ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0098.5—2012

中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

China financial mobile payment—Test specifications—
Part 5: Embedded software security of secure element (SE)

2012－12－12 发布 2012－12－12 实施

中国人民银行 发布

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 6
5　测试条件 6
6　SE 嵌入式软件安全检测 6
7　SE 多应用平台安全检测 25
8　移动支付 SE 规格符合性检测 33
附录 A（规范性附录）　SE 嵌入式软件安全要求 37
附录 B（资料性附录）　多应用平台安全与嵌入式软件 SFRs 参照 60
参考文献 65

前　言

《中国金融移动支付 检测规范》标准由以下8部分构成：

——第1部分：移动终端非接触式接口；

——第2部分：安全芯片；

——第3部分：客户端软件；

——第4部分：安全单元（SE）应用管理终端；

——第5部分：安全单元（SE）嵌入式软件安全；

——第6部分：业务系统；

——第7部分：可信服务管理系统；

——第8部分：个人信息保护。

本部分为该标准的第5部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分负责起草单位：中国人民银行科技司、中国人民银行金融信息中心、中国金融电子化公司。

本部分参加起草单位：北京银联金卡科技有限公司（银行卡检测中心）、中金国盛认证中心、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、上海市信息安全测评认证中心、信息产业信息安全测评中心、北京软件产品质量检测检验中心、中钞信用卡产业发展有限公司、上海华虹集成电路有限责任公司、上海复旦微电子股份有限公司、东信和平智能卡股份有限公司、大唐微电子技术有限公司、武汉天喻信息产业股份有限公司、恩智浦半导体有限公司。

本部分主要起草人：李晓枫、陆书春、潘润红、杜宁、李兴锋、张雯华、刘力慷、刘志刚、聂丽琴、李晓、尚可、郭栋、熊文韬、宋铮、李宏达、王冠华、胡一鸣、张晓、平庆瑞、张志茂、陈君、彭美玲、李微、陈吉、程恒。

引　言

随着移动支付新业务、新产品、新管理模式的不断涌现，以客户需求为主导的移动支付业务出现了不断交融和细化的趋势，不同机构、不同部门、不同业务之间的信息交换和信息共享变得越来越频繁。

SE作为移动支付客户端安全部件，负责对交易关键数据进行安全存储和运算，SE嵌入式软件的安全直接影响到移动支付系统的安全性。标准本部分针对SE嵌入式软件安全功能及安全保证要求提出通用性检测指导，并对SE的多应用平台安全特性提供参考用检测案例。前者供SE嵌入式软件评估与检测单位参考，后者供SE嵌入式软件设计、制造单位进行产品设计生产参考。

中国金融移动支付　检测规范
第5部分：安全单元（SE）嵌入式软件安全

1　范围

由于移动支付对多应用的支持，SE嵌入式软件需考虑实现多应用平台以支持SE内容动态管理。相应地，SE嵌入式软件安全包括：SE多应用平台安全和SE应用安全。此外，由于移动支付SE需配合实现不同的移动支付商业模式，其平台软件应实现移动支付所需的特定基本服务、辅助安全域设置、安全通道协议等。

本部分规范的第6章旨在针对移动支付SE嵌入式软件安全功能及安全保证要求提出通用性检测指导；第7章针对SE多应用平台安全特性设计了相关的检测案例；第8章根据针对SE的特定配置需求，给出了相关的规格符合性测试指导。

SE多应用平台软件与上层应用无关，多应用平台安全用以保障SE多应用管理相关的安全属性，其安全检测应参照标准本部分的SE多应用平台安全检测规范；SE应用包括金融支付应用和非金融支付应用，其安全检测需根据标准本部分的第6章，配合具体业务功能进行制定；移动支付SE定制规范涉及的内容因影响到移动支付SE的安全性及联网通用性，应参照标准本部分的移动支付SE规格符合性检测规范进行相应的检测。

本部分的使用对象主要为从事SE嵌入式软件设计、制造、评估与检测单位。SE的发行机构也可参考本部分以获得对移动支付SE产品安全风险的进一步了解，以协助产品选型和风险控制过程。

2　规范性引用文件

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

GB/T 18336　信息技术 安全技术 信息技术安全性评估准则

JR/T 0025.12　中国金融集成电路（IC）卡规范 第12部分：非接触式IC卡支付规范

JR/T 0097-2012　中国金融移动支付 可信服务管理技术规范

JR/T 0089.2-2012　中国金融移动支付 安全单元 第2部分：多应用管理规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

持卡者验证方法　cardholder verification method (CVM)

用于确保当前持卡者即合法持卡者的方法。

3.2

授权管理者　controlling authority

借助强制性的数据鉴别模式的确认，拥有对SE内容进行管理控制权限的角色。

3.3

DAP 数据块 DAP block

加载文件中用于对加载文件数据块进行可信性验证的部分。

3.4

DAP 验证 DAP verification

安全域对加载文件的可信性进行验证的机制。

3.5

委托管理 delegated management

由认证后的应用提供方来执行的、预先授权的对SE内容进行改变的行动。

3.6

可执行加载文件 executable load file

实际存在于SE上的包含一个或多个应用的可执行代码（可执行模块）的容器，它既可以保存在只读内存中，也可以作为加载文件数据块的映像在可变内存中生成。

3.7

可执行模块 executable module

可执行加载文件中包含一个单独应用的可执行代码。

3.8

内部通信信道 internal communication channel

TOE各分离部分间的通信信道。

3.9

TOE 内部传送 internal TOE transfer

在TOE各分离部分之间交换数据。

3.10

TSF 间传送 inter-TSF transfer

在TOE与其它可信IT产品的安全功能之间交换数据。

3.11

发行者安全域 issuer security domain (ISD)

负责对SE管理者（通常是SE发行方）的管理、安全、通信需求进行支持的SE上首要实体。

3.12

生命周期状态 life cycle state

SE或SE内容在生命周期中的某个特定状态。

3.13

加载文件 load file

传送加载到多应用SE上的某种文件，包含了加载文件数据块以及一个或者多个DAP数据块（DAP Block）。

3.14

消息鉴别码 message authentication code (MAC)

经由对称加密转换得到的数据码，用于确保原始数据来源的合法性和数据自身的一致性。

3.15

平台环境 OPEN

拥有平台注册表的SE上的核心管理实体。OPEN的主要职能包括：向应用提供API，命令转发，应用选择，逻辑通道管理以及SE内容管理。

3.16

组织安全策略 organizational security policies

一个组织为其运转而强制推行的一个或多个安全规则、过程、规范和指南。

3.17

个人化 personalization

SE发行者职责的最后流程，通过该流程配置SE、装载安全参数和设置密钥。个人化流程结束后，SE就可以完全操作并可发到最终用户手中。

3.18

平台 platform

芯片上操作系统、运行时环境和平台软件的总称。

3.19

预个人化数据 pre-personalization data

所有由软件开发者提供并由IC制造方存放至非易失性存储器里的数据。

3.20

收条 receipt

SE根据SE发行方要求出具的一个加密值，用来作为一个委托管理操作已经执行的证据。

3.21

识别数据 recognition data

由SE制造方定义并在SE生命周期的制造和测试阶段存放于非易失性存储器的数据，用于追溯使用。

3.22

运行时环境 runtime environment

为SE上的多应用操作提供安全运行环境的核心功能，它是SE管理器的一个补充。

3.23

安全属性 security attribute

用于执行TSP的，主体、用户、客体、信息或资源的特征。

3.24

安全通道 secure channel

为SE外部实体和SE之间的信息交换提供某种安全保障的通信机制。

3.25

安全通道协议 secure channel protocol

安全通信协议和相关安全服务的统称。

3.26

安全通道会话 secure channel session

应用会话期间建立的一种特殊会话。开始于安全通道的初始化，结束于安全通道的终结或者应用会话或SE会话的终结。

3.27

安全域 security domain (SD)

负责对某个SE外部实体（例如SE发行方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的SE内部实体。

3.28

安全功能(SF) security function (SF)

为执行TSP中一组紧密相关的规则子集而必须依赖的TOE的一个或多个部分。

3.29

安全功能策略(SFP) security function policy (SFP)

由一个SF执行的安全策略。

3.30

SE 管理器 SE manager

负责对SE及SE上资源进行管理的SE嵌入式软件组件的统称，包括：平台环境、发行者安全域、持卡者验证方法服务提供方等等。

3.31

安全目的 security objective

意在对抗特定的威胁或满足特定的组织安全策略和假设的一种陈述。

3.32

安全要求 security requirements

安全要求包括安全功能要求SFR(Security Functional Requirements)和安全保证要求SAR(Security Assurance Requirements)。

3.33

安全目标(ST)　security target (ST)

作为一个既定TOE的评估基础使用的一组安全要求和规范。

3.34

辅助安全域　supplementary security domain (SSD)

发行者安全域之外的其它安全域。

3.35

评估对象(TOE)　target of evaluation (TOE)

作为评估主体的一个IT产品或系统以及相关的指导性文档。

3.36

TOE 安全功能(TSF)　TOE security function (TSF)

正确执行TSP所必须依赖的所有TOE硬件、软件和固件的集合。

3.37

TOE 安全功能接口(TSFI)　TOE security function interface (TSFI)

一组接口，不管是交互式（人机接口）的，还是编程式（应用编程接口）的，TSF通过这些接口访问调配TOE资源，或者通过它们从TSF中获取信息。

3.38

TOE 安全策略(TSP)　TOE security policy (TSP)

规定在一个TOE中如何管理、保护和分配资产的一组规则。

3.39

TOE 安全策略模型　TOE security policy model

TOE所执行的安全策略的一种结构化表示。

3.40

令牌　token

SE发行方出具的一个加密值，用来作为一个委托管理操作已经被授权进行的证据。

3.41

TSF 控制外传送　transfers outside TSF control

与不受TSF控制的实体交换数据。

3.42

可信信道　trusted channel

一种手段，通过该手段一个TSF能同远程的一个可信IT产品进行具有必要的信任的通信以支持TSP。

3.43

可信路径　trusted path

一种手段，通过该手段一个用户能同一个TSF进行具有必要信任的通信以支持TSP。

3.44

TSF 数据 TSF data

可能会影响TOE操作的、TOE产生的或为TOE产生的数据。

3.45

TSF 控制范围(TSC) TSF scope of control (TSC)

可与TOE或在TOE中发生的，并服从TSP规则的交互的集合。

4 缩略语

以下符号和缩略语适用于本部分。

CC	Common Criteria	通用准则
EAL	Evaluation Assurance Level	评估保证级
IT	Information Technology	信息技术
PP	Protection Profile	保护轮廓
SAR	Security Assurance Requirements	安全保证要求
SF	Security Function	安全功能
SFP	Security Function Policy	安全功能策略
SFR	Security Functional Requirements	安全功能要求
SOF	Strength of Function	功能强度
ST	Security Target	安全目标
TOE	Target of Evaluation	评估对象
TSC	TSF Scope of Control	TSF控制范围
TSF	TOE Security Functions	TOE安全功能
TSFI	TSF Interface	TSF接口
TSP	TOE Security Policy	TOE安全策略

5 测试条件

默认环境条件（温度、湿度等）是指常温20±3℃，相对湿度在20%-80%RH之间。如无特殊说明，后续案例均采用此环境条件。

6 SE 嵌入式软件安全检测

6.1 嵌入式软件安全概述

根据GB/T 18336相关内容，移动支付SE嵌入式软件需满足的安全功能要求及安全保证要求见规范性附录A.1。

6.2 SE 嵌入式软件安全检测

6.2.1 安全功能检测

6.2.1.1 FAU 类：安全审计

6.2.1.1.1 安全告警（FAU_ARP.1）

检测目的：验证 SE 具备安全告警功能。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 具备安全告警功能。模拟潜在的安全侵害，如改变工作电压、扰乱时钟频率以及穷举 PIN 等，验证当检测到侵害时，TSF 应采取动作作为响应，防止安全侵害。

通过标准：当检测到可能的安全侵害时，TSF 采取相应的动作作出响应，防止安全侵害。

6.2.1.1.2 审计列表生成（FAU_GEN.1）

检测目的：验证 SE 具备审计列表生成功能。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 具备审计列表生成功能。模拟审计事件，使 SE 生成审计记录，然后读出生成的审计记录，验证结果是否包含必要的信息。

通过标准：安全功能应能为下述可审计事件生成审计记录：在评估对象初始化操作、其它专门定义的可审计事件审计级别之内的所有可审计事件。如：安全功能在初始化操作中记录的审计记录，包括：

a) IC 制造日期和序列号；

b) 操作软件标识和发布日期。

6.2.1.1.3 潜在侵害分析（FAU_SAA.1）

检测目的：验证 SE 具备依据规则触发审计事件的能力。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 依据规则触发审计事件。模拟各种审计事件触发条件，验证 SE 是否依据规则触发审计事件。

通过标准：安全功能支持用预定的一系列规则去监控审计事件，并根据这些规则指示出对安全策略的潜在侵害。

6.2.1.1.4 可选择的审计（FAU_SEL.1）

检测目的：验证 SE 具备删除或添加审计规则的能力。

测试过程：审查厂商提交的文档，验证厂商已声明依据特定属性删除或添加的审计规则。尝试为 SE 添加或删除审计规则，审计规则的修改依据特定的属性进行。

通过标准：安全功能可以根据以下属性包括或从以下一套被审计事件中排除可审计事件：客体身份、用户身份、主体身份、主机身份、事件类型。

6.2.1.1.5 受保护的审计踪迹存储（FAU_STG.1）

检测目的：验证 SE 具备保护审计记录的能力。

测试过程：审查厂商提交的文档，验证厂商已声明为审计记录提供适当的权限保护；对 SE 内存储的审计记录进行读取、修改和删除操作，验证 SE 为审计记录提供的权限保护有效。

通过标准：安全功能可保护所存储的审计记录，避免未授权的删除和修改。

6.2.1.1.6 在审计数据可能丢失情况下的行为（FAU_STG.3）

检测目的：验证在审计记录超限时，SE 能确保交易完整性。

测试过程：审查厂商提交的文档，验证厂商已声明在审计记录超限时，SE 能确保交易的完整性。模拟审计记录超限的情景，如审计区溢出等，验证 SE 提供适当的控制措施，以保证交

易的完整性。

通过标准：如果审计踪迹超过预定的限制，安全功能采取相应的行为，确保交易的完整性。

6.2.1.2 FCS 类：加密支持

6.2.1.2.1 密钥生成（FCS_CKM.1）

检测目的：验证 SE 密钥生成算法和长度符合安全要求。

测试过程：审查厂商提交的文档，验证厂商声明的密钥生成算法和长度符合安全要求。执行 SE 的密钥生成功能，验证密钥生成的算法和长度是否与厂商声明一致，并且符合安全要求。

通过标准：安全功能将根据符合相关标准的特定密钥生成算法和特定密钥长度来产生密钥。

6.2.1.2.2 密钥分发（FCS_CKM.2）

检测目的：验证 SE 的密钥分发方式符合要求。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 的密钥分发方式符合要求。执行密钥分发命令，尝试分发密钥，验证 SE 的密钥分发方式与厂商声明一致，只允许按照规定的安全方式进行分发。

通过标准：安全功能将根据符合相关标准的特定密钥分发方法来分发密钥。

6.2.1.2.3 密钥访问（FCS_CKM.3）

检测目的：验证 SE 的密钥访问方式符合要求。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 的密钥访问方式符合要求。执行可能的读写命令，尝试访问 SE 内存在的密钥，验证 SE 的密钥访问方式与厂商声明一致，只允许通过适当的方式访问。

通过标准：只有在核心模块的控制下才能读到并还原密钥，不能将密钥送到密码运算单元之外的任何地方。

6.2.1.2.4 密码运算（FCS_COP.1）

检测目的：验证 SE 密码算法符合要求并具有正确性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 密码算法符合要求。执行密码算法相关的命令，将输出结果与期望结果比较，验证 SE 的密码算法是否符合要求。

通过标准：SE 的密码算法符合相关要求，输出结果与期望值一致。

6.2.1.2.5 密钥销毁（FCS_CKM.4）

检测目的：验证 SE 密钥销毁机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 密码销毁安全功能。执行密钥销毁操作，验证已安全销毁不再需要的密钥，不会有敏感信息泄露。

通过标准：安全功能可根据符合相关标准的一个特定的密钥销毁方法来销毁密钥，已销毁密钥信息不可获得。

6.2.1.3 FCO 类：通信

6.2.1.3.1 强制性原发证明（FCO_NRO.2）

检测目的：强制性原发证明机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现强制性原发性证明机制。执行信息传送，验

证仅当存在传送消息的原发证据且验证有效的情况下，消息传送方可执行。

通过标准：安全功能在任何时候都应对所传送的信息类型强制产生原发证据；
安全功能应能将信息原发者的属性和信息的信息域与证据相关联。

6.2.1.4 FDP 类：用户数据保护

6.2.1.4.1 子集访问控制（FDP_ACC.1）

检测目的：验证 SE 具备子集访问安全控制策略。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 已实现子集访问控制策略。执行 SE 的安全功能，验证只有在满足子集控制策略的条件下，才能正确执行相应的安全功能。

通过标准：安全功能将对安全功能策略覆盖的主体、客体和它们之间的特定操作执行软件访问控制策略。

6.2.1.4.2 完全访问控制（FDP_ACC.2）

检测目的：验证 SE 具备安全访问控制策略。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 具备安全功控制策略。执行 SE 的安全功能，验证只有在满足控制策略的条件下，才能正确执行相应的安全功能。

通过标准：安全功能应对主体和客体及策略所涵盖主体和客体之间的所有操作执行访问控制策略；
安全功能应确保安全功能控制范围内的任何主体和客体之间的所有操作都被一个访问控制策略涵盖。

6.2.1.4.3 基于安全属性的访问控制（FDP_ACF.1）

检测目的：验证 SE 安全功能基于安全属性决定访问控制。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 的所有安全功能基于安全属性和安全属性组。执行安全功能，验证 SE 基于安全属性和安全属性组的控制策略是否有效。

通过标准：安全功能基于安全属性和安全属性组，对客体执行软件访问控制策略；
安全功能执行预定规则，以决定受控主体与受控客体间的操作是否被允许；
安全功能基于安全属性的授权主体访问客体的规则来授权主体访问客体；
安全功能基于预定规则明确拒绝主体对客体的访问。

6.2.1.4.4 基本数据鉴别（FDP_DAU.1）

检测目的：验证 SE 基本数据鉴别有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 实现基本数据鉴别安全功能。执行安全功能，验证 SE 基本数据鉴别机制的有效性。

通过标准：安全功能提供一种能力，以生成能用来作为客体或不同类型信息有效性担保的证据。

6.2.1.4.5 不带安全属性的用户数据输出（FDP_ETC.1）

检测目的：SE 应保证输出不带相关安全属性的用户数据。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 执行访问控制策略和（或）信息流控制策略。执行读数据命令，验证输出结果不带相关的安全属性。

通过标准：安全功能在安全功能策略控制下输出用户数据到 SE 安全控制范围之外时，执行访问控制策略和（或）信息流控制策略；
安全功能输出不带相关安全属性的用户数据。

6.2.1.4.6 子集信息流控制（FDP_IFC.1）

检测目的：SE 基于特定要素执行信息流控制策略。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 基于特定要素执行信息流控制策略。执行读写命令，验证 SE 信息流子集控制策略有效。

通过标准：安全功能对主体、信息及安全功能策略所覆盖导致受控信息流入、流出受控主体的操作执行信息流控制策略。

6.2.1.4.7 完全信息流控制（FDP_IFC.2）

检测目的：SE 对所有操作执行信息流控制策略。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 实现安全信息流控制机制。执行读写命令，验证 SE 完整信息流控制策略有效性。

通过标准：安全功能对主体和信息及控制策略所涵盖导致信息流入、流出主体的所有操作执行信息流控制策略；

安全功能确保导致安全功能控制范围内任意信息流入、流出安全功能控制范围内任意主体的所有操作都至少被一个信息流控制策略涵盖；

安全功能应对任意两个有效的信息流控制安全属性执行下列关系：

a) 存在一个有序函数，也就是说，给定两个有效的安全属性，可判断它们是否相等，是否其中一个大于另一个，还是两者不可比较；

b) 在安全属性集合中存在一个“最小上界”，也就是说，给定任意两个有效的安全属性，存在一个有效的安全属性大于或等于这两个安全属性；

c) 在安全属性集合中存在一个“最大下界”，也就是说，给定任意两个有效的安全属性，存在一个有效的安全属性不大于这两个安全属性。

6.2.1.4.8 简单安全属性（FDP_IFF.1）

检测目的：基于主体类型和信息安全属性的 SE 简单信息流控制策略的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 简单信息流控制策略基于主体类型和信息安全属性。执行读写命令，验证 SE 能够根据简单安全属性明确接收或拒绝信息流。

通过标准：安全功能在预定主题类型和信息安全属性的基础上执行信息流控制策略；

如果对每一个操作，在主体和信息安全属性间必须有基于安全属性的关系，安全功能允许受控主体和受控信息之间存在经由受控操作的信息流；

安全功能执行附加的信息流控制策略；

安全功能提供附加的安全功能策略能力；

安全功能根据基于安全属性的规则明确授权信息流；

安全功能根据基于安全属性，明确拒绝信息流的规则明确拒绝信息流。

6.2.1.4.9 分级安全属性（FDP_IFF.2）

检测目的：基于主体类型和信息安全属性的 SE 完全信息流控制策略的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 完全信息流控制策略基于主体类型和信息安全属性。执行读写命令，验证 SE 能够根据完整安全属性明确接收或拒绝信息流。

通过标准：安全功能应基于指定策略控制下的主体和信息，以及每个对应的安全属性，执行信息流控制策略；

如果基于安全属性间有序关系支持：对每一个操作，在主体和信息安全属性之间必须支

持基于安全属性的关系，安全功能应允许信息在受控主体和受控信息之间经由受控操作流动；
安全功能应执行附加的信息流控制策略规则；
安全功能应提供策略能力；
安全功能应根据基于安全属性明确批准信息流的规则，明确批准一个信息流；
安全功能应根据基于安全属性明确拒绝信息流的规则，明确拒绝一个信息流。

6.2.1.4.10 不带安全属性的用户数据输入（FDP_ITC.1）

检测目的：不带安全属性的用户数据输入策略的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明从 SE 外输入数据应执行访问控制策略和信息流控制策略。执行写命令向 SE 输入数据，验证 SE 忽略与数据相关的安全属性；向 SE 写入符合安全控制规则的数据，验证 SE 是否接受；向 SE 写入不符合安全控制规则的数据，验证 SE 是否拒绝。
通过标准：安全功能在安全功能策略控制下从评估对象安全控制范围之外输入用户数据时，应执行访问控制策略和信息流控制策略；
安全功能应略去任何与评估对象安全控制范围之外输入的数据相关的安全属性；
安全功能在安全功能策略控制下从安全控制范围之外输入数据时应执行附加的输入控制规则。

6.2.1.4.11 带安全属性的用户数据输入（FDP_ITC.2）

检测目的：带安全属性的用户数据输入策略的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明从 SE 外输入数据应执行访问控制策略和信息流控制策略。执行写命令向 SE 输入数据，验证 SE 忽略与数据相关的安全属性；向 SE 写入符合安全控制规则的数据，验证 SE 是否接受；向 SE 写入不符合安全控制规则的数据，验证 SE 是否拒绝。
通过标准：在策略控制下从安全功能控制范围之外输入用户数据时，安全功能执行访问控制策略或信息流控制策略；
安全功能使用与所输入数据相关的安全属性；
安全功能确保所使用协议在安全属性和接收到的用户数据之间提供了明确的关联；
安全功能确保对所输入用户数据的安全属性的解释与用户数据源的解释是一样的；
在策略控制下从 TSC 之外输入用户数据时，安全功能执行附加的输入控制规则。

6.2.1.4.12 基本内部传输保护（FDP_ITT.1）

检测目的：SE 在内部各部分间传输的数据应执行访问控制策略和信息流控制策略。
测试过程：审查厂商提交的文档，验证厂商已声明对 SE 内部各部分间传输的数据执行访问控制策略和信息流控制策略；执行任何可行的实验，验证 SE 执行的访问控制策略和信息流控制策略与厂商声明的一致。
通过标准：在评估对象物理上分隔的部分间传递用户数据时，安全功能执行访问控制策略和信息流控制策略，以防止用户数据泄露。

6.2.1.4.13 子集剩余信息保护（FDP_RIP.1）

检测目的：验证 SE 清除回收资源的信息内容。
测试过程：审查厂商提交的文档，验证厂商已声明对 SE 内回收的资源进行了清除。通过审查源代

码以及任何可行的实验，验证 SE 的相关实现与厂商声明一致。

通过标准：安全功能应保证在客体收回资源的情况下，资源以前的信息内容不可得。

6.2.1.4.14 基本回滚（FDP_ROL.1）

检测目的：验证 SE 基本回滚机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现基本回滚机制。通过审查源代码以及任何可行的实验，验证 SE 的相关实现与厂商声明一致。

通过标准：安全功能执行访问控制策略或信息流控制策略，以允许对信息或客体的操作进行回滚；安全功能提供回退全部操作的能力，但用户只能选择针对回退策略或回退可进行的边界条件回退其中一部分操作。

6.2.1.4.15 存储数据完整性监视和反应（FDP_SDI.2）

检测目的：验证存储数据完整性监视和反应机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现存储数据完整性监视和反应机制。通过审查源代码以及任何可行的实验，验证 SE 的实现与厂商声明一致。

通过标准：安全功能基于用户数据属性，对所有客体，监视存储在评估对象内的用户数据是否存在完整性错误；

检测到完整性错误时，安全功能应采取的动作。

6.2.1.4.16 数据交换完整性（FDP_UIT.1）

检测目的：验证 SE 具备保证数据交换完整性的措施。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 具备保证数据交换完整性的措施。执行相关命令，验证 SE 保证数据完整性的措施是否有效。

通过标准：安全功能应执行访问控制策略和/或信息流控制策略以能够传输和接受用户数据，避免修改错误。

6.2.1.5 FIA 类：标识与鉴别

6.2.1.5.1 鉴别失败处理（FIA_AFL.1）

检测目的：验证 SE 检测并记录鉴别失败次数并采取相应措施。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 检测并记录鉴别失败次数并采取相应措施。模拟鉴别失败情景，验证 SE 采取的措施是否有效。

通过标准：安全功能成功检测与鉴别事件相关的不成功鉴别尝试的规定次数；

当达到或超过规定的不成功鉴别尝试次数时，安全功能采取相应动作。

6.2.1.5.2 用户属性定义（FIA_ATD.1）

检测目的：安全功能应为每一个用户保存安全属性列表。

测试过程：审查厂商提交的文档，验证厂商已声明为每一个用户保存安全属性列表。执行任何可行的实验，验证 SE 的实现与厂商声明一致。

通过标准：安全功能应为每一个用户保存安全属性列表。

6.2.1.5.3 鉴别定时（FIA_UAU.1）

检测目的：在用户鉴别成功前 SE 应限制可执行的操作。

测试过程：审查厂商提交的文档，验证厂商已声明在用户鉴别成功前 SE 应限制可执行的操作。执行模拟交易，在用户被鉴别前直接执行受安全功能控制的操作，验证 SE 响应是否正确。

通过标准：在用户被鉴别之前，安全功能可以允许代表用户实施受安全功能控制的某些动作；只有在用户已被成功鉴别后，SE 才能代表用户执行所有其它受安全功能控制的动作。

6.2.1.5.4 一次性鉴别（FIA_UAU.4）

检测目的：一次性鉴别的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 实现一次性鉴别机制。执行模拟交易，在使用同一鉴别机制的情况下，验证鉴别数据不可重复使用。

通过标准：安全功能可防止与确定的鉴别机制有关的鉴别数据的再次使用。

6.2.1.5.5 受保护的鉴别反馈（FIA_UAU.7）

检测目的：SE 应保证鉴别反馈的安全性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 应保证鉴别反馈的安全性。模拟各种鉴别命令，接收并分析 SE 的反馈数据是否泄漏敏感信息。

通过标准：在鉴别过程中，安全功能不应提供任何敏感信息给用户。

6.2.1.5.6 识别定时（FIA_UID.1）

检测目的：在用户鉴别成功前 SE 应限制可执行的操作。

测试过程：审查厂商提交的文档，验证厂商已声明在用户识别成功前 SE 应限制可执行的操作。执行模拟交易，在用户识别前直接执行受安全功能控制的操作，验证 SE 是否拒绝。

通过标准：在用户被识别之前，安全功能允许代表用户实施受安全功能控制的某些动作。
只有在用户已被成功识别后，SE 才能代表用户执行所有其它受安全功能控制的动作。

6.2.1.5.7 任何动作前的用户标识（FIA_UID.2）

检测目的：在任何动作前进行用户标识的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现任何动作前进行用户标识。执行模拟交易，验证在用户被成功标识前后，允许该用户的标识机制有效性。

通过标准：在用户被成功标识前，仅允许执行代表该用户的、在安全功能介导动作列表中的动作；在允许执行代表该用户的任何其它安全功能介导动作之前，该用户必须首先被成功识别。

6.2.1.5.8 用户-主体绑定（FIA_USB.1）

检测目的：验证用户-主体绑定机制有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现用户-主体绑定机制。执行模拟交易，验证用户-主体绑定机制的有效性。

通过标准：安全功能将用户安全属性与代表用户活动的主体相关联；
安全功能执行属性初始关联规则，将用户安全属性与代表用户活动的主体初始关联；
安全功能执行属性更改规则，管理与代表用户活动的主体相关联的用户安全属性的改变。

6.2.1.6 FMT 类：安全管理

6.2.1.6.1 安全功能行为的管理（FMT_MOF.1）

检测目的：验证 SE 仅允许已授权并识别的角色修改相应的安全功能行为。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 仅允许已授权并识别的角色修改相应的安全功能行为。执行模拟交易，验证 SE 拒绝未授权或未识别的角色修改安全功能行为。

通过标准：安全功能应仅限于已授权并识别的角色修改下列安全功能行为：

a) 数据访问级别的管理（该级别一旦确定，不能变更）；
b) 在安全告警事件中要采取行为的管理；
c) 通过在规则集中增加、修改或删除规则，来维护违规分析规则；
d) 密钥属性变更的管理，密钥属性包括密钥类型（例如：公钥、私钥），有效期和用途（电子签名、密钥加密、密钥协议、数据加密）；
e) 在鉴别失败事件中要采取行为的管理；
f) 在用户成功被鉴别之前所能采取行为的管理；
g) 如果授权管理者能改变用户被识别之前所能采取的行为列表，应对授权管理者的此种行为进行管理；
h) 对撤消规则的管理；
i) 对重放中所采取行为的管理；
j) SE自检发生（如初始化启动、定期间隔、其它特定条件）时的条件的管理；
k) ST中附加明确陈述的安全功能的管理。

6.2.1.6.2 安全属性的管理（FMT_MSA.1）

检测目的：验证 SE 仅允许已识别的角色修改相应的安全属性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 仅允许已识别的角色修改相应的安全属性。执行模拟交易，验证 SE 拒绝未授权或未识别的角色修改安全属性。

通过标准：安全功能执行访问控制策略和信息流控制策略，仅允许已识别的授权角色对安全属性进行改变默认值、查询、修改、删除或其它操作。

6.2.1.6.3 安全的安全属性（FMT_MSA.2）

检测目的：验证 SE 安全属性只接受安全的值。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 安全属性只接受安全的值。执行模拟交易，使用不在安全范围的值对安全属性进行修改，验证 SE 是否拒绝操作。

通过标准：安全功能确保安全属性只接受安全的值。

6.2.1.6.4 静态属性初始化（FMT_MSA.3）

检测目的：SE 应支持为安全属性设置初始值。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 允许授权角色为安全属性提供受限制的默认值，并支持为生成的客体规定新的初始值。执行模拟交易，尝试为 SE 的安全属性设置默认值，验证 SE 的行为与厂商声明的一致。

通过标准：安全功能执行访问控制策略和信息流控制策略，以便为用于执行安全功能策略的安全属性提供受限制的默认值；

安全功能允许已识别的授权角色为生成的客体或信息规定新的初始值以代替原来的默认值。

6.2.1.6.5 安全功能数据的管理（FMT_MTD.1）

检测目的：验证 SE 仅允许已识别的授权角色对安全功能数据进行修改。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 仅允许已识别的授权角色对安全功能数据进行修改。执行模拟交易，验证 SE 拒绝未授权的角色修改安全功能数据。

通过标准：安全功能仅允许已识别了的授权角色能够对安全功能数据进行改变默认值、查询、修改、删除、清空或其它操作。

6.2.1.6.6 对安全功能数据限值的管理（FMT_MTD.2）

检测目的：验证 SE 仅允许已识别的授权角色对安全功能数据限值进行管理。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 仅允许已识别的授权角色对安全功能数据限值进行管理。执行模拟交易，验证 SE 拒绝未授权的角色修改安全功能数据限值。执行模拟交易，使 SE 安全功能数据超过限值，验证 SE 是否采取相应的措施。

通过标准：安全功能仅允许已识别的授权角色对以下安全功能数据限值：

a) 对不成功鉴别尝试次数阈值的管理；

b) 其它详细定义的阈值的管理；

当安全功能数据达到或超过了指明的限值时，安全功能采取相应的动作响应。

6.2.1.6.7 安全的安全功能数据（FMT_MTD.3）

检测目的：验证 SE 安全功能数据只接受安全的值。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 安全功能数据只接受安全的值。执行模拟交易，使用不在安全范围的值对安全功能数据进行修改，验证 SE 是否拒绝操作。

通过标准：安全功能确保安全功能数据只接受安全的值。

6.2.1.6.8 撤消（FMT_REV.1）

检测目的：验证 SE 仅允许已标识的授权角色撤销安全属性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 仅允许已标识的授权角色撤销安全属性。

通过标准：安全功能仅允许已标识的授权角色撤销安全控制范围内与用户、主体、客体或其它附加资源相关的安全属性。

6.2.1.6.9 管理功能规范（FMT_SMF.1）

检测目的：验证 SE 已实现管理功能规范。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 实现管理功能规范。

通过标准：安全功能能够根据相关安全管理功能列表执行安全管理功能。

6.2.1.6.10 安全角色（FMT_SMR.1）

检测目的：验证安全角色管理机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现安全角色管理机制。

通过标准：安全功能可正常维护已标识的授权角色；

能够把用户和角色关联起来。

6.2.1.7 FPT 类：安全功能保护

6.2.1.7.1 抽象机测试（FPT_AMT.1）

检测目的：验证作为安全功能基础的抽象机所提供的安全假设是否正确运转。

测试过程：在初始化启动期间、正常运转时周期性地、授权用户提出请求时等条件下，运行一套测

试，以验证作为安全功能基础的抽象机所提供的安全假设是否正确运转。

通过标准：作为安全功能基础的抽象机所提供的安全假设可正确运转。

6.2.1.7.2 带保存安全状态的失败（FPT_FLS.1）

检测目的：验证 SE 安全功能在失败发生时保存一个安全状态。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 在安全功能失败时保存一个安全状态。模拟安全功能失败的各种情景，验证 SE 在该情景下是否保存安全状态。

通过标准：安全功能可在失败发生时成功保存安全状态。

6.2.1.7.3 内部安全功能修改的检测（FPT_ITI.1）

检测目的：检测是否具备检测安全功能数据在安全功能与远程可信 IT 产品之间传送时是否被修改的能力，假如远程可信 IT 产品知道所使用的安全机制。

测试过程：审查厂商提交的文档，验证厂商已声明实现内部安全功能修改检测。通过在安全功能和远程可信 IT 产品之间传送安全功能数据时对其进行修改，验证 SE 已实现内部安全功能修改检测。

通过标准：当安全功能数据在安全功能与远程可信 IT 产品之间传送过程中被修改时，可检测到该修改的发生。

6.2.1.7.4 内部安全功能数据传输的基本保护（FPT_ITT.1）

检测目的：SE 应保证内部传输的安全功能数据的安全性。

测试过程：审查厂商提交的文档，验证厂商已声明保证内部传输的安全功能数据的安全性。通过文档审查或任何可行的实验，验证 SE 的实现与厂商声明一致。

通过标准：安全功能可保护安全功能数据在评估对象各部分间传输时不被泄露。

6.2.1.7.5 防止物理攻击（FPT_PHP.3）

检测目的：安全功能应通过自动响应防止对安全功能的物理攻击。

测试过程：审查厂商提交的文档，验证厂商已声明安全功能通过自动响防止对安全功能的物理攻击。执行任何可行的物理攻击实验，验证安全功能是否能够自动响应，有效防止对安全功能的篡改。

通过标准：安全功能可通过自动响应防止对安全功能设备/元素的环境压力、信息监控、以及其它物理篡改情况。

6.2.1.7.6 无过度损失的自动恢复（FPT_RCV.3）

检测目的：验证无过度损失的自动恢复机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 不能从失败或服务中断自动恢复时，安全功能应进入维护模式。模拟交易过程中意外掉电的情景，验证 SE 返回安全状态；模拟任何其它可能的失败或服务中断情景，验证 SE 返回安全状态。

通过标准：当不能从失败或服务中断自动恢复时，安全功能应进入维护模式，该模式使得评估对象能返回到一个安全状态；

操作过程中意外掉电时，安全功能可确保自动地使评估对象返回到一个安全状态；

安全功能提供从失败或服务中断状态恢复的功能，可确保在安全控制范围内的安全功能数据或客体在无过度损失的情况下恢复到初始状态；

安全功能可提供确定客体能否被恢复的能力。

6.2.1.7.7 功能恢复（FPT_RCV.4）

检测目的：SE 在安全功能完成或失败情况后恢复安全状态。

测试过程：审查厂商提交的文档，验证厂商已声明安全功能完成或者失败后恢复安全状态。模拟安全功能完成和失败的各种情景，验证 SE 恢复安全状态。

通过标准：安全功能确保涉及恢复、复位、掉电或撤销操作完成之前的情况的安全功能有如下特性：即安全功能或者成功完成，或者出现指明的失败情况后，可恢复到一个安全状态。

6.2.1.7.8 重放检测（FPT_RPL.1）

检测目的：SE 具备检测重放攻击能力并正确响应。

测试过程：审查厂商提交的文档，验证厂商已声明验证 SE 具备检测重放攻击能力，并执行相应的安全功能。执行模拟交易，进行重放攻击，验证 SE 能够检测到重放攻击并拒绝交易。

通过标准：安全功能可检测确定实体的重放；
检测到重放时，安全功能应执行相应的安全功能。

6.2.1.7.9 安全策略的不可旁路性（FPT_RVM.1）

检测目的：验证 SE 的安全策略不可旁路。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 的安全策略具有不可旁路性。执行模拟交易，尝试旁路安全策略进行交易，验证交易是否拒绝。

通过标准：安全功能应确保在安全控制范围内的每一项功能被允许继续执行前，安全策略的执行功能都已被调用。

6.2.1.7.10 安全功能域的隔离（FPT_SEP.1）

检测目的：安全功能域隔离机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明在安全功能执行时维持一个安全域，防止不可信主体的干扰和篡改。执行任何可行的实验，验证 SE 的实现与厂商声明的一致。

通过标准：在安全功能执行时，维持一个安全域，防止不可信主体的干扰和篡改；
安全功能在安全控制范围内隔离各主体的安全域。

6.2.1.7.11 安全功能间基本的安全功能数据一致性（FPT_TDC.1）

检测目的：安全功能间基本的安全功能数据的一致性。

测试过程：审查厂商提交的文档，验证厂商已声明实现保证安全功能间基本安全功能数据一致性。

通过标准：当安全功能与其他可信 IT 产品共享安全功能数据时，安全功能具备提供对安全功能数据类型进行一致性解释的能力；
当解释来自其它可信 IT 产品的安全功能数据时，安全功能使用安全功能使用的解释规则。

6.2.1.7.12 安全功能检测（FPT_TST.1）

检测目的：SE 安全功能具备自检能力。

测试过程：审查厂商提交的文档，验证厂商已声明 SE 安全功能在启动初始化期间和正常工作期间周期性地或应授权用户的要求执行自检。检查其它相关文档，如源代码等，验证是否支持厂商的声明。执行自检的专有命令，观察自检是否按照厂商声明的执行。执行任何其它可行的测试，验证自检的实现与厂商声明的一致。

通过标准：安全功能在启动初始化期间和正常工作期间周期性地或应授权用户的要求，在满足产生自检的条件时执行自检；
已指明安全功能的正确操作；
安全功能为授权用户提供对安全功能数据完整性的验证能力；
安全功能为授权用户提供对所存储的安全功能可执行代码完整性的验证能力。

6.2.1.8 FPR 类：私密性

6.2.1.8.1 不可观察性（FPR_UNO.1）

检测目的：验证不可观察性。
测试过程：审查厂商提交的文档，验证厂商已声明实现保证不可观察性的措施。执行任何其它可行的测试，验证不可观察性的实现与厂商声明的一致。
通过标准：安全功能确保用户或主体不能观察由受保护的用户或主体对客体进行的操作。

6.2.1.9 FRU 类：资源利用

6.2.1.9.1 容错（FRU_FLT.1）

检测目的：验证容错机制的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现容错机制。执行失效测试，验证评估对象的能力是否正常发挥。
通过标准：安全功能确保当失效类型发生时，评估对象的能力能正常发挥。

6.2.1.9.2 最高限额（FRU_RSA.1）

检测目的：验证实现最高限额控制有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现最高限额控制有效性。执行受控资源分配测试，验证最高限额控制有效性。
通过标准：安全功能对受控资源进行最高配额分配，以便单个用户、预定义用户组、或主体能同时或在规定的时间间隔内使用。

6.2.1.10 FTP 类：可信路径/信道

6.2.1.10.1 TSF 间可信信道（FTP_ITC.1）

检测目的：验证安全功能间可信信道的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现安全功能间可信信道。模拟可信端点，验证安全功能间可信信道的有效性。
通过标准：安全功能在它自己和一个远程可信 IT 产品之间提供一条通信信道，此信道在逻辑上与其它通信信道截然不同，并提供其末端点有保证的标识，以及保护信道中数据免遭修改或泄露；
安全功能允许安全功能或远程的可信 IT 产品经由可信信道发起通信；
对于需要可信信道的功能，安全功能经由可信信道发起通信。

6.2.2 安全保证检测

6.2.2.1 ACM 类：配置管理

6.2.2.1.1 部分配置管理自动化（ACM_AUT.1）

检测目的：检查开发者使用配置管理系统使配置管理自动化。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者使用配置管理系统；
开发者提供配置管理计划；
配置管理系统能够提供一种自动方式，通过该方式确保只能对评估对象的实现表示进行已授权的变更；
配置管理系统能够提供一种自动方式来支持评估对象的生成；
配置管理计划描述配置管理系统中使用的自动工具；
配置管理计划描述在配置管理系统中如何使用自动工具。

6.2.2.1.2 配置管理过程（ACM_CAP.4）

检测目的：开发者产生支持和接受过程符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者为评估对象提供一个编号；
开发者使用配置管理系统；
开发者提供配置管理文档；
评估对象编号对评估对象的每一个版本是唯一的；
为每一个评估对象标记其编号；
配置管理文档包括配置清单、配置管理计划和接受计划；
配置清单描述组成评估对象的配置项；
配置管理文档描述对配置项进行唯一标识的方法；
配置管理系统唯一标识所有配置项；
配置管理计划描述配置管理系统是如何使用的；
证据证明配置管理系统的运作与配置管理计划相一致；
配置管理文档提供证据证明所有的配置项都被配置管理系统有效地维护；
配置管理系统提供方法保证对配置项只进行授权修改；
配置管理系统支持评估对象的产生；
接受计划描述用来接受修改过的或新建的作为评估对象一部分的配置项的程序。

6.2.2.1.3 配置管理跟踪（ACM_SCP.2）

检测目的：配置管理跟踪符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供配置管理文档；
配置管理文档可以说明配置管理系统至少能跟踪以下几项：评估对象实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档和安全缺陷；
配置管理文档描述配置管理系统是如何跟踪配置项的。

6.2.2.2 ADO 类：交付与运行

6.2.2.2.1 修改监测（ADO_DEL.2）

检测目的：开发者修改监测符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者对评估对象交付给用户的程序进行记录；

开发者使用交付程序；
交付文档描述在将不同版本的评估对象分发给用户时，用以维护安全所必需的所有程序；
交付文档描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户端收到的版本之间的任何差异；
交付文档描述如何使用多种程序来发现伪装成开发者的尝试，甚至是在开发者没有向用户发送任何东西的情况下。

6.2.2.2.2 安装、生成和启动程序（ADO_IGS.1）

检测目的：验证开发者安装、生成和启动程序符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者以文档的形式记录评估对象的安全安装、生成和启动所必需的程序；
文档描述评估对象的安全安装、生成和启动所必需的步骤。

6.2.2.3 ADV 类：开发文档

6.2.2.3.1 完全定义的外部接口（ADV_FSP.2）

检测目的：验证开发者定义的外部接口符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供功能规范；
功能规范用非形式化的风格来描述安全功能及其外部接口；
功能规范是内在一致的；
功能规范描述使用所有外部安全功能接口的用途与方法，提供所有影响、异常情况和错误信息的详情；
功能规范可完备地表示安全功能；
功能规范包括安全功能被完备表示的基本原理。

6.2.2.3.2 安全加强的高层设计（ADV_HLD.2）

检测目的：验证开发者高层设计符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供安全功能的高层设计；
高层设计的表示是非形式化的；
高层设计是内在一致的；
高层设计按子系统来描述安全功能的结构；
高层设计描述安全功能的每一个子系统所提供的安全功能；
高层设计标识安全功能要求的底层硬件、固件和软件，连同这些硬件、固件或软件实现的支持性保护机制提供的功能表示；
高层设计标识安全功能子系统的所有接口；
高层设计标识安全功能子系统的哪些接口是外部可见的；
高层设计描述安全功能子系统所有接口的用途和使用方法，并适当提供影响、异常情况和错误信息的详情；
高层设计描述把评估对象分成安全策略-实施和其它子系统的这种分离。

6.2.2.3.3 安全功能实现的子集（ADV_IMP.2）

检测目的：验证开发者安全功能实现的子集符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者应为整个安全功能集提供实现表示；
实现表示应当无歧义而且详细地定义安全功能，使得无须进一步设计就能生成安全功能；
实现表示应当是内在一致的；
实现表示应描述个部分实现之间的关系。

6.2.2.3.4 模块化（ADV_INT.1）

检测目的：验证开发者模块化设计符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者以模块方式设计和构建安全功能，以避免设计模块之间出现不必要的交互作用；
开发者提供结构化描述；
结构化描述标识安全功能的模块；
结构化描述描述每一个安全功能模块的用途、接口、参数和影响；
结构化描述描述安全功能设计是如何使得独立的模块间避免不必要的交互作用。

6.2.2.3.5 描述性低层设计（ADV_LLD.1）

检测目的：验证开发者安全功能的低层设计符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供安全功能的低层设计；
低层设计的表示是非形式化的；
低层设计是内在一致的；
低层设计以模块方式来描述安全功能；
低层设计描述每一个模块的用途；
低层设计依据所提供的安全功能性和对其它模块的依赖性关系两方面来定义模块间的相互关系；
低层设计描述如何提供每一个安全策略实施功能；
低层设计标识安全功能模块的所有接口；
低层设计标识安全功能模块的哪些接口是外部可见的；
低层设计描述安全功能模块的所有接口的用途与方法，适当时，应提供影响、异常情况和错误信息的详情；
低层设计描述如何将评估对象分离成安全策略实施模块和其它模块。

6.2.2.3.6 非形式化对应性阐明（ADV_RCR.1）

检测目的：验证开发者非形式化对应性阐明符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者在所提供的安全功能表示的所有相邻对之间提供对应性分析；
对于所提供的安全功能表示的每一个相邻对，分析可论证，较为抽象的安全功能表示的所有相关安全功能在较不抽象的安全功能表示中得到正确和完备地细化。

6.2.2.3.7 非形式化评估对象安全策略模型（ADV_SPM.1）

检测目的：验证开发者非形式化评估对象安全策略模型符合要求。

测试过程：检查提交的相关文档，验证是否支持厂商的声明。

通过标准：开发者提供安全策略模型；

开发者阐明功能规范和安全策略模型之间的对应性；

安全策略模型是非形式化的；

安全策略模型描述所有可以模型化的安全策略的规则与特征；

安全策略模型包括一个基本原理，即论证该模型对于所有可模型化的安全策略来说是一致的和完备的；

安全策略模型和功能规范之间的对应性论证可说明，所有功能规范中的安全功能对于安全策略模型来说是一致的和完备的。

6.2.2.4 AGD 类：指导性文档

6.2.2.4.1 管理者指南（AGD_ADM.1）

检测目的：验证开发者提供的管理者指南符合要求。

测试过程：检查提交的相关文档，验证是否支持厂商的声明。

通过标准：开发者提供针对系统管理人员的管理者指南；

管理者指南描述评估对象管理员可使用的管理功能和接口；

管理者指南描述如何以安全的方式管理评估对象；

管理者指南包含在安全处理环境中必须进行控制的功能和权限的警告；

管理者指南描述所有与评估对象的安全运行有关的用户行为的假定；

管理者指南描述所有管理者控制下的安全参数，合适时，应指明安全值；

管理者指南描述每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能控制的实体的安全特性；

管理者指南与为评估所提供的其他所有文档保持一致；

管理者指南描述与管理者有关的信息技术环境的所有的安全要求。

6.2.2.4.2 用户指南（AGD_USR.1）

检测目的：验证开发者提供的用户指南符合要求。

测试过程：检查提交的相关文档，验证是否支持厂商的声明。

通过标准：开发者提供用户指南；

用户指南描述评估对象的非管理员用户可用的功能和接口；

用户指南描述评估对象提供的用户可访问的安全功能和接口的用法；

用户指南包含在安全处理环境中必须控制的用户可访问的功能和权限的警告；

用户指南清楚地阐述评估对象安全运行中所有必要的用户职责，包括有关在评估对象安全环境阐述中找得到的用户行为的假设；

用户指南与为评估提供的其它所有文档保持一致；

用户指南描述与用户有关的信息技术环境的所有安全要求。

6.2.2.5 ALC 类：生命周期支持

6.2.2.5.1 安全措施指示（ALC_DVS.2）

检测目的：验证开发者提供的安全措施指示符合要求。

测试过程：检查提交的相关文档，验证是否支持厂商的声明。

通过标准：开发者应提供开发安全文档；

开发安全文档应描述在评估对象的开发环境中，用以保护评估对象的设计和实现的保密性和完整性所有必要的物理、程序、人员以及其它安全措施；
开发安全文档应提供在TOE的开发和维护过程中执行安全措施的证据；
证据应证明安全措施提供了必需的保护级别以维护TOE的保密性和完整性；

6.2.2.5.2 开发者定义的生命周期模型（ALC_LCD.1）

检测目的：验证开发者定义的生命周期模型符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者建立开发和维护评估对象时使用的生命周期模型；
开发者提供生命周期定义文档；
生命周期定义文档描述用于开发和维护评估对象的模型；
生命周期模型提供对评估对象开发和维护的必要的控制。

6.2.2.5.3 明确定义的开发工具（ALC_TAT.1）

检测目的：验证开发者定义的开发工具符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者标识用于开发评估对象的工具；
开发者为选择的依赖实现的开发工具提供文档；
所有用于实现的开发工具都有明确定义；
开发工具文档无歧义地定义实现中使用的每个语句的含义；
开发工具文档无歧义地定义所有基于实现的选项的含义。

6.2.2.6 ATE 类：测试

6.2.2.6.1 范围分析（ATE_COV.2）

检测目的：验证开发者测试范围分析符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供对测试覆盖范围的分析；
测试覆盖范围的分析论证了测试文档中所标识的测试和功能规范中所描述的安全功能之间的对应性；
测试覆盖范围的分析论证了功能规范中所描述安全功能和测试所文档标识的测试之间的对应性是完备的。

6.2.2.6.2 高层设计（ATE_DPT.1）

检测目的：验证开发者对高层设计的测试符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供对测试深度的分析；
深度分析论证了测试文档中所标识的测试足以论证该安全功能是和高层设计一致的。

6.2.2.6.3 功能测试（ATE_FUN.1）

检测目的：验证开发者功能测试符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者测试安全功能，并对结果形成文档；

开发者提供测试文档；
测试文档包括测试计划、测试程序描述、预期的测试结果和实际的测试结果组成；
测试计划标识要测试的安全功能，描述要执行的测试目标；
测试过程描述标识要执行的测试，并描述每个安全功能的测试概况。这些概况包括对于其他测试结果的顺序依赖性；
期望的测试结果可表明成功测试运行后的预期输出；
开发者执行的测试的结果论证了每一个被测试的安全性功能按照规定进行运作了。

6.2.2.6.4 独立性测试—抽样（ATE_IND.2）

检测目的：验证开发者独立性测试—抽样符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供评估对象进行测试；
评估对象要与测试相适应；
开发者提供一个与开发者的安全功能功能测试中使用的资源相当的集合。

6.2.2.7 AVA 类：脆弱性评定

6.2.2.7.1 分析确认（AVA_MSU.2）

检测目的：验证开发者分析确认符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者提供指导性文档；
开发者对指导性文档的分析形成文档；
指导性文档确定对评估对象的所有可能的运行方式（包括失败和操作失误后的运行），它们的后果和对于保持安全运行的意义；
指导性文档是完整的、清晰的、一致的、合理的；
指导性文档列出所有对目标环境的假定；
指导性文档列出所有对外部安全措施（包括外部程序的、物理的或人员的控制）的要求；
分析文档阐明指导性是完备的。

6.2.2.7.2 安全功能强度评估（AVA_SOF.1）

检测目的：验证开发者安全功能强度评估符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者对 ST 中标识的每一个具有评估对象安全功能强度的安全机制进行评估对象安全功能强度的分析；
对于具有评估对象安全功能强度申明的每个安全机制，评估对象安全功能强度分析说明该机制达到或超过 ST 定义的最低强度；
对于具有特定评估对象安全功能强度申明的每个安全机制，评估对象安全功能强度分析证明该机制达到或超过 ST 定义的特定功能强度。

6.2.2.7.3 高级抵抗力（AVA_VLA.4）

检测目的：验证开发者安全功能强度评估符合要求。
测试过程：检查提交的相关文档，验证是否支持厂商的声明。
通过标准：开发者分析 TOE 的交付材料，以寻找用户违反安全策略的途径，并将分析结果文档化；

开发者文档化已标识的脆弱性的分布；
对所有已标识的脆弱性，文档能说明在所预期的评估对象环境中无法利用这些脆弱性；
脆弱性分析至少应考虑以下各项：

a） 评估对象可能易遭受暴露内部电路和结构的解构；
b） 评估对象可能易遭受结构和内部存储器内容、数据传输机制、安全功能和测试方法的篡改；
c） 评估对象可能易遭受通过监测电路和结构的元素间的连接对设备内部信息的分析；
d） 评估对象可能易遭受逻辑命令的使用以产生导致安全脆弱性的响应；
e） 评估对象可能易遭受导致安全脆弱性的定义的操作边界外的操作；
f） 评估对象可能易遭受通过监测发射信号或与设备的连接对设备外部信息的分析（包括电源、场所、时钟、输入/输出和复位）；
g） 评估对象可能易遭受相同或类似评估对象前述生成中标识的脆弱性。

文档证明对于具有已标识脆弱性的评估对象可以抵御明显的穿透性攻击；
证据能说明对脆弱性的搜索是系统化的；
分析文档提供理由说明分析完全能满足 TOE 的交付。

7 SE 多应用平台安全检测

7.1 SE 多应用平台安全概述

根据GPCSRS GlobalPlatform Card Security Requirements Specification V1.0，SE多应用平台需满足的安全特性要求见规范性附录A.2，多应用平台安全与嵌入式软件SFRs的参照关系见附录B。

7.2 SE 多应用平台安全检测

7.2.1 SE 管理器安全

7.2.1.1 ISD 访问控制安全

检测目的：验证 SE 平台所实现的 ISD 访问控制安全策略的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明 ISD 访问控制安全策略与规范要求中规定一致。通过选定 ISD，执行 ISD 相关的安全功能，验证只有在满足控制策略的条件下，才能正确执行相应的安全功能。

通过标准：当 ISD 被选择为当前应用时，无论是否在安全通道下，都可以正常执行 SE 外部实体发送的 GET DATA 指令；
当 ISD 被选择为当前应用时，必须基于安全通道条件下，方可正常执行 SE 外部实体发送的其它指令（DELETE、GET STATUS、INSTALL、PUT KEY、SET STATUS、STORE DATA）；
加载文件验证需要一个带有 DAP 权限或者强制 DAP 权限的安全域，负责执行 DAP 验证的结果。ISD 通过验证相关安全域的加载指令是否被预授权，来决定允许下载或者拒绝下载。

7.2.1.2 SE 内容管理安全

7.2.1.2.1 加载（Load）

检测目的：验证 SE 文件安全加载机制的有效性。

测试方法：审查厂商提交的文档，验证厂商已声明应用加载过程符合规范要求。执行 SE 文件加载过程，验证 SE 内容加载安全机制与声明的一致。

通过标准：文件加载过程在安全通道条件下进行，指令执行安全域须处于合适的生命周期状态；
拥有权限的主体才可执行文件加载操作，拥有权限的主体包括 SE 发行机构以及通过 SE 发行机构进行授权或是委托的被授权机构和代理机构；
委托管理情况下，加载指令令牌验证确保令牌发放者对加载过程和加载文件数据块的内容的加载操作进行了预授权；（可选）
加载文件数据块的散列值确保文件完整性；（可选）
对最后一条加载命令的响应标志着加载过程的结束。当加载过程完全结束后，一个可选的收条被返回给了执行委托管理操作的安全域，而且必须被该安全域发送到 SE 外部实体；（可选）
在符合安全机制控制条件下，当文件加载所需资源可获得，SE 内容关联安全域已存在的情况下，可成功执行文件加载操作。

7.2.1.2.2 安装和可选化（Install & Make Selectable）

检测目的：验证 SE 应用安装与可选化过程安全机制的有效性。

测试方法：审查厂商提交的文档，验证厂商已声明应用安装与可选化过程符合规范要求。执行 SE 内容安装及可选化过程，验证 SE 应用安装与可选化机制与声明的一致。

通过标准：文件安装过程在安全通道条件下进行，指令执行安全域须处于合适的生命周期状态；
拥有权限的主体才可执行文件安装及可选化操作，拥有权限的主体包括 SE 发行机构以及通过 SE 发行机构进行授权或是委托的被授权机构和代理机构；
委托管理情况下，安装指令令牌验证机制确保 SE 发行方对安装过程进行授权；（可选）
对安装及可选命令的响应标志着安装过程的结束。当安装过程完全结束后，一个可选的收条被返回给了执行委托管理操作的安全域，而且必须被该安全域发送到 SE 外部实体；（可选）
在符合安全机制控制条件下，应用安装所需资源可获得，SE 内容可以被成功地安装；
当应用生命周期状态为“安装”，可成功执行可选化操作；

7.2.1.2.3 个人化（Personalize）

检测目的：验证 SE 应用个人化安全机制的有效性。

测试方法：审查厂商提交的文档，验证厂商已声明应用个人化过程符合规范要求。执行 SE 个人化过程，验证 SE 应用个人化机制与声明的一致。

通过标准：应用个人化过程在安全通道条件下进行，指令执行安全域须处于合适的生命周期状态；
验证 SE 外部实体为合法的应用提供方；
在将 STORE DATA 命令转发到目标应用之前，根据当前安全级别，对该命令进行预处理；
在符合安全机制控制条件下，若 SE 内部实体没有对个人化进行限制，SE 应用个人化成功。

7.2.1.2.4 迁移（Extradite）

检测目的：验证 SE 应用迁移安全机制的有效性。

测试方法：审查厂商提交的文档，验证厂商已声明应用迁移过程符合规范要求。设计攻击验证场景，执行 SE 内容迁移过程，验证 SE 内容安装安全机制与声明的一致。

通过标准：SE 应用迁移在安全通道条件下进行，指令执行安全域须处于合适的生命周期状态；
SE 应用迁移操作可以在应用生命周期的任何时候进行；
拥有权限的主体才可执行应用迁移操作，拥有权限的主体包括 SE 发行机构以及通过 SE 发行机构进行授权或是委托的被授权机构和代理机构；
任何处于 PERSONALIZED 状态的安全域，或者生命周期状态既不处于 CARD_LOCKED 状态也不处于 TERMINATED 状态的发行者安全域，都能够接受被迁移的应用；
委托管理情况下，迁移令牌验证机制确保 SE 发行方对迁移过程进行授权；（可选）
对迁移命令的响应标志着迁移过程的结束。当迁移过程结束后，一个可选的收条被返回给了执行委托管理操作的安全域，而且必须被该安全域发送到 SE 外部实体；（可选）
在符合安全机制控制条件下，当 SE 内容迁移的目标安全域同意迁移的情况下，SE 内容被成功迁移。

7.2.1.2.5 删除（Delete）

检测目的：验证 SE 应用删除安全机制的有效性。

测试方法：审查厂商提交的文档，验证厂商已声明 SE 应用删除机制符合规范要求。执行 SE 应用删除过程，验证 SE 应用删除机制与声明的一致。

通过标准：SE 应用删除在安全通道条件下进行，指令执行安全域须处于合适的生命周期状态；
拥有权限的主体才可执行应用删除操作，拥有权限的主体包括 SE 发行机构以及通过 SE 发行机构进行授权或是委托的被授权机构和代理机构；
应用的删除可以是物理删除或是逻辑删除，如在易失性存储区中的应用可以被完全删除，而在永久性存储区中的应用只能被逻辑删除。任何对被删除应用的存储空间的访问都是非法的。应用在删除后，其残留的数据将被覆盖或是禁止访问；
对删除命令的响应标志着迁移过程的结束。当删除过程结束后，一个可选的收条被返回给了执行委托管理操作的安全域，而且必须被该安全域发送到 SE 外部实体；（可选）
在安全机制控制下，当前应用或数据未被其它应用引用，或当前 SD 未被其它应用关联，或没有其它应用要从该可执行模块中实例化，SE 内容可以被安全的删除。

7.2.1.3 令牌验证安全（可选）

检测目的：验证令牌验证安全机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明令牌验证机制符合规范要求。在委托管理情况下，分别执行经 SE 发行者预授权的 SE 内容管理相关指令和未经预授权的 SE 内容管理相关指令，通过指令操作的成功与否，验证令牌验证机制是否有效。

通过标准：在委托管理情况下，安全域执行预授权的 LOAD、INSTALL、EXTRADITE 指令，可通过指令令牌验证，成功执行相关操作，反之操作失败；
DELETE 指令不必获得预授权，操作可直接执行。

7.2.1.4 收条生成安全（可选）

检测目的：验证收条生成能力。

测试过程：审查厂商提交的文档，对于厂商声明实现收条生成功能的情况下，其生成过程符合规范要求。在委托管理情况下，执行收条生成安全功能，验证收条生成过程与厂商申明一致。

通过标准：委托管理情况下，如果 SE 发行者的安全策略要求生成收条的话，当应用的装载、安装、移交和删除操作成功后生成相关的收条，返回给执行委托管理操作的安全域，而且被该

安全域发送到 SE 外部实体。

7.2.1.5 生命周期状态管理安全

检测目的：验证 SE 组件的生命周期状态管理安全机制的有效性。

测试过程：审查厂商提交的文档，验证厂商声明实现的生命周期模型与规范要求一致。通过执行特定 APDU 命令或进行 API 调用，使 SE 或 SE 内容生命周期状态发生迁移，验证生命周期状态迁移的情况符合规范要求。

通过标准：SE 及 SE 内容的生命周期状态迁移符合规范要求中关于生命周期状态迁移的定义。
仅在适当的生命周期状态下，可执行 SE 安全功能。

7.2.1.6 其它 SE 管理功能安全

检测目的：验证 SE 其它管理功能安全机制的有效性。

测试过程：审查厂商提交的文档，验证厂商声明实现的 GET DATA 和 STORE DATA 安全机制符合规范性附录 A.2 的要求。通过执行相关指令，验证数据读取和保存操作符合相关安全机制。

通过标准：GET DATA 参数所指向的数据可获得；
STORE DATA 指令需被验证通过后方可执行；
STORE DATA 指令确保被成功发送给指定应用，数据保证格式正确的情况下，成功执行数据保存操作；
STORE DATA 应受失败处理机制控制，当失败发生时进行事务回滚。

7.2.1.7 密钥管理安全

7.2.1.7.1 密钥生成

检测目的：验证密钥生成安全机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明的会话密钥生成规则符合规范性附录 A.2 中的安全要求。通过厂商提交的相关源代码，验证 SE 的实现与厂商声明的一致。

通过标准：安全功能将根据符合相关标准的特定密钥生成算法和特定密钥长度来产生密钥。

7.2.1.7.2 密钥加载

检测目的：验证密钥安全加载机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明的密钥加载过程符合规范性附录 A.2 中的安全要求。通过厂商提交的相关源代码，验证 SE 的实现与厂商声明的一致。执行密钥加载安全功能，验证只有在满足控制策略的条件下，才能正确成功加载密钥。

通过标准：在 SE 进入生命周期的“就绪”状态前，初始化密钥必须已被安全加载；
发行者安全域的初始密钥由初始化密钥进行加密加载。安全域初始密钥由 SE 发行者安全域的 K_{DEK} 或初始化密钥进行加密加载；
安全域中随后的静态密钥由安全域中之前加载的 K_{DEK} 进行加密加载，并通过带会话密钥的安全通道进行保护；
发行者安全域的其它密钥被加载时，要用发行者安全域密钥集中的 K_{DEK} 加密，并通过带会话密钥的安全通道进行保护；
在成功的更新或替换掉旧的密钥后，密钥管理安全特性要使旧密钥无效（密钥销毁）；
在处理 APDU 命令过程中，密钥管理保证只分发合法的密钥，拒绝任何不符合 SE 规范

规定长度的密钥；
提供通过 API 为应用提供分发其它密钥的功能。

7.2.1.7.3 密钥访问

检测目的：验证密钥安全访问机制的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明的对安全通道密钥集的访问控制策略符合规范性附录 A.2 中的安全要求。通过对指定安全通道密钥集的访问，验证仅当符合密钥访问安全策略的情况下，才能执行相应的安全功能。
通过标准：在安全通道会话条件下，所访问的密钥存在且有效时，可通过适当的方式访问获得；
提供通过 API 为应用提供访问其它密钥的功能。

7.2.1.7.4 密钥销毁

检测目的：验证对密钥安全销毁机制的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现密钥销毁机制。通过对已销毁密钥数据区进行访问，验证密钥销毁机制的有效性。
通过标准：安全销毁不再需要的密钥，避免敏感信息泄露；
提供通过 API 为应用提供销毁其它密钥的功能。

7.2.2 安全域安全

7.2.2.1 SD 访问控制安全

检测目的：验证 SE 访问控制安全策略的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明 SD 访问控制安全策略符合规范性附录 A.2 中的要求。通过选定 SD，执行 SD 相关的安全功能，验证只有在满足控制策略的条件下，才能正确执行相应的安全功能。
通过标准：当安全域被选择为当前应用时，无论是否在安全通道下，都可以正常执行 SE 外部实体发送的 GET DATA 指令；
当安全域被选择为当前应用时，必须基于安全通道条件下，方可正常执行 SE 外部实体发送的其它指令（DELETE、GET STATUS、INSTALL、PUT KEY、SET STATUS、STORE DATA）；
委托管理情况下，安全域需具备委托管理权限，且需准备好预授权的 LOAD、INSTALL、EXTRADITE 或 DELETE 指令，供发行者安全域或具有“令牌验证权限”的安全域进行验证；
授权管理情况下，安全域具备授权管理权限，即可直接执行 LOAD、INSTALL、EXTRADITE 或 DELETE 指令进行 SE 内容管理。

7.2.2.2 安全通道安全

检测目的：验证 SE 安全通道有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现符合规范性附录 A.2 要求的安全通道。通过使用不同方式发起安全通道初始化，在安全通道下执行消息传递、密钥及敏感数据接收等服务，验证只有在满足安全通道安全策略的条件下，才能正确执行相应的安全功能；通过不同方式终止当前安全通道，确认安全通道有效重置；设计攻击场景，验证 SE 平台提供的安全通道通信的有效性。

通过标准：根据规范性附录 A.2 中的安全要求，支持用不同方式发起对安全通道通信的初始化；
只有通过认证的 SE 外部实体，可建立与 SE 之间的安全通道；
安全通道建立情况下，SE 外部实体可请求与该安全域相关的应用管理操作及其它安全域服务，根据安全域特定安全通道协议，提供诸如：消息完整性检查、MAC 链的计算，会话密钥等手段确保消息完整性及认证、消息数据机密性；
对敏感数据及密钥的接收服务，支持相应的解密保存操作；
当通过 APDU 指令或 API 终止一个安全通道会话时，设置安全级别为“无安全级别”，并且清除所有的会话密钥和初始向量；
攻击手段无法突破安全通道的安全防御。

7.2.2.3 无安全通道安全

检验目的：验证 SE 平台无安全通道安全机制有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现的无安全通道安全特性。模拟 SE 外部实体不使用安全通道与 SE 通信（向应用发送 APDU 命令），验证不存在绕过 SE 访问安全策略对 APDU 命令缓冲区的访问。

通过标准：无安全通道条件下对 SE 发送 APDU 指令，通过对特定 APDU 缓存区的读写操作，确认不存在绕过 SE 访问安全策略对 APDU 命令缓冲区的访问。

7.2.2.4 DAP 验证安全（可选）

检验目的：验证 SE 平台所实现的 DAP 验证安全机制有效性。

测试过程：审查厂商提交的文档，当厂商已声明实现具有“DAP 验证权限”的 SD，验证其 DAP 验证机制符合规范性附录 A.2 中的要求。在要求 DAP 验证的情况下，通过执行文件加载操作，确认 DAP 验证的有效性。

通过标准：执行文件加载操作过程中，当加载应用相关的安全域具有“DAP 验证权限”（应具有 DAP 验证密钥），加载文件数据中须存在相关验证数据（DAP 块）；
加载文件 HASH 值验证通过；
加载文件指令中的 DAP 块经指定应用提供者安全域验证通过，成功执行到 SE 的文件加载。

7.2.2.5 强制 DAP 验证安全（可选）

检验目的：验证 SE 平台所实现的强制 DAP 验证安全机制的有效性。

测试过程：审查厂商提交的文档，当厂商已声明实现具有“强制 DAP 验证权限”的 SD，验证其强制 DAP 验证机制是否符合规范性附录 A.2 中的要求。在要求强制 DAP 验证的情况下，通过执行文件加载操作，确认满足 DAP 验证机制，才能正确执行相应的文件加载功能。

通过标准：执行文件加载操作过程中，当 SE 上存在具有“强制 DAP 验证”权限的安全域（应具有 DAP 验证密钥）时，加载文件数据中须存在相关验证数据（DAP 块）；
加载文件 HASH 值验证通过；
加载文件指令中的 DAP 块经授权安全域验证通过，成功执行到 SE 的文件加载。

7.2.3 全局服务应用安全（CVM）（可选）

检测目的：验证 SE 平台实现的 CVM 安全机制的有效性。

测试方法：审查厂商提交的文档，验证厂商已声明的 CVM 应用实现符合规范性附录 A.2 的要求。
通过不同权限的应用访问 CVM 的相关服务，验证 CVM 访问控制安全机制的有效性。

设计攻击场景，验证 SE 平台实现的 CVM 机制的有效性。

通过标准：CVM 验证服务可以被任何应用访问；

CVM 管理服务只能由 SE 内授权应用访问；

CVM 应用也可以通过 APDU 接口向经过适当方式认证的 SE 外部实体提供 CVM 管理服务；

CVM 值及尝试限次的修改必须符合原子操作；

通过应用对 CVM 的不同操作，CVM 状态迁移符合规范性附录 A.2 中的安全要求；

锁定和解锁 CVM 操作的请求需通过 SE 上具有相关权限应用的许可；

CVM 管理数据（CVM 值，CVM 状态，CVM 最大尝试次数以及 CVM 已尝试次数）被安全持有，无法通过攻击手段进行篡改。

7.2.4 API 安全

检测目的：验证 SE 平台应用编程接口安全机制的有效性。

测试方法：分析厂商提交的材料，评估 SE 平台提供应用编程接口执行 SE 资源的访问控制。评估只能通过应用编程接口访问平台服务和资源，不存在其它的访问方式。设计攻击场景，验证应用编程接口的实现与厂商声明一致。

通过标准：API 约束特定的访问控制规则、用户验证机制，以及对各种加密等功能的调用；

应用程序在使用 SE 平台服务以及 SE 平台资源时必须通过预定义的应用编程接口方式实现；

运行时环境及平台自身的安全机制不会被规避、无效化、崩溃以及以其它方式进行任何危害。

7.2.5 运行时环境安全

7.2.5.1 监管者安全

检测目的：验证 SE 运行时环境是否具有有效的管理控制。

测试过程：审查厂商提交的文档，验证厂商已声明保证管理员安全特性。通过文档审查或任何可行的实验，验证 SE 的实现与厂商声明一致。

通过标准：确保安全特性都在适当的时间执行，安全特性不能被绕过、失效、破坏或以其他方式回避；

APDU 指令被正确分发。

7.2.5.2 防火墙安全

检测目的：验证防火墙安全机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现防火墙安全功能。通过直接读写、间接读写或者请求访问存储空间，验证只有符合防火墙安全机制的条件下，才能成功地执行相应的数据访问。

通过标准：不同应用之间不能互相访问程序代码和私有数据；

每个应用的代码、数据（包括瞬时会话数据）和运行时环境自身的代码、数据（包括瞬时会话数据）一样，不会遭受任何来自 SE 内部的未经授权的访问；

当 SE 支持超过一个以上的逻辑通道时，每个被并行选择的应用的代码、数据（包括瞬时会话数据）和运行时环境自身的代码、数据（包括瞬时会话数据）一样不会遭受任何来自 SE 内部的未经授权的访问。

7.2.5.3 对象复用安全

检测目的：验证对象复用安全机制的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现对象复用安全机制。设计攻击场景，对已使用数据资源进行读取操作，确认对象复用安全机制的有效性。

通过标准：被删除应用的对象数据不可被读取；
特定应用的 APDU 缓存内容不可被其它应用获取；
特定应用的算法缓存中的内容不可被其它应用读取；
特定对象的临时数据不能被新对象获取。

7.2.5.4 事件行为安全

检测目的：验证 SE 事件行为策略的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现的事件行为安全策略；分析事件安全策略，确保其正确性和有效性。通过任何可行的实验，验证 SE 处理响应符合厂商声明的事件行为策略。

通过标准：所有事件行为策略中定义的事件都严格按照事件行为策略进行处理响应并清除相应的告警。

7.2.5.5 主体/对象识别安全

检测目的：验证 SE 主体/对象识别安全的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现主体/对象识别安全；通过任何可行的实验，验证 SE 平台环境对每个对象/主体都能正确识别。

通过标准：SE 平台环境对每个对象/主体都能正确识别。

7.2.5.6 SE 审计安全

检测目的：验证 SE 审计安全功能有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现的 SE 审计安全功能。通过直接读写 SE 静态审计记录，或在执行应用过程中读写 SE 动态审计记录，验证 SE 审计安全机制有效性。

通过标准：当发行者安全域处于“准备状态”前，且 SE 可以在安全环境下使用时，SE 制造商预先在 SE 上加载有具有唯一区分性信息；
平台记录其它一些审计信息：比如 SE 发行者标识，SE 标识，SE 注册信息或者其它可能被写入到发行者安全域中的 SE 发行者信息；
动态审计信息记录数量的限制根据业务需要进行约定。如果给审核数据分配的存储空间用完了，再有新的记录进来，就要把最旧的记录删掉；
SE 审计安全要保证审核记录数据的安全，审核记录不能被未经授权删除或修改。

7.2.5.7 自检安全

检测目的：验证 SE 自检安全功能的有效性。

测试过程：审查厂商提交的文档，验证厂商已声明实现自检安全功能。通过实验，验证在系统启动、正常运行时的某个周期或者在某些预定条件出现时，启动自检，提示相关预警或执行相关失败管理操作。

通过标准：自检在系统启动、正常运行时的某个周期或者在某些预定条件出现时发生；

SE 掉电（可能是异常的掉电）后，特定存储区（非易失性内存区）的内容应保持不变；
芯片制造商自定义的 IC 检测机制，应该能够确保运行正常：当检测到异常情况时，SE 应产生一个警告。

7.2.5.8 失败管理安全

检测目的：验证失败管理安全机制的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现失败管理功能。通过设计异常实验，验证 SE 在遇到异常时保持安全性。
通过标准：SE 正在运行时异常，导致当前操作失败或出现内部错误，SE 能根据需要保存注册表和易失存储器内容；
内存的恢复过程应能保证数据的安全性和一致性。

8 移动支付 SE 规格符合性检测

8.1 移动支付 SE 规格要求概述

移动支付SE需根据移动支付系统中的安全认证体系及运营管理模式的要求，支持特定的规格设置，其规格要求参照规范性附录A.3。

8.2 移动支付 SE 规格符合性测试

8.2.1 PAMID

检测目的：验证 PAMID 仅限一次写入，在写入后只可读取 PAMID 标识，不可修改或覆盖。
测试过程：执行扩展指令或 API 调用，进行 PAMID 的写入、读取等操作。
通过标准：PAMID 只可写入一次。
通过执行可能的数据修改操作，无法对已经写入的 PAMID 进行修改；
PAMID 在写入后可正常读取。

8.2.2 加密算法

检测目的：验证加密算法的有效性。
测试过程：审查厂商提交的文档，验证厂商已声明实现 DES/3DES，RSA，SHA-1 等通用加密算法，或 SM4，SM2，SM3 国产加密算法；验证基于上述加密算法 SE 及 SE 应用的安全机制的有效性。
通过标准：执行基于所声明加密算法的密钥安全管理操作，验证基于所申明加密算法的密钥生成、加载、访问及销毁均符合 SE 平台安全要求；
通过执行基于所申明加密算法的加解密相关服务，验证可实现完整的 SE 多应用平台安全机制；
验证基于所申明加密算法，可确保对满足 SE 应用安全需求。（见 7.2）

8.2.3 基本安全域设置

8.2.3.1 FCSD（发行方为可信管理者的开放共享模式）

检测目的：验证 FCSD 符合 JR/T 0097-2012 相关要求。
测试过程：审查厂商提交的文档，验证厂商已声明：实现针对以发行方为可信管理者的开放共享模

式下的辅助安全域 FCSD，且 FCSD 的实现符合 JR/T 0097-2012 中对 FCSD 的属性、权限、生命周期、安全通道协议等要求。

通过标准：在以发行方为可信管理者的开放共享模式下，SE 须支持 FCSD 安全域动态下载；
FCSD 安全域关联到自身，不能被发行者安全域及其它安全域锁定、删除；
FCSD 仅可以被公共服务平台主体删除和锁定；
FCSD 直接继承了 SE 生命周期状态，通过对 ISD 生命周期的修改，也都将反映到对应的 FCSD 生命周期状态上；
FCSD 已实现对 SCP10 安全通道协议的支持。

8.2.3.2 FMSD（公共服务平台作为可信第三方的开放共享模型）

检测目的：验证 FMSD 符合 JR/T 0097-2012 中对 FMSD 的要求。

测试过程：审查厂商提交的文档，验证厂商已声明：实现针对以公共服务平台作为可信第三方的开放共享模式下的授权管理安全域 FMSD。且 FMSD 的实现符合 JR/T 0097-2012 中对 FMSD 的属性、权限、生命周期、安全通道协议等要求。

通过标准：在以公共服务平台作为可信第三方的开放共享模式下，SE 须预置 FMSD 安全域；
FMSD 安全域关联到自身，不能被发行者安全域及其它安全域锁定、删除；
FMSD 仅可以被公共服务平台主体删除和锁定；
FMSD 直接继承了 SE 生命周期状态，通过对 ISD 生命周期的修改，也都将反映到对应的 FMSD 生命周期状态上；
FMSD 具有授权管理权限，令牌校验权限，DAP 权限，具有辅助安全域管理功能；
FMSD 已实现对 SCP10 安全通道协议的支持。

8.2.4 基本基础服务

8.2.4.1 金融目录管理应用

检测目的：验证金融目录管理应用符合 JR/T 0097-2012 中的要求。

测试过程：审查厂商提交的文档，验证厂商已声明实现并加载 JR/T 0097-2012 中的要求的应用选择服务。通过选定金融目录管理应用，执行应用定义 APDU 指令或 API 访问应用中的金融目录下的各用户信息文件。

通过标准：发行方为可信管理者的开放共享模式下，金融目录管理应用关联到发行者安全域；
管理 TSM 作为可信第三方的开放共享模式下，金融目录管理应用关联到 FMSD；
仅在安全通道建立的条件下，SE 外部实体可对金融目录管理应用进行访问；
SE 上其它应用通过金融目录管理应用的共享接口进行访问；
金融目录管理应用所管理的金融目录文件结构，及基本信息文件定义见 JR/T 0089.2-2012 相关部分的描述。

8.2.4.2 应用选择服务

检测目的：验证非接支付场景下，SE 上非接金融应用选择符合 JR/T 0025.12 的相关要求。

测试过程：审查厂商提交的文档，验证厂商已声明实现 SE 支持非接终端以 SELECT PPSE 方式对金融应用进行选定；通过客户端修改默认银行信息文件，确认通过 SELECT PPSE 返回的应用 AID 信息始终与其同步发生变化。

通过标准：非接支付环境下，受理终端与 SE 之间的应用选择交互符合 JR/T 0025.12 中关于 PPSE 选择流程的描述；

通过 SELECT PPSE 返回的 FCI 内 AID 信息与默认银行信息文件所含应用 AID 信息一致；

通过客户端修改默认银行信息文件后，非接受理终端通过 PPSE 选定的应用 AID 信息同步发生变化；

下载新应用到 SE，除非对默认信息文件作更新，否则新应用不会自动更新为 PPSE 选定的应用。

8.2.4.3 SE 可信服务

检测目的：验证 SE 可信服务符合 JR/T 0097-2012 中的要求。

测试过程：审查厂商提交的文档，验证厂商已声明实现 FCSD/FMSD 的 SCP10 安全域安全通道协议。通过建立安全通道，验证安全通信机制符合 SCP10 安全通信协议；执行对 SE 相关辅助安全域的访问，测试安全通道协议的有效实现。

通过标准：FCSD 安全域中存有持卡者的非对称密钥、公钥证书和公共服务平台的公钥证书；

SE 外部实体模拟公共服务平台与 FCSD/FMSD 建立 SCP10 方式的安全通道，互认证通过，安全通道成功建立；

支持用不同方式发起对安全通道通信的初始化；

安全通道建立情况下，SE 外部实体可请求与 FCSD/FMSD 相关的应用管理操作及其它安全域服务，安全通道负责提供符合 SCP10 的安全服务，如：消息完整性检查、MAC 链的计算，会话密钥等手段确保消息完整性及认证、消息数据机密性；

对敏感数据及密钥的接收服务，支持相应的解密保存操作；

当通过 APDU 指令或 API 终止一个安全通道会话时，设置安全级别为“无安全级别”，并且清除所有的会话密钥和初始向量。

8.2.4.4 SE 的 PIN 验证

检测目的：验证 SE 上支付应用执行前均需使用 CVM 全局服务验证用户 PIN。

测试方法：审查厂商提交的文档，验证厂商已声明 SE 实现 CVM 全局服务及扩展 APDU 指令 VERIFY PIN。模拟应用管理终端访问 SE 内支付应用，通过发送 VERIFY PIN 调用 SE 上 CVM 服务，对持卡人 PIN 进行验证，仅当 PIN 验证通过的情况下方可执行 SE 内支付应用。

通过标准：客户端试图访问 SE 支付应用时，首先通过 VERIFY PIN 指令来调用 CVM 全局服务，验证持卡人 PIN，仅当 CVM 验证通过的情况下，SE 上支付应用可执行；

CVM 管理服务符合规范性附录 A.3 中的安全要求。

8.2.5 APDU 指令

检测目的：验证 SE 是否支持规定的 APDU 指令集。

测试方法：审查厂商提交的文档，验证厂商已声明实现规定的 APDU 指令集。通过在 SE 外部对 SE 发送相应的 APDU 指令，验证指令执行的安全策略的有效性以及执行实现的正确性。

通过标准：SE 正确支持以下 APDU 指令，其安全策略符合多应用平台安全要求，且响应及返回数据正确。

——DELETE

——GET DATA

——GET STATUS

——INSTALL

——LOAD
——MANAGE CHANNEL
——PUT KEY
——SELECT
——SET STATUS
——STORE DATA
——PERFORM SECURITY OPERATION
——GET CHALLENGE
——EXTERNAL AUTHENTICATION
——INTERNAL AUTHENTICATION
——MANAGE SECURITY ENVIRONMNET
——VERIFY PIN

8.2.6 安全通道通信

8.2.6.1 应用可信通信

检测目的：验证应用与 SE 外部实体之间符合预定义的安全通道协议。

测试方法：审查厂商提交的文档，验证厂商已声明实现应用关联辅助安全域安全通道协议。通过执行 SE 外部对应用的访问，测试应用相关辅助安全域安全通道协议的实现是否与声明一致。

通过标准：辅助安全域的安全通道类型由应用提供方与辅助安全域的创建者协商确定，支持用不同方式发起对安全通道通信的初始化；

只有通过认证的 SE 外部实体，可建立与 SE 之间的安全通道；

安全通道建立情况下，SE 外部实体可请求与该安全域相关的应用管理操作及其它安全域服务，根据安全域特定安全通道协议，提供诸如：消息完整性检查、MAC 链的计算，会话密钥等手段确保消息完整性及认证、消息数据机密性；

对敏感数据及密钥的接收服务，支持相应的解密保存操作；

当通过 APDU 指令或 API 终止一个安全通道会话时，设置安全级别为“无安全级别”，并且清除所有的会话密钥和初始向量。

附 录 A
（规范性附录）
SE 嵌入式软件安全要求

A.1 SE嵌入式软件安全要求

A.1.1 安全功能要求

A.1.1.1 FAU类：安全审计

A.1.1.1.1 安全告警（FAU_ARP.1）

当检测到潜在的安全侵害时，安全功能将进行安全告警，如限制口令尝试次数，异常重启等。

A.1.1.1.2 审计列表生成（FAU_GEN.1）

——安全功能应能为下述可审计事件生成审计记录:在评估对象初始化操作、其它专门定义的可审计事件审计级别之内的所有可审计事件；
——安全功能应在每个审计记录中至少记录如下信息：在评估对象初始化操作中记录的审计记录，包括 IC 制造日期、序列号、操作软件标识和发布日期。

A.1.1.1.3 潜在侵害分析（FAU_SAA.1）

——安全功能应能用一系列的规则去监控审计事件，并根据这些规则指示出对安全策略的潜在侵害；
——安全功能用下列规则来监控审计事件:已知的用来指示潜在安全侵害的可审计事件子集的积累或组合。

A.1.1.1.4 可选择的审计（FAU_SEL.1）

安全功能应能根据以下属性包括或从以下一套被审计事件中排除可审计事件：客体身份、用户身份、主体身份、主机身份、事件类型。

A.1.1.1.5 受保护的审计踪迹存储（FAU_STG.1）

——安全功能应保护所存储的审计记录，以避免未授权的删除；
——安全功能应能防止对审计记录的修改。

A.1.1.1.6 在审计数据可能丢失情况下的行为（FAU_STG.3）

——如果审计踪迹超过预定的限制,如审计区溢出,安全功能应采取相应的行为,确保交易的完整性。

A.1.1.2 FCS类：加密支持

A.1.1.2.1 密钥生成（FCS_CKM.1）

安全功能将根据符合相关标准的特定密钥生成算法和特定密钥长度来产生密钥。

A.1.1.2.2 密钥分发（FCS_CKM.2）

安全功能应根据相关标准的一个特定的密钥分发方法来分发密钥。

A.1.1.2.3 密钥访问（FCS_CKM.3）

安全功能将根据符合相关标准的特定密钥访问方法来访问密钥。

A.1.1.2.4 密码运算（FCS_COP.1）

安全功能将根据符合相关标准的特定密码算法和密钥长度来执行密码运算。

A.1.1.2.5 密码销毁（FCS_CKM.4）

安全功能应根据符合相关标准的一个特定的密钥销毁方法来销毁密钥。

A.1.1.3 FCO类：通信

A.1.1.3.1 强制性原发证明（FCO_NRO.2）

——安全功能在任何时候都应对所传送的信息类型强制产生原发证据；
——安全功能应能将信息原发者的属性和信息的信息域与证据相关联。

A.1.1.4 FDP类：用户数据保护

A.1.1.4.1 子集访问控制（FDP_ACC.1）

——安全功能将对安全功能策略覆盖的主体、客体和它们之间的特定操作执行软件访问控制策略。

A.1.1.4.2 完全访问控制（FDP_ACC.2）

——安全功能应对主体和客体及策略所涵盖主体和客体之间的所有操作执行访问控制策略；
——安全功能应确保安全功能控制范围内的任何主体和客体之间的所有操作都被一个访问控制策略涵盖。

A.1.1.4.3 基于安全属性的访问控制（FDP_ACF.1）

——安全功能将基于安全属性和确定的安全属性组，对客体执行软件访问控制策略；
——安全功能执行预定规则，以决定受控主体与受控客体间的操作是否被允许；
——安全功能将基于安全属性的授权主体访问客体的规则来授权主体访问客体；
——安全功能将基于预定规则明确拒绝主体对客体的访问。

A.1.1.4.4 不带安全属性的用户数据输出（FDP_ETC.1）

——安全功能应在安全功能策略控制下输出用户数据到 SE 安全控制范围之外时执行访问控制策略和（或）信息流控制策略；
——安全功能应输出不带相关安全属性的用户数据。

A.1.1.4.5 子集信息流控制（FDP_IFC.1）

安全功能应对包含在安全功能策略中的以下各项执行信息流控制策略：主体、信息和导致受控信息流入流出受控主体的操作。

A.1.1.4.6 完全信息流控制(FDP_IFC.2)

——安全功能应对主体和信息及控制策略所涵盖导致信息流入、流出主体的所有操作执行信息流控制策略；
——安全功能应确保导致安全功能控制范围内任意信息流入、流出安全功能控制范围内任意主体的所有操作都被一个信息流控制策略涵盖。

A.1.1.4.7 简单安全属性（FDP_IFF.1）

——安全功能应在预定主题类型和信息安全属性的基础上执行信息流控制策略；
——如果对每一个操作，在主体和信息安全属性间必须有基于安全属性的关系，安全功能应允许受控主体和受控信息之间存在经由受控操作的信息流；
——安全功能应执行附加的信息流控制策略；
——安全功能应提供附加的安全功能策略能力；
——安全功能应根据基于安全属性的规则明确授权信息流；
——安全功能应根据基于安全属性，明确拒绝信息流的规则明确拒绝信息流。

A.1.1.4.8 分级安全属性（FDP_IFF.2）

——安全功能应基于指定策略控制下的主体和信息，以及每个对应的安全属性，执行信息流控制策略；
——如果基于安全属性间有序关系支持：对每一个操作，在主体和信息安全属性之间必须支持基于安全属性的关系，安全功能应允许信息在受控主体和受控信息之间经由受控操作流动；
——安全功能应执行附加的信息流控制策略规则；
——安全功能应提供策略能力；
——安全功能应根据基于安全属性明确批准信息流的规则，明确批准一个信息流；
——安全功能应根据基于安全属性明确拒绝信息流的规则，明确拒绝一个信息流。

A.1.1.4.9 不带安全属性的用户数据输入（FDP_ITC.1）

——安全功能在安全功能策略控制下从评估对象安全控制范围之外输入用户数据时应执行访问控制策略和信息流控制策略；
——安全功能应略去任何与评估对象安全控制范围之外输入的数据相关的安全属性；
——安全功能在安全功能策略控制下从安全控制范围之外输入数据时应执行附加的输入控制规则。

A.1.1.4.10 带有安全属性的用户数据输入（FDP_ITC.2）

——在策略控制下从安全功能控制范围之外输入用户数据时，安全功能应执行访问控制策略或信息流控制策略；
——安全功能应使用与所输入数据相关的安全属性；
——安全功能应确保所使用协议在安全属性和接收到的用户数据之间提供了明确的关联；
——安全功能应确保对所输入用户数据的安全属性的解释与用户数据源的解释是一样的；
——在策略控制下从安全功能控制范围之外输入用户数据时，安全功能应执行附加的输入控制规则。

A.1.1.4.11 基本内部传输保护（FDP_ITT.1）

在评估对象物理上分隔的部分间传递用户数据时，安全功能应执行访问控制策略和信息流控制策略，以防止用户数据泄露。

A.1.1.4.12 子集剩余信息保护（FDP_RIP.1）

安全功能应保证在客体收回资源的情况下，资源以前的信息内容不可得。

A.1.1.4.13 基本回滚（FDP_ROL.1）

——安全功能应执行访问控制策略或信息流控制策略，以允许对信息或客体的操作进行回滚；
——安全功能提供回退全部操作的能力，但用户只能选择仅回退其中一部分操作（针对回退策略或回退可进行的边界条件）。

A.1.1.4.14 存储数据完整性监视和反应（FDP_SDI.2）

——安全功能应基于用户数据属性，对所有客体，监视存储在 TOE 内的用户数据是否存在完整性错误；
——检测到完整性错误时，安全功能应采取的动作。

A.1.1.4.15 数据交换完整性（FDP_UIT.1）

——安全功能应执行访问控制策略和/或信息流控制策略以能够传输和接受用户数据，避免修改错误；
——收到用户数据时，安全功能应能确定修改是否已发生。

A.1.1.5 FIA类：标识与鉴别

A.1.1.5.1 鉴别失败处理（FIA_AFL.1）

——安全功能应检测与鉴别事件相关的不成功鉴别尝试的规定次数；
——当达到或超过规定的不成功鉴别尝试次数时，安全功能将采取相应动作。

A.1.1.5.2 用户属性定义（FIA_ATD.1）

安全功能应为每一个用户保存安全属性。

A.1.1.5.3 鉴别定时（FIA_UAU.1）

——在用户被鉴别之前，安全功能应允许代表用户实施受安全功能控制的某些动作；
——只有在用户已被成功鉴别后，SE 才能代表用户执行所有其它受安全功能控制的动作。

A.1.1.5.4 受保护的鉴别反馈（FIA_UAU.7）

在鉴别过程中，安全功能不应提供任何敏感信息给用户。

A.1.1.5.5 识别定时（FIA_UID.1）

——在用户被识别之前，安全功能应允许代表用户实施受安全功能控制的某些动作；
——只有在用户已被成功识别后，SE 才能代表用户执行所有其它受安全功能控制的动作。

A.1.1.5.6 任何动作前的用户标识（FIA_UID.2）

——在用户被成功标识前，仅在安全功能介导动作列表中的动作可执行；
——在允许执行代表该用户的任何其它安全功能介导动作之前，该用户必须首先被成功识别。

A.1.1.5.7 用户-主体绑定（FIA_USB.1）

——安全功能应将用户安全属性与代表用户活动的主体相关联；
——安全功能应执行属性初始关联规则，将用户安全属性与代表用户活动的主体初始关联；
——安全功能应执行属性更改规则，管理与代表用户活动的主体相关联的用户安全属性的改变。

A.1.1.6 FMT类：安全管理

A.1.1.6.1 安全功能行为的管理（FMT_MOF.1）

——安全功能应仅限于已授权并识别的角色修改下列安全功能行为：

- 数据访问级别的管理（该级别一旦确定，不能变更）；
- 在安全告警事件中要采取行为的管理；
- 通过在规则集中增加、修改或删除规则，来维护违规分析规则；
- 密钥属性变更的管理，密钥属性包括密钥类型（例如：公钥、私钥），有效期和用途（电子签名、密钥加密、密钥协议、数据加密）；
- 在鉴别失败事件中要采取行为的管理；
- 在用户成功被鉴别之前所能采取行为的管理；
- 如果授权管理者能改变用户被识别之前所能采取的行为，应对授权管理者的此种行为进行管理；
- 对撤消规则的管理；
- 对重放中所采取行为的管理；
- SE 自检发生（如初始化启动、定期间隔、其它特定条件）时的条件的管理；
- ST 中附加明确陈述的安全功能的管理。

A.1.1.6.2 安全属性的管理（FMT_MSA.1）

安全功能应执行访问控制策略和信息流控制策略，仅限于已识别了的授权角色对安全属性进行改变默认值、查询、修改、删除或其它操作。

A.1.1.6.3 安全的安全属性（FMT_MSA.2）

安全功能应确保安全属性只接受安全的值。

A.1.1.6.4 静态属性初始化（FMT_MSA.3）

——安全功能应执行访问控制策略和信息流控制策略以便为用于执行安全功能策略的安全属性提供受限制的默认值；
——安全功能应允许已识别了的授权角色为生成的客体或信息规定新的初始值以代替原来的默认值。

A.1.1.6.5 安全功能数据的管理（FMT_MTD.1）

安全功能应仅限于已识别了的授权角色能够对安全功能数据进行改变默认值、查询、修改、删除、清空或其它操作。

A.1.1.6.6 对安全功能数据限值的管理（FMT_MTD.2）

——安全功能应仅限于已识别了的授权角色对以下安全功能数据限值：

- 对不成功鉴别尝试次数阈值的管理；

- ST 中详细定义的其它阈值的管理。当安全功能数据达到或超过了指明的限值时，安全功能将采取相应的动作。

A.1.1.6.7 安全的安全功能数据（FMT_MTD.3）

安全功能应确保安全功能数据只接受安全的值。

A.1.1.6.8 撤消（FMT_REV.1）

——安全功能应仅限于已标识的授权角色能够撤销安全控制范围内与用户、主体、客体或其它附加资源相关的安全属性；
——安全功能应执行撤销规则。

A.1.1.6.9 安全角色（FMT_SMR.1）

——安全功能应维护已标识的授权角色；
——能够把用户和角色关联起来。

A.1.1.7 FPT类：安全功能保护

A.1.1.7.1 抽象机测试（FPT_AMT.1）

安全功能应在初始化启动期间、正常运转时周期性地、授权用户提出请求时、等条件下，运行一套测试，以验证作为安全感功能基础的抽象机所提供的安全假设是否正确运转。

A.1.1.7.2 带保存安全状态的失败（FPT_FLS.1）

安全功能在失败发生时应保存一个安全状态。

A.1.1.7.3 内部安全功能修改的检测（FPT_ITI.1）

A.1.1.7.4 安全功能数据在安全功能与远程可信IT产品之间传送时

具备检测安全功能数据在安全功能与远程可信 IT 产品之间传送时是否被修改的能力。

A.1.1.7.5 安全功能数据传输的基本保护（FPT_ITT.1）

安全功能应保护安全功能数据在评估对象各部分间传输时不被泄露。

A.1.1.7.6 防止物理攻击（FPT_PHP.3）

安全功能应通过自动响应防止对安全功能设备/元素的环境压力、信息监控、其他物理篡改情况，这样就不会违反评估对象安全策略。

A.1.1.7.7 无过度损失的自动恢复（FPT_RCV.3）

——当不能从失败或服务中断自动恢复时，安全功能应进入维护模式，该模式使得评估对象能返回到一个安全状态；
——操作过程中意外掉电时，安全功能应确保自动地使评估对象返回到一个安全状态；
——安全功能提供的从失败或服务中断状态恢复的功能应确保在安全控制范围内的安全功能数据或客体在无过度损失的情况下恢复到初始状态；
——安全功能应提供确定客体能否被恢复的能力。

A.1.1.7.8 功能恢复（FPT_RCV.4）

安全功能应确保涉及恢复、复位、掉电或撤销操作完成之前的情况的安全功能有如下特性，即安全功能或者成功完成，或者出现指明的失败情况后，应恢复到一个安全状态。

A.1.1.7.9 重放检测（FPT_RPL.1）

——安全功能应检测确定实体的重放；
——检测到重放时，安全功能应执行相应的安全功能。

A.1.1.7.10 安全策略的不可旁路性（FPT_RVM.1）

安全功能应确保在安全控制范围内的每一项功能被允许继续执行前，安全策略的执行功能应被成功激活。

A.1.1.7.11 安全功能域的隔离（FPT_SEP.1）

——在安全功能执行时，应维持在一个独立安全域内，防止不可信主体的干扰和篡改；
——安全功能应在安全控制范围内分离各主体的安全域。

A.1.1.7.12 安全功能测试（FPT_TST.1）

——安全功能在启动初始化期间和正常工作期间周期性地或应授权用户的要求在满足产生自检的条件时将进行自检，以指明安全功能的正确操作；
——安全功能为授权用户提供对安全功能数据完整性的验证能力；
——安全功能为授权用户提供对所存储的安全功能可执行代码完整性的验证能力。

A.1.1.7.13 安全功能间基本的安全功能数据一致性（FPT_TDC.1）

——当安全功能与其他可信 IT 产品共享安全功能数据时，安全功能应提供对安全功能数据类型进行一致性解释的能力；
——当解释来自其他可信 IT 产品的安全功能数据时，安全功能应使用安全功能使用的解释规则。

A.1.1.7.14 安全功能检测（FPT_TST.1）

——安全功能应在初始化启动期间、正常工作期间周期性地、授权用户要求时、满足产生自检的条件时，运行一套自检以证明安全功能操作的正确性；
——安全功能应为授权用户提供验证安全功能数据完整性的能力；
——安全功能应为授权用户提供验证所存储的安全功能可执行代码完整性的能力。

A.1.1.8 FPR类：私密性

A.1.1.8.1 不可观察性（FPR_UNO.1）

安全功能应确保用户或主体不能观察由受保护的用户或主体对客体进行的操作。

A.1.1.9 FRU类：资源利用

A.1.1.9.1 容错（FRU_FLT.1）

安全功能应确保当失效类型发生时，评估对象的能力能正常发挥。

A.1.1.9.2 最高限额（FRU_RSA.1）

安全功能应对受控资源分配最高配额，以便单个用户、预定义用户组、或主体能同时或在规定的时间间隔内使用。

A.1.1.10 FTP类：可信路径/信道

A.1.1.10.1 安全功能间可信信道（FTP_ITC.1）

——安全功能应在它自己和一个远程可信 IT 产品之间提供一条通信信道，此信道在逻辑上与其他通信信道截然不同，并提供其末端点有保证的标识，以及保护信道中数据免遭修改或泄露；
——安全功能应允许安全功能或远程的可信 IT 产品经由可信信道发起通信；
——对于需要可信信道的功能，安全功能应经由可信信道发起通信。

A.1.1.10.2 安全功能内部信任的通道（FTP_TRP.1）

——安全功能应在自身和远程信任的 IT 产品间提供与其他通信通道逻辑上不同的通信通道并提供信任的端点识别，避免通道数据修改或泄露；
——安全功能应允许安全功能和远程信任的 IT 产品通过信任的通道发起通信；
——对于要求信任通道的功能，安全功能应通过信任的通道发起通信。

A.1.2 安全保证要求

A.1.2.1 ACM类：配置管理

A.1.2.1.1 部分配置管理自动化（ACM_AUT.1）

——研发机构应当在研发过程中使用配置管理系统，并提供配置管理计划；
——配置管理系统应该能够提供一种自动方式实现对研发数据的已授权的变更；
——配置管理计划需描述配置管理系统中使用的自动工具，及其使用方法。

A.1.2.1.2 配置管理过程（ACM_CAP.4）

——开发人员在设计开发过程应用配置管理系统，提供配置管理文档。建议采用如下过程：

- 开发者应为每一个程序版本确定唯一的编号；
- 在配置管理文档中应包括配置清单、配置管理计划、和接受计划；
- 配置管理清单应描述组成对象程序的配置项；
- 配置管理文档应描述对配置项进行唯一标识的方法；
- 应能证明配置管理系统的运作与配置管理计划相一致；
- 配置管理文档需能够证明所有的配置项都被配置管理系统有效地维护；
- 配置管理系统应提供方法保证对配置项只进行授权修改。

A.1.2.1.3 配置管理跟踪（ACM_SCP.2）

——配置管理文档用来跟踪开发者在开发过程中的安全处理行为，在配置管理文档中应包含如下内容：

- 对象程序的实现进度；
- 设计文档；
- 测试文档；
- 用户文档；
- 安全缺陷。

——配置管理文档应描述配置管理系统是如何跟踪配置项的。

A.1.2.1.4 修改监测（ADO_DEL.2）

——开发者应对评估对象交付给用户的程序进行记录；
——开发者应使用交付程序；
——交付文档应描述在将不同版本的评估对象分发给用户时，用以维护安全所必需的所有程序；
——交付文档应描述如何提供多种程序和技术上的措施来检测修改或检测开发者的主拷贝和用户端收到的版本之间的任何差异；
——交付文档应描述如何使用多种程序来发现伪装成开发者的尝试甚至是在开发者没有向用户发送任何东西的情况下。

A.1.2.2 ADO类：交付与运行

A.1.2.2.1 安装、生成和启动程序（ADO_IGS.1）

——开发者应以文档的形式记录评估对象的安全安装、生成和启动所必需的程序：
- 文档应描述评估对象的安全安装、生成和启动所必需的步骤。

A.1.2.3 ADV类：开发文档

A.1.2.3.1 完全定义的外部接口（ADV_FSP.2）

——开发者应当提供功能规范：
- 功能规范应当用非形式化的风格来描述安全功能及其外部接口；
- 功能规范应当是内在一致的；
- 功能规范应当描述使用所有外部安全功能接口的用途与方法，提供所有影响、异常情况和错误信息的详情；
- 功能规范应当完备地表示安全功能；
- 功能规范将包括安全功能被完备表示的基本原理。

A.1.2.3.2 安全加强的高层设计（ADV_HLD.2）

——开发者将提供安全功能的高层设计：
- 高层设计的表示应当是非形式化的；
- 高层设计应当是内在一致的；
- 高层设计应当按子系统来描述安全功能的结构；
- 高层设计应当描述安全功能的每一个子系统所提供的安全功能；
- 高层设计应当标识安全功能要求的底层硬件、固件和软件，连同这些硬件、固件或软件实现的支持性保护机制提供的功能表示；
- 高层设计应当标识安全功能子系统的所有接口；
- 高层设计应当标识安全功能子系统的哪些接口是外部可见的；
- 高层设计应当描述安全功能子系统所有接口的用途和使用方法，并适当提供影响、异常情况和错误信息的详情；
- 高层设计应当描述把评估对象分成安全策略-实施和其它子系统的这种分离。

A.1.2.3.3 安全功能实现的子集（ADV_IMP.1）

——开发者应当为以下所选的安全功能子集提供实现表示：

- 与评估对象物理结构相关的子集：

a) 结构大小、组织结构和布局；
b) 互联和数据总线布局；
c) 溶化位置；
d) 物理结构包括屏蔽层和包装；
e) EEPROM 操作；
f) RAM 访问。

- 与评估对象逻辑结构相关的子集：

a) 命令范围和合法性检查；
b) 中断和复位功能；
c) 保密数据检查和操作；
d) 定义的应用之外命令的可得性；
e) 应用或功能间信息的传输。

- 与评估对象结构不可更改数据相关的子集：

a) 序列号和其他生命周期标识；
b) 调试功能的锁定或删除。

——实现表示应当无歧义而且详细地定义安全功能，使得无须进一步设计就能生成安全功能；
——实现表示应当是内在一致的。

A.1.2.3.4 模块化（ADV_INT.1）

——开发者应当以模块方式设计和构建安全功能，以避免设计模块之间出现不必要的交互作用；
——开发者应当提供结构化描述：

- 结构化描述应当标识安全功能的模块；
- 结构化描述应当描述每一个安全功能模块的用途、接口、参数和影响；
- 结构化描述应当描述安全功能设计是如何使得独立的模块间避免不必要的交互作用。

A.1.2.3.5 描述性低层设计（ADV_LLD.1）

——开发者应当提供安全功能的低层设计：

- 低层设计的表示应当是非形式化的；
- 低层设计应当是内在一致的；
- 低层设计应当以模块方式来描述安全功能；
- 低层设计应当描述每一个模块的用途；
- 低层设计应当依据所提供的安全功能性和对其它模块的依赖性关系两方面来定义模块间的相互关系；
- 低层设计应当描述如何提供每一个安全策略实施功能；
- 低层设计应当标识安全功能模块的所有接口；
- 低层设计应当标识安全功能模块的哪些接口是外部可见的；
- 低层设计应当描述安全功能模块的所有接口的用途与方法，适当时，应提供影响、异常情况和错误信息的详情；
- 低层设计应当描述如何将评估对象分离成安全策略实施模块和其它模块。

A.1.2.3.6 非形式化对应性阐明（ADV_RCR.1）

——开发者应当在所提供的安全功能表示的所有相邻对之间提供对应性分析：

- 对于所提供的安全功能表示的每一个相邻对，分析应当论证，较为抽象的安全功能表示的所有相关安全功能在较不抽象的安全功能表示中得到正确和完备地细化。

A.1.2.3.7 非形式化评估对象安全策略模型（ADV_SPM.1）

——开发者应提供安全策略模型；

——开发者应阐明功能规范和安全策略模型之间的对应性：

- 安全策略模型应当是非形式化的；
- 安全策略模型应当描述所有可以模型化的安全策略的规则与特征；
- 安全策略模型应当包括一个基本原理，即论证该模型对于所有可模型化的安全策略来说是一致的和完备的；
- 安全策略模型和功能规范之间的对应性论证应当说明，所有功能规范中的安全功能对于安全策略模型来说是一致的和完备的。

A.1.2.4 AGD类：指导性文档

A.1.2.4.1 管理者指南（AGD_ADM.1）

——开发者应当提供针对系统管理人员的管理者指南：

- 管理者指南应当描述评估对象管理员可使用的管理功能和接口；
- 管理者指南应当描述如何以安全的方式管理评估对象；
- 管理者指南应当包含在安全处理环境中必须进行控制的功能和权限的警告；
- 管理者指南应当描述所有与评估对象的安全运行有关的用户行为的假定；
- 管理者指南应当描述所有管理者控制下的安全参数，合适时，应指明安全值；
- 管理者指南应当描述每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能控制的实体的安全特性；
- 管理者指南应当与为评估所提供的其他所有文档保持一致；
- 管理者指南应当描述与管理者有关的信息技术环境的所有的安全要求。

A.1.2.4.2 用户指南（AGD_USR.1）

——开发者应当提供用户指南：

- 用户指南应该描述评估对象的非管理员用户可用的功能和接口；
- 用户指南应该描述评估对象提供的用户可访问的安全功能和接口的用法；
- 用户指南应该包含在安全处理环境中必须控制的用户可访问的功能和权限的警告；
- 用户指南应该清楚地阐述评估对象安全运行中所有必要的用户职责，包括有关在评估对象安全环境阐述中找得到的用户行为的假设；
- 用户指南应该与为评估提供的其它所有文档保持一致；
- 用户指南应该描述与用户有关的信息技术环境的所有安全要求。

A.1.2.5 ALC类：生命周期支持

A.1.2.5.1 安全措施指示（ALC_DVS.1）

——开发者应提供开发安全文档；

——开发安全文档应描述在评估对象的开发环境中，用以保护评估对象的设计和实现的保密性和完整性所有必要的物理、程序、人员以及其它安全措施；

——开发环境应包括开发和构造评估对象必要的所有设施和设施间的运输和交付；（在标准本部分

中评估对象定义为可操作的 SE 平台，由集成电路和操作软件组成，包括允许与外界通信的机制。评估对象由能够建立信任通道的硬件和软件组成。）

评估对象设计和实现至少包括以下信息：

- 设计信息：

a) IC 规范和技术；
b) IC 设计；
c) IC 硬件安全机制；
d) IC 软件安全机制；
e) 掩膜；
f) 开发工具；
g) 初始化流程；
h) 访问控制机制；
i) 认证系统；
j) 数据保护系统；
k) 存储器分区；
l) 密码程序。

- 数据：

a) 初始化数据；
b) 个人化数据；
c) 密码；
d) 密钥。

- 测试信息：

a) 测试工具；
b) 测试流程；
c) 测试程序；
d) 测试结果。

- 物理实例化

a) 硅样本；
b) 外合芯片；
c) 预初始化 SE；
d) 预个人化 SE；
e) 个人化但未发行的 SE。

——开发安全文档应提供开发和维护评估对象时执行安全措施的证据。

A.1.2.5.2 开发者定义的生命周期模型（ALC_LCD.1）

——开发者应建立开发和维护评估对象时使用的生命周期模型；

——开发者应提供生命周期定义文档：

- 生命周期定义文档应描述用于开发和维护评估对象的模型；
- 生命周期模型应提供对评估对象开发和维护的必要的控制。

A.1.2.5.3 明确定义的开发工具（ALC_TAT.1）

——开发者应标识用于开发评估对象的工具；

——开发者应为选择的依赖实现的开发工具提供文档：

- 所有用于实现的开发工具都必须有明确定义；
- 开发工具文档应无歧义地定义实现中使用的每个语句的含义；
- 开发工具文档应无歧义地定义所有基于实现的选项的含义。

A.1.2.6 ATE类：测试

A.1.2.6.1 范围分析（ATE_COV.2）

——开发者应提供对测试覆盖范围的分析：

- 测试覆盖范围的分析将论证测试文档中所标识的测试和功能规范中所描述的安全功能之间的对应性；
- 测试覆盖范围的分析将论证功能规范中所描述安全功能和测试所文档标识的测试之间的对应性是完备的。

A.1.2.6.2 测试：高层设计（ATE_DPT.1）

——开发者将提供对测试深度的分析：

- 深度分析应当论证测试文档中所标识的测试足以论证该安全功能是和高层设计一致的。

A.1.2.6.3 功能测试（ATE_FUN.1）

——开发者应当测试安全功能，并对结果形成文档；

——开发者应提供测试文档：

- 测试文档应当包括测试计划、测试程序描述、预期的测试结果和实际的测试结果组成；
- 测试计划应标识要测试的安全功能，描述要执行的测试目标；
- 测试过程描述应当标识要执行的测试，并描述每个安全功能的测试概况。这些概况包括对于其它测试结果的顺序依赖性；
- 期望的测试结果应当表明成功测试运行后的预期输出。

——开发者执行的测试的结果应当论证了每一个被测试的安全性功能按照规定进行运作了。

A.1.2.6.4 独立性测试—抽样（ATE_IND.2）

——开发者要提供评估对象进行测试：

- 评估对象要与测试相适应。

——开发者要提供一个与开发者的安全功能功能测试中使用的资源相当的集合。

A.1.2.7 AVA类：脆弱性评定

A.1.2.7.1 分析确认（AVA_MSU.2）

——开发者应提供指导性文档；

——开发者应将对指导性文档的分析形成文档：

- 指导性文档应该确定对评估对象的所有可能的运行方式(包括失败和操作失误后的运行)，它们的后果和对于保持安全运行的意义；
- 指导性文档应该是完整的、清晰的、一致的、合理的；
- 指导性文档应该列出所有对目标环境的假定；
- 指导性文档应该列出所有对外部安全措施（包括外部程序的、物理的或人员的控制）的要求；
- 分析文档应该阐明指导性是完备的。

A.1.2.7.2 安全功能强度评估（AVA_SOF.1）

——开发者应对ST中标识的每一个具有评估对象安全功能强度的安全机制进行评估对象安全功能强度的分析：

- 对于具有评估对象安全功能强度申明的每个安全机制，评估对象安全功能强度分析应说明该机制达到或超过ST定义的最低强度；
- 对于具有特定评估对象安全功能强度申明的每个安全机制，评估对象安全功能强度分析应证明该机制达到或超过ST定义的特定功能强度。

A.1.2.7.3 高级抵抗力（AVA_VLA.3）

——开发者应当分析TOE的交付材料，以寻找用户违反安全策略的途径，并将分析结果文档化；

——开发者应当文档化已标识的脆弱性的分布：

- 对所有已标识的脆弱性，文档应当能说明在所预期的评估对象环境中无法利用这些脆弱性。脆弱性分析至少应考虑以下各项：

a) 评估对象可能易遭受暴露内部电路和结构的解构；
b) 评估对象可能易遭受结构和内部存储器内容、数据传输机制、安全功能和测试方法的篡改；
c) 评估对象可能易遭受通过监测电路和结构的元素间的连接对设备内部信息的分析；
d) 评估对象可能易遭受逻辑命令的使用以产生导致安全脆弱性的响应；
e) 评估对象可能易遭受导致安全脆弱性的定义的操作边界外的操作；
f) 评估对象可能易遭受通过监测发射信号或与设备的连接对设备外部信息的分析（包括电源、场所、时钟、输入/输出和复位）；
g) 评估对象可能易遭受相同或类似评估对象前述生成中标识的脆弱性。

- 文档应当证明对于具有已标识脆弱性的评估对象可以抵御明显的穿透性攻击；
- 证据应当能说明对脆弱性的搜索是系统化的；
- 分析文档应当提供理由说明分析完全能满足TOE的交付。

A.2 SE多应用平台安全要求

A.2.1 SE管理器安全特性组

该安全组中包括了以下部分的安全特性：

——发行者安全域访问；
——生命周期状态管理；
——密钥管理；
——SE内容管理功能，包括：加载、安装、移交、个人化、删除；
——令牌验证；
——生成收条；
——其它。

A.2.1.1 发行者安全域访问安全特性

发行者安全域访问安全特性强制要求以下三条访问控制规则（关联安全特性参考A.2.2.2）：

——当发行者安全域被选择为当前应用时，无需安全通道，即可以使用GET DATA指令；
——当发行者安全域被选择为当前应用时，使用其它（DELETE、GET STATUS、INSTALL、PUT KEY、SET STATUS、STORE DATA）指令必须基于安全通道；

——加载文件验证需要一个带有 DAP 权限或者强制 DAP 权限的安全域，负责执行 DAP 验证的结果。ISD 通过验证相关安全域的加载指令是否被预授权，来决定允许下载或者拒绝下载。

A.2.1.2 SE内容管理安全特性

A.2.1.2.1 加载（Load）

加载安全特性规定了指令被认证通过后（关联安全特性参考A.2.1.1和A.2.1.3），将文件加载到SE所需要遵循的安全规则：

——待加载文件 AID 在当前系统注册表中不存在；

——待加载文件的关联 SD 在系统注册表中存在且具有安全域权限；

——加载文件所需的 SE 资源可获得。

A.2.1.2.2 安装和可选（Install & Make Selectable）

安装和可选中安全特性规定了指令被认证通过后（关联安全特性参考A.2.1.1和A.2.1.3），可执行模块的安所需要遵循的安全规则：

Install指令：

——可执行加载文件 AID 在当前系统注册表中存在；

——应用 AID 在当前系统注册表中不存在；

——应用安装所需的资源可获得。

Make selectable指令：

——应用 AID 在系统注册表中存在；

——应用在系统注册表中的生命周期状态是“已安装”。

A.2.1.2.3 迁移（Extradite）

移交安全特性规定了指令被认证通过后（关联安全特性参考A.2.1.1和A.2.1.3），应用的移交所需要遵循的安全规则：

——应用 AID 存在于系统注册表中；

——迁移目标安全域 AID 存在于系统注册表中，且具有安全域权限；

——迁移目标安全域的生命周期状态为“个人化”；

——迁移目标安全域同意应用的迁移。

A.2.1.2.4 个人化（Personalize）

个人化安全特性规定了指令被认证通过后（关联安全特性参考A.2.1.1和A.2.1.3），应用个人化所需要遵循的安全规则：

——应用 AID 存在于系统注册表中；

——应用所属安全域 AID 存在于系统注册表中。

A.2.1.2.5 删除（Delete）

删除安全特性规定了指令被认证通过后（关联安全特性参考A.2.1.1和A.2.1.3），应用或者可执行模块的删除所需要遵循的安全规则：

删除应用：

——应用 AID 存在于系统注册表中；

——该应用或应用数据未被其它应用引用；
——如果删除的应用是安全域，则保证没有应用或可执行加载文件与其关联。
删除可执行加载文件：
——可执行加载文件存在于系统注册表中；
——该可执行加载文件未被其它可执行模块引用；
——没有其它应用要从该可执行模块中实例化。

A.2.1.3 令牌验证安全特性（可选）

令牌验证安全特性允许SE管理者控制委托管理过程或是SE外部实体不属于安全域提供方时的授权管理过程（关联安全特性参考A.2.2.1）。该安全特性可选。

安全域需获得LOAD、INSTALL、EXTRADITE或者DELETE指令的预授权，除DELETE指令可被自动授权执行，其它指令均须被通过发行者安全域令牌验证后才得以执行。安全规则包括：
——应用的安全域 AID 在注册表中存在；
——发行者安全域拥有令牌验证密钥；
——文件加载指令下，下载文件数据块 HASH 值验证通过；
——指令令牌验证通过。

A.2.1.4 收条生成安全特性（可选）

收条生成安全特性通过提供基于结果的反馈，支持委托管理过程。这个安全特性是可选的，支持此项安全特性时，发行者安全域必须拥有收条生成密钥。（关联安全特性参考A.2.1.2）

A.2.1.5 生命周期状态管理安全特性

生命周期状态管理安全特性保证所有的生命周期状态迁移都必须是符合要求的。如果状态迁移是对一个APDU命令的执行或一次API调用的响应，那么状态迁移操作必须先被相应的APDU安全特性或API安全特性验证过才行。（关联安全特性参考A.2.1.1、A.2.2.1及A.2.4）

A.2.1.6 其它SE管理功能安全特性

其它SE内容管理功能安全特性规定了GET DATA和STORE DATA等命令被验证通过后所需要遵循的安全规则，GET DATA始终是被许可的。（关联安全特性参考A.2.1.1及A.2.2.1）

A.2.1.7 密钥管理安全特性

密钥管理安全特性提供了密钥的生成、分发、访问和销毁功能，它包括四个部分，每个部分对应一种功能。

A.2.1.7.1 密钥生成服务

这部分密钥管理的安全特性安全特性主要责任是生成唯一的会话密钥，会话密钥生成规则参考JR/T 0089.2-2012的相关要求。（关联安全特性参考A.2.2.2.2）

密钥管理的安全特性也负责通过API为应用提供生成其它密钥的功能。

A.2.1.7.2 密钥加载服务

该部分安全特性支持把SE外生成的密钥加载到SE上。（关联安全特性参考A.2.1.1及A.2.2.1）

——发行者安全域的初始密钥由初始化密钥进行加密加载。安全域初始密钥由发行者安全域的 K_{DEK} 或初始化密钥进行加密加载。安全域中随后的静态密钥由安全域中之前加载的 K_{DEK}

进行加密加载，并通过带会话密钥的安全通道进行保护。发行者安全域的其它密钥被加载时，要用发行者安全域密钥集中的 K_{DEK} 加密，并通过带会话密钥的安全通道进行保护；

——在 SE 进入生命周期的“就绪（READY）”状态前，须确保初始化密钥已被安全加载；

——在成功的更新或替换掉旧的密钥后，密钥管理安全特性要使旧密钥无效，这是通过密钥销毁服务完成的；

——在处理 APDU 命令过程中，密钥管理安全特性为保证只分发合法的密钥，会拒绝任何不符合 SE 规范规定长度的密钥。

密钥管理的安全特性也负责通过 API 为应用提供分发其它密钥的功能。

A.2.1.7.3 密钥访问服务

该部分安全特性支持对指定安全通道密钥集的访问，所访问的密钥应该存在且未被“锁定”。（关联安全特性参考A.2.2.2.2）

密钥管理的安全特性也负责通过API为应用提供访问其它密钥的功能。

A.2.1.7.4 密钥销毁服务

该部分安全特性支持安全销毁那些不再需要的密钥，避免敏感信息泄露。（关联安全特性参考A.2.1.1，A.2.2.1及A.2.2.2.6）

密钥管理的安全特性也负责通过API为应用提供销毁其它密钥的功能。

A.2.2 安全域安全特性组

该安全组包括6个特性，分别是：安全域访问、安全通道、非安全通道、DAP验证、强制DAP验证和CVM处理。

A.2.2.1 安全域访问安全特性

安全域访问安全特性执行以下访问控制规则。安全域访问安全特性仅适用于支持安全域的SE（关联安全特性参考A.2.2.2）。

——当安全域被选择为当前应用时，无论是否在安全通道条件下，都可以正常执行 SE 外部实体发送的 GET DATA 指令；

——当安全域被选择为当前应用时，必须基于安全通道条件下，方可正常执行 SE 外部实体发送的其它指令（DELETE、GET STATUS、INSTALL、PUT KEY、SET STATUS、STORE DATA）；

——若指令执行安全域具备委托管理权限，且其所执行的 LOAD、INSTALL、EXTRADITE 指令需被预授权，供发行者安全域或具有“令牌验证权限”的安全域进行验证；

——若指令执行安全域具备授权管理权限，且安全域提供方在 SE 外部实体被合法认证为该安全域的所有者时，无需预授权（即不用令牌）就可以执行 SE 内容管理。但是当 SE 外部实体被认证为非安全域提供方的合法实体时，令牌仍然是必须的。

A.2.2.2 安全通道安全特性

安全通道安全特性代表发行者安全域或其它安全域实现安全通道协议。安全通道总是用于从SE外向SE上传输与安全有关的数据，也可以传输用户数据。

它包括六个子功能：

——安全策略；

——安全通道初始化；

——消息完整性和认证；

——消息数据机密性；
——密钥和其它安全数据接收服务；
——安全通道终止。

A.2.2.2.1 安全策略

安全策略用以保证只有通过认证的用户才能按照安全域相关的安全策略请求SE内容管理操作（关联安全特性参考A.2.5.1）。

A.2.2.2.2 安全通道初始化

该部分安全特性支持SE管理者或安全域用户通过其安全域或一个应用来初始化安全通道通信（关联安全特性参考A.2.4及A.2.2.2）。安全通道初始化安全特性针对不同的安全通道发起方式有所不同，但都应支持：

——静态安全通道密钥存在并可选；
——成功实现与 SE 外部实体的相互认证。

A.2.2.2.3 消息完整性和认证

该部分安全特性保证SE接收到的数据确实是从经过认证的SE外部实体发送过来的，并且命令的正确顺序没有经过任何篡改（关联安全特性参考A.2.4及A.2.2.2）。消息完整性检查、MAC链的计算，再结合会话密钥的唯一性，使得安全通道安全特性能够支持：

——检测到攻击者在不正确的时间重放的 APDU 指令序列或不符合正确顺序的 APDU 指令序列；
——防止会话被修改。

A.2.2.2.4 消息数据机密性

该安全特性用以保证攻击者无法窃听发送到SE的APDU命令，如果支持在响应时使用R—MAC机制，可保证响应数据也无法被窃听（关联安全特性参考A.2.4及A.2.2.2）。

A.2.2.2.5 密钥和其它敏感数据的接收服务

该安全特性可以确保密钥或其它敏感数据（例如：CVM值）在从SE外向SE上传输过程中的机密性（关联安全特性参考A.2.4及A.2.1.7.2）。SE外部加密密钥传输到SE内后被解密后保存，具体解密算法参考JR/T 0089.2-2012的相关要求。

A.2.2.2.6 安全通道终止

该安全特性保证：当通过APDU指令或API终止一个安全通道会话时，需要将当前安全通道重置。重置工作包括：设置安全级别为“无安全级别”，并且清除所有的会话密钥和初始向量。（关联安全特性参考A.2.2.2，A.2.4及A.2.5.1）

A.2.2.3 无安全通道安全特性

无安全通道安全特性提供了一种SE外部实体不使用安全通道与SE通信的手段。这时，不允许任何绕过SE访问安全策略对APDU命令缓冲区的访问（关联安全特性参考A.2.5.1）。

这种安全特性一般用于向应用发送APDU命令，而非向发行者安全域或其它安全域发送命令。需要注意的是，应用仍可以通过使用API安全特性来利用安全通道机制。

A.2.2.4 DAP验证安全特性（可选）

DAP验证安全特性支持具有相应权限的安全域用户确认其相关应用加载文件在从应用提供者通过应用下载者加载到SE上之前未被修改过（关联安全特性参考A.2.1.1及A.2.2.1）。这项安全特性可选。

当加载文件时，须保证：

——加载文件 HASH 值已验证通过；

——加载文件的相关安全域具有 DAP 权限和 DAP 验证密钥；

——加载文件指令中的 DAP 块经指定安全域验证通过。

A.2.2.5 强制DAP验证安全特性（可选）

强制DAP验证安全特性支持控制授权中心或验证授权中心在确认待加载应用文件已经被授权机构认证（例如：成功的通过SE外应用编码验证）之前，有权禁止在SE上加载和安装该应用（关联安全特性参考A.2.1.1及A.2.2.1）。这项安全特性可选。

当加载应用时，须保证：

——加载文件 HASH 值已验证通过；

——加载文件的相关安全域具有强制 DAP 验证权限和 DAP 验证密钥；

——加载文件指令中的 DAP 块经指定安全域验证通过。

A.2.3 全局服务应用安全特性

一个全局服务应用必须：

——能够向其他应用提供 CVM 之类的服务；

——安全地持有全局服务应用相关的数据；

——提供服务时，执行内部的安全评估；

CVM处理安全特性实现了SE使用者验证方法，CVM的形式可以是一个PIN码。这个安全特性仅在SE配置CVM管理功能时需要。CVM只是用来验证用户，而不是标识他们。连续多次的验证失败意味SE可能正在遭受攻击或者SE使用者的确忘记了PIN码。在多次尝试PIN码的操作之间，SE甚至可能被加电、断电。

——锁定和解锁 CVM 操作的请求通过 SE 相关权限应用的许可；

——CVM 值及尝试限次的修改必须符合原子操作。

（关联安全特性参考 A.2.4 及 A.2.5.1）

A.2.4 API安全特性

应用必须使用SE平台提供的应用编程接口（API）调用SE系统资源。API约束特定的访问控制规则，用户验证机制，以及对各种加密等功能的调用（关联安全特性参考A.2.5.1）。

A.2.5 运行时环境安全特性组

运行时环境包括六个安全特性，分别是监管者、防火墙、对象复用、事件行为、主体/对象识别和SE审核。

A.2.5.1 监管者安全特性

——监管者安全特性保证 SE 进行有效的管理控制，使所有的安全特性都在正确的时间被执行，不能被绕过、失效、破坏或以其它方式规避；

——它同时担当 APDU 指令分发者的角色，但它并不负责 APDU 指令的正确性和完整性。

A.2.5.2 防火墙安全特性

——防火墙安全特性确保应用之间不能互相访问程序代码和私有数据（关联安全特性参考A.2.5.1）；

——读写操作无论是直接读写、间接读写或者请求访问存储空间都需要符合防火墙安全特性要求；

——直接读写是指应用直接引用对象，并对对象属性进行操作的行为。针对应用或者平台数据进行直接读写时，需要检查所访问的对象是否存在，且应用的安全权限满足对该对象的操作要求；

——间接读写是指应用通过平台 API 对指定对象进行的操作，这类操作必须通过运行时环境所支持的应用间通信通道进行，并确保满足运行时环境所定义的访问控制规则及信息流控制规则。

A.2.5.3 对象重用安全特性

对象复用安全特性确保重用对象的使用者不能访问到对象原内容（关联安全特性参考A.2.5.1）。具体安全特性包括：

——清空非易失性数据；

——被删除应用的对象数据不可被读取；

——特定应用的 APDU 缓存内容不可被其它应用获取；

——特定应用的算法缓存中的内容不可被其它应用读取；

——特定对象的临时数据不能被新对象获取。

A.2.5.4 事件行为安全特性

事件动作安全特性捕捉潜在的安全问题，保证根据事件行为策略中的规定采取处理响应（关联安全特性参考A.2.5.2，A.2.5.7及A.2.5.8）。

所有“事件行为策略”中定义的行为都必须严格按照“事件行为策略”中定义的规则进行处理以消除相应的警告。

A.2.5.5 对象/主体识别安全特性

主体/对象识别安全性确保平台环境对每个对象/主体都能正确识别（关联安全特性参考A.2.5.1）。

A.2.5.6 SE审核安全特性

SE审核安全特性使唯一鉴别SE设备变得容易，而且SE审计还支持记录事件，提供传统意义的审核用（关联安全特性参考A.2.5.1）。

一种情况下：当发行者安全域处于“准备状态”前，且SE可以在安全环境下使用时，SE制造商预先在SE上加载有具有唯一区分性信息，如：芯片识别标识、平台代码标识。

另一种情况：平台记录其它一些审计信息：比如SE发行者标识，SE标识，SE注册信息或者其它可能被写入到发行者安全域中的SE发行者信息。

此外，一些动态审计信息是可选的，比如：

——当前所选择的应用；

——APDU 类型；

——当前应用最后执行的行为；

——事件行为策略中定义的事件。

这些动态审计信息只需要记录到上次发生的事件就可以了，如果有多个记录，则记录数量的限制取决于SE制造商。如果给审核数据分配的存储空间用完了，再有新的记录进来，就要把最旧的记录删掉。

SE审核安全特性要保证审核记录数据的安全，审核记录不能被未经授权删除或修改。审核记录必须包括哪些数据由SE发行者和SE制造商协商决定。

A.2.5.7 自检安全特性

自检安全特性使SE管理者能够验证SE上安全数据和其它与安全有关的可执行代码的完整性（关联安全特性参考A.2.5.1）。平台并不要求安全特性的执行一定是由APDU命令发起的。自检在系统启动、正常运行时的某个周期或者在某些某些预定条件出现（如：非正常掉电后的第一次加电）时发生。安全规则要求如下：

——SE 掉电（可能是异常的掉电）后，特定存储区（非易失性内存区）的内容应保持不变；

——芯片制造商自定义的 IC 检测机制，应该能够确保运行正常：当检测到异常情况时，SE 应产生一个警告。

A.2.5.8 失败管理安全特性

失败管理安全特性确保SE在遇到异常时保持安全性（关联安全特性参考A.2.1.2，A.2.1.5，A.2.1.6，A.2.1.7.2，A.1.7.4，A.2.4及A.2.5.1）。比如SE正在运行时异常掉电，导致当前操作失败或出现内部错误，该安全特性确保SE能根据需要保存注册表和易失存储器内容。内存的恢复过程应能保证数据的安全性和一致性。

A.3 移动支付SE规格要求

A.3.1 PAMID

每个SE都具有一个唯一的身份标识PAMID，PAMID由公共服务平台负责统一分配和备案管理，由发行方写入SE中，PAMID写入后不能够被更改。

A.3.2 加密算法

厂商除实现SE的通用加密算法外，应考虑支持以下国产加密算法（可选）。具体包括：

——对称加密：SM4，3DES；

——非对称算法：SM2，RSA；

——杂凑算法：SM3，SHA-1。

A.3.3 基本安全域设置

SE 中的安全域分为如下几类：

——主安全域：主安全域即发行方安全域，由发行方持有，主安全域没有安全域生命周期状态，他直接继承了 SE 生命周期状态；

——辅助安全域：主安全域以外的其他安全域称为辅助安全域；

——FCSD 安全域：FCSD 安全域是一种特殊的辅助安全域，安全域关联到自身，直接继承了 SE 生命周期状态，由公共服务平台持有，不能被主安全域锁定、删除。其主要更能是进行 SE 合法性的验证；

——FMSD 安全域：FMSD 安全域是一种特殊的辅助安全域，安全域关联到自身，直接继承了 SE 生命周期状态，具有授权管理者权限，由公共服务平台持有，不能被主安全域锁定、删除。

A.3.3.1 FCSD（发行方为可信管理者的开放共享模式）

在以发行方为可信管理者的开放共享模式下，SE 中需预置的安全域为：

——主安全域；

——FCSD安全域。

图1描述了该模型下SE的一个实现结构：

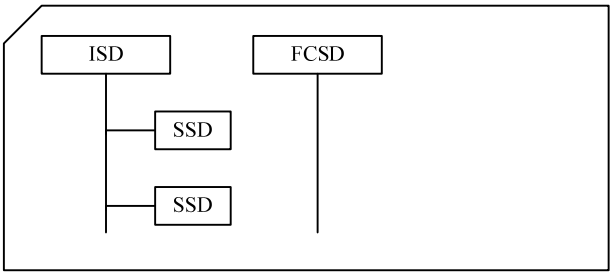

图1　发行方作为可信管理者开放模型下的 SE 实现

A.3.3.2　FMSD（公共服务平台作为可信第三方的开放共享模型）

在以公共服务平台作为可信第三方的开放共享模式下，SE 中需预置的功能安全域如下：

——主安全域；

——FCSD 安全域；

——FMSD安全域。

实现中要求将FMSD安全域功能集成到FCSD安全域中，图2描述了该模型下SE的一个实现结构：

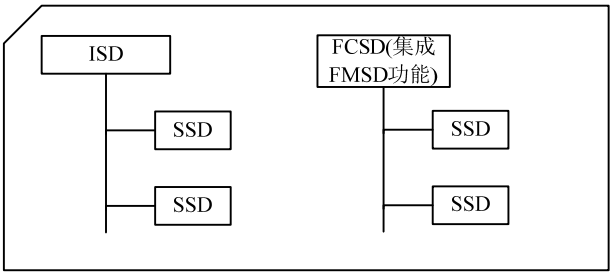

图2　以公共服务平台作为可信第三方开放模型下的 SE 实现

A.3.4　基本基础服务

A.3.4.1　应用选择服务

该服务通过金融目录文件及其配套的管理应用实现。金融目录管理应用在 SE 上作为必选应用装载。该应用提供两个基本用户信息文件支持应用的选择。金融目录文件结构如图 3 所示。

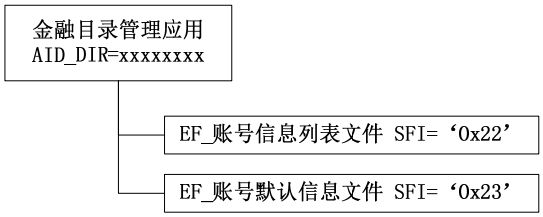

图3　SE 中的应用选择服务

利用该服务提供的 SE 应用信息，可以协助终端与 POS 设备建立用户人机交互操作界面列表。

A.3.4.2　SE可信身份认证服务

SE 可信身份验证服务是由公共服务平台调用的局部服务，用于提供 SE 及其持有者实体身份验证

和实名身份传递。

SE 可信身份验证服务由 FCSD 安全域提供，FCSD 安全域中存有 PAMID、SE 持有者的非对称密钥、公钥证书和公共服务平台的公钥证书。当进行 SE 的合法性检查时，公共服务平台与 FCSD 安全域建立 SCP10 方式的安全通道，如安全通道成功建立则说明 SE 合法。

A.3.4.3 SE的PIN校验

SE 的 PIN 校验服务是一个全局服务，用于当管理客户端访问 SE 时进行 PIN 校验。

SE 的 PIN 校验由 OPEN 提供，OPEN 具备 CVM 管理权限，当管理客户端试图访问 SE 内支付应用时，发送 VERIFY PIN 指令，OPEN 调用 GP API 进行 PIN 校验。

A.3.5 APDU命令

SE 支持的 APDU 命令包括：

——DELETE；
——GET DATA；
——GET STATUS；
——INSTALL；
——LOAD；
——MANAGE CHANNEL；
——PUT KEY；
——SELECT；
——SET STATUS；
——STORE DATA；
——PERFORM SECURITY OPERATION；
——GET CHALLENGE；
——EXTERNAL AUTHENTICATION；
——INTERNAL AUTHENTICATION；
——MANAGE SECURITY ENVIRONMNET；
——VERIFY PIN。

A.3.6 安全通道

A.3.6.1 应用可信通道

辅助安全域的安全通道类型由应用提供方与辅助安全域的创建者协商确定，标准本部分不做定义。

附 录 B
（资料性附录）
多应用平台安全与嵌入式软件 SFRs 参照

B.1 多应用平台安全与嵌入式软件SFRs参照

表B.1 SE 多应用平台安全与嵌入式软件 SFRs 参照表

SE 多应用平台安全特性	SFRs
GP API 访问安全特性	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.2, FMT_MTD.1, FMT_MTD.3, FPR_UNO.1**
RTE API 访问安全特性	FMT_MOF.1, FMT_MSA.2, FMT_MTD.3, FPR_UNO.1**, FCS_CKM.1**, FCS_CKM.2**, FCS_CKM.3**, FCS_CKM.4**, FCS_COP.1**
安全域访问安全特性	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.2, FMT_MTD.1, FMT_MTD.3, FDP_ACC.2**
强制 DAP 验证安全特性	FCS_COP.1, FDP_IFC.2**, FDP_IFF.2**, FDP_MSA.1**, FDP_MSA.2**, FMT_MSA.3**, FRU_RSA.1**, FCO_NRO.2**
DAP 验证安全特性	FCS_COP.1
安全通道安全特性 安全通道初始化 消息数据机密性 消息完整性及认证 密钥及其它敏感数据	 FTP_ITC.1, FCS_COP.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FDP_IFC.2**, FDP_IFF.1**, FMT_MSA.1**, FMT_MSA.3** FCS_COP.1 FCS_COP.1, FDP_UIT.1, FPT_ITI.1, FPT_RPL.1 FCS_COP.1
非安全通道安全特性	FDP_ETC.1, FDP_ITC.1
CVM 处理安全特性 其它功能安全特性	FIA_UAU.7, FIA_AFL.1, FMT_MTD.2 FIA_UID**
发行者安全域访问安全特性	FDP_ACC.1, FDP_ACF.1,

SE 多应用平台安全特性	SFRs
	FMT_MOF.1, FMT_MSA.2, FMT_MTD.1, FMT_MTD.3, FIA_UID.1**
SE 内容管理安全特性	FDP_ACC.2**, FDP_ACF.1**, FDP_ITC.2**
令牌验证安全特性	FCS_COP.1, FDP_ACC.2**, FDP_ACF.1**
收条生成安全特性	FCS_COP.1
生命周期管理安全特性	FDP_ACC.1, FDP_ACF.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.3, FMT_REV.1
密钥管理安全特性 密钥生成服务 密钥分发服务 密钥访问服务 密钥销毁服务	 FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4
自检安全特性	FPT_TST.1, FPT_AMT.1**
失败管理安全特性	FPT_FLS.1, FPT_RCV.3, FPT_RCV.4, FPT_RVM.1**
监管者安全特性	FIA_ATD.1, FMT_SMR.1, FPT_RVM.1, FMT_SMR.1**
防火墙安全特性	FMT_MSA.3, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FMT_MSA.1, FPT_SEP.1, FDP_ACC.2**, FMT_MSA.2**, FMT_MSA.3**, FMT_MTD.1**
对象复用安全特性	FDP_RIP.1
事件行为安全特性	FAU_ARP.1, FAU_SAA.1
主体/对象识别安全特性	FIA_ATD.1, FMT_MTD.1, FMT_SMR.1, FIA_UID.2**, FIA_USB.1**
SE 审计安全特性	FAU_GEN.1, FAU_SAA.1**, FAU_SEL.1, FAU_STG.1, FAU_STG.3

注：由’**’所标记的SFRs派生自JCSPP

B.2 SE安全威胁与多应用平台防护措施

B.2.1 SE安全威胁

B.2.1.1 伪装

对于传统的伪装性攻击的根本防御措施是要保证安全通道的安全特性，特别是实现安全通道初始化子功能。根据安全通信策略（TOE与可信CAD之间的安全通信协议及过程）实现安全通信通道安全，可用以抵御攻击者可能会伪装成SE管理者或者一个安全域的使用者进行攻击的可能性。

CVM处理的安全特性可抵御伪装持卡者的应用程序进行攻击的风险。通过RTE的API，运行时环境可以提供相关功能。

安全通道的安全特性和CVM处理的安全特性，确保了在主机或持卡者认证上发生反复的不成功的攻击时，不会将那些有助于攻击成功的信息泄漏给攻击者。

B.2.1.2 窃听

假设包括密钥管理过程在内的SE外部安全管理措施会挫败以攻击SE外部系统为目的的伪装企图，但攻击者还可能会在SE上窃听与主机间的通信。安全通信策略被设计用来抵御该类攻击，对这种类型的攻击的主要防御手段是实现安全通道安全特性。应当指出，并不是每条信息都必须加密，根据商业上的需求和相关应用的风险状态，应用提供者可以选择使用怎样的信息（包括请求和响应命令）。运行时环境的加密功能也可以通过运行时的API提供。

窃听的目的可能是窃取下载文件用于安全性分析。这样当应用在别处使用时，可以较为容易地窃取到该应用。

B.2.1.3 开发环境中的缺陷

SE本身并不能直接的抵御这种攻击，是因为这种窃取行为发生在SE外环境中。但是，SE提供了一种手段，使得当SE外系统侦测到类似攻击时，发送命令将SE上的应用进行锁定。应用锁定的能力主要由生命周期状态管理安全特性来保证。

B.2.1.4 重放攻击

窃听的另外一个目的是窃取真实的APDU命令序列，按照攻击者的意愿修改它，然后再发出去。对该类攻击的主要防御是通过保证安全通道安全特性，对于每个安全通道会话都要生成新的密钥。

B.2.1.5 未授权的访问

一旦SE管理员或者安全域的使用者被成功的进行了认证，将需要按照GP的访问控制策略对每个角色所能进行的操作进行约束。风险来自用户尝试做未经授权的事。

对于这种攻击的主要防御是通过保证SE发行者安全域访问安全特性和安全域访问安全特性。应用可能会尝试做未被授权的操作，在这种情况下，主要防御是通过保证API访问安全特性。

API访问安全特性控制对于CVM管理者的访问。防火墙安全特性控制对其它对象的访问。

B.2.1.6 无效输入和强力攻击

即便访问控制机制的有效，一个被认证通过的访问者也可能在他的被许可的范围内，进行试探平台能力的操作，以求发现安全漏洞。除了各种各样的访问控制策略，对于这种风险的主要防御手段是通过保证事件行为安全特性。在检测到潜在的安全侵害时，或SE发行者定义的某些风险行为时，该安全特性将会支持锁定SE。

另外，对于所有的这些安全特性有一个常规性的要求：安全特性输入数据检查该数据的有效性。此外，通过选择加密算法，也会使强力攻击进一步落空。

B.2.1.7 未授权的应用

一个特定的情形涉及到未被授权的应用的下载。SE的管理者被授权执行应用下载、安装和迁移。对于攻击者伪装成SE管理者的风险防御手段主要是对主机端认证。拥有相应特权的安全域（由安全域访问安全特性控制）能够对属于他们自己的应用执行委托下载、安装和迁移操作。假定安全域拥有委托管理的特权，为防止SE外未经SE管理者授权的安全域所有者改变SE的内容，需要实现令牌验证安全特性。SE发行者生成与应用绑定的令牌，以确认该行为是被授权的。如果，安全域并没有委托管理特权，那么对于相关应用委托下载、安装和迁移的请求将会被拒绝。

另外一种类型的攻击可能通过激活安装在IC上的测试功能进行，这种情况下主要的防御手段是通过保证SE存储器管理安全特性实现。

B.2.1.8 未授权的应用删除

未授权访问的另一种情况与应用的未授权删除有关。SE管理者被授权做应用删除，防御应用未授权删除通过安全通道安全特性的安全通道初始化部分，确定用户是真正的SE管理者。安全性也依赖于在SE外的限制策略防止SE管理者进行不必要的应用删除操作。有相应特权的安全域能够删除它们自己的应用，该行为由安全域访问安全特性控制。

B.2.1.9 被篡改的应用下载

未认证应用的一种风险情况是在应用在下载之前被篡改，安全通道安全特性的信息的完整性和认证部分对应防御此项威胁，对于具有DAP校验特权的安全域，通过校验安全特性或强制DAP校验安全特性来防御这类威胁。这些安全特性通过验证应用DAP体现，DAP是由应用提供者创建，用来保证在从应用提供者到应用加载者之间传输过程中应用没有被修改。DAP是被预期提供的，这样就能阻止欺诈性应用加载者在不要求提供完整性的校验的情况下，移走DAP并篡改应用，再将修改后的下载文件提交给SE。

需要提供一种安全措施，避免应用违背安全域所有者的意愿关联到其安全域上。做法是确认安全域准备接收相关应用的迁移。

B.2.1.10 数据加载失常

非授权应用的另一种风险是在发行前阶段，SE激活者设置SE时进行的攻击。防御由安全通道安全特性以及发行前阶段相关的SE外安全措施来保证。

B.2.1.11 非预期的程序交互

尽管采用了阻止欺诈性应用被下载到SE上防御措施，但一个下载的应用可能会试图访问另外的一个应用的地址空间，包括通过COS读写数据，特别是安全相关的数据，或者如果物理上可能的情况下进行数据修改。对于这类风险的主要防御手段是要确保存储器内容安全特性和防火墙安全特性。

B.2.1.12 摄取遗留数据

一个与访问风险相关的类似攻击是：当包含某应用信息的资源被重新分配的时候，其它应用使用该应用使用过的数据。对于这种情况的防御由对象重用安全特性来保证。

B.2.1.13 绕过应用的安全性

应用通过充分利用安全通道，CVM，RTE的API，密码和PIN功能以及应用特定的措施，可以提供额外的安全特性。存在一种攻击风险，攻击者可能会绕过这些安全措施。这样的企图由管理员安全特性进行防御，它保证COS安全机制不能被绕过，即：COS不能成为被作为绕过应用特定安全措施的工具。

B.2.1.14 强制性重启

SE不能够防止断电或者突然从读卡环境取出，这样SE必须解决的另外一种威胁就被称为强制重启，攻击者可能会使用这种方式使SE进入一种不安全的生命周期状态。对于这种情况的根本的防御措施是失败管理安全特性。

B.2.2 安全防护措施

表B.2是从威胁到安全要求或安全防护的一个映射表，每一个威胁都将被至少一个安全要求或安全防护覆盖。它说明了安全要求和安全防护的组合确实能够防止所有的威胁。

表B.2 安全威胁与安全要求/防御映射表

安全威胁	安全要求/安全防御
伪装	安全通道安全特性–安全通道初始化（A.2.2.2.2） 安全通道安全特性–密钥和其它保密数据的接收服务（A.2.2.2.5） 安全通道安全特性（A.2.2.2） CVM 处理安全特性（A.2.2.6） 主体/对象识别安全特性（A.2.4.5）
窃听	安全通道安全特性–消息数据加密（A.2.2.2.4）
开发环境中的缺陷	生命周期状态管理安全特性（A.2.1.5）
重放攻击	消息完整性与认证安全特性（A.2.2.2.3） 密钥管理安全特性-密钥生成服务（A.2.1.7.1）
未授权的访问	发行者安全域访问安全特性（A.2.1.1） 安全域访问安全特性（A.2.2.1） API 安全特性（A.2.4） 防火墙安全特性（A.2.5.2）
无效输入和强力攻击	事件行为安全特性（A.2.5.4）
未授权的应用	安全域访问安全特性（A.2.2.1） 令牌验证安全特性（A.2.1.3） 存储器内容安全特性（A.2.6）
未授权的应用删除	安全通道安全特性–安全通道初始化（A4.2.2.2） 安全域访问安全特性（A.2.2.1）
被篡改的应用下载	安全通道安全特性–消息完整性及认证（A.2.2.2.3） SE 内容安全管理特性–迁移（A.2.1.2.1） DAP 验证特性（A.2.2.4） 强制 DAP 验证安全特性（A.2.2.5）
数据加载失常	SE 内容管理安全特性（A.2.1.2） 安全通道安全特性（A.2.2.2）
非预期的程序交互	存储器内容安全特性（A.2.6） 防火墙安全特性（A.2.5.2）
摄取遗留数据	对象复用安全特性（A.2.5.3） 防火墙安全特性（A.2.5.2）
绕过应用的安全性	监管者安全特性（A.2.5.1）
强制性重启	失败管理安全特性（A.2.5.8）

参 考 文 献

[1] GlobalPlatform Card Specification, version 2.1.1, May 2003 and version 2.2, March 2006
[2] GlobalPlatform Card Security Specification 1.0, May 2003
[3] Java Card System Protection Profile Collection, Version 1.0, April 2003, Sun Microsystems Inc
[4] The Smart Card Security User Group Smart Card Protection Profile, Version 3.0, September 2001
[5] QCUP 040.2-2011　银联卡芯片安全规范 第 2 部分 嵌入式软件规范