ICS 31.200
CCS L56

团　体　标　准

T/TAF 355—2026

多合一 eUICC 芯片并发和安全隔离技术要求

Convergence eUICC chip concurrency and security isolation technical requirements

2026-06-17 发布　　2026-06-17 实施

电信终端产业协会　发布

版权声明

邮箱：tafrb@taf.org.cn

电话：010-82052809

目　　次

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、上海优咔网络科技有限公司、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：董雯、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技术要求

1 范围

本文件针对面向消费电子类产品的多合一eUICC芯片的eUICC域与芯片上的其他域并发和安全隔离进行了规范和要求。

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。

GB/T 22186—2016 信息安全技术具有中央处理器的IC卡芯片安全技术要求

GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第1部分：简介和一般模型

GB/T 18336.2—2024 网络安全技术 信息技术安全评估准则 第2部分：安全功能组件

GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第3部分：安全保障组件

GB/T 18336.4—2024 网络安全技术 信息技术安全评估准则 第4部分：评估方法和活动的规范框架

GB/T 18336.5—2024 网络安全技术 信息技术安全评估准则 第5部分：预定义的安全要求包

CCMB-2022-11-001 信息技术安全评估通用准则 第1部分：简介和一般模型，CC2022 修订版1，2022年11月（Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC2022 Revision 1, November 2022）

CCMB-2022-11-002 信息技术安全评估通用准则 第2部分：安全功能组件，CC2022 修订版1，2022年11月（Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC2022 Revision 1, November 2022）

CCMB-2022-11-003 信息技术安全评估通用准则 第3部分：安全保障组件，CC2022 修订版1，2022年11月（Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC2022 Revision 1, November 2022）

CCMB-2022-11-004 信息技术安全评估通用准则 第4部分：评估方法和活动的规范框架，CC2022 修订版1，2022年11月（Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC2022 Revision 1, November 2022）

CCMB-2022-11-005 信息技术安全评估通用准则 第5部分：预定义的安全要求包，CC2022 修订版1，2022年11月（Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC2022 Revision 1, November 2022）

ISCCC-TR-041-2017 Java卡通用安全技术要求（评估保障级EAL4+）

CCRC-EAL-TR-015-2019 用于消费类设备的嵌入式UICC产品安全技术要求（评估保障级EAL4+）

3 术语和定义

下列术语和定义适用于本文件。

3.1

签约数据文件 profile

包含运营商数据和应用的集合，可下载至eUICC为用户提供运营商服务。

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-Ingegrated 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）

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 技术方案

多合一eUICC芯片是一个硬件和软件的组合。通过相应技术手段将eUICC功能与其他功能模块集成为多合一eUICC实现方案。

硬件上，多合一eUICC芯片融合了eUICC、嵌入式安全元件（eSE）、以及可选的NFC控制器和其他接口（如SWP，I2C，SPI等，可用于eUICC和eSE的对外通信）。软件上，通过应用程序域，独立或共享方式支持标准的蜂窝通信及其他功能和应用。

多合一eUICC芯片可以通过多种方式进行分类。

根据硬件实现方式对多合一eUICC芯片进行分类。

a) 单芯片实现方案：一张多合一eUICC芯片中只有一个芯片硬件载体，同时融合实现eSIM、eSE、NFC等功能。

b) 多芯片实现方案：一张多合一eUICC芯片合封至少两个芯片硬件载体。不同芯片通过合封的方式进行集成。

根据软件实现方式对多合一eUICC芯片进行分类。

a) 单COS实现方案：一张多合一eUICC芯片中只有一个COS。该COS同时实现eSIM、eSE等应用/功能。
b) 多COS实现方案：一张多合一eUICC芯片中具有多个独立的COS。不同的COS分别负责eSIM和eSE的功能。

6 性能及并发要求

6.1 概述

多合一eUICC芯片应具备并发仲裁机制，以确保在预期的业务时间内，遵循本章节的性能及功能要求来协调命令请求的执行。

在平台性能要求允许的情况下，并发APDU的处理可以序列化，eSE和eUICC按照IO接口收到APDU命令的先后顺序依次处理。当某些业务指令对响应时间有严格要求（如eUICC的鉴权命令）时，多合一eSIM的域控制器需要采用抢占策略，确保业务指令可以在规定的时间内返回处理结果。

6.2 业务时间要求

若有并发事件发生，业务时间要求参考附录A。

6.3 功能限制性要求

在多合一eUICC芯片上 ,不同域内的应用和相应的接口的并发处理 应遵循“任务照常执行”原则，保证不同业务能正常工作,尤其要确保蜂窝和其他通信网络不受并发场景的严重干扰。

以NFC功能并行场景为例，应符合表1要求。

表 1 NFC 功能并发场景

序号	并发场景	功能限制要求
1	eSIM profile远程安装过程中执行非接触式近场支付	Profile 安装应执行成功，其他业务均应执行成功或告知用户中断端或延后处理，不出现因并发导致的错误
2	在网络鉴权、通话或短信过中执行非接触式近场支付	基本电信业务应不会被中断。

不同域的应用及接口应有被中断的保护机制，确保在并行场景中业务中断时能及时恢复。一些特殊命令应具备保护上下文和重新尝试等功能，命令的执行可以被延迟，但命令执行时间及性能不能严重降低。

6.4 稳定性要求

各类多合一eUICC方案，其应满足下列稳定性要求：

a) 当并发事件发生时，被挂起的eUICC命令请求处理任务，既不应被删除，也不应出现执行失败。例如eUICC芯片执行NFC刷卡时进行通信鉴权，刷卡和鉴权均应成功执行。
b) eUICC命令请求的处理时间，其由于并发导致的延迟，不应影响业务执行。

7 eUICC 隔离安全要求

7.1 概述

多合一eUICC应满足域隔离要求。多合一eUICC芯片内的其他模块/域，如eSE，不能影响eUICC的安全性。

注：域隔离要求应符合本文件附录B，该保护轮廓中所定义的脆弱性分析要求攻击分值计算方法，详见于附录C。如存在攻击路径，则攻击分值应不小于31分。

7.2 eUICC 数据及代码访问控制

多合一 eUICC 芯片的域隔离应实现基于安全属性的，明确授权主体访问客体规则的访问控制，以确定在受控主体与客体之间的操作是否被允许。在明确的规则下，域隔离访问控制应明确在哪些规则下，可授权访问，哪些规则下，应拒绝访问。在多合一 eUICC 方案中，eUICC 域的用户数据，及 eUICC 的代码及配置数据，不能被其他域采用类型混淆等攻击方式进行恶意访问。域之间任何交换（如操作系统或服务）都应由 eUICC 认证范围内的域控制器控制。

7.3 eUICC 域控制权限管理

多合一 eUICC 芯片在功能实现上，应确保其域控制器具有最高权限。

7.4 eUICC 域的数据和代码防篡改

多合一 eUICC 芯片在功能实现上，应确保属于 eUICC 域的数据和代码，不会被其他非 eUICC 域非法篡改。

7.5 跨域代码运行安全

多合一 eUICC 芯片在功能实现上，应确保属于 eUICC 的代码运行安全，不受其他域的影响。

7.6 eUICC 域标识防伪造

多合一 eUICC 芯片在功能实现过程中，应确保有效识别合法用户。

在多合一 eUICC 方案中，用于域控制器识别 eUICC 域的域标识应被 eUICC 域隔离所保护，防止其他域伪造其标识冒充 eUICC。

7.7 防拒绝服务

多合一 eUICC 芯片在功能实现过程中，应由域控制器根据优先级管理其调度，以防止域之间共用的重要资源被消耗殆尽而导致 eUICC 域不能正常运行。

仅域控制器有权限管理优先级权限。

8 通用说明

根据产品情况或运营商要求支持基础要求或者增强要求：

a) 基础要求。多合一eUICC可具备NFC功能。如支持NFC控制器与eUICC域通信宜满足以下要求。
   - ETSI TS 102.613 V7.10.0及以上SWP协议及相关要求。
   - ETSI TS 102.622 V7.10.0及以上HCI协议及相关要求。

b) 增强要求。NFC相关功能在多合一eUICC产品应支持以下要求。
   - 具备NFC控制功能的多合一eUICC产品，应保证eUICC域具备使用本芯片内NFC功能的能力，且保证芯片的NFC控制器功能能正常给外部UICC提供SWP和HCI协议通信。eUICC芯片内的NFC控制器与eUICC域通信，宜满足ETSI TS 102.613 V7.10.0及以上SWP协议及相关要求，ETSI TS 102.622 V7.10.0及以上HCI协议及相关要求。

- 对于不具备NFC控制器功能的多合一eUICC产品，eUICC域应支持HCI/SWP接口的能力。应遵循ETSI TS 102.613 V7.10.0及以上SWP协议及相关要求，ETSI TS 102.622 V7.10.0及以上HCI协议及相关要求。应保证eUICC域具备使用外部NFC功能的能力。

附 录 A
（资料性）
业务时间要求

本文所需的业务时间参考要求如表 A.1 所示。

表 A.1 业务时间要求

测试项	说明 （ms/3000 次平均时间）	输入长度（字节）	标准值/ms
SM2	SM2 密钥对生成	—	18
	SM2 签名	64	20
	SM2 验签	128	20
	SM2 加密	150	40
	SM2 解密	246	40
RSA1024	RSA1024 生成密钥对	—	500
	RSA1024 签名	32	40
	RSA1024 验签	160	10
	RSA1024 加密	128	8
	RSA1024 解密	128	20
	CRT 模式 RSA1024 生成密钥对	—	180
	CRT 模式 RSA1024 签名	20	16
	CRT 模式 RSA1024 解密	128	15
RSA2048	RSA2048 生成密钥对	—	2000
	RSA2048 签名	32	100
	RSA2048 验签	32	10
	RSA2048 加密	256	14
	RSA2048 解密	256	100
	CRT 模式 2048 生成密钥对	—	1200
	CRT 模式 2048 签名	32	40
	CRT 模式 2048 解密	256	40
SM3	SM3 算法	256	7
SHA-256	SHA 256 算法	256	3
3DES	3DES CBC 加密	256	14
	3DES CBC 解密	256	14
	3DES ECB 加密	256	13
	3DES ECB 解密	256	13
AES	AES 128 CBC 加密	256	12
	AES 128 CBC 解密	256	12
	AES 128 ECB 加密	256	12
	AES 128 ECB 解密	256	12
SM4	SM4 CBC 加密	256	14
	SM4 CBC 解密	256	14
	SM4 ECB 加密	256	14
	SM4 ECB 解密	256	14
BIP 建立连接	—	—	80
IMSI 加密	ProfileA 算法	A	40
	ProfileB 算法	B	40
鉴权	MILENAGE	—	15

附 录 B
（规范性）
多合一 eUICC 芯片方案域隔离保护轮廓

B.1 符合性声明

本保护轮廓遵从以下通用安全评估准则国家标准：

——GB/T 18336.1—2024；

——GB/T 18336.2—2024；

——GB/T 18336.3—2024；

——GB/T 18336.4—2024；

——GB/T 18336.5—2024。

或国际通用安全评估准则：

——Common Criteria Part 1；

——Common Criteria Part 2；

——Common Criteria Part 3；

——Common Criteria Part 4；

——Common Criteria Part 5。

鉴于国家标准和国际通用安全准则内容是等同的，文档也一一对应。以下章节皆以国家标准描述，若选择国际通用安全评估准则进行安全评估，请安全目标作者自行进行替换。保护轮廓同理。

基于该保护轮廓进行的安全评估，应基于eUICC芯片和操作系统满足EAL 4+及以上安全要求。

本保护轮廓的EAL4+，是在遵从GB/T 18336.5—2024中定义的评估保障级4级的基础上，将AVA_VAN.3增强为AVA_VAN.5，将ATE_DPT.1增强为ATE_DPT.2。

B.2 安全问题定义

B.2.1 资产

B.2.1.1 资产概述

在通用安全评估准则中，安全定义，威胁分析，攻击方法等，核心都是基于资产（assets-based）。资产的定义尤其重要，通用安全评估准则是围绕着资产保护进行的。安全功能组件（SFR）是为了抵御对资产的威胁而申明的具体安全要求，安全保障组件（SAR）定义的是对产品宣称的实现安全功能组件（SFR）的具体设计实现的评估要求。本安全轮廓中定义的资产，源于CCRC所要求的三个安全标准（CCRC-EAL-TR-015-2019，ISCCC-TR-041-2017，GB/T 22186—2016）。由于GB/T 22186—2016在资产定义中只区分TSF数据，用户数据和安全服务，无法区分在多合一场景下的具体资产，其中硬件TSF数据资产为系统共用，而用户数据资产定义，可由java卡系统以及UICC部件的评估安全标准所定义的资产覆盖，因此，本保护轮廓范围内定义对eUICC域的资产定义皆来自Java卡系统（ISCCC-TR-041-2017），以及消费类嵌入式UICC（CCRC-EAL-TR-015-2019）。这些需要在域安全隔离中被定义的eUICC资产，在本保护轮廓中也被分为了两大类，eUICC TSF数据以及eUICC用户数据。

B.2.1.2 eUICC TSF 数据

本文所涉及的 eUICC TSF 数据如表 B.1 所示。

表 B.1　eUICC TSF 数据

资产 ID	资产描述
D.API_DATA	API 的 Private 数据，如他的私有字段内容。
D.CRYPTO	在运行时进行加密运算用到的加密数据，如用于生成密钥的随机数种子。
D.TSF_CODE	Java 卡系统和 eUICC 部件的代码。
D.RUNTIME_DATA	JVM 和 JCRE 运行时的数据，包括在 Java 卡系统标准 ISCCC-TR-041-2017[2]中定义的 D.JCS_DATA & D.SEC_DATA，以及多合一方案里不同的域的域识别符。
D.MAN_DATA	eUICC 的管理数据，包括消费类嵌入式 UICC 标准 CCRC-EAL-TR-015-2019[3]定义的 D.PLATFORM_DATA, D.DEVICE_INFO 以及 D.PLATFORM_RAT。
D.ID_MAN_DATA	用于验证行为人身份真实性的识别管理数据，包括 CCRC-EAL-TR-015-2019[3]标准定义的 D.SK.EUICC.ECDSA, D.CERT.EUICC.ECDSA, D.PK.CI.ECDSA, D.EID, D.SECRETS, D.CERT.EUM.ECDSA 以及 D.CRLs。

B.2.1.3　eUICC 用户数据

本文所涉及的 eUICC TSF 数据如表 B.2 所示。

表 B.2　eUICC 用户数据

资产 ID	资产描述
D.PROFILE_CODE	在 UICC 配置（profile）中包含的代码。
D.PROFILE_DATA	UICC 配置（profile）的数据，比如对象中包含的数据，包中的 static 字段，方法执行中的本地变量，操作数堆栈的位置信息，以其他需要保护的机密敏感信息。
D.MNO_KEYs	MNO OTA 平台用于请求 ISD-P 进行管理操作的密钥。这些密钥需要在预配置时，在 MNO SD 的控制下加载到产品上。

B.2.2　主体

安全目标的作者需要明确定义域隔离安全功能策略的主体。

B.2.3　对象

安全目标的作者需要明确定义域隔离安全功能策略的对象。

B.2.4　威胁

本文所涉及的威胁定义如表 B.3 所示。

表 B.3　威胁

T.CONFID-DOMAIN	eUICC 域的数据和代码泄露 攻击者可以通过其他的域获得本属于 eUICC 域的数据和代码（比如应用程序数据，Java 卡系统代码，Java 卡系统数据，eUICC 数据等）。 直接受威胁的资产如下： D.API_DATA, D.CRYPTO, D.TSF_CODE, D.RUNTIME_DATA, D.MAN_DATA, D.ID_MAN_DATA, D.PROFILE_CODE, D.PROFILE_DATA, D.MNO_KEYs

表 B.3　威胁（续）

T.INTEG-DOMAIN	eUICC 域的数据和代码被非法更改 攻击者通过其他域对本属于 eUICC 域的代码和数据进行非法更改（比如应用程序代码，应用程序数据，发送到 eUICC TOE 上的应用程序数据包，Java 卡系统代码，Java 卡系统数据，eUICC 数据）。 直接受威胁的资产如下： D.API_DATA, D.CRYPTO, D.TSF_CODE, D.RUNTIME_DATA, D.MAN_DATA, D.ID_MAN_DATA, D.PROFILE_CODE, D.PROFILE_DATA, D.MNO_KEYs
T.EXE-DOMAIN	通过其他域运行 eUICC 的代码 攻击者通过其他域非授权运行了属于 eUICC 域的 method，method fragment，arbitrary data，或 native code。 直接受威胁的资产如下： D.RUNTIME_DATA
T. DOMAIN-DOS	域之间拒绝服务 攻击者通过其他域消耗某些共用的重要资源妨碍 eUICC 域的正常运行。 直接受威胁的资产如下： D.RUNTIME_DATA
T.DOMAIN-SID	域的识别 攻击者在其他域中运行有危害的 OS，冒充 eUICC 域。 直接受威胁的资产如下： D.RUNTIME_DATA

B.2.5　组织安全策略

无额外组织安全策略。

B.2.6　假设

本文所涉及的假设定义如表 B.4 所示。

表 B.4　假设

A.DOMAINS	此处需以具体实现方案选择适合的选项。 选项一：假定多合一方案中的其他域由相同的 eUICC TSF 开发人员以与 eUICC 域相同的安全方式开发。 选项二：假设多合一方案中的其他域由其他第三方公司开发，则 ST 作者需要在安全功能组件里额外声明如何管理并验证来自于第三方的域，此情况下，多合一产品的 TSFI 包括开放给来自第三方域的接口。第三方域视为多合一 eUICC 评估范围内的 TOE 需要进行检验的部分，视同于运行在 eUICC 上的 applet。同时假设其他的域是由可信的第三方团队以安全方式生产的。
A.DOMAINS_APP	假设其他的域的应用程序是由可信的开发团队以安全的方式生产的，并且其他域在加载安装运行在其上的应用程序时，采取了足够的检查来验证这些应用程序的真实性和完整性。

B.3 安全目的

B.3.1 对 TOE 的安全目的

本文所涉及的对 TOE 的安全目的如表 B.5 所示。

表 B.5 对 TOE 的安全目的

SO.CONT-SEP	域隔离 多合一方案应防止在另一个域中运行的软件未经授权访问（读取/写入/执行）eUICC 域内存、外围设备或资源。域之间的任何交换（如操作系统或服务）都应由 eUICC 认证范围内的域控制器控制。
SO.CONT-PRIV	权限管理 多合一方案的 eUICC 产品应确保其域控制器对在产品上运行的任何其他软件部分拥有最高权限。
SO.CONT-DOS	拒绝服务 DoS 多合一方案产品的域控制器域应通过根据优先级管理域上下文的调度来防止拒绝服务。

B.3.2 对 TOE 环境的安全目的

本文所涉及的对 TOE 环境的安全目的如表 B.6 所示。

表 B.6 对 TOE 环境的安全目的

OE.DOMAINS	此处需以具体实现方案选择适合的选项。 选项一：多合一方案中的其他域必须由相同的 eUICC TSF 开发人员以与 eUICC 域相同的安全方式开发。 选项二：多合一方案中的其他域由其他第三方公司开发，ST 作者必须在安全功能组件里额外声明如何管理并验证来自于第三方的域。此情况下，多合一产品的 TSFI 包括开放给来自第三方域的接口。第三方域视为多合一 eUICC 评估范围内的 TOE 需要进行检验的部分，视同于运行在 eUICC 上的应用程序，属于 TOE 运行环境的一部分。同时其他的域必须是由可信的第三方团队以安全方式生产的。
OE.DOMAINS_APP	其他的域的应用程序必须是由可信的开发团队以安全的方式生产的，并且其他域在加载安装运行在其上的应用程序时，必须采取足够的检查来验证这些应用程序的真实性和完整性。

B.4 安全组件

B.4.1 安全功能组件

本文所涉及的安全功能组件定义如表 B.7～表 B.13 所示。

*标下划线且斜体*的部分是留给安全目标作者填写的具体说明。粗体字是在本安全轮廓中细化的赋值。

表 B.7　完全访问控制

FDP_ACC.2	完全访问控制
从属于	FDP_ACC.1 子集访问控制
依赖关系	FDP_ACF.1 基于安全属性的访问控制
FDP_ACC.2.1	TSF 应对[*赋值：主体与客体列表*] 及 SFP 所涵盖主体和客体之间的所有操作执行[**赋值：域隔离 SFP**]。
FDP_ACC.2.2	TSF 应确保 TSF 控制内的任何主体和客体之间的所有操作都被一个访问控制 SFP 涵盖。

表 B.8　基于安全属性的访问控制

FDP_ACF.1	基于安全属性的访问控制
从属于	无其他组件
依赖关系	FDP_ACC.1 子集访问控制 FMT_MSA.3 静态属性初始化
FDP_ACF.1.1	TSF 应基于[*赋值：指定 SFP 控制下的主体和客体列表，以及每个与 SFP 的相关安全属性或与 SFP 相关的已命名安全属性组*]对客体执行[**赋值：域隔离 SFP**]
FDP_ACF.1.2	TSF 应执行以下规则,以确定在受控主体与受控客体间的一个操作是否被允许：[*赋值：在受控主体和受控客体间，通过对受控客体采取受控操作来管理访问的一些规则*]。
FDP_ACF.1.3	TSF 应基于以下附加规则：[*赋值：基于安全属性的,明确授权主体访问客体的规则*]，明确授权主体访问客体。
FDP_ACF.1.4	TSF 应基于[*赋值：基于安全属性的，明确拒绝主体访问客体的规则*]明确拒绝主体访问客体。

表 B.9　静态属性初始化

FMT_MSA.3	静态属性初始化
从属于	无其他组件.
依赖关系	FMT_MSA.1 安全属性的管理 FMT_SMR.1 安全角色
FMT_MSA.3.1	TSF 应执行[**赋值：域隔离 SFP**]，以便为用于执行 SFP 的安全属性提供[**赋值：受限的**]默认值。
FMT_MSA.3.2	TSF 应允许[*赋值：已标识的授权角色*]在创建客体或信息时指定替换性的初始值以代替原来的默认值。

表 B.10　安全属性的管理

FMT_MSA.1	安全属性的管理
从属于	无其他组件

表 B.10　安全属性的管理（续）

依赖关系	[FDP_ACC.1 子集访问控制，或 FDP_IFC.1 子集信息流控制] FMT_SMR.1 安全角色 FMT_SMF.1 管理功能规范
FMT_MSA.1.1	TSF 应执行[**赋值：域隔离 SFP**],以仅限于[*赋值:已标识的授权角色*]能够对安全属性[*赋值:安全属性列表*]进行[*选择:改变默认值、查询、修改、删除、[赋值:其他操作]*]。

表 B.11　管理功能规范

FMT_SMF.1	管理功能规范
从属于	无其他组件
依赖关系	无依赖关系
FMT_SMF.1.1	TSF 应能够执行如下管理功能：[*赋值：TSF 提供的安全管理功能列表*]。

表 B.12　安全角色

FMT_SMR.1	安全角色
从属于	无其他组件
依赖关系	FIA_UID.1 Timing of identification.
FMT_SMR.1.1	TSF 应维护角色[*赋值:已标识的授权角色*]。
FMT_SMR.1.2	TSF 应能够把用户和角色关联起来。

表 B.13　标识的时机

FIA_UID.1	标识的时机
从属于	无其他组件
依赖关系	无依赖关系
FIA_UID.1.1	在用户被识别之前,TSF 应允许执行代表用户的[*赋值：TSF 促成的动作列表*]。
FIA_UID.1.2	在允许执行代表该用户的任何其他 TSF 仲裁动作之前,TSF 应要求每个用户身份都已被成功识别。

B.4.2　安全保障组件

加强的安全保障组件有AVA_VAN.5和ATE_DPT.2。

——AVA_VAN.5提出了评估标准中最高的脆弱性分析要求。

——ATE_DPT.2的加强是为了和现有的标准对齐。

详细的安全保障组件如下表B.14所示。

表 B.14　安全保障组件

要求的安全保障类	要求的安全保障组件
ASE	ASE_INI.1

表 B.14　安全保障组件（续）

要求的安全保障类	要求的安全保障组件
ASE	ASE_CCL.1
	ASE_SPD.1
	ASE_OBJ.2
	ASE_ECD.1
	ASE_REQ.2
	ASE_TSS.1
ADV	ADV_FSP.4 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。
	ADV_IMP.1
	ADV_ARC.1
	ADV_TDS.3
AGD 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 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
	ATE_DPT.2
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.5

AVA_VAN.5高级的系统的脆弱性分析，要求如下。

——AVA_VAN.5.1D 开发者应提供用于测试的TOE。

——AVA_VAN.5.1C TOE应适合测试。

——AVA_VAN.5.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

——AVA_VAN.5.2E 评估者应执行公共领域的调查以标识TOE的潜在脆弱性。

——AVA_VAN.5.3E 评估者应针对TOE执行独立的、系统的脆弱性分析去标识TOE潜在的脆弱性，在分析过程中使用指导性文档、功能规范、TOE设计、安全结构描述和实现表示。

——AVA_VAN.5.4E 评估者应基于已标识的潜在脆弱性实施穿透性测试,确定TOE能抵抗具有高等攻击潜力的攻击者的攻击。

B.4.3　安全组件合理性

B.4.3.1　安全目的合理性

本文所涉及的安全目的合理性要求如表 B.15 和表 B.16 所示。

表 B.15　安全目的合理性-威胁

威胁	对 TOE 的安全目的	合理性说明
T.CONFID-DOMAIN	SO.CONT-SEP	将会阻止泄露从属于 eUICC 域的数据或代码给其他域。
T.INTEG-DOMAIN	SO.CONT-SEP	将会阻止其他域非法修改从属于 eUICC 域的数据或代码。
T.EXE-DOMAIN	SO.CONT-SEP SO.CONT-PRIV	将会阻止其他域非法获得或者修改 eUICC 域的数据或代码。属于最高权限域的代码在其他域的执行将被阻止。
T. DOMAIN-DOS	SO.CONT-SEP SO.CONT-PRIV SO.CONT-DOS	域控制器永远拥有最高特权，而且只有域控制器拥有最高特权。所有域将通过多域控制器的维护始终保持可访问性。这将防止未经授权访问其他域的硬件外围设备和资源。
T.DOMAIN-SID	SO.CONT-SEP SO.CONT-PRIV	将会阻止其他域非法获得或者修改 eUICC 域的数据或代码。属于最高权限域的代码在其他域的执行将被阻止。

表 B.16　安全目的合理性-假设

假设	对 TOE 环境的安全目的	合理性说明
A.DOMAINS	OE.DOMAINS	选项一： 通过确保同一开发人员对其他域进行相同安全级别的开发来支持这一假设。 选项二： 关于多合一产品透露给第三方域的 TSFI 将由 TOE 的环境要求变为 TOE 评估的一部分，以此来满足假设。同时通过确保第三方开发人员的可信程度以及确保第三方按照所提供的说明文档来进行开发，以此来满足假设。
A.DOMAINS_APP	OE.DOMAINS_APP	通过确保在其他域上安装之前检查其他域的应用程序的完整性和真实性来坚持这一假设。

B.4.3.2　安全功能组件合理性

本文所涉及的安全功能组件合理性要求如表 B.17 和表 B.18 所示。

表 B.17　安全功能组件合理性-1

对 TOE 的安全目的	安全功能组件	合理性说明
SO.CONT-SEP	FDP_ACC.2, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1, FMT_SMR.1, FIA_UID.1	所有的安全功能组件都被涵盖。都为确保和执行域分离 SFP 做出贡献。
SO.CONT-PRIV	FDP_ACC.2, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1, FMT_SMR.1, FIA_UID.1	所有的安全功能组件都被涵盖。都为确保和执行域分离 SFP 做出贡献。
SO.CONT-DOS	FDP_ACC.2, FDP_ACF.1, FMT_MSA.3, FMT_MSA.1, FMT_SMF.1, FMT_SMR.1, FIA_UID.1	所有的安全功能组件都被涵盖。都为确保和执行域分离 SFP 做出贡献。

表 B.18　安全功能组件合理性-2

安全功能组件	对 TOE 的安全目的追溯
FDP_ACC.2	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS
FDP_ACF.1	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS
FMT_MSA.3	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS
FMT_MSA.1	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS
FMT_SMF.1	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS
FMT_SMR.1	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS
FIA_UID.1	SO.CONT-SEP, SO.CONT-PRIV, SO.CONT-DOS

B.4.3.3　安全功能组件依赖性

本文所涉及的安全功能组件依赖性要求如表 B.19 所示。

表 B.19　安全功能组件依赖性

安全功能组件	通用标准依赖性要求	依赖性满足
FDP_ACC.2	FDP_ACF.1 基于安全属性的访问控制	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 子集访问控制 FMT_MSA.3 静态属性初始化	FDP_ACC.2, FMT_MSA.3
FMT_MSA.3	FMT_MSA.1 安全属性的管理 FMT_SMR.1 安全角色	FMT_MSA.1, FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 子集访问控制，或 FDP_IFC.1 子集信息流控制] FMT_SMR.1 安全角色 FMT_SMF.1 管理功能规范	FDP_ACC.2, FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	无依赖关系	—
FMT_SMR.1	FIA_UID.1 标识的时机	FIA_UID.1
FIA_UID.1	无依赖关系	—

附 录 C
（资料性）
攻击分值计算方法

C.1 概述

一般性漏洞指南包括：

——规避安全机制（Bypassing）；

——篡改安全功能（tampering）；

——任何用于测试排列性机制、概率性机制及其他机制的直接攻击（direct attacks）；

——对TOE信号的监控（monitoring）；

——对TOE的非预期使用（misuse）。

在对任何产品的脆弱性分析中，起码要覆盖以上五类一般性漏洞。针对于芯片类产品，需要评估人员做脆弱性分析时额外考虑以下方面：

——物理攻击 （Physical attacks）；

——绕过传感器或过滤器 （Overcoming sensors and filters）；

——扰动攻击 （Perturbation attacks）；

——利用故障分析提取密钥（Retrieving keys with Fault Analysis）；

——侧信道攻击 （Side channel attacks）；

——利用测试特性 （Exploitation of Test features）；

——随机数生成器攻击 （Attacks on RNG）；

——软件攻击 （Software attacks）；

——应用隔离 (Application isolation)。

漏洞评估活动的目的是确定TOE在其运行环境中是否存在缺陷或弱点，以及这些缺陷或弱点是否可被利用。该判断基于评估人员所进行的分析，并辅以评估人员的测试结果加以支持。

AVA_VAN.5评估安全目标如下：

——评估人员应通过系统性的方法化漏洞分析，以识别目标评估对象（TOE）中可能存在的潜在漏洞；

——评估人员应执行渗透测试，以验证这些潜在漏洞在TOE的实际运行环境中是否无法被利用；

——评估人员所实施的渗透测试应在假设攻击潜力为“高”（High）的前提下。

AVA_VAN.5评估人员执行要素如下：

——评估人员应确认所提供的信息符合所有关于证据内容和呈现方式的要求；

——评估人员应查阅公共领域的信息来源，以识别目标评估对象（TOE）、第三方组件清单中的组件，以及TOE所依赖的环境中具体IT产品中可能存在的潜在漏洞；

——评估人员应使用指导文档、功能规格说明、TOE设计、安全架构描述以及实现表示，对TOE进行独立的、系统性的方法化漏洞分析，以识别其中可能存在的潜在漏洞；

——评估人员应基于已识别的潜在漏洞开展渗透测试，以确定TOE是否能够抵御具备高攻击潜力的攻击者所实施的攻击。

在网络安全技术信息技术安全评估方法中，对脆弱性级别以及达到该级别需相对应抵御攻击潜力分值定义如下。对AVA_VAN.5级别，TOE的抵抗力需大于或等于31分。攻击者在准备攻击已存在的威胁时必须首先识别出威胁。因此将攻击划分为标识和攻击两个阶段。标识阶段主要是创建各种攻击思路，并论证攻击思路的可能性，包括设计攻击用测试设备。攻击阶段主要是通过分析及利用标识阶段设计的

测试设备来完成某项攻击。两个阶段都应被考虑进攻击分值计算。当某一因素的评估值接近评分区间的边界时，评估人员应考虑在表格所列数值之间选择一个中间值。例如，如果执行某项攻击需要二十个样本，则该因素的评分可在“1到4”之间选择一个适当的值；又如，如果某设计基于公开可获得的设计方案，但开发者进行了某些修改，则应根据评估人员对这些设计变更影响的判断，在“0到3”之间选择一个合适的值。以下评分表仅作为评估的参考指南。

对于识别阶段，以及攻击阶段的分析，攻击潜力分值计算，需考虑6个具体因素：

——消耗时间；

——攻击者技术水平；

——安全芯片知识；

——安全芯片样本；

——攻击设备；

——开放样本。

C.2 消耗时间

本文所涉及的消耗时间定义如表C.1所示。

表 C.1 消耗时间分值

消耗时间	标识阶段	攻击阶段
<1小时	0	0
<1天	1	3
<1周	2	4
<1个月	3	6
>1个月	5	8
不可实施	*	*

不可实施的定义为，在攻击者可用的时间范围内，该攻击路径是不可利用的（通用假设，3-5年）。在评估结束时，评估者必须评定实施最小攻击路径所用的时间。

C.3 攻击者技术水平

指在应用领域或者产品类型等方面的通用知识等级。详细攻击者的技术水平定义见表C.2和表C.3。

表 C.2 攻击者等级说明

专业级别	等级说明
外行	是指和专家和精通人员相比是外行，不具备专业技术的人员。
精通	熟悉安全特性以及典型攻击的人员。
专家	对安全芯片相关的算法，协议，硬件，安全的概念及原理等方面非常熟悉的人员，以及对新的攻击的定义，技术及工具非常熟悉的人员。
多领域专家	具有不同领域的专业知识的人员，且这些领域应严格不同，比如硬件和加密算法。

表 C.3　攻击者等级分值

专业级别	标识阶段	攻击阶段
外行	0	0
精通	2	2
专家	5	4
多领域专家	7	6

C.4　对安全目标的了解

指获取特定的和安全芯片相关的专门技术。安全芯片知识包括公开，受限，敏感，关键和非常关键五个等级。详细定义见表C.4和C.5。

表 C.4　安全芯片知识等级

安全芯片知识	等级说明
公开	和安全芯片相关的信息，每个人都很容易获得（例如从互联网）的信息，或者可由厂商提供给任何客户的信息，这些都被认为是公开的。
受限	和安全芯片相关的信息（例如从厂商技术规格说明书中获得的信息）。如果他是先申请后发放，并且发放需要注册，则此类信息也被认为是受限制的信息。
敏感	高层设计和低层设计资料。
关键	安全芯片设计实现相关资料和源代码。
非常关键	这些知识不仅能够区分高级设计和低级设计，同时还包括产品的原理图和源代码。

表 C.5　安全芯片知识等级分值

安全芯片知识	标识阶段	攻击阶段
公开	0	0
受限	2	2
敏感	4	3
关键	6	5
非常关键	9	*
不可实施	*	*

如果信息仅由高度安全的IT系统维护（例如在受保护的场所中，类似于对关键或非常关键级别信息的保护），则该信息被视为不具备实用性。

C.5　安全芯片样本数

攻击场景可能需要多个安全芯片样本，根据攻击者需要获得安全芯片的样本数，分为四个等级。详细等级值定义见表C.6。

表 C.6　安全芯片样本数等级分值

安全芯片样本数	标识阶段	攻击阶段
<10	0	0

表 C.6　安全芯片样本数等级分值（续）

<100	2	4
>100	3	6
不可实施	*	*

此处不可实施的解释为：

——对于标识阶段：不可实施标识所需样品数大于2000个，或者大于一个整数，这个整数是小于或等于n/(1+(log n)^2)的最大整数，这里n是估计产品生产数；

——对于攻击阶段：不可实施标识所需样品数大于500个，或者大于一个整数，这个整数是小于或等于n/(1+(log n)^3)的最大整数，这里n是估计产品生产数。

C.6　攻击设备

本文所涉及的攻击设备定义如表 C.7 和表 C.8 所示。

表 C.7　攻击设备

攻击所需设备	等级说明
无	不需要攻击设备。
标准	指用于分析漏洞或者进行攻击的，对攻击者来说可以快速使用设备。这类设备很容易获得，例如，已经在市面上公开销售或者从互联网下载下来的。这类设备可能包含简单的攻击脚本，个人计算机，读卡器，模式发生器，简单光学显微镜，供电电源或者简单的机械装备。
专业	攻击者不能马上获得，但是可以经过正当途径获得的设备。这包括购买中等数量的设备，（例如专门的电子卡片，专用的测试平台，协议分析器，示波器，微探针工作站，化学工作台，精确铣床设备等等）或者开发更多的攻击脚本或程序。
定制	指对公众来说还没有的设备，可能需要专门的定制，（例如，非常专业的软件）或者因为设备太专业，控制发放，甚至严格限制。也有可能时这个设备非常昂贵，（例如离子聚焦光束，扫描式电子显微镜以及激光打磨器）可以租用到的定制设备可以视为专门设备，在分析阶段开发的软件也可认为是定制设备。
多个定制	不同攻击步骤需要不同类型的定制设备。

表 C.8　攻击设备等级分值

攻击所需设备	标识阶段	攻击阶段
无	0	0
标准	1	2
专业	3	4
定制	5	6
多个定制	7	8

C.7　开放样本

开放样本是指评估员加载了带有目的性的软件到硬件平台上的样本，或是硬件平台上开放了可调的参数。此操作的目的是使不具有软件抗攻击手段的测试软件进行评估，而不会使IC内部抗攻击机制失效，

另一种可能性是评估员能够自主定义一个或多个可调的参数，如一些安全机制的开关。开放样本主要用于负责评估，只有当不使用开放样本进行攻击不可实施时，才会考虑使用开放样本。详细开放样本等级说明见表C.9和C.10。

表 C.9　开放样本等级

开放样本	等级说明
公开	开放样本：样本无保护，无发布控制，或IC用于非安全应用。 带有可调参数的样本：相关的安全参数没有可调节的外部接口。
受限	开放样本：收到安全芯片的说明书，IC的数据手册等典型保护，或发布没有额外的控制，IC用于非安全应用。 带有可调参数的样本：提供可调节的安全参数，已知可调节参数对于攻击者可用。
敏感	开放样本：高层设计/低层设计受保护。 带有可调参数的样本：除关键安全参数之外的安全参数全部可调，已知可调节参数对于攻击者可用。
关键	开放样本：实现级受保护，这要求非常少的开放样本被生产，并且有非常严格的发布控制，确保接受机构能被设置相同级别的控制。 带有可调参数的样本：关键安全参数可调，已知可调节参数对于攻击者可用。

表 C.10　开放样本等级分值

开放样本	标识阶段	攻击阶段
公开	0	*
受限	2	*
敏感	4	*
关键	6	*

攻击分值计算示例见表C.11。

表 C.11　攻击分值计算示例

因素	标识阶段分值		攻击阶段分值	
攻击时间	<1天	1	<1月	6
攻击者技术水平	多领域专家等级	7	多领域专家等级	6
安全芯片知识	受限	2	受限	2
安全芯片样本数	<10个	0	<10个	0
攻击设备	专业	3	专业	4
开放样本	无	0	无	0
每个阶段攻击分值		13		18
总攻击分值				31

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技术要求

T/TAF 355—2026

*

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