则（PPR）。</li> <li>c. 启用配置文件 P1。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。</li> <li>b. 创建 AES 密钥（256 字节）并初始化。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 检查在 GetProfilesInfo（ES10b）响应中返回的 PPR 值。</li> <li>b. 再次从 ISDR 读取检查 RAT 值。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，RAT 的值不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

表 24 eUICC 身份管理数据隔离-1

|      |                                        |
|------|----------------------------------------|
| 测试编号 | ATE_TestCase_12                        |
| 测试名称 | eUICC（身份管理数据-eUICC Identity / D.EID）隔离 |

表 24 eUICC 身份管理数据隔离-1（续）

|        |                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试目标   | eUICC 身份 (EID) 由 eUICC 制造商设置，在 eUICC 的整个运行生命周期内不得更改，并且不得因任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）在 eSE 域上被“更改”，并且应无缝运行。                                                                                                                                                                                                                                                                  |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 从 ISDR 读取 EID（在 eUICC 制造和个性化过程中设置）。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。</li> <li>b. 创建 AES 密钥（256 字节）并初始化。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 再次从 ISDR 读取 EID。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，EID 的值不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                           |

表 25 eUICC 身份管理数据隔离-2

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_13                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 测试名称   | eUICC（身份管理数据-D.SK.EUICC.ECDSA（eUICC 私钥）隔离）eUICC（身份管理数据-eUICC Identity / D.EID）隔离                                                                                                                                                                                                                                                                                                                                                                                                               |
| 测试目标   | eUICC 私钥不得因 eSE 域上的任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）而被“更改”，并且在 eUICC 上与远程实体生成共享密钥/生成用于双向认证的签名应能够无缝工作。                                                                                                                                                                                                                                                                                                                                                                              |
| 测试步骤   | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 使用 GetEuiccInfo（ES10c）检索证书链。</li> <li>b. 检查 D.PK.CI.ECDSA 的 SKID（个性化过程中生成）。</li> </ol> </li> <li>2. eSE 域： <ol style="list-style-type: none"> <li>a. 在接触接口上安装并选择基于 Java 的小程序（“A”）。</li> <li>b. 创建 AES 密钥（256 字节）并初始化。</li> </ol> </li> <li>3. eUICC 域： <ol style="list-style-type: none"> <li>a. 触发 RSP 会话并验证 eUICC 证书是否出现在 AuthenticatServer（ES10b）响应里并检查 eUICC 证书里签名一致性。</li> </ol> </li> </ol> |
| 预期测试结果 | 在 eUICC 域中，eUICC 证书和 D.SK.EUICC.ECDSA 的值不得因 eSE 操作而被更改或影响。                                                                                                                                                                                                                                                                                                                                                                                                                                     |

表 26 eUICC 身份管理数据隔离-3

|      |                                                                                                                                                                                                 |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ATE_TestCase_14                                                                                                                                                                                 |
| 测试名称 | eUICC（身份管理数据-D.PK.CI.ECDSA（eUICC CA 公钥）隔离）                                                                                                                                                      |
| 测试目标 | eSIM CA 公钥（D.PK.CI.ECDSA）不得因任何操作（内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作）在 eSE 域上被“更改”，并且其在验证 eUICC 和远程实体的证书链中的使用应无缝运行。                                                                         |
| 测试步骤 | <ol style="list-style-type: none"> <li>1. eUICC 域： <ol style="list-style-type: none"> <li>a. 使用 GetEuiccInfo（ES10c）检索证书链。</li> <li>b. 检查 D.PK.CI.ECDSA 的 SKID（个性化过程中生成）。</li> </ol> </li> </ol> |

表 26 eUICC 身份管理数据隔离-3 (续)

|        |                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试步骤   | 2. eSE 域:<br>a. 基于 Java 的小程序 (“A”) 通过接触接口安装并被选中。<br>b. 创建 AES 密钥 (256 字节) 并初始化该密钥。<br>3. eUICC 域:<br>a. 触发 RSP 会话, 在 RSP 操作期间使用指定的 PK.CI.ECDSA 验证服务器证书及签名。 |
| 预期测试结果 | 在 eUICC 域中的 D.PK.CI.ECDSA 的值不会因 eSE 域的操作被更改或影响。                                                                                                            |

表 27 eUICC 身份管理数据隔离-4

|        |                                                                                                                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号   | ATE_TestCase_15                                                                                                                                                                                                                                                                                                                                                        |
| 测试名称   | eUICC (身份管理数据-D.SECRETS 隔离)                                                                                                                                                                                                                                                                                                                                            |
| 测试目标   | eSIM CA 公钥 (D.PK.CI.ECDSA) 不得因任何操作 (内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作) 在 eSE 域上被 “更改”, 并且其在验证 eUICC 和远程实体的证书链中的使用应无缝运行。                                                                                                                                                                                                                                          |
| 测试步骤   | 1. eUICC 域:<br>a. 下载 GSMA TS.48 eUICC (eSIM) 测试配置文件, 在 RSP 会话过程中生成 otSK.EUICC.ECKA、otPK.EUICC.ECKA。<br>2. eSE 域:<br>a. 基于 Java 的小程序 (“A”) 通过接触接口安装并被选中。<br>b. 创建 AES 密钥 (256 字节) 并初始化该密钥。<br>3. eUICC 域:<br>a. 检查 GetBoundProfilePackage (ES9+) 命令生成的 eUICC 数据及签名一致性并确保后续的测试配置文件加密下载所使用的会话密钥是基于 otSK.EUICC.ECKA、otPK.EUICC.ECKA (在 ES10b.LoadBoundProfilePackage 响应中)。 |
| 预期测试结果 | 在 eUICC 域中的配置文件下载结果不会因 eSE 域操作被更改或影响。                                                                                                                                                                                                                                                                                                                                  |

表 28 eUICC 身份管理数据隔离-5

|      |                                                                                                                                                                                                                                                                               |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试编号 | ATE_TestCase_16                                                                                                                                                                                                                                                               |
| 测试名称 | eUICC (身份管理数据-D.CERT.EUM.ECDSA (EUM 证书) 隔离)                                                                                                                                                                                                                                   |
| 测试目标 | EUM 证书不得因任何操作 (内存分配、释放、GlobalPlatform/JavaCard 操作或加密操作) 在 eSE 域上被 “更改”, 并且其与 SMDP+/SMDS 服务器进行双向认证中的使用应无缝运行。                                                                                                                                                                   |
| 测试步骤 | 1. eUICC 域:<br>a. 使用 GetEuiccInfo (ES10c) 检索证书链。<br>b. 检查 D.PK.CI.ECDSA 的 SKID (个性化过程中生成)。<br>2. eSE 域:<br>a. 基于 Java 的小程序 (“A”) 通过接触接口安装并被选中。<br>b. 创建 AES 密钥 (256 字节) 并初始化该密钥。<br>3. eUICC 域:<br>触发 RSP 会话并验证 EUM 证书是否出现在 AuthenticacaeServer (ES10b) 响应里并检查 EUUM 证书里签名一致性。 |

表 28 eUICC 身份管理数据隔离-5（续）

|        |                                                          |
|--------|----------------------------------------------------------|
| 预期测试结果 | 在 eUICC 域中，EUM 证书和 D.CERT.EUM.ECDSA 的值不得因 eSE 操作而被更改或影响。 |
|--------|----------------------------------------------------------|

应用说明：厂家应覆盖以上测试用例。同时厂家可依据自身产品设计向实验室提供更多测试用例。

7.2.3 安全功能测试覆盖

本章节描述了所建议的安全功能测试用例与 T/TAF 355—2026 中所宣称的安全功能组件对应关系。

表 29 安全功能组件与测试用例映射

|             |            |
|-------------|------------|
| 安全功能组件（SFR） | 由以下测试用例覆盖  |
| FDP_ACC.2   | 厂家提供具体测试项目 |
| FDP_ACF.1   | 厂家提供具体测试项目 |

所定义测试用例对 T/TAF 355—2026 第七章 eUICC 隔离安全要求的映射，如表 30 所示。

表 30 隔离安全要求与测试用例映射

|                 |            |
|-----------------|------------|
| 隔离安全要求          | 由以下测试用例覆盖  |
| eUICC 数据及代码访问控制 | 厂家提供具体测试项目 |
| eUICC 域控制权限管理   | 厂家提供具体测试项目 |

应用说明：以上映射关系，应由安全评估实验室基于厂家提供的具体测试用例完成。

7.3 安全渗透测试

安全评估实验室脆弱性分析，以及渗透测试设计，请详见附录 C。渗透测试必须考虑产品实际的对外接口和攻击面。渗透测试具体用例的设计，必须考虑安全设计审查和得到功能测试的分析结果。

8 eUICC NFC 功能通用测试要求

如果多合一 eUICC 产品具备 NFC 功能，且相应的 NFC 控制器与 eUICC 域通信满足 ETSI 定义的 SWP 和 HCI 协议及相关要求，参照 T/TAF 355—2026 第八章，那么 eUICC 域的 NFC 功能测试宜满足以下要求：

- SWP：ETSI TS 102.694-2 v7.2.0；
  - HCI：ETSI TS 102.695-2 v7.0.0。
- 本章节中所建议的测试，供应商应根据实际产品支持情况提供。

## 附录 A (规范性) 各域和接口测试业务

本文所需的 eSE 域测试业务如表 A.1 所示。

表 A.1 不同接口下的 eSE 域业务

| 接口          | 可选业务                                                                                                                                            |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| SPI (OMAPI) | ——Global Platform: 卡内容管理 (应用下载和升级、安装、个性化、删除)<br>——应用特定操作 (向应用发送命令)                                                                              |
| HCI         | ——Global Platform: 卡内容管理 (应用下载和升级、安装、个性化、删除)<br>——应用特定操作 (向应用发送命令)                                                                              |
| NFC CL      | ——应用特定操作: <ul style="list-style-type: none"> <li>• 钱包 - 支付交易</li> <li>• 交通交易</li> <li>• 门禁交易</li> <li>• 车钥匙交易</li> </ul> ——场强开/关 (Field ON/OFF) |

本文所需的 eUICC 域测试业务如表 A.2 所示。

表 A.2 ISO7816 接口上的 eUICC 域业务

| 接口       | 业务                                                                                                                                                                                                                                                                                                                              |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO 7816 | ——GSMA RSP 操作服务: <ul style="list-style-type: none"> <li>• 测试 profile 下载、删除、激活、去激活、eUICC 内存重置及其他操作, 参考 GSMA SGP.22 规范</li> </ul> ——eUICC 电信服务: <ul style="list-style-type: none"> <li>• 网络鉴权 (Milenage/SUCI)</li> <li>• 远程文件管理操作 (创建文件、读/写文件)</li> <li>• 主动式命令操作</li> <li>• 远程应用管理操作 (下载、安装、删除应用及密钥操作)</li> </ul> ——复位 (热复位/冷复位) |
|          | ——算法相关测试: <ul style="list-style-type: none"> <li>• DES、AES、RSA-1024、RSA-2048、SM2、SM3、SM4、SHA-256 等</li> <li>• BIP HTTPs 连接</li> </ul>                                                                                                                                                                                           |

本文所需的 NFC 服务如表 A.3 所示。

表 A.3 NFC 服务

| 接口     | 可选业务                            |
|--------|---------------------------------|
| NFC CL | ——NFC 开关 (ON/OFF)<br>——NFC 固件下载 |

附 录 B  
(规范性)  
测试环境配置

本文所需的测试环境配置如表 B.1 所示。

表 B.1 测试环境配置

| 测试配置                  | eSE 域接口<br>(上位机通过以下接口连接至 eSE) | eUICC 域接口<br>(上位机通过以下接口连接至 eUICC) |
|-----------------------|-------------------------------|-----------------------------------|
| Test Configuration #1 | OMAP1-SPI                     | ISO7816-T0/T1                     |
| Test Configuration #2 | ETSI-HCI                      | ISO7816-T0/T1                     |
| Test Configuration #3 | NFC/HCI (用于 NFC 特定操作)         | ISO7816-T0/T1                     |
| Test Configuration #4 | NFC CL (非接口)                  | ISO7816-T0/T1                     |



## 附录 C (资料性) 脆弱性分析及渗透测试方案

### C.1 概述

本附录主要描述了对多合一 eUICC 芯片的脆弱性攻击方案。

### C.2 目标

识别并验证多合一 eUICC 产品在高攻击潜力环境下的潜在脆弱性，确保其能够抵御具有高等攻击潜力的攻击者。尝试破坏或绕过 T/TAF 355—2026 内定义的 eUICC 隔离安全要求，证明 TOE 在“高攻击潜力”下可被利用。

eUICC 隔离安全要求规定的 6 条安全要求为：

- eUICC 数据及代码访问控制；
- eUICC 域控制权限管理；
- eUICC 域的数据和代码防篡改；
- 跨域代码运行安全；
- eUICC 域标识防伪造；
- 防拒绝服务。

其中对上述的 6 个安全要求进行脆弱性攻击分析。

### C.3 脆弱性攻击原则

脆弱性攻击攻击应满足以下原则。

- 系统性分析：对开发文档、设计规范、实现表示等进行结构化、全面化分析。
- 公开信息利用：广泛搜集并分析公开渠道中可能存在的脆弱性信息。
- 测试验证：通过穿透性测试验证潜在脆弱性的可利用性。
- 环境适配性：评估脆弱性是否适用于 TOE 的实际运行环境。
- 攻击潜力导向：仅关注可被高等或更低攻击潜力的攻击者利用的脆弱性。

### C.4 脆弱性攻击测试方法

脆弱性攻击测试方法如下：

#### a) AVA\_VAN.5-1：检查测试配置与 ST 一致性

目的：确认测试用的 TOE 配置与安全目标（ST）一致。

行为：

- 核对 TOE 引用名与 ST 中一致；
- 检查运行环境安全目的是否在测试中满足；

#### b) AVA\_VAN.5-2：确认 TOE 安装与状态

目的：确保 TOE 正确安装并处于已知状态。

要点：

- 可依赖先前 AGD\_PRE.1 结果；
- 若状态未知，需按开发者文档重新安装；
- 安装成功可视为满足 AGD\_PRE.1-3。

c) AVA\_VAN.5-3: 公开信息来源搜索潜在脆弱性

目的: 利用公开资源识别 TOE 可能存在的已知脆弱性。

要点:

- 搜索范围包括: 专业出版物、研究文献、会议论文、互联网资源;
- 特别关注与 TOE 技术来源相关的产品;
- 搜索方法需记录, 支持迭代发现;
- 可结合评估者经验、TOE 类型、攻击潜力等调整搜索策略。

d) AVA\_VAN.5-4: 系统性分析开发证据识别潜在脆弱性

目的: 通过结构化分析识别 TOE 内部潜在缺陷。

要点:

- 分析对象包括: ST、功能规范、TOE 设计、安全架构、实现表示;
- 使用“缺陷假设”方法, 建立攻击假设;
- 关注通用脆弱性类型: 旁路、篡改、直接攻击、监控、误用;
- 方法需完备、系统, 覆盖所有证据内容;
- 可与授权机构协商方法细节。

e) AVA\_VAN.5-5: 记录适用于运行环境的潜在脆弱性

目的: 筛选出适用于实际运行环境的脆弱性。

要点:

- 若运行环境已有措施可缓解, 则排除;
- 不适用的需记录排除理由;
- 形成最终测试用脆弱性列表;
- 写入评估技术报告, 作为穿透性测试输入。

f) AVA\_VAN.5-6: 设计穿透性测试

目的: 基于识别的脆弱性设计测试, 验证其可利用性。

要点:

- 针对每个脆弱性设计测试用例;
- 测试目标包括 TSFI 及其他接口;
- 不测试超出高等攻击潜力的脆弱性;
- 若发现超出者, 作为残余脆弱性记录;
- 测试应覆盖安全架构描述中的所有机制。

g) AVA\_VAN.5-7: 编制穿透性测试文档

目的: 确保测试可重复、可追溯。

要点:

文档需包括:

- 脆弱性标识;
  - 测试设备与配置;
  - 初始条件与前提;
  - 激发与观察 TSF 的方法;
  - 预期结果与分析方法;
  - 测试后状态说明;
- 每个测试用例应对应一个潜在脆弱性;
- 文档应详尽, 支持他人复现。

h) AVA\_VAN.5-8: 执行穿透性测试

目的：实际运行测试，验证脆弱性可利用性。

要点：

- 按测试文档执行；
- 可根据测试结果追加专门测试；
- 若测试表明脆弱性不存在，需反思分析或交付件是否完整；
- 不强制测试超出高等攻击潜力的脆弱性；
- 所有测试需记录。

i) AVA\_VAN.5-9：记录测试结果

目的：确保测试结果真实、可追溯。

要点：

- 实际结果与预期应一致；
- 若存在差异，需调查并说明影响；
- 所有结果需记录，支持后续分析。

j) AVA\_VAN.5-10：在评估技术报告中报告穿透性测试工作

目的：总结测试方法、配置、结果，供评估机构审查。

要点：

- 报告内容包括：
  - 测试配置；
  - 测试接口；
  - 测试方法与深度；
  - 总体结果判断；
- 不需复制每个测试步骤，但需足够详细；
- 支持其他评估者理解与复现。

k) AVA\_VAN.5-11：判断 TOE 是否可抵御高等攻击潜力攻击者

目的：得出最终评估结论。

要点：

- 若存在可被攻击潜力小于或等于“高”等级利用的脆弱性，评估不通过；
- 无需每次都计算攻击潜力，存疑时才需量化。

l) AVA\_VAN.5-12：报告所有可利用与残余脆弱性

目的：全面披露发现的脆弱性。

要点：

- 报告内容：
  - 来源（分析、公开信息、测试等）；
  - 涉及安全功能要求；
  - 描述；
  - 是否可利用或残余；
  - 利用所需攻击潜力（时间、知识、设备等）；
- 所有脆弱性需分类、详细说明；
- 写入评估技术报告，作为最终评估依据。

## C.5 脆弱性攻击基线

基于脆弱性测试方法，基于多合一 eUICC 产品特性，至少应包含如下案例。

——跨域代码运行安全如表 C.1 所示。

表 C.1 跨域代码运行安全

|      |                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试目的 | 测试 eUICC 域控制器完成切换后，通过软件和物理攻击的方式篡改 eSE 的 RAM 和 NVM 存储区域的运行时数据，eUICC 是否能够安全运行。                                                                                                                                                                 |
| 测试步骤 | 步骤 1：构造一个由 eUICC 域、eSE 域并发运行的环境。<br>步骤 2：eUICC 域控制器完成切换后，在 eSE 域通过虚拟机字节码攻击的方式篡改 RAM 和 NVM 存储区域的运行时数据。eUICC 域控制器完成切换后，验证 eUICC 是否能够安全运行。<br>步骤 3：eUICC 域控制器完成切换后，在 eSE 域通过错误注入攻击的方式篡改 RAM 和 NVM 存储区域的运行时数据。eUICC 域控制器完成切换后，验证 eUICC 是否能够安全运行。 |
| 预期结果 | 在步骤 1、2、3 后，eUICC 域未安全运行。                                                                                                                                                                                                                    |

——eUICC 域标识防伪造如表 C.2 所示。

表 C.2 eUICC 域标识防伪造

|      |                                                                                                                                                                                     |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 测试目的 | 测试 eUICC 域控制器的 eUICC 域标识是否具备抵抗物理攻击的能力，以防止通过物理攻击来篡改 eUICC 域标识。                                                                                                                       |
| 测试步骤 | 步骤 1：在 eUICC 域控制器切换域的过程中，使用错误注入的方式攻击 eUICC 域控制器的 eUICC 域标识，验证 eUICC 域控制器的 eUICC 域标识具有抵抗错误注入攻击的能力，错误注入攻击包括但不限于——毛刺注入攻击、光注入攻击、电磁注入攻击等；<br>步骤 2：查看 eUICC 域控制器的 eUICC 域标识是否被篡改，并获取额外权限。 |
| 预期结果 | 在步骤 1、2、3 后，能够篡改 eUICC 域控制器的 eUICC 域标识。                                                                                                                                             |

——防拒绝服务如表 C.3 所示。

表 C.3 防拒绝服务

|      |                                                                                     |
|------|-------------------------------------------------------------------------------------|
| 测试目的 | 测试 eUICC 域在重要资源被 eSE 消耗殆尽的情况下能否正常提供服务。                                              |
| 测试步骤 | 步骤 1：在 eSE 下持续进行消耗资源的操作（如读写 NVM、RAM、密钥运算等），并行运行 eUICC 操作，检查 eUICC 是否能够抢占资源，并完成相应操作。 |
| 预期结果 | 在步骤 1 后，eUICC 未抢占资源，无法提供正常的服务。                                                      |



电信终端产业协会团体标准  
多合一 eUICC 芯片并发和安全隔离测试方法

T/TAF 356—2026

\*

版权所有 侵权必究

电信终端产业协会发布  
地址：北京市西城区新街口外大街 28 号  
电话：010-82052809  
电子版发行网址：[www.taf.org.cn](http://www.taf.org.cn)