ICS 35.040
L 80

中华人民共和国国家标准

GB/T 34095—2017

信息安全技术 用于电子支付的基于近距离无线通信的移动终端安全技术要求

Information security technology—Technology requirements for electronic payment of mobile terminal security based on short-range radio communication technology

2017-07-31 发布　　2018-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:工业和信息化部电信研究院、中国移动通信集团公司、中国联合网络通信集团有限公司、中国电信集团公司、中国银联股份有限公司、北京握奇数据系统有限公司、重庆电信研究院。

本标准主要起草人:夏骆辉、孙宇涛、成秋良、任晓明、张强、纪成军、谭颖、张楚、范雨晓、袁浩。

信息安全技术
用于电子支付的基于近距离无线通信的移动终端安全技术要求

1 范围

本标准规定了基于近距离无线通信的移动终端电子支付的智能卡和内置安全单元安全技术要求，内容包括评估对象(TOE)定义、安全问题定义、安全目的描述、安全要求描述等。

本标准适用于基于近距离通信技术、支持电子支付业务的载有智能卡或内置安全单元的移动终端电子设备。

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 25069—2010 信息安全技术 术语

GM/T 0005—2012 随机性检测规范

ISO/IEC 7816-2:2007 识别卡 集成电路卡 第2部分:带触点的卡 触点的尺寸和定位(Identification cards—Integrated circuit cards—Part 2: Cards with contacts—Dimensions and location of the contacts)

ISO/IEC 7816-6:2004 识别卡 集成电路卡 第6部分:交换用业内数据元素(Identification cards—Integrated circuit cards—Part 6:Interindustry data elements for interchange)

ISO/IEC 15946-1:2008 信息技术 安全技术 基于椭圆曲线的密码技术 第1部分:总则(Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 1:General)

ISO/IEC 15946-3:2002 信息技术 安全技术 基于椭圆曲线的密码技术 第3部分:键的确定(Information technology—Security techniques—Cryptographic techniques based on elliptic curves—Part 3: Key establishment)

ISO/IEC 9797-1:2011 信息技术 保密技术 消息真实性代码 第1部分:块代码机制[Information technology. Security techniques. Message Authentication Codes (MACs)—Part 1:Mechanisms using a block cipher]

ISO/IEC 10116:2006 信息技术 安全技术 n 位块密码算法的操作方式(Information technology—Security techniques—Modes of operation for an n-bit block cipher)

GP22:2011 全球平台卡规范(GlobalPlatform Card Specification)

3 术语和定义、缩略语

3.1 术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

Java 程序　applet

写入 Java Card 智能卡内的应用程序。

3.1.2

应用协议数据单元　application protocol data unit;APDU

智能卡与通信设备之间的标准的消息传递协议数据单元。

3.1.3

非对称加密　asymmetric cryptography

一种运用了两种变换的加密技术，即由公开密钥组件定义的公开转换和由私有密钥组件定义的私有转换；该公私钥对具备一种特殊的属性，即不能由公钥推断出私钥。

3.1.4

卡持有者　cardholder

智能卡或嵌入式安全单元的最终用户。

3.1.5

卡发行商　card issuer

对智能卡进行个人化操作的组织。

3.1.6

嵌入式软件　embedded software

在嵌入式设备中运行的软件，具有可访问资源有限的特点。

3.1.7

可执行的装载文件　executable load file

实际存在于智能卡内的包含一个或多个应用的可执行代码的容器，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。

3.1.8

移动支付　mobile payment

基于采用 NFC-SWP 方式或 NFC 全终端方式的手机终端近距离支付业务。

3.1.9

私钥　private key

非对称加密密钥对中，非公开的密钥。

3.1.10

公钥　public key

非对称加密密钥对中，公开的密钥。

3.1.11

安全信道　secure channel

为智能卡外实体和智能卡之间的信息交换提供某种安全保障的通信机制。

3.1.12

安全域　security domain

负责对某个智能卡外实体（例如发卡方、应用提供方、授权管理者）的管理、安全、通信需求进行支持的智能卡内实体。

3.1.13

安全单元　secure element;SE

用于设备中的防篡改组件，提供安全性、保密性以及支持不同业务模型的多应用环境，安全单元可以各种不同形式存在，如 UICC、嵌入式安全单元等。

3.1.14

通用用户识别模块　universal subscriber identifier module;USIM

通用用户身份模块(用于 3G 移动网络)。

3.1.15

打开组件　open

GlobalPlatform 平台的实时运行环境组件。

3.1.16

Java 卡　Java card

运用于智能卡领域的软件技术,包括 Java Card 系统、Java Card 平台、Java Card Applet 等内容。

3.1.17

全球平台　globalplatform

运用于智能卡领域的软件技术,包括卡片管理器、辅助安全域、GlobalPlatform 应用编程接口等内容。

3.1.18

近场通信　near field communication;NFC

近距离无线通信技术。

3.2　缩略语

下列缩略语适用于本文件。

AID　应用标识符(Application Identifier)

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

API　应用编程接口(Application Programming Interface)

ATR　响应复位命令(Answer To Reset)

CAD　智能卡接收设备(Card Acceptor Device)

CA　证书认证机构(Certificate Authority)

CASD　证书认证机构安全域(Certificate Authority Security Domain)

CC　通用准则(Common Criteria)

CCM　智能卡内容管理(Card Content Management)

CLF　非接触前端(Contactless Front-end)

CPLC　智能卡生产生命周期数据(Card Production Life Cycle Data)

CVM　智能卡持有人验证方法(Cardholder Verification Method)

DAP　数据验证模式(Data Authentication Pattern)

DES　数据加密标准(Data Encryption Standard)

DFA　差分故障分析(Differential Fault Analysis)

DPA　微分功率分析(Differential Power Analysis)

EAL　评估保证级(Evaluation Assurance Level)

EEPROM　电可擦可编程只读存储器(Electrically Erasable Programmable Read Only Memory)

EMA　电磁分析(Electro-Magnetic Analysis)

EPA　发散功率分析(Emanation Power Analysis)

GP　全球平台(GlobalPlatform)

ISD　智能卡发行商安全域(Issuer Security Domain)

NFC　近场通信(Near Field Communication)

OS　操作系统(Operating System)

PP　保护轮廓(Protection Profile)

SC	安全信道(Secure Channel)
SCP	智能卡平台(Smart Card Platform)
SD	安全域(Security Domain)
SE	安全单元(Secure Element)
SF	安全功能(Security Function)
SFP	安全功能策略(Security Function Policy)
SIM	用户身份模块(Subscriber Identity Module)
SSD	辅助安全域(Supplementary Security Domain)
ST	安全目标(Security Target)
TOE	评估对象(Target of Evaluation)
TSF	TOE 安全功能(TOE Security Functions)
TSP	TOE 安全策略(TOE Security)
VA	验证机构(Verification Authority)
VASD	验证机构安全域(Verification Authority Security Domain)
UICC	通用集成电路卡(Universal Integrated Circuit Card)

4 概述

无线通信技术包括蓝牙、无线局域网 802.11、红外数据传输、无线 1394、近距离通信等，其中近距离通信技术通信信道距离短，而且可以直接由 SIM 卡模块或嵌入式安全单元进行访问，是移动电子支付的一个安全方案。本标准针对基于近距离通信技术的移动电子支付进行安全约束。

本标准采用 Common Criteria(通用标准)安全认证体系，对基于近距离无线通信技术的移动电子支付的设备进行安全约束。

在移动电子支付终端上，SIM(Subscriber Identity Module，用户身份模块)卡、SAM(Secure Access Module，安全访问模块)卡或内置安全单元是安全方案的核心，负责身份鉴别、数据加解密、保密数据存储等功能。本标准对 SIM 卡、SAM 卡和内置安全单元进行了安全约束。

智能卡在移动电子支付终端上存在两种形式：一种是 UICC(Universal Integrated Circuit Card，通用集成电路)卡，即 SIM 卡或 USIM(Universal SIM，通用 SIM)卡，安装在手机的 SIM 卡槽中，除用于入网身份鉴别外，还支持移动电子支付功能；另一种是内置安全单元，嵌入移动终端的主板板卡上，用于支持移动电子支付功能。

5 评估对象(TOE)

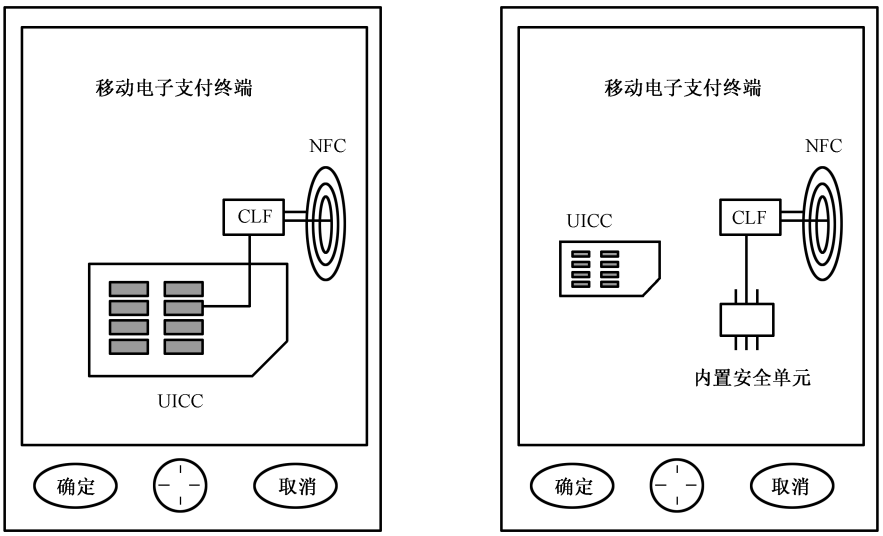
5.1 概述

本标准所述评估对象(TOE)，是指用于移动电子支付的 UICC 卡和内置安全单元。

TOE 为电子支付提供身份鉴别、系统服务、交易安全防护、关键数据管理等功能。

本标准所述 TOE 有两种形式：UICC 卡和内置安全单元。UICC 卡，即 SIM/USIM 卡，除支持移动电子支付功能外，还支持电信功能；内置安全单元仅支持移动电子支付功能，不支持电信功能。

TOE 的应用场景如图 1 所示。



UICC卡形式　　内置安全单元形式

图 1　应用场景示意图

5.2　内置安全单元

5.2.1　结构

内置安全单元的主要组件以及评估对象的范围如图 2 所示。其中，虚线框内的组件是需要认证的，而移动支付 Applet(Java Card 应用)及其他 Applet 不在本标准的认证范围内。

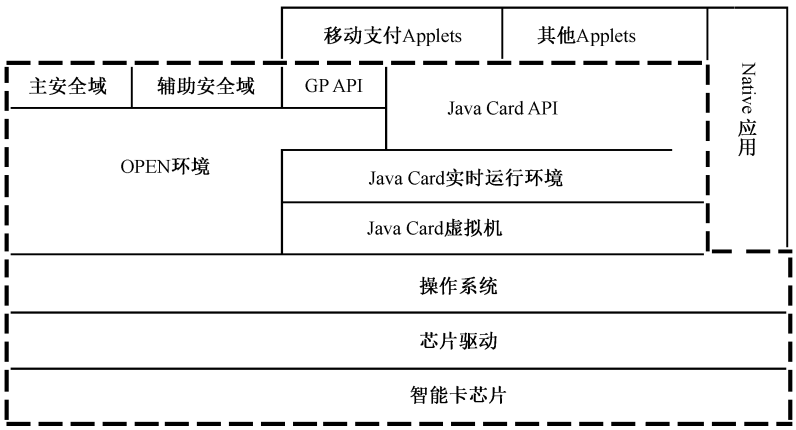


图 2　内置安全单元结构

5.2.2　功能

内置安全单元应支持如下功能：

a)　芯片驱动：根据智能卡芯片厂商安全指南，安全使用智能卡芯片各个功能模块，启动安全传感器，执行安全检查；

b)　操作系统：包括存储管理模块、通讯模块、安全算法模块；

c)　Java Card 系统：包括 Java Card 虚拟机、Java Card 实时运行环境、Java Card API(应用编程接口)；

d) GlobalPlatform 平台：包括 OPEN 运行环境、主安全域、辅助安全域、GlobalPlatform API。

5.2.3 组件

5.2.3.1 智能卡芯片

安全集成电路芯片的内部硬件组成如图 3 所示。

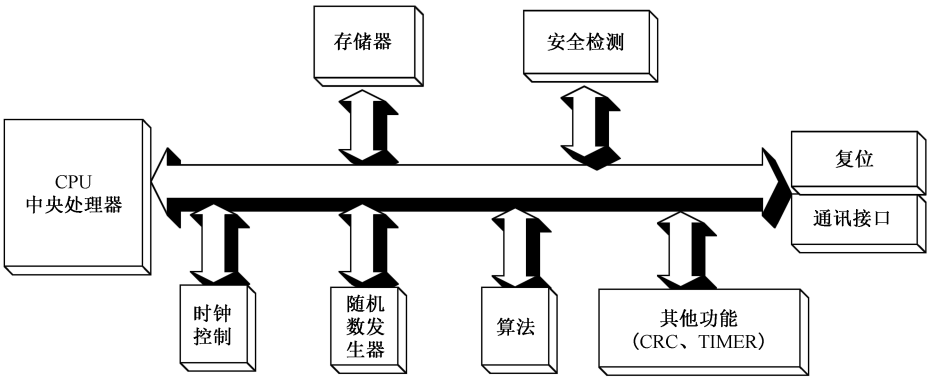


图 3 安全集成电路芯片(Secure IC Chip)结构

SE(安全单元)/UICC 集成电路是由处理单元、存储、安全组件以及 I/O(输入/输出)接口等组成的硬件设备，实现安全功能能够确保：

a) 设备处理或流动的信息的完整性和保密性；

b) 抵御各种危害存储或流动的敏感资产的外部攻击。

安全芯片也可包括其他附加功能，如非接触或者 SWP(单线协议)接口。

IC 专有的软件(或者固件)，提供便于安全芯片使用的附件功能(如密码算法库)。

芯片所具备安全功能构成的安全特征和非安全功能构成的 IT 特征。

安全功能构成的安全特征包括以下 8 个方面：

a) 安全告警——电源电压、时钟频率若超出允许范围，芯片则发出报警信号，并且不再接受任何命令直至芯片复位。芯片所执行的命令若超出权限范围，芯片则不响应此命令，并返回“指令错误”的响应。

b) 保存安全状态——若时钟频率异常，电源电压异常，芯片则应保存一个安全状态。

c) 密码运算——芯片应根据相关标准来进行密码算法。

d) 访问控制——芯片对存储器区域操作和权限的控制。

e) 信息流控制——芯片对存储器区域数据流入、流出的控制。

f) 残余信息保护——芯片对密码运算时写入密钥的保护。

g) 数据加密——芯片应确保数据在传送时不被泄露。

h) 抗物理攻击——芯片应通过测试电路的不可再利用、版图总线采用随机布线、具有屏蔽层来抵抗对其物理篡改。

非安全功能构成的 IT 特征包括以下 3 个方面：

a) 存储管理——芯片可以用于在存储器进行数据存储和调用；

b) 系统控制——包括芯片的时钟控制、低功耗控制、复位控制、IO(输入输出)控制和中断管理；

c) 通信——芯片可以与外界进行信息通信。

5.2.3.2 操作系统

操作系统是嵌入到安全芯片的软件，管理芯片提供的功能以及资源，为 Java Card 运行环境提供服务；至少要包括 I/O、RAM(易失性存储区)、ROM(掩膜存储区)、EEPROM(电可擦除存储区)、Flash(闪存)以及呈现在芯片内的任何其他硬件组件的驱动程序。

5.2.3.3 Java Card 系统

Java Card 系统是在操作系统基础上实现了 Java Card 虚拟机、Java Card 实时运行环境和 Java Card API 的上层应用。

Java Card 平台是一个启用了 Java Card 技术的智能卡平台，允许在一张智能卡上运行多个 Applet 应用程序，并提供应用安全互操作性的机制。

本标准适用于符合 Java Card 2.2.x 或者 3.0.x 经典版规范的智能卡。

Java Card 虚拟机是嵌入到智能卡的字节码解释器，Java Card 运行环境负责智能卡资源管理、通信、Applet 执行以及智能卡系统和应用的安全；智能卡可以配置能下载并安装应用，甚至在智能卡已发行到持卡人以后，这就允许智能卡发行商动态响应客户的需求，不同商家的应用可共存于一张智能卡内，它们甚至可以彼此间共享信息；

由于智能卡应用通常用于存储高度敏感的信息，信息的共享应仔细地控制，Java Card 运行环境定义的防火墙机制可以达到应用隔离的目的，每个 Applet 被阻止访问另一个 Applet 拥有的对象的字段以及方法，除非这些 Applet 提供特定的接口(即共享接口)用于这个目的。

Java Card API 为 Java Card 应用的核心功能提供类和接口，它定义了 Applet 访问 JCRE(Java Card 实时运行环境)以及 JCRE 提供的各种服务的调用约定。

5.2.3.4 GlobalPlatform 平台

GlobalPlatform 平台是在 Java Card 系统基础上实现了卡片管理器和 GlobalPlatform API 的上层软件。

GlobalPlatform 平台应符合[GP22：2011]规范，且应实现如下功能：

a) 通过安全信道对用户的鉴别；
b) Java Card 应用的下载、安装、删除以及执行时的选择操作；
c) 智能卡和应用的生命周期管理；
d) 智能卡已安装的所有应用间共享全局公共 PIN；
e) 支持基于非对称密钥的 DAP(Data Authentication Pattern，数据认证模式)校验；
f) 支持强制 DAP 权限；
g) 支持多逻辑信道；
h) 支持 SCP(Secure Channel Protocol，安全通道协议)‘02’协议；
i) 支持规范[TS102.225]规定的 SCP ‘80’协议；
j) 支持非接触应用管理；
k) 支持辅助安全域的安装、个人化和删除；
l) 实现可信路径特权管理；
m) 实现委托管理特权管理；
n) 实现规范[GP-UICC]规定的发行后安全域的个人化流程；
o) 实现规范[GP-UICC]规定的应用个人化流程。

5.3 通用集成电路卡(UICC)

5.3.1 结构

UICC 卡的主要组件以及评估对象的范围如图 4 所示。其中,虚线框内的组件是需要认证的,而移动支付 Applet、其他 Applet 及电信环境不在本标准的认证范围内。

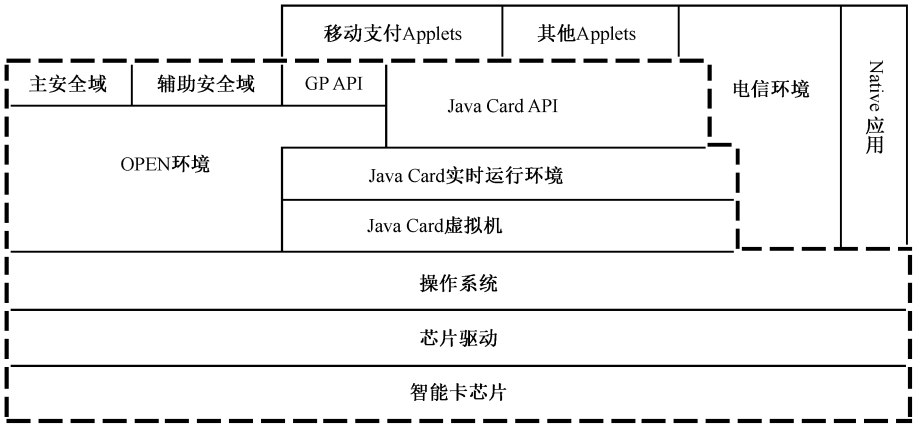


图 4 UICC 卡结构

5.3.2 功能

除内置安全单元支持的功能外,UICC 卡还应支持电信环境下的各项功能,例如 UICC API、(U)SIM API、OTA(Over The Air,空中下载)、BIP(Bearer Independent Protocol,载体独立协议,即透明传输协议)、Toolkit(工具套件)等。

5.3.3 组件

5.3.3.1 智能卡芯片

同内置安全单元中的描述。

5.3.3.2 操作系统

同内置安全单元中的描述。

5.3.3.3 Java Card 系统

同内置安全单元中的描述。

5.3.3.4 GlobalPlatform 平台

同内置安全单元中的描述。

5.4 生命周期

内置安全单元和 UICC 产品的生命周期可分为以下 7 个阶段,各个阶段内容如表 1 所示。

表 1　TOE 生命周期

阶段	活动	角色
阶段 1	智能卡芯片开发	智能卡芯片开发者 ● 设计智能卡芯片； ● 开发智能卡专用软件； ● 为嵌入式软件开发者提供智能卡芯片相关的信息，包括软件和开发工具； ● 通过可信交付和检验接收由开发者提供的智能卡嵌入式软件； ● 根据智能卡芯片设计，智能卡专用软件和/或智能卡嵌入式软件的信息，智能卡芯片设计者构造智能卡芯片数据库，以便进行智能卡芯片的制造
阶段 2	智能卡嵌入式软件开发	智能卡嵌入式软件开发者 ● 智能卡嵌入式软件开发，包括芯片驱动、操作系统、Java Card 系统、GlobalPlatform 平台等； ● 智能卡预个人化需求说明
阶段 3	智能卡芯片制造与测试	智能卡芯片制造者 ● 通过智能卡芯片制造，智能卡芯片测试，智能卡芯片预个人化 3 个主要步骤，生成智能卡芯片。 智能卡掩膜制造者 ● 基于智能卡芯片数据库，生产用于智能卡芯片制造的掩膜版
阶段 4	智能卡芯片封装与测试	智能卡芯片封装者 ● 智能卡芯片模块封装和测试
阶段 5	制卡	智能卡产品生产者 ● 智能卡产品的成卡和测试
阶段 6	智能卡个人化	个人化管理员 ● 智能卡个人化和最终测试。在个人化阶段嵌入式软件和应用软件下载到智能卡
阶段 7	智能卡使用	智能卡发行者 ● 将成品智能卡交付给最终用户，以及用户的使用和废弃

在阶段 2 设计的智能卡嵌入式软件在阶段 3 或阶段 5 期间写入集成电路。

这个技术要求仅包括智能卡经过个人化步骤后[智能卡至少要达到 INITIALIZED(初始的)生命周期状态]，智能卡使用阶段以及嵌入式软件的开发阶段，所有其他阶段的超出这个技术的范围。

开发环境应设置访问控制策略和严格执行访问控制措施，保证开发过程的可追溯行。

智能卡在发行以后，使用环境难以控制，攻击者可能会采取各种手段对智能卡进行攻击，以便获得敏感数据，因此智能卡嵌入式软件应保证系统内的信息在使用环境下的机密性和完整性。

安全芯片 IC-Chip 作为智能卡产品的硬件平台，它的生命周期包含在智能卡产品的生命周期之中，其中设计开发、制造、封装、测试等阶段，即阶段 1 和阶段 4，与 TOE 紧密相关，其他阶段则与智能卡产品的使用关系更加密切。

阶段 1，IC 的设计开发阶段。其中 IC 的设计主要流程为产品需求分析、产品架构设计、设计输入、仿真验证、综合、布局布线、时序分析、版图验证，直到最后生成版图文件。最终的版图数据的生成，不依赖于 IC 专用软件和阶段 2 中产生的 IC 嵌入软件。

阶段 2，智能卡嵌入软件的开发阶段。嵌入软件开发人员，需要根据 IC 设计开发者提供的 IC 使用

手册以及嵌入软件具体的应用需求，开发适用于 TOE 硬件平台的嵌入软件。开发过程中，可利用 IC 开发人员提供的 IC 开发工具进行软件的调试。软件开发完成后，可以在阶段 3 或者阶段 4～5，自行下载嵌入软件到 IC 芯片中，也可以委托 IC 开发方或者第三方完成下载。

阶段 3，IC 的制造和生产测试阶段。制造过程主要包括光刻掩膜板的制造、流片。光刻掩膜板根据阶段 1 提供的版图数据文件完成制造。流片主要包括以下流程：浅沟道隔离，阱注入，浮栅淀积，栅淀积，LDD 注入，介质层淀积，金属线互联，钝化层制造，完成在晶圆上制造 IC 的过程。

阶段 4，IC 的封装测试阶段。阶段 3 的晶圆经过剪薄划片之后，将芯片引脚引到外部触点并封装成模块，便于和其他部件连接。封装后须进行物理和功能测试，剔除不合格产品。

阶段 5，制卡阶段，将封装成模块的芯片，安装在符合 ISO/IEC 7816-2：2007 要求的卡基上，并按照客户要求对卡基处理，完成制卡过程。封装后须进行物理和功能测试，剔除不合格产品。

生命周期阶段 1、4 是评估 TOE 所涉及的范围，生命周期阶段 2、3、阶段 5～7，不属于本次评估的范围。

5.5 角色

内置安全单元 SE 和智能卡 UICC 内可存在几个实体的代表：

a) 移动网络运营商（MNO 或移动运营商）：SIM/USIM Java Card 的发卡商，TOE 保证发卡商一旦被鉴别，可管理应用的加载，实例化以及删除等操作。

b) 应用程序提供商（AP）：负责应用及其相关服务的实体或机构。可以是金融机构（银行），交通运营商或第三方运营商。

c) 证书认证机构（CA）：独立于 MNO，负责密钥安全地创建和应用提供者安全域（APSD）的个人化（推、拉个人化模式[GP-UICC]）。

d) 验证机构（VA），可信的第三方，代表 MNO 并负责在加载过程中验证应用的签名（强制 DAP）。

6 安全问题

6.1 资产

6.1.1 资产构成

资产由 TOE 直接保护的安全相关的信息或资源组成，可分为由用户创建并使用的用户数据以及由 TOE 创建并使用的 TOE 数据。

为保护上述资产，智能卡开发和生产阶段使用的各种信息和工具，也需要保护。

需要保护的资产包括：

a) 安全芯片存储和处理的用户数据（例如嵌入式软件所使用的数据）；

b) 安全芯片存储和处理的安全功能数据（例如安全属性、认证数据、访问控制列表、密钥等）；

c) 安全芯片嵌入式软件；

d) 安全芯片专用软件；

e) 安全芯片的逻辑设计信息，物理设计信息；

f) 特定的安全芯片开发辅助工具（例如掩膜数据生成工具）；

g) 与测试和特征有关的数据；

h) 支持嵌入式软件开发的信息（例如开发资料和开发平台）；

i) 掩膜版；

j) 初始化数据与预个人化数据；

k) 其他与特定功能有关的重要资产(例如智能卡芯片产生的随机数)。

6.1.2 用户数据

用户数据应包括以下内容:

D.APP_CODE

下载到智能卡内的 Applet 和库的代码,需要受到保护以免遭未经授权的修改。

D.APP_C_DATA

应用程序的保密性敏感的数据,如对象包含的数据,包的静态字段,当前执行方法的局部变量,操作数栈的位置,需要受到保护以免遭未经授权的暴露。

D.APP_I_DATA

应用程序的完整性敏感的数据,如对象包含的数据、包的静态字段、当前执行方法的局部变量以及操作数栈的位置等,需要受到保护以免遭未经授权的修改。

D.PIN

任何终端用户的 PIN,需要受到保护以免遭未经授权的暴露和修改。

D.APP_KEYs

Applet 拥有的密钥,需要受到保护以免遭未经授权的暴露和修改。

D.ISD_KEYS

GP 发行商安全域密钥,需要受到保护以免遭未经授权的暴露和修改。

D.APSD_KEYS

GP 应用提供商安全域密钥,用于和应用提供商建立安全信道,如果安全域有适当特权,这些密钥能用于装载以及安装应用,需要受到保护以免遭未经授权的暴露和修改。

D.CASD_KEYS

控制机构安全域密钥,需要受到保护以免遭未经授权的暴露和修改。

D.VASD_KEYS

验证机构安全域密钥,用于核对应用的 DAP 签名,需要受到保护以免遭未经授权的暴露和修改。

D.(U)SIM_DATA

(U)SIM 应用的私有数据,需要受到保护以免遭未经授权的暴露和修改。

D.(U)SIM_CODE

(U)SIM 应用代码,需要受到保护以免遭未经授权的修改。

6.1.3 系统数据

系统数据应包括以下内容:

D.CARD_MNGT_DATA

智能卡管理数据,如应用的标识符、特权、生命周期状态、存储资源的限额等,需要受到保护以免遭未经授权的修改。

D.GP_CODE

GlobalPlatform 框架的代码,需要受到保护以免遭未经授权的修改。

D.JCS_CODE

Java Card 系统的代码,需要受到保护以免遭未经授权的暴露和修改。

D.JCS_DATA

Java 虚拟机执行必要的内部运行时数据区,例如,栈帧、程序计数器、对象的类,为数据分配的长度以及任何用于链接数据结构的指针等,需要受到保护以免遭未经授权的暴露和修改。

D.SEC_DATA

Java Card 运行时安全数据，如用于标识已安装的 Apple、当前选择的 Applet，每个对象的拥有者以及执行的当前上下文的 AID，需要受到保护以免遭未经授权的暴露和修改。

D.API_DATA

应用编程接口的私有数据，象私有字段的内容，需要受到保护以免遭未经授权的暴露和修改。

D.JCS_KEYs

当下载文件到智能卡内时使用的密钥，需要受到保护以免遭未经授权的暴露和修改。

D.CRYPTO

运行时密码计算使用的密码数据，如生成密钥的种子，需要受到保护以免遭未经授权的暴露和修改。

6.2 用户与主体

用户与主体应包括以下内容：

S.APP

一个应用实例是实现智能卡提供的服务卡内实体，可通过 GP API 使用 GlobalPlatform 提供的服务。

S.OPEN

OPEN 是一个负责派发 APDU 命令道应用实例的嵌入式软件组件。

S.SD

安全域是智能卡上负责执行应用提供商安全策略的一个应用实例，可以是发行商安全域、应用提供商、控制机构(Controlling Authority)以及验证机构(ValidationAuthority)。

S.ISD

发行商安全域是智能卡上负责执行发行商安全策略的一个显著的应用实例。

根据 GlobalPlatform 规范，这个主体体现[PP-JCS]引入的下述主体的角色和责任：

a) S.INSTALLER (Applet installer)；

b) S.ADEL (Applet deletion manager)。

S.CAD

和智能卡上实体 S.SD 通信的智能卡外实体。

S.APPLET

任何 Applet 实例。

S.JCRE

Java 程序执行的运行环境。

S.JCVM

运行时执行防火墙检查的字节码解释器。

S.PACKAGE

定义用户库或者一个或多个 Applet。

6.3 假设

假设应包括以下内容：

Native 方法(A.APPLET)

假设运行环境 OE.APPLET 的安全目的被坚持，它确保没有后发行装载的 Applet 包含本地(native)代码。

字节码校验(A.VERIFICATION)

假设运行环境 OE.VERIFICATION 的安全目的被坚持,它保证所有的字节码应至少验证一次,装载之前或者安装之前或在执行前,以确保在执行时每个字节码是有效的。

本条所描述假设,覆盖以下两个方面:

a) 有关嵌入式软件开发的假设。根据 TOE 的定义,嵌入式软件开发不在 TOE 的评估范围之内。

b) 生命周期阶段 4~7,有关 TOE 安全使用和交付的假设。

智能卡芯片的安全条件影响到整个智能卡芯片系统,因此安全系统中最薄弱的环境决定了整个系统的安全性。使用智能卡芯片产品的安全系统须要考虑本节所描述的假设。

角色管理(A.Role_Man)

假设角色以一种安全的方式被管理。

智能卡芯片通常通过对口令的鉴别来确认这些角色,但对角色的管理功能不一定由智能卡芯片提供。

CAD 的通信安全(A.CAD_Sec-Com)

假设智能卡芯片与 CAD 之间的连接是安全的。

CAD 能够与智能卡芯片间建立安全通信的通道。其典型的实现方式是通过共享密钥、公/私钥对,或者利用存储的其他密钥来产生会话密钥。假设当这些安全连接建立以后,智能卡芯片就可以认为在可信通信中 CAD 是足够安全的。由于 CAD 的安全功能失败而引入的攻击超过了本标准的范围。

安全芯片之外的数据存储(A.Data_Store)

假设存储在智能卡芯片之外的智能卡芯片数据以一种安全的方式管理。

关于智能卡芯片结构、个人化数据、所有者身份等敏感信息将被发行者或其他智能卡芯片之外的数据库存储。这些信息一旦泄露,将危及智能卡芯片的安全。因此这些数据得到充分的维护是很重要的。

密钥维护(A.Key_Supp)

假设存储在智能卡芯片之外的加密密钥按照一种安全的方式进行维护。

由于使用智能卡芯片都可能引入不同的密钥,这些密钥包括共享密钥、公/私钥对等。这些密钥将由执行智能卡芯片功能的系统中能够控制操作的实体所提供。假设这些密钥的生成、分发、维护、销毁都是足够安全的。

6.4 威胁

6.4.1 安全集成电路芯片相关威胁

在智能卡芯片生命周期中,TOE 可能会受到各种各样的攻击。他们中间有些是无意识的行为,例如在交易过程中可能出现的一些误操作;有些是蓄意的,例如使用非法卡作弊、截取并篡改交易过程中所交换的信息等行为。根据各种攻击所采用的手段和攻击的对象的不同,我们考虑了以下几种威胁。

在生命周期 2~7 阶段,安全芯片大体存在以下 7 类威胁:

a) 物理威胁;

b) 逻辑威胁;

c) 与访问控制相关的威胁;

d) 与不可预测的相互作用相关的威胁;

e) 有关密码功能的威胁;

f) 监控信息的威胁;

g) 各种其他威胁。

6.4.2 物理威胁

对集成电路的物理探测(T.P_Probe)

攻击者可能对智能卡芯片实施物理探测,以获取智能卡芯片的设计信息和操作内容。

物理探测可能是利用智能卡芯片失效性分析和采用半导体逆向工程技术来从智能卡芯片中获取数据。这种探测可能包括对电气功能的探测,由于这种探测需要直接接触智能卡芯片内部,所以仍把它归为物理探测。攻击者的目的是获取诸如硬件安全机制、访问控制机制、鉴别系统、数据保护系统、存储器分区,以及密码算法程序等设计细节。弄清软件设计中诸如初始化数据、个人化数据、口令或密钥等也是他们的目标。智能卡芯片可能会在为上电或已上电状态下受到探测攻击并且在遭受这样的攻击后可能会处于无法操作状态。

对安全芯片的物理更改(T.P_Alter)

攻击者可能对智能卡芯片实施物理更改,以获取智能卡芯片的设计信息和操作内容,或者改变安全功能及安全功能数据,从而非法使用智能卡芯片。

对智能卡芯片的更改可能利用智能卡芯片失效性分析或采用半导体逆向工程技术来实现。攻击者的目的是获取诸如硬件安全机制,访问控制机制、鉴别系统、数据保护系统、存储器分区,以及密码算法程序等设计细节。弄清软件设计中诸如初始化数据、个人化数据、口令或密钥等也是他们的目标。更进一步的目标可能是修改或操纵调试阶段的锁定操作、初次使用标记、卡使用锁定、锁定功能配置、卡锁定标志、卡终止标志等,以便非法使用智能卡芯片。

环境压力(T.MALFUNCTION)

攻击者可以通过环境压力导致智能卡的安全功能或者智能卡芯片的嵌入式软件出现故障,以便:(i)失效或者修改智能卡的安全特征或者功能,(ii)失效或者修改智能卡芯片的嵌入式安全功能。

6.4.3 逻辑威胁

信息泄露(T.INF-LEAK)

攻击者可以利用智能卡使用期间泄露的信息暴露保密的安全功能数据,信息泄露可能是正常操作固有的或者是由攻击者导致的。

缺陷插入(T.Flt_Ins)

攻击者可能通过反复地插入选定的数据,并观察相应的输出结果,从而获得智能卡芯片安全功能或用户相关的信息。

这种威胁的特点是有目的选择和控制输入数据,而不是随机选择或控制。通过插入选定的数据并观察输出结果的变化,是对密码设备的一种常见攻击手段,这种手段也可用于对智能卡芯片的攻击。其目的是通过观察智能卡芯片如何对选定的输入做出响应来获取与安全功能或用户相关的信息。这种威胁的特点是有意选择和控制输入数据,而不是随机选择数据或控制输入输出操作中的物理特性。

错误输入(T.Inv_Inp)

攻击者可能通过引入无效的输入数据来危及智能卡芯片的安全功能数据的安全。

错误输入操作形式包括错误的格式、索要的信息超过记录范围、试图找到并执行无正式书面文件的命令。这样的输入可能在正常使用过程中的任意时间发生,包括访问授权前。其结果是该攻击可能会危及安全功能,在操作中产生可利用的错误或者泄露所保护的数据。

未授权程序装载(T.Ua_Load)

攻击者可能利用未授权的程序探测或修改智能卡芯片安全功能代码及数据。

每个授权角色都有特定的权限仅用于下载指定的程序。未授权程序可能包括在正常操作期间不希望执行的合法程序,也可能包括用于有意刺探或修改智能卡芯片安全功能的未授权装载程序。

6.4.4 与访问控制相关的威胁

非法访问(T.Access)

使用者或攻击者可能在未经信息或资源的拥有者或责任者许可的条件下对信息或资源进行访问。

授权角色都有特定的权限来访问智能卡芯片的信息,如果访问超出规定权限,会导致安全相关信息的暴露。

对初始使用权的欺骗(T.First_Use)

攻击者可能通过未授权使用新的或未发行的智能卡芯片而非法获得智能卡芯片信息。

6.4.5 与不可预测的相互作用相关的威胁

使用被禁止的生命周期功能(T.Lc_Ftn)

攻击者可能会利用相关命令,尤其是测试和调试命令来获取智能卡芯片安全功能数据或敏感的用户数据,这些命令在智能卡芯片生命周期的以往某些阶段是必要的,但在现阶段是被禁止的。

这些命令在操作执行的特殊阶段是不必要的或被禁止的。例如在操作阶段使用测试命令或调试命令来显示内存或执行其他功能。

6.4.6 有关密码功能的威胁

密码攻击(T.Crypt_Atk)

攻击者可能实施密码攻击或穷举攻击危及智能卡芯片的安全功能。

这种攻击可能用到一些加密函数、编码/解码函数或随机数发生器、攻击者的目标时发现密码算法中的脆弱性或通过穷举来发现密钥和输入数据。攻击者的目的在于暴露智能卡芯片的安全功能数据从而危及用户敏感数据的安全。

随机数的缺陷(T.RND)

由于被提供的随机数熵值的不足,攻击者可以预测或获取在某些情况下借助的智能卡芯片辅助工具所产生的随机数的信息。

6.4.7 监控信息的威胁

信息泄露(T.I_Leak)

智能卡芯片应提供控制和限制智能卡芯片信息泄露的方法,以免有用的信息暴露在电源、地面、时钟、复位或者 I/O 线路中。攻击者可对正常使用期间智能卡芯片泄露的信息加以利用。

智能卡芯片应被设计和编程为,例如通过分析电源消耗不能泄露处理运算或危及安全的信息。该类泄露包括功耗、I/O 特性、时钟频率的变化或所需处理时间的变化等。这可理解为一个隐蔽的传输途径,但与操作参数的测量密切相关。这些泄露信息可通过直接(接触)测量或测量辐射信号得到,并且可能与正在执行的操作有关。能量分析就是一个信息泄露的例子。

综合分析,相关性分析(T.Link)

攻击者可能观察到一个实体使用的多种资源和服务,联系这些使用,便可推导出这个实体希望保护的安全功能数据。

攻击者综合利用观察到的智能卡芯片在一段时间内多次使用的结果,或对不同操作所获取的知识进行综合,就能够得到相关信息,利用这些信息攻击者或者可以直接获取安全信息,或者可以总结出一种攻击手段,进而获取智能卡芯片要保护的安全信息。

6.4.8 各种其他威胁

环境压力(T.Env_Strs)

攻击者可通过将智能卡芯片暴露在有压力的环境下来达到项安全功能数据引入错误的目的。

将集成电路暴露在超出其使用范围的情况下,将导致其故障或安全临界元素的失败,从而达到允许操纵程序或数据的目的。这种情况可能是正常参数的极值(高或低)如温度、电压、时钟频率,也可能是不正常的环境如外部能量场。该攻击的目的在于产生一个直接的错误导致安全信息的泄露,或者是模拟中止进程来产生一个结束使用期限的失败。

接续攻击(T.Lnk_Att)

攻击者在智能卡芯片不稳定或其安全功能的某些方面下降时实施后续攻击,从而获取安全功能数据或敏感的用户数据。

克隆(T.Clon)

攻击者可能克隆部分或全部智能卡芯片的功能以开发进一步的攻击手段。

攻击者可能通过对智能卡芯片本身的详细观察来获取克隆部分或全部智能卡芯片所必需的信息。攻击者通过开发智能卡芯片的物理模型来实验其不同的功能和处理过程,从而实现进一步的攻击以达到成功暴露安全功能数据和敏感用户数据的目的。

智能卡芯片的更改和重新使用(T.Carrier_Tamper)

攻击者在原始载体上修改智能卡芯片并伪装成原始的智能卡芯片从而非法使用用户数据。

移动、修改或者重新将智能卡芯片插入到载体中伪装成原始的智能卡芯片,其目的在于访问被保护的资产。

管理者权力滥用(T.Priv)

管理者或其他特权用户可能通过执行暴露智能卡芯片安全功能或受保护数据的操作而威胁其安全特性。

一个特权用户或管理者可以实施基于上述所有威胁的攻击。

6.4.9 智能卡管理相关威胁

T.IMPERSONATE

攻击者可能会尝试冒充持卡人以获得提供给持卡人的服务,冒充持卡人意味着泄露或者猜测存储在 CVM 中的 PIN 码。

直接威胁的资产:D.PIN,D.APP_I_DATA,D.APP_C_DATA。

T.REPLAY

攻击者通过重新使用授权用户以前完成(或部分完成)的操作可以刺探智能卡的安全。

重放已完成或部分完成的操作企图绕过安全机制或暴露安全相关的信息;例如攻击者可以尝试发送他在先前会话中截获的 APDU 命令到智能卡;攻击者也可以使用以前传送到他的身份验证信息以暴露或修改存储在智能卡中被其他应用目前使用的信息;例如,攻击者可以利用曾经有效的身份验证信息,但不再有效,如旧的 PIN 值或密钥。

直接威胁的资产:D.PIN,D.ISD_KEYS,D.CASD_KEYS,D.APSD_KEYS,D.APP_C_DATA,D.APP_I_DATA,D.APP_CODE 以及 D.CARD_MNGT_DATA。

T.BRUTE-FORCE

攻击者可搜寻整个用户可访问的数据空间以便识别出平台以及应用数据。

可以重复传输(调用)APDU 命令(API 方法)以尝试暴力提取诸如密钥或 PIN 秘密。重复使用请求范围有效的命令以暴露尽可能多的数据空间,例如,攻击者可能利用不同形式的输入系统地实验;攻击可基于黑盒软件工程技术建立算法的性质和谓词。如果详尽地执行,它可方便特定应用的逆向工程,以及提取使用和安全相关的信息;攻击也可以在智能卡使用时产生错误。

直接威胁的资产:D.PIN、D.ISD_KEYS, D.CASD_KEYS, D.APSD_KEYS。

T.INVALID-INPUT

攻击者可确定安全相关的信息,通过无效输入的引入导致智能卡出现故障或其他危害安全的行为;

无效的输入可能采取未正确格式化的操作,请求超出注册限制的信息,或尝试寻找可能未公开的命令等形式;提供正常操作这种输入可在智能卡正常使用阶段的任何时候产生,包括访问授权前。攻击也可以使用无效的数据和不恰当的操作,如不在范围的请求(或格式)的命令(或功能),以其他不符合可接受的用法的方式;这种攻击的结果可以是危害安全功能、操作过程中产生可利用的错误以及受保护的数据的泄露等。

直接威胁的资产:所有资产。

T.INVALID-ORDER

攻击者通过意外的顺序激活接口提供的功能破毁内部的数据结构。

直接威胁的资产:D.CARD_MNGT_DATA,D.SEC_DATA,D.JCS_DATA

T.FORCED-RESET

攻击者通过对选择的操作的不适当的终止可能强制智能卡进入不安全的生命周期状态。

直接威胁的资产:所有资产

T.LIFE-CYCLE

攻击者访问其预期的可用性范围之外的应用,如此违反应用的不可逆的生命周期阶段(例如,攻击者重新个人化应用)。

直接威胁的资产: D.APP_I_DATA, D.APP_C_DATA, D.CARD_MNGT_DATA。

T.UNAUTHORIZED_CARD_MNGT

攻击者进行下列未经授权的智能卡管理操作(例如冒充智能卡的参与者),以便利用授予这个参与者的特权或服务取得诸如欺骗这样的好处。

a) 装载包文件;

b) 安装包文件;

c) 迁移包或 Applet;

d) 个人化 Applet 或安全域;

e) 删除包文件或者 Applet;

f) 更新 Applet 或者安全域的特权。

直接威胁的资产: D.ISD_KEYS, D.CASD_KEYS, D.APSD_KEYS, D.APP_C_DATA, D.APP_I_DATA,D.APP_CODE 以及 D.CARD_MNGT_DATA。

T.OBJ-DELETION

攻击者执行 Java Card 的垃圾回收功能,以便查找垃圾回收的缺陷,从而使得智能卡进入不安全状态。

直接威胁的资产:D.JCS_DATA。

6.4.10 运行环境相关威胁

无。

6.4.11 保密性

T.CONFID-APPLI-DATA

攻击者执行应用暴露属于另一个应用的数据。

直接威胁的资产：D.APP_C_DATA，D.PIN 以及 D.APP_KEYs。

T.CONFID-JCS-CODE

攻击者执行应用暴露 Java Card 系统的代码。

直接威胁的资产：D.JCS_CODE。

T.CONFID-JCS-DATA

攻击者执行应用暴露属于 Java Card 系统的数据。

直接威胁的资产：D.API_DATA，D.SEC_DATA，D.JCS_DATA 以及 D.CRYPTO。

6.4.12 完整性

T.INTEG-APPLI-CODE

攻击者执行应用改变自身或其他应用的代码。

直接威胁的资产：D.APP_CODE。

T.INTEG-APPLI-CODE.LOAD

当应用包被传送到智能卡安装时，攻击者修变自身或其他应用的代码。

直接威胁的资产：D.APP_CODE。

T.INTEG-APPLI-DATA

攻击者执行应用改变自身或其他应用的数据。

直接威胁的资产：D.APP_I_DATA，D.PIN 以及 D.APP_KEYs。

T.INTEG-APPLI-DATA.LOAD

当应用包被传送到智能卡安装时，攻击者修变包含在应用包中的初始化数据。

直接威胁的资产：D.APP_I_DATA 以及 D_APP_KEY。

T.INTEG-JCS-CODE

攻击者执行应用修改 Java Card 系统的代码。

直接威胁的资产：D.JCS_CODE。

T.INTEG-JCS-DATA

攻击者执行应用修改 Java Card 系统或者 API 的数据。

直接威胁的资产：D.API_DATA，D.SEC_DATA，D.JCS_DATA 以及 D.CRYPTO。

6.4.13 身份窃取

T.SID.1

一个应用冒充另一个应用甚至 Java Card 运行环境，以便非法访问智能卡或者最终用户或终端相关一些资源。

直接威胁的资产：D.SEC_DATA（其他资产可能受到损害如果这种攻击成功，例如，JCRE 的身份被窃取），D.PIN 以及 D.APP_KEYs。

T.SID.2

攻击者修改特权角色的 TOE 属性(例如,默认的 Applet 和当前选择的 Applet),它允许非法冒充这个角色。

直接威胁的资产:D.SEC_DATA(其他资产可能受到损害如果这种攻击成功,取决于那种身份被伪造)。

6.4.14 未经授权执行

T.EXE-CODE.1

应用执行未经授权的方法。

直接威胁的资产:D.APP_CODE。

T.EXE-CODE.2

应用执行任意数据或者一个方法的片段。

直接威胁的资产:D.APP_CODE。

T.NATIVE

应用执行一个绕过如防火墙等 TOE 安全功能的本地方法。

直接威胁的资产:D.JCS_DATA。

6.4.15 拒绝服务

T.RESOURCES

攻击者通过消耗智能卡资源(RAM 或者 NVRAM)阻止 Java Card 系统正确操作

直接威胁的资产:D.JCS_DATA。

6.4.16 服务

无。

6.4.17 环境相关威胁

T.LEAKAGE

攻击者可能会利用智能卡在使用过程中从 TOE 泄露出的信息以暴露机密的资产;这种攻击是非侵入的,并不要求和智能卡内部进行直接的物理接触,通过放射、功耗的变化、I / O 特性、时钟频率或处理时间要求的变化等可能会发生泄露;其中一个例子是差分能量分析攻击(DPA),另一个安全问题是利用集成电路的敏感性把 TOE 置于不安全状态。

T.FAULT

攻击者可能会通过环境压力导致 TSF 或者智能卡嵌入式软件出现故障,以便(1)停用或修改的 TOE 的安全特性或功能,或(2)取消或修改智能卡嵌入式软件的安全功能,这可能通过非正常条件下使用智能卡实现。

6.5 组织安全策略

6.5.1 安全集成电路芯片相关组织安全策略

数据访问(P.Data_Acc)

除已定义好的操作集外,对特定数据和客体的访问权限的定义依据:

a） 客体的拥有者；

b） 尝试访问客体的主体标识；

c） 客体的拥有者授予的显式或隐式的访问权限。

安全芯片可能涉及多个不同的授权者，例如智能卡芯片开发者、智能卡芯片制造者、智能卡芯片封装者。他们均能以特定的规则或角色访问智能卡芯片中的数据。

标识（P.Ident）

智能卡芯片应被唯一标识。

智能卡芯片通常包括硬件和专用软件两种元素。专用软件可能是通过硬掩膜存储在非易失存储器中。硬件具有是否使能的可选特性。一个正确的标识应是最终智能卡芯片产品的精确实例化。需要对每个智能卡芯片进行唯一标识。

密码标准（P.Crypt_Std）

密码实体、数据鉴别及批准的功能都应符合国家标准及行业或组织的信息技术安全标准或规范。

安全通信（P.Sec_Com）

智能卡芯片与智能卡接收设备间的通信使用安全的协议和程序。

智能卡芯片可能要进行从简单的状态检查到安全的数据传输等多种通信。至少，智能卡芯片应具备为可信的源建立可信信道来加载应用，或执行其他潜在的特权指令。而要一直确保完整性。

6.5.2 应用管理组织安全策略

OSP.VERIFICATION

该策略应确保用于验证的导出文件和用于安装已验证文件的导出文件之间的一致性，该策略还应确保验证机构签名和验证之间文件没有进行任何修改。

OSP. APPS-VALIDATION

应用应关联一个数字签名，在装载到 TOE 时由验证机构验证；除 Java 规范陈述的规则外，验证过程执行如下检测：

a） 不能是库；

b） 不能使用 RMI；

c） 不能使用没有认证的专用库（系统库除外）。

6.5.3 数据存储组织安全策略

OSP.OTA-SERVERS

移动运营商应使用一个安全策略确保存储在服务器上的应用的安全。

6.5.4 密钥管理组织安全策略

OSP.CASD-KEYS

智能卡个人化时 CA 的安全域密钥应安全地生成并存储到（U）SIM 卡，这些密钥在智能卡发行后不能被修改。

OSP.VASD-KEYS

智能卡个人化时 VA 的安全域密钥应安全地生成并存储到（U）SIM 卡。

6.5.5 智能卡管理组织安全策略

OSP.KEY-CHANGE

在对安全域进行任何操作前 AP 应修改初始的安全域密钥。

OSP.QUOTAS

安全域创建时须遵守内存配额。

7 安全目的

7.1 TOE 安全目的

7.1.1 安全集成电路芯片安全目的

逻辑保护(O.Log_Prot)

智能卡芯片应具有抗逻辑操纵或修改的结果,以抵抗逻辑攻击。

智能卡芯片的设计和编程应达到下述要求:能够抵抗通过对逻辑操作的攻击来威胁安全特性的企图。当智能卡芯片受到逻辑探测和命令修改的攻击时,应能保证其内部安全信息不被泄露。

防信息泄露(O.I_Leak)

智能卡芯片应提供控制和限制信息泄露的方法,使得有用信息不会通过电源、时钟、复位、I/O 线而泄露。

智能卡芯片的设计和编程应达到下述要求:攻击者无法通过分析诸如功耗等因素的变化来获取操作过程的信息或其他安全信息。

初始化(O.Init)

智能卡芯片应假定在上电、复位或其他重启操作之后必须进入指定初始状态。

无论以何种方式复位,智能卡芯片都应进入定义好的受控初始状态。此目的应能防止攻击者操纵智能卡芯片使其处于未定义的状态。

防缺陷插入(O.Flt_Ins)

智能卡芯片应能抵御插入缺陷数据重复探测的攻击。

智能卡芯片应能够防止通过分析重复探测的响应而导致的信息泄露。目标是通过检测攻击并且开始校正来抵御这种尝试。

设置顺序(O.Set_Up)

在智能卡芯片投入使用之前,应为其设置操作顺序。

智能卡芯片应在受控且经过定义的方式下操作。这是为了防止在智能卡芯片的安全保护机制被使能或保护代码被输入之前使用此智能卡芯片。

数据访问控制(O.DAC)

智能卡芯片应基于单个用户或已标识用户组,为用户提供控制和限制访问他们所拥有的或负责的对象和资源的方法。

对智能卡芯片来说,不同的使用者、管理者、发行者等都要对自己掌握的资产进行控制。这些规则表现为数据拥有者的需求,应在安全功能要求中的基于安全属性的访问控制(FDP_ACF.1)的安全功能策略中给出。

数据读取格式(O.D_Read)

数据在智能卡芯片的各个模块间传输时,应对数据格式保持一致的要求。

智能卡芯片应以某种方式保证发生在数据传输过程中的探针攻击不会发生在存储位置的探针攻击获得更多的信息。

生命周期功能(O.Life_Cycle)

智能卡芯片应提供控制或限制在某阶段使用特定命令、特殊测试和调试命令的方法。

在智能卡芯片的特定生命周期阶段有效的专有命令，在其他阶段应被禁止。因此，类似调试和识别注册信息的一次性装载在智能卡芯片的使用过程中应被禁止。

物理保护（O.Phys_Prot）

智能卡芯片应抵抗物理攻击，或能够给此类攻击获得信息制造困难。

智能卡芯片的设计和制造应达到下述要求：攻击者要综合具备复杂的装备、知识、技巧和时间才能够通过对集成电路的物理攻击获取详细设计信息、存储器内容或其他信息，以达到攻破智能卡芯片安全功能的目的。

密码（O.Crypt）

智能卡芯片应以一个安全的方式支持密码功能。

智能卡芯片使用的密码算法应符合国家及行业或组织的密码管理相关标准或规范。

防综合分析（O.Unlink）

智能卡芯片可以使用多种资源和服务，但在多种操作过程中，都不应当暴露危机其他操作安全的信息。

智能卡芯片在设计和制造时应考虑在智能卡芯片的正常操作中避免任何危机安全的信息泄露。

标识（O.Ident）

智能卡芯片应能记录并保存标识信息。

智能卡芯片包括硬件和专用软件两种元素。专用软件可能是通过硬掩膜存储在非易失存储器中。硬件具有是否使能的可选特性。一个正确的标识应是最终智能卡芯片产品的精确实例化。需要对每个智能卡芯片进行唯一标识。

信息技术标准（O.IT_Std）

智能卡芯片应遵守相关信息技术标准。

环境压力（O.Env_Strs）

智能卡芯片应具有某种结构以使其暴露在非标准（高或低）环境下时，避免泄露安全信息或以一种不安全的方式进行操作，这些影响因素包括温度、电压、时钟频率或外部能量场。

智能卡芯片设计和制造的基本要求是即使在遭受到环境压力的情况下，也能够连续地为重要信息提供安全，这些信息包括用户资产和内部安全信息。环境压力可能来自于智能卡芯片正常使用的环境也可能表示受到攻击。在受到攻击的情况下，压力可能是独立进行攻击也可能与其他攻击手段联合实施攻击。目的是在这些情况下智能卡芯片都能防止安全信息泄露。

安全通信（O.Sec_Com）

智能卡芯片和可信的 CAD 之间支持安全通信协议和程序。

智能卡芯片应提供一种机制以保证建立和维护与 CAD 之间的安全信息，完整性是应确保的。

随机数（O.RND）

智能卡芯片能够确保随机数发生器的密码质量。例如，在具有足够的熵值情况下，随机数不应该被预测出来。

在产生密码密钥之后，智能卡芯片能够确保不存在所产生随机数的相关信息被攻击者可利用。

TOE 安全目的应依赖于环境。比如，TOE 本身不传递克隆所需的信息以保证 TOE 能够满足 O.CLON 安全目的要求。应保证在 TOE 设计和生产的每一阶段，其可能用于克隆的信息都不会被泄露，而不能依赖于 TOE 自身的技术机制。同样，对于 O.DIS-MEMORY 和 O.MOD-MEMORY 的实现应依赖于软件的应用，因为 TOE 自己并不能识别出恶意的应用而中断运行或对其数据进行保密。

O.PROT-INF-LEAK

IC 须提供保护防止智能卡芯片存储和（或）处理的机密的 TSF 数据的泄露：

涵盖 TSF 数据泄露的保护措施须有：

a) 信号形状和振幅的分析和测量，或通过对电磁场中的信号、能量消耗、时钟或者 I/O 线的测量找到事件之间的时间；

b) 迫使的 TOE 故障和/或物理操纵 TOE。

O.PROT-MALFUNCTION

IC 须确保它的正确使用。

IC 应拒绝非正常条件下的使用，这种条件下可靠性和安全操作还没有被证明或测试；这是必要的，以防止导入错误；环境条件可能包括外部能源（特别是电磁）场，电压（在任何触点上），时钟频率或温度等。

O.PROT-PHYS-TAMPER

IC 须确保用户数据、TSF 数据以及智能卡芯片的嵌入式软件的保密性和完整性

这包括对高攻击的潜能的保护：

a) 测量通过电流接触，这是在芯片的表面上直接物理探测，除了在被粘结的焊盘上（使用标准的工具，用于测量电压和电流）；

b) 测量不使用电流接触，但其他类型的物理交互（使用固态物理研究和 IC 失效分析工具）；

c) 硬件和它的安全功能的操纵；

d) 可控的存储器内容操作（用户数据，TSF 数据）；

e) 这些攻击要求逆向工程理解设计、它的属性以及功能。

随机数质量（O.RND）

IC 应有助于确保随机数是不可预测的，并应具有足够的熵。

7.1.2 操作系统安全目的

断电保护（O.SCP.RECOVERY）

当有操作进行时智能卡掉电或从智能卡接收设备中拔出，智能卡平台的操作系统应允许 TOE 成功地完成中断的操作或者恢复到一致且安全的状态。

安全服务支持（O.SCP.SUPPORT）

智能卡平台应支持 TOE 的安全功能。

a) 不允许 TOE 的安全功能被旁路或修改，且不容许访问除对 API 包可用功能其他低级功能，防止 Java Card 系统对私有数据和代码的暴露和修改；

b) 向 Java Card 系统提供安全的低级密码处理功能；

c) 支持对持久化对象和类字段原子性更新，以及可能的低级事务机制；

d) 允许 Java Card 系统在持久化、易失性内存存储数据，取决于需要（如临时对象不能存储在非易失性内存），内存模型被结构化允许低级控制访问。

7.1.3 智能卡管理器安全目的

拒绝请求（O.REQUEST）

TOE 应拒绝任何包含的数据不是预期的格式的智能卡管理请求，尤其是那些按照相关功能规范不规范的 APDU 命令应不被处理，短整数、字节类型的值不在预期范围外也应当被 JC 和 GP 的 API 方法拒绝。

信息来源鉴别（O.INFO-ORIGIN）

TOE 应鉴别智能卡接收到的智能卡管理请求的来源，并向智能卡管理员鉴别自己的身份，其的目

标是确保修改智能卡安全属性的信息来至于可信的参与者，他已认真分地析了智能卡管理操作的后果，即智能卡管理员。反过来，智能卡管理员的卡上代表应证明自己身份给特权用户，以防止暴露敏感信息给一个恶意的 Applet。

应用说明：

这个目标概括了[PP-JCS]引入的 O.LOAD 和 O.INSTALL 目标，来源的验证适用于所有智能卡管理操作，而不仅仅是加载新的可执行文件。

信息完整性(O.INFO-INTEGRITY)

在智能卡使用阶段，TOE 应验证智能卡收到的智能卡管理请求的完整性，这个目标确保被智能卡处理的智能卡管理操作确是智能卡管理员的一个请求；除此之外，智能卡上已安装的每个应用也可请求 ISD 验证用于个人化它的命令的完整性，这只适用于智能卡使用阶段，这是智能卡处于一个潜在的敌对的环境中

应用注解：

这个目标概括了在[PP-JCS]引入的和 O.INFO-INTEGRITY 同样方式的 O.LOAD 和 O.INSTALL 目标。

信息保密性(O.INFO-CONFIDENTIALITY)

TOE 应能够处理包含加密数据的保密请求，其目标是防止泄露能够打开 ISD 和智能卡管理员之间的安全信道的秘密钥匙；此外，应用供应商可能想保护他们传送给智能卡的应用代码；最后，应用实例也可以要求 ISD 提供安全信道为它们自身的个人化提供保密性。

会话密钥(O.NO-KEY-REUSE)

TOE 应确保会话密钥只能使用一次，密钥用于确保智能卡管理要求的来源，完整性和保密性应包含由 TOE 随机选择的一段不可预知的数据，因此它们只能在生成它们的会话中有效。

7.1.4 智能卡内容管理安全目的

应用安装安全(O.INSTALL)

TOE 应确保安装的应用程序是安全的，为了安全在安装过程中应满足以下要求：

a) 当安装失败或取消时，不管何种原因，TOE 应能够取消所有的安装步骤；

b) 安装一个应用应不能影响已安装的 Applet 的代码和数据，尤其是新应用或可执行文件的安装不应当隐藏智能卡上已存在的任何应用或者文件，或者使它们不可访问；

c) 安装过程不应用于旁路 TSF，它应当是安全的原子操作，对其他 Applet 的状态无有害的影响，尤其是，授予应用的一组特权应和每个特权打算的含义一致，并且平台实现的 GP 配置一致。安装应用的过程应确保安装请求、授予应用特权的完整性和来源。

应用下载安全(O.LOAD)

装载和安装可执行文件的过程应确保该文件的完整性和真实性，TOE 须检查每个可执行文件实际来自智能卡管理员，他已事先检查它对智能卡上已安装的其他应用无害，为进一步的安全性，智能卡应检查负责执行检查的验证机构的 DAP 签名，这个签名被附加可执行的装载文件。

应用删除安全(O.DELETION)

TOE 应确保应用和可执行文件的删除时安全的，删除机制应考虑以下问题：

a) 删除已安装的 Applet(可执行文件)不得引入对垃圾收集的代码或数据的无效引用的形式的安全漏洞，也不改变剩余的 Applet 的完整性或者保密性。删除过程不得被恶意利用以绕过 TSF。

b) 擦除，如果认为是成功的，应确保由 Applet 拥有的任何数据不在可访问(共享对象应防止删除或无法被访问)；一个被删除的 Applet 不能被选择或接收 APDU 命令，一个可执行文件的删除使其代码不在可执行。

c) 实现应考虑到处理过程出现电源故障或其他故障时应维持的 TSP。这并没有强制整个过程是原子性的，而是它可以切成小和原子的删除步骤，比如，一个中断的删除可能导致用户数据的丢失，只要它不违反 TSP。

d) 不得将删除 Java Card 和 GP API 对应的可执行文件。

应用说明：

对于存贮在 ROM 中的这些可执行文件逻辑删除是可接受的，而存储在 EEPROM 的已删除的可执行文件应从智能卡上物理删除。

7.1.5 运行环境安全目的

无。

7.1.6 标识

O.SID

TOE 应在授予主体访问任何服务前，唯一地标识每个主体(Applet 或者包)。

7.1.7 Applets 执行

本条关注的安全目的是 Applet 实例的代码被执行的方式。

O.FIREWALL

TOE 应确保不同包的 Applet 或 JCRE 拥有的数据容器的受控共享以及在 Applet 和 TSF 之间的受控共享。

O.GLOBAL_ARRAYS_CONFID

TOE 应确保当 Applet 选择时，被所有应用共享的 APDU 缓冲区的内容总是被清除

TOE 应确保当用于选择的 Applet 的 install 方法的调用的全局字节数组的内容总是被清除，当从 install 方法返回时。

O.GLOBAL_ARRAYS_INTEG

TOE 应确保当只有当前选择的应用可以写访问 APDU 缓冲区以及用于被选择 Applet 的 install 方法调用的全局字节数组。

O.NATIVE

Java Card 虚拟机提供给应用执行本地代码的唯一方法是调用 Java Card API 或者任何附加 API 的方法。

O.OPERATE

TOE 须确保安全功能连续正确运行。

O.REALLOCATION

TOE 应确保为 Java Card 虚拟机运行区再分配的内存块没有暴露任何以前在这块内存存储的信息。

O.RESOURCES

TOE 应控制用于应用的资源的可用性。

7.1.8 提供给 Applet 的服务

本条关注的安全目的是运行时环境通过 Java Card API 提供给 Applet 实例的服务。

O.ALARM

TOE 应提供适当的反馈信息，一旦检测到潜在的安全违反。

O.CIPHER

TOE 应为应用提供方法以安全方式加密敏感的数据，尤其是 TOE 须支持符合密码使用处理和标准的算法。

O.KEY-MNGT

TOE 应提供安全管理密钥的方法，这涉及密钥的正确生成、分发、访问以及销毁等操作。

O.PIN-MNGT

TOE 应提供方法安全滴管理 PIN 对象。

应用说明：

PIN 对象在客户应用的安全结构中可能起关键的作用，它们在智能卡中存储和管理的方式应仔细考虑，适用于整个对象，不仅是 PIN 的值，例如，重试计数器的值和 PIN 的值同样敏感。

O.TRANSACTION

TOE 须提供原子性地执行一组操作的方法。

应用说明：

O.KEY-MNGT、O.PIN-MNGT、O.TRANSACTION 以及 O.CIPHER 实际上以 Java Card API 的方式提供给 Applet 使用。

7.1.9 对象删除

O.OBJ-DELETION

TOE 应确保对象的删除应不破坏对对象的引用。

7.2 环境安全目的

7.2.1 安全集成电路芯片环境安全目的

数据存储(OE.Data_Store)

根据用户的不同需求保证在智能卡芯片以外的数据存储的机密性和完整性。

智能卡芯片的不同信息可能存储在智能卡芯片之外，这些信息包括拥有者或用户信息、个人化数据等。管理这些信息的人员和系统有责任维护信息的安全性。

人员(OE.Perss)

作为管理者或其他拥有特定权限的人员应当经过精心挑选，是值得信任的并严格培训为可靠的。

经过精心挑选并严格培训的管理者和其他拥有特定全县的人员负责监测、防范或抵御各种攻击。

CAD 安全操作(OE.CAD_Sec-Opp)

可信的 CAD 为操作提供安全的环境。CAD 应该能够与智能卡芯片间的操作提供一个安全的环境。

密钥支持(OE.Key_Supp)

所有进口的智能卡芯片应根据用户需求生成相关秘钥。

由于智能卡芯片的使用而引入不同的密钥，包括共享密钥、公/私钥对等。这种密钥将由执行智能卡芯片功能的系统中能够控制操作的实体所提供。要求负责这些密钥的产生、分发、维护、销毁的人和系统都是安全的。

篡改标记(OE.Tamper)

如果智能卡芯片被移出或重新插入,那么智能卡芯片的载体应该有篡改标记。

负责检查智能卡芯片载体的人有责任通过载体观测是否被篡改。当载体呈现在这些人面前且其物理上式可检查的情况下可以达到该目的。

CAD 安全通信(OE.CAD_Sec-Com)

可信的 CAD 用于与智能卡芯片间的安全通信。CAD 应能够接收并维护与智能卡芯片间的安全通信。

7.2.2 应用管理安全目的

后下载 Applet 不包含 Native 方法(OE.APPLET)

发行后装载的 Applet 应不包含本地(native)代码。

字节码校验(OE.VERIFICATION)

依至智能卡的能力,所有的字节码应在装载前、安装前或执行前至少验证一次,以确保每条字节码在执行时是有效的。

OE. APPS-VALIDATION

验证过程须对应用进行分析,确保坚持 TOE 正确使用的规则。

7.2.3 数据存储安全目的

服务器应用安全(OE.OTA-SERVERS)

移动运营商应使用一个安全策略确保存储在服务器上的应用的安全。

7.2.4 密钥管理安全目的

OE.SECRETS

攻击者应不能从 TOE IT 或 non-IT 环境得到存储在内的用于生成 DAP 签名的私钥、任何 PIN 和机密密钥。

OE.CA-KEYS

存储到智能卡前 CA 的安全域密钥应安全地生成。

OE.VA-KEYS

并存储到智能卡前 VA 的安全域密钥应安全地生成。

OE.KEY-LENGTH

验证机构应仅验证这些 Applet,它们遵守了本标准安全功能要求提供的关于密钥长度的限制。

7.2.5 智能卡管理安全目的

OE.KEY-CHANGE

在对安全域进行任何操作前 AP 应修改初始的安全域密钥。

OE.QUOTAS

安全域创建时须遵守内存配额。

7.3 安全目的对应关系

安全目的能应对所有可能的威胁、假设和组织安全策略,即每一种威胁、假设和组织安全策略都至少有一个或以上安全目的与其对应,因此是完备的。没有一个安全目的没有相应的威胁、假设和组织安全策略与之对应,这证明每个安全目的都是必要的;没有多余的安全目的不对应威胁、假设和组织安全策略。因此说明了安全目的是充分的。威胁和安全目的的对应关系如表 2,威胁、假设、组织安全策略

与运行环境安全目的的对应关系如表 3。

表 2　威胁和安全目的的对应关系

威胁	安全目的																									
	O.REQUEST	O.INFO-ORIGIN	O.INFO-INTEGRITY	O.INFO-CONFIDENTIALITY	O.INSTALL	O.LOAD	O.DELETION	O.SID	O.FIREWALL	O.GLOBAL_ARRAYS_CONFID	O.GLOBAL_ARRAYS_INTEG	O.NATIVE	O.OPERATE	O.REALLOCATION	O.RESOURCES	O.ALARM	O.CIPHER	O.KEY-MNGT	O.PIN-MNGT	O.TRANSACTION	O.OBJ-DELETION	O.SCP.RECOVERY	O.SCP.SUPPORT	O.PROT-INF-LEAK	O.PROT-PHYS-TAMPER	O.PROT-MALFUNCTION	O.RND
T.IMPERSONATE		√																	√								
T.REPLAY			√																								
T.BRUTE-FORCE		√																									
T.INVALID-INPUT	√																										
T.INVALID-ORDER			√																								
T.FORCED-RESET					√	√	√																				√
T.LIFE-CYCLE																											
T.UNAUTHORIZED_CARD_MNGT	√	√	√	√	√	√	√											√	√	√							
T.INTEG-APPLI-DATA	√	√	√	√				√	√		√		√	√		√	√	√	√	√		√	√				
T.CONFID-APPLI-DATA	√	√	√	√				√	√	√			√	√		√	√	√	√	√		√	√				
T.INTEG-APPLI-DATA.LOAD	√	√	√	√		√																					
T.INTEG-JCS-DATA	√	√	√	√				√	√				√			√						√	√				
T.CONFID-JCS-DATA	√	√	√	√				√	√				√			√						√	√				
T.INTEG-APPLI-CODE	√	√	√	√				√	√			√	√														
T.INTEG-APPLI-CODE.LOAD	√	√	√	√		√		√	√				√														
T.INTEG-JCS-CODE	√	√	√	√								√															
T.CONFID-JCS-CODE	√	√	√	√				√	√				√														
T.SID.1	√	√	√	√	√			√	√	√	√																
T.SID.2					√			√	√				√									√	√				
T.RESOURCES					√								√		√							√	√				
T.OBJ-DELETION																					√						
T.RND																											√
T.P_Alter																									√		
T.MALFUNCTION																										√	
T.INF-LEAK																								√			

表 3　威胁、假设、组织安全策略与安全目的的对应关系

威胁 假设 组织安全策略	运行环境安全目的										
	OE.APPLET	O.NATIVE	OE.VERIFICATION	OE.APPS-VALIDATION	OE.SECRETS	OE.KEY-LENGTH	OE.CA-KEYS	OE.VA-KEYS	OE.OTA-SERVERS	OE.KEY-CHANGE	OE.QUOTAS
T.INTEG-APPLI-DATA			√								
T.CONFID-APPLI-DATA			√								
T.INTEG-APPLI-DATA.LOAD			√								
T.INTEG-JCS-DATA			√								
T.CONFID-JCS-DATA			√								
T.INTEG-APPLI-CODE			√								
T.INTEG-APPLI-CODE.LOAD			√								
T.INTEG-JCS-CODE			√								
T.CONFID-JCS-CODE			√								
T.EXE-CODE.1			√								
T.EXE-CODE.2			√								
T.NATIVE	√	√	√								
A.APPLET	√										
A.VERIFICATION			√								
OSP.VERIFICATION			√								
OSP. APPS-VALIDATION				√							
OSP.OTA-SERVERS									√		
OSP.CASD-KEYS					√		√				
OSP.VASD-KEYS					√			√			
OSP.KEY-CHANGE										√	
OSP.QUOTAS											√

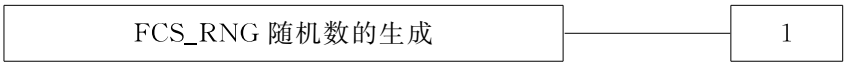
8　扩展组件定义

8.1　FCS_RNG 族定义

族行为：

本族定义了生成随机数的质量要求，其目的是要用于加密操作。

组件层次：



FCS_RNG.1

随机数的生成要求随机数符合规定的质量指标。

管理：FCS_RNG.1

尚无预见的管理活动。

审计：FCS_RNG.1

没有定义的可审计行为。

8.2 FCS_RNG.1 随机数的质量指标

从属于：无其他组件。

依赖关系：无依赖关系。

FCS_RNG.1.1 TSF 应提供一个[选择：物理、非物理真实的、确定性的、混合的]随机数生成器来实现：[分配：安全能力列表]。

FCS_RNG.1.2 TSF 应提供随机数满足[分配：定义的质量度量]。

应用说明：

物理随机数发生器(RNG)通过基于物理随机过程的噪声源产生随机数；非物理的真随机数使用基于非物理的随机过程，如人机交互(击键，鼠标移动)的噪声源；确定性的 RNG 使用随机种子产生的伪随机输出；混合 RNG 组合物理和确定性的随机数的原理生成随机数。

9 安全功能要求

9.1 概述

本标准的安全功能要求须在 TOE 中给予实现。

表 4 是本标准要求的所有安全功能的汇总表。具体运用中，要对表中每一项安全功能要求进行落实。如果安全功能要求描述中有“[赋值...]”标识的，在实际产品安全说明中须选择其中列出的一项。

表 4 安全功能要求组件

类/组件	名称	依赖性
FAU 类：安全审计		
FAU_ARP.1	安全告警	(FAU_SAA.1)
FAU_ARP.1/IC		
FAU_SAA.1/IC	潜在侵害分析	
FCO 类：通信		
FCO_NRO.2/SC	原发抗抵赖	(FIA_UID.1)
FCS 类：密码支持		
FCS_CKM.1/APP-RSA FCS_CKM.1/APP-EC FCS_CKM.1/APP-DH	密钥生成	(FCS_CKM.2 或 FCS_COP.1) 与 (FCS_CKM.4)
FCS_CKM.3/SC-KL	密钥访问	(FDP_ITC.1 或 FDP_ITC.2 或 FCS_CKM.1) 与 (FCS_CKM.4)

表 4（续）

类/组件	名称	依赖性
FCS_COP.1/APP-RSA FCS_COP.1/DAP FCS_COP.1/IC FCS_COP.1/SC_02 FCS_COP.1/SC_02-CBC FCS_COP.1/SC_02-ECB FCS_COP.1/SC_02-FINAL FCS_COP.1/SC_02-ICV	密码运算	（FDP_ITC.1 或 FDP_ITC.2 或 FCS_CKM.1）与（FCS_CKM.4）
FCS_COP.1/IC		
FCS_RND.1/APP	随机数的质量度量	无
FDP 类：用户数据保护		
FDP_ACC.1/SD	子集访问控制	（FDP_ACF.1）
FDP_ACC.1/IC		
FDP_ACC.2/FIREWALL FDP_ACC.2/ADEL	完全访问控制	（FDP_ACF.1）
FDP_ACF.1/SD FDP_ACF.1/FIREWALL FDP_ACF.1/ADEL	基于安全属性的访问控制	（FDP_ACC.1）与（FMT_MSA.3）
FDP_ACF.1/IC		
FDP_ETC.1/IC	不带安全属性的用户数据输入	
FDP_IFC.1/JCVM FDP_IFC.1/IC	子集信息流控制	（FDP_IFF.1）
FDP_IFC.2/SC	完全信息流控制	（FDP_IFF.1）
FDP_IFF.1/JCVM FDP_IFF.1/SC	简单安全属性	（FDP_IFC.1）与（FMT_MSA.3）
FDP_IFF.1/IC	简单安全属性	
FDP_ITC.1/SC-KL	不带安全属性的用户数据输入	（FDP_ACC.1 或 FDP_IFC.1）与（FCS_MSA.3）
FDP_ITC.1/IC		
FDP_ITC.2/Installer	带有安全属性的用户数据输入	（FDP_ACC.1 或 FDP_IFC.1）与（FTP_ITC.1 或 FTP_TRP.1）与（FPT_TDC.1）
FDP_ITT.1/IC	基本内部传送保护	（FDP_ACC.1 或 FDP_IFC.1）
FDP_RIP.1	子集残余信息保护	
FDP_RIP.1/IC		
FDP_ROL.1/CCM FDP_ROL.1/FIREWALL	基本回退	（FDP_ACC.1 或 FDP_IFC.1）

表 4（续）

类/组件	名称	依赖性
FDP_SDI.2	存储数据的完整性监视和反应	无
FDP_UIT.1/CCM	数据交换的完整性	（FDP_ACC.1 或 FDP_IFC.1）与 （FTP_ITC.1 或 FTP_TRP.1）
FIA 类：标识和识别		
FIA_AFL.1/CVM FIA_AFL.1/KEYS FIA_AFL.1/SC	鉴别失败处理	（FIA_UAU.1）
FIA_ATD.1/AID	用户属性定义	无
FIA_ATD.1/IC		
FIA_UAU.4/SC	一次性鉴别机制	无
FIA_UAU.1/IC	鉴别定时	
FIA_UID.2/AID	任何动作前的用户标识	无
FIA_UID.1/IC	标识定时	
FIA_USB.1/AID	用户主体绑定	（FIA_ATD.1）
FMT 类：安全管理		
FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_MSA.1/ADEL FMT_MSA.1/SD	安全属性管理	（FDP_ACC.1 或 FDP_IFC.1）与 （FMT_SMR.1）与（FMT_SMF.1）
FMT_MSA.1/IC		
FMT_MOF.1/IC	安全功能行为的管理	
FMT_MSA.2/FIREWALL_JCVM FMT_MSA.2/SC-KEYS	安全的安全属性	（FDP_ACC.1 或 FDP_IFC.1）与 （FMT_MSA.1）与（FMT_SMR.1）
FMT_MSA.2/IC		
FMT_MSA.3/SD FMT_MSA.3/SC FMT_MSA.3/JCVM FMT_MSA.3/ FIREWALL FMT_MSA.3/ADEL	静态属性初始化	（FMT_MSA.1）与（FMT_SMR.1）
FMT_MSA.3/IC		
FMT_MTD.1/JCRE	TSF 数据的管理	（FMT_SMR.1）与（FMT_SMF.1）
FMT_MTD.3/JCRE	安全的 TSF 数据	（FMT_MTD.1）
FMT_SMF.1 FMT_SMF.1/FIREWALL FMT_SMF.1/ISD FMT_SMF.1/SD FMT_SMF.1/SC	管理功能规范	无

表 4（续）

类/组件	名称	依赖性
FMT_SMR.1/ISD FMT_SMR.1/CA FMT_SMR.1/SD FMT_SMR.1/JCRE FMT_SMR.1/PRV FMT_SMR.1/ADEL FMT_SMR.1/Installer	安全角色	（FIA_UID.1）
FPR 类：私密性		
FPR_UNO.1	不可观察性	无
FPT 类：安全功能保护		
FPT_FLS.1 FPT_FLS.1/Installer FPT_FLS.1/ADEL FPT_FLS.1/ODEL FPT_FLS.1/IC	带保存安全状态的失败	无
FPT_ITT.1/IC	内部安全功能数据传送的基本功能	无
FPT_PHP.3/IC	物理攻击抵抗	无
FPT_RCV.3/Installer FPT_RCV.3/ SCP	无过度损失的自动恢复	（AGD_OPE.1）
FPT_RCV.4/ SCP	功能恢复	无
FPT_RCV.4/IC		
FPT_RVM.1/IC	安全策略的不可旁路性	
FPT_TDC.1 FPT_TDC.1/SC-KL	TSF 间基本 TSF 数据一致性	无
FPT_SEP.1/IC	安全功能域的隔离	
FPT_FLT.2/IC	受限容错	
FTP 类：可信信道		
FTP_ITC.1/SC	传送过程中 TSF 间的保密性	无
FRU 类：资源利用		
FRU_FLT.2/IC	受限容错	（FRU_FLT.1）

9.2 安全芯片 IC-Chip 安全功能要求

9.2.1 概述

以下列出了 THC20 系列芯片依据的信息技术安全功能组件开发的安全功能要求，并给出了详细

的说明。这部分包括标准的安全功能要求和扩展的安全功能要求。

9.2.2 基本安全功能要求

9.2.2.1 概述

表 5 是本标准要求的芯片相关的所有安全功能的汇总表。

表 5 芯片安全功能要求组件

安全功能组件	组件名称
FAU_ARP.1	安全告警
FAU_SAA.1	潜在侵害分析
FCS_COP.1	密码运算
FDP_ACC.1	子集访问控制
FDP_ACF.1	基于安全属性的访问控制
FDP_ETC.1	不带安全属性的用户数据输出
FDP_IFC.1	子集信息流控制
FDP_IFF.1	简单安全属性
FDP_ITC.1	不带安全属性的用户数据输入
FDP_ITT.1	基本内部传送保护
FDP_RIP.1	子集残余信息保护
FIA_ATD.1	用户属性定义
FIA_UAU.1	鉴别定时
FIA_UID.1	标识定时
FMT_MOF.1	安全功能行为的管理
FMT_MSA.1	安全属性的管理
FMT_MSA.2	安全的安全属性
FMT_MSA.3	静态属性初始化
FPT_FLS.1	带保存安全状态的失败
FPT_ITT.1	内部安全功能数据传送的基本保护
FPT_PHP.3	物理攻击抵抗
FPT_RCV.4	功能恢复
FPT_RVM.1	安全策略的不可旁路性
FPT_SEP.1	安全功能域的隔离
FPT_FLT.2	受限容错

9.2.2.2 FAU_ARP.1 安全告警

FAU_ARP.1.1 当检测到潜在的安全侵害时，智能卡芯片安全功能将进行[赋值：最小扰乱行动表]。

9.2.2.3 FAU_SAA.1 潜在侵害分析

FAU_SAA.1.1 智能卡芯片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智能卡芯片安全策略的潜在侵害。

FAU_SAA.1.2 智能卡芯片安全功能用下列规则来监控审计事件：

a) 已知的用来指示潜在安全侵害的[赋值：已定义的可审计事件子集]的积累或组合；

b) [赋值：任何其他规则]。

9.2.2.4 FCS_COP.1 密码运算

FCS_COP.1.1 智能卡芯片安全功能将根据符合[赋值：标准列表]的密码算法[赋值：密码算法]和密钥长度[赋值：密钥长度]来执行[赋值：密码运算列表]。

9.2.2.5 FDP_ACC.1 子集访问控制

FDP_ACC.1.1 智能卡芯片安全功能应对[赋值：安全功能策略覆盖的主体列表、客体列表及其他之间的操作列表]执行[赋值：智能卡芯片访问控制安全功能策略]。

9.2.2.6 FDP_ACF.1 基于安全属性的访问控制

FDP_ACF.1.1 智能卡芯片安全功能应基于[赋值：安全属性命名的安全属性组]对客体执行[赋值：智能卡芯片访问控制安全功能策略]。

FDP_ACF.1.2 智能卡芯片安全功能应执行[赋值：在受控主体和受控客体中，通过对受控客体采取受控操作来管理访问的规则]，以决定受控主体与受控客体间的操作是否被允许。

FDP_ACF.1.3 智能卡芯片安全功能应基于[赋值：安全属性的授权主体访问客体的规则]授权主体访问客体。

FDP_ACF.1.4 智能卡芯片应基于[赋值：安全属性明确拒绝主体访问客体的规则]明确拒绝主体对客体的访问。

9.2.2.7 FDP_ETC.1 不带安全属性的用户数据输出

FDP_ETC.1.1 智能卡芯片安全功能在安全功能策略控制下，输出用户数据到 IC 卡芯片安全控制范围之外时，应执行[选择：IC 卡芯片访问控制策略，IC 卡芯片信息流控制策略]。

FDP_ETC.1.2 智能卡芯片安全功能应输出未关联安全属性的用户数据。

9.2.2.8 FDP_IFC.1 子集信息流控制

FDP_IFC.1.1 智能卡芯片安全功能应对包含在安全功能策略中的[赋值：主体列表、信息列表和导致受控信息流入流出受控主体的操作]执行[赋值：智能卡芯片信息流控制策略]。

应用说明：

用户数据和 TSF 数据不应当从 IC 可访问，除非当嵌入式软件决定通过一个外部接口传送用户数据，保护应当仅适用保密数据但并不区分嵌入式软件控制的属性。

9.2.2.9 FDP_IFF.1 简单安全属性

FDP_IFF.1.1 智能卡芯片安全功能应在安全属性[赋值：安全属性的最小数目和类型的基础上执行赋值：智能卡芯片信息流控制策略]。

FDP_IFF.1.2 如果有下面的规则[赋值：对每一个操作，在主体和信息安全属性间应有基于安全属性的关系]，智能卡芯片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。

FDP_IFF.1.3 智能卡芯片安全功能应执行[赋值:附加的信息流控制策略]。

FDP_IFF.1.4 智能卡芯片安全功能应提供[赋值:附加的安全功能策略能力列表]。

FDP_IFF.1.5 智能卡芯片安全功能应根据[赋值:基于安全属性,明确授权信息流的规则]明确授权信息流。

FDP_IFF.1.6 智能卡芯片安全功能应根据[赋值:基于安全属性,明确拒绝信息流的规则]明确拒绝信息流。

9.2.2.10 FDP_ITC.1 不带安全属性的用户数据输入

FDP_ITC.1.1 智能卡芯片安全功能在安全功能策略控制下,从智能卡芯片安全控制范围之外输入用户数据时,应执行[赋值:智能卡芯片访问控制策略,智能卡芯片信息流控制策略]。

FDP_ITC.1.2 智能卡芯片安全功能应略去任何与智能卡芯片安全控制范围之外输入的数据相关的安全属性。

FDP_ITC.1.3 智能卡芯片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[赋值:附加的输入控制规则]。

9.2.2.11 FDP_ITT.1 基本内部传送保护

FDP_ITT.1.1 在智能卡芯片的物理上分隔的部分间传递用户数据时,智能卡芯片安全功能应执行[选择:智能卡芯片访问控制策略,智能卡芯片信息流控制策略],以防止泄露、篡改或丢失。

应用说明:

不同存储、CPU 和 TOE 的其他功能单元(密码协处理器)被看成是 TOE 的物理分隔部分。

9.2.2.12 FDP_RIP.1 子集残余信息保护

FDP_RIP.1.1 智能芯片安全功能对下列客体[赋值:客体列表][选择:分配,释放资源]时,应确保资源中任何以前的信息内容不再可用。

9.2.2.13 FIA_ATD.1 用户属性定义

FIA_ATD.1.1 智能卡芯片安全功能应为每个用户保存[赋值:安全属性列表]。

9.2.2.14 FIA_UAU.1 鉴别定时

FIA_UAU.1.1 在用户被鉴别之前,智能卡芯片安全功能应允许智能卡芯片代表用户的[赋值:智能卡芯片安全功能促成的行动列表]被执行。

FIA_UAU.1.2 在允许任何其他代表用户的智能卡芯片安全功能促成的行动执行前,智能卡芯片安全功能应要求该用户已被成功鉴别。

9.2.2.15 FIA_UID.1 标识定时

FIA_UID.1.1 在用户被标识之前,智能卡芯片安全功能应允许智能卡芯片代表用户的[赋值:智能卡芯片安全功能促成的行动列表]被执行。

FIA_UID.1.2 在允许任何其他代表用户的智能卡芯片安全功能促成的行动执行前,智能卡芯片安全功能应要求该用户已被成功标识。

9.2.2.16 FMT_MOF.1 安全功能行为的管理

FMT_MOF.1.1 智能卡芯片安全功能应仅限于[赋值:已识别授权角色]对功能[赋值:功能列表]具有

[选择：确定其行为，禁止，允许，修改其行为]的能力：

a) 管理数据访问级别，该级别一旦确定，不能变更；
b) 在安全告警事件中要执行行为的管理；
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) 改变密钥属性行为的管理，密钥属性包括密钥类型，比如公钥、私钥、有效期和用途，比如数字签名、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) 授权管理员如果能改变用户被识别之前所能采取的行为列表，应对授权管理员的此种行为进行管理；
h) 对撤销规则的管理；
i) 对重放中所采取行为的管理；
j) 智能卡芯片自检发生[选择：初始化启动、定期间隔、其他特定条件]时的条件的管理；
k) ST 中附件[赋值：安全功能列表的管理]。

9.2.2.17 FMT_MSA.1 安全属性的管理

FMT_MSA.1.1 智能卡芯片安全功能应执行[赋值：智能卡芯片访问控制策略和智能卡芯片信息流控制策略]，仅限于[赋值：已识别了的授权角色]对安全属性进行[选择：改变默认值、查询、修改、删除][赋值：其他操作]。

9.2.2.18 FMT_MSA.2 安全的安全属性

FMT_MSA.2.1 智能卡芯片安全功能应确保安全属性只接受安全的值。

9.2.2.19 FMT_MSA.3 静态属性初始化

FMT_MSA.3.1 智能卡芯片安全功能应执行[赋值：智能卡芯片访问控制策略和智能卡信息流控制策略]，以便为用于执行安全功能策略的安全属性提供[选择：受限的，许可的，其他特性]默认值。

FMT_MSA.3.2 智能卡芯片安全功能应允许[赋值：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。

9.2.2.20 FPT_FLS.1 带保存安全状态的失败

FPT_FLS.1.1 智能卡芯片安全功能在失败[赋值：安全功能的失败类型列表]发生时应保存一个安全状态。

9.2.2.21 FPT_ITT.1 内部安全功能数据传送的基本保护

FDP_ITT.1.1 智能卡芯片安全功能应保护智能卡芯片安全功能数据在智能卡芯片的分离部分传送时不被[选择：泄露、篡改，丢失]。

应用说明：

不同存储、CPU 和 TOE 的其他功能单元(密码协处理器)被看成是 TOE 的物理分隔部分。

9.2.2.22 FPT_PHP.3 物理攻击抵抗

FPT_PHP3.1 智能卡芯片安全功能应通过自动应答来抵抗对[赋值：智能卡芯片安全功能设备/元件列表]的[赋值：各种物理篡改]，以遵从智能卡芯片安全策略。

应用说明：

智能卡芯片应实现适当的措施连续地应对物理操控和物理探测，由于这些攻击（尤其是操控）的性质，智能卡芯片可能无法检测对其所有组件的攻击；因而，对这些攻击的持久保护被要求确保 TSP 任何时候都不被违反；这儿的“自动响应”意味：(i)假设任何时候可能有一个攻击，(ii)任何时候对策被提供。

9.2.2.23 FPT_RCV.4 功能恢复

FPT_RCV.4.1 智能卡芯片应确保[赋值：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。

9.2.2.24 FPT_RVM.1 安全策略的不可旁路性

FPT_RVM.1.1 智能卡芯片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。

9.2.2.25 FPT_SEP.1 安全功能域的隔离

FPT_SEP.1.1 在智能卡芯片安全功能执行时，应维持一个安全域，防止不可信主体的干扰和篡改。

FPT_SEP.2.1 智能卡芯片安全功能应在安全控制范围内分离各主体的安全域。

9.2.2.26 FRU_FLT.2 受限容错

FRU_FLT.2.1 智能卡芯片安全功能应能确保当[赋值：故障类型列表发生]时，所有智能卡芯片能力均能运行。

9.2.2.27 FRU_FLT.1 降级容错

FRU_FLT.1.1 TSF 应确保当以下失效：[赋值：失效类型类表]发生时，[赋值：TOE 能力列表]能正常发挥。

应用说明：

这个要求应当被用于指定 SCP 的支持 Java Card 系统/智能卡管理器能力列表，在提到失效（EEPROM 不可使用、EEPROM 缺少、随机数发生器失效等）发生时仍然能运转，一旦失效发生最小的功能允许复位/沉默/阻塞智能卡。

9.2.2.28 FRU_FLT.2 受限容错

FRU_FLT.2.1 TSF 应确保当以下失效：暴露到 FPT_FLS.1 要求没有被检测出的条件发生时，所有 TOE 能力均能正常发挥。

9.2.3 扩展安全功能要求

9.2.3.1 概述

表 6 是本标准要求的扩展安全功能的汇总表。

表 6 扩展的安全功能要求组件

安全功能组件	组件名称
FAU_SAS.1	审计存储
FCS_RNG.1	随机数生成

9.2.3.2 FAU_SAS.1 审计存储

FAU_SAS.1.1 智能卡芯片安全功能应提供具有存储[赋值:审计信息列表]能力的[赋值:主体列表],及其被存储于[赋值:持续性存储器的类型]。

9.2.3.3 FCS_RNG.1 随机数生成

FCS_RNG.1.1 智能卡芯片安全功能应提供[选择:物理的、非物理真实的、决定性的或混合的]随机数发生器,以执行[赋值:安全能力列表]。

FCS_RNG.1.2 智能卡芯片安全功能应提供随机数来满足[赋值:定义的质量要求]。

9.3 智能卡管理安全功能要求

9.3.1 智能卡内容管理

9.3.1.1 概述

下载、安装以及删除应用的安全策略,修改智能卡内容操作的原则性要求,代码的正确接收和解释,新应用的特权;安全策略的另一个目标是确认智能卡管理员已经完成智能卡外实体的验证确保导入的代码是无害的,没有被修改。

9.3.1.2 FDP_UIT.1/CCM 数据交换的完整性

FDP_UIT.1.1/CCM TSF 应执行安全信道信息流控制和安全域访问控制策略,以便能接收用户数据,并保护数据避免带来篡改、删除、插入、重发错误。

FDP_UIT.1.2/CCM TSF 应能判断用户数据的接收过程,是否发生了篡改、删除、插入、重发错误。

9.3.1.3 FDP_ROL.1/CCM 基本回退

FDP_ROL.1.1/CCM TSF 应执行 SD 访问控制,以允许对客体可执行文件以及应用实例的安装操作进行回退。

FDP_ROL.1.2/CCM TSF 应允许在以下边界限制范围内:直到可执行文件或应用实例已经被添加到 Applet 的注册项中为止的条件下进行回退操作。

应用说明:

每当收到被破坏或者乱序的 LOAD 命令,不管被下载文件的长度如何,平台应当能够安全地终止新的可执行文件的下载操作。

9.3.1.4 FCS_COP.1/DAP 密码操作

FCS_COP.1.1/DAP TSF 应执行附加到可执行装入文件的 DAP 签名的验证,根据符合下述标准的特定的算法和密钥长度:

算法:

a) PKC Scheme: SHA-1 哈希和 PKCS#1 RSA 签名;
b) 或者 DES Scheme: Single DES plus final Triple DES MAC (Retail MAC);
c) 或者 SM3 和 SM2;
d) 或者 SM4。

密钥大小:

a) PKC Scheme: RSA 密钥的最小长度 1 024 位;
b) DES Scheme: DES 密钥的最小长度 16 字节;

c) SM4:16 字节密钥;
d) SM2:256 位密钥。

满足以下标准:

a) [GP]的 Sections C.1.2 和 C.6;
b) PKC Scheme: PKCS#1 定义的 SSA-PKCS1-v1_5;
c) DES Scheme: ISO/IEC 9797-1:2011 定义的 Retail MAC;
d) SM2:国密算法标准;
e) SM3:国密算法标准;
f) SM4:国密算法标准。

9.3.2 安全域

9.3.2.1 FDP_ACC.1/SD 子集访问控制

FDP_ACC.1.1/SD TSF 应对以下主体、客体及 SFP 所涵盖主体和客体之间的操作列表执行安全域访问控制 SFP:

a) 主体: S.INSTALLER, S.ADEL, S.CAD 以及 S.SD ;
b) 客体: 委托令牌, DAP 块以及下载文件;
c) 操作: GlobalPlatform 的智能卡内容管理 APDU 命令以及 API 方法;
d) [赋值:主体、客体及 SFP 所涵盖主体和客体之间的操作列表]。

9.3.2.2 FDP_ACF.1/SD 基于安全属性的访问控制

FDP_ACF.1.1/SD TSF 应对客体执行安全域访问控制 SFP,基于以下安全属性:

主体:

a) S.INSTALLER, 在[PP-JCS]定义,由智能卡上 GlobalPlatform 环境(OPEN)所代表,智能卡生命周期状态属性;
b) S.ADEL,也在[PP-JCS]定义,由智能卡上 GlobalPlatform 环境(OPEN)所代表;
c) S.SD,使用一组特权、生命周期状态以及安全通信的安全级,通过 APDU 或 API 接收智能卡管理命令;
d) S.CAD,在 [PP-JCS]定义, 通过 S.SD 和 S.INSTALLER 通信的智能卡外实体。

客体:

a) 委托令牌,在委托管理操作的情况下,此属性存在或不存在;
b) DAP 块,在应用下载的情况下,此属性存在或不存在;
c) 装入文件或可执行文件,在应用下载、安装、迁移或注册项更新的情况下,用打算的特权以及关联安全域的 AID;
d) [赋值:指定 SFP 控制下的主体和客体列表,以及每个对应的 SFP 相关安全属性或 SFP 相关属性的已命名组]。

FDP_ACF.1.2/SD TSF 应执行以下规则,已决定在受控主体与受控客体间的一个操作是否被允许:

由 GlobalPlatform 定义的运行时行为:

a) 下载;
b) 安装;
c) 迁移;
d) 注册项更新;
e) 内容删除。

FDP_ACF.1.3/SD　TSF 应基于以下附加规则：[赋值：基于安全属性，明确授权主体访问客体的一些规则]，明确授权主体访问客体。

FDP_ACF.1.4/SD　TSF 应基于以下附加规则：[赋值：基于安全属性，明确拒绝主体访问客体的一些规则]，明确拒绝主体访问客体；GlobalPlatform 定义的规则至少有一条没有符合。

9.3.2.3　FMT_MSA.1/SD 安全属性管理

FMT_MSA.1.1/SD　TSF 应执行安全域访问控制 SFP，以仅限于安全域以及应用实例自身能够对安全属性：[赋值：安全属性列表]，进行修改。

9.3.2.4　FMT_MSA.3/SD 静态属性初始化

FMT_MSA.3.1/SD　TSF 应执行安全域访问控制 SFP，以便为用于执行 SFP 的安全属性提供受限的默认值。

FMT_MSA.3.2/SD　TSF 应当允许[赋值：已标识的授权用户]在创建客体或者信息时指定替换性的初始值以代替原来的默认值。

9.3.2.5　FMT_SMF.1/SD 管理功能规范

FMT_SMF.1.1/SD　TSF 应能够执行如下安全管理功能：

a)　当接收到 DELETE 命令时，从 GP 注册表删除指定的注册项；

b)　当安装新应用实例时授予智能卡管理员指定的特权；

c)　按照 GP UICC 配置指定的规则迁移应用实例或者整个智能卡的生命周期状态。

9.3.2.6　FMT_SMR.1/SD 安全角色

FMT_SMR.1.1/SD　TSF 应维护角色[赋值：授权的已识别角色]。

FMT_SMR.1.2/SD　TSF 应能够把用户和角色关联。

9.3.3　安全信道——标识和鉴别

9.3.3.1　概述

关注打开安全信道前，主体可能完成的活动的要求。

9.3.3.2　FIA_UAU.4/SC 一次性鉴别机制

FIA_UAU.4.1/SC　TSF 应防止用于打开一个安全通信信道的鉴别机制有关的鉴别数据的再次使用。

9.3.4　安全信道——信息流安全策略

9.3.4.1　FTP_ITC.1/SC TSF 间可信信道

FTP_ITC.1.1/SC　TSF 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，其端点具有保证标识，并且能保护信道中的数据免遭修改或泄露。

FTP_ITC.1.2/SC　TSF 应允许其他可信 IT 产品经由可信信道发起通信

FTP_ITC.1.3/SC　TSF 应经由可信信道发起通信，对于所有智能卡管理功能：

a)　下载；

b)　安装；

c)　迁移；

d) 注册表更新；
e) SD 个人化；
f) [赋值：需要可信信道的功能列表]。

9.3.4.2 FCO_NRO.2/SC 强制性原发证明

FCO_NRO.2.1/SC TSF 在任何时候都应对所传送的应用包强制产生原发证据。
FCO_NRO.2.2/SC TSF 应能将信息原发者的身份和证据适用的信息中包含的应用包关联。
FCO_NRO.2.3/SC 给定[赋值：原发证据的限制]，TSF 应能为原发者提供验证信息原发证据的能力。

9.3.4.3 FDP_IFC.2/SC 完全信息流控制

FDP_IFC.2.1/SC TSF 应对下述主体和信息及 SFP 所涵盖导致信息流入、流出主体的所有操作执行安全信道信息流控制 SFP：

a) 主体 S.CAD 和 S.SD，涉及智能卡和 CAD 间通过可能不安全的通信信道的进行消息交换；
b) 这个策略控制的信息是智能卡内容管理命令，包括个人化命令，发送到智能卡的 APDU 以及相应的返回到 CAD 的应答；
c) [赋值：主体列表和信息列表]。

FDP_IFC.2.2/SC TSF 应确保导致 TOE 内任意信息流入、流出 TOE 内任意主体的所有操作都被一个信息流控制 SFP 涵盖。

9.3.4.4 FDP_IFF.1/SC 简单安全属性

FDP_IFF.1.1/SC TSF 应当基于以下类型的主体和信息的安全属性执行安全信道协议信息流控制策略(SCP)：

a) 智能卡内主体和智能卡外主体交换的信息有一个安全属性，即 MAC，确保消息的完整性以及信息起源；
b) 智能卡内主体和智能卡外主体由如下安全属性：
   1) 挑战是由主体生成的随机数用于标识当前会话；
   2) 密码是和当前智能卡会话相关的秘密，用于鉴别智能卡内主体和智能卡外主体；密码由智能卡和终端的挑战派生产生；
   3) 密钥组用于加密分散数据以便生成会话密钥，每组密钥包括安全信道加密密钥(S-ENC)、命令消息鉴别码密钥(C-MAC)以及数据加密密钥(DEK)；
   4) 静态密钥是一组密钥，每组密钥由密钥版本号标识；
   5) 会话密钥是一组密钥用于验证接受到的消息的来源以及完整性，解密它们的内容，包括如下密钥：
      - 命令消息鉴别码密钥(C-MAC 会话密钥)；
      - 加密密钥(S-ENC 会话密钥)；
      - 数据加密密钥(DEK 会话密钥)；
   6) 顺序计数器是附加每组密钥的一个计数器用于分散会话密钥；
   7) 初始级联向量用于计算消息的 MAC 值，它和当前会话以前的消息相关；
c) 除前面提到的安全属性外，ISD 有一个额外的属性，即为智能卡通过安全信道接受的消息定义的命令安全级，可能的安全级有：NO-SEC（明文），C-AUTHENTICATED（命令的发行方鉴别），C-MAC（发行方鉴别和命令的完整性），C-DEC(发行方鉴别，命令的完整性和保密性)。

9.3.4.5 FMT_MSA.3/SC 静态属性初始化

FMT_MSA.3.1/SC TSF 应执行安全信道协议 SCP 信息流控制 SFP，以便为用于执行 SFP 的安全属性提供受限的默认值。

FMT_MSA.3.2/SC TSF 应允许智能卡管理员在创建客体或者信息时指定替换性的初始值以代替原来的默认值。

应用说明：

智能卡管理员可以为 SCP 策略的静态密钥属性指定替换性的默认值。

9.3.4.6 FMT_SMR.1/CA 安全角色

FMT_SMR.1.1/CA TSF 应当维护智能卡管理员角色。

FMT_SMR.1.2/CA TSF 应当能够把用户和角色关联。

应用说明：

安全域只是智能卡发行商卡内对等物，引入单独角色便于区分代表智能卡发行商的智能卡内应用以及智能卡管理员。

9.3.4.7 FIA_AFL.1/SC 鉴别失败处理

FIA_AFL.1.1/SC TSF 应当检测何时发生，一次与智能卡管理命令来源的鉴别相关的未成功鉴别尝试。

FIA_AFL.1.2/SC 当达到或超过所定义的未成功鉴别尝试次数时，TSF 应采取关闭和外部用户的安全信道。

9.3.5 安全信道——密码操作

9.3.5.1 概述

通过安全信道接收到的智能卡管理命令的来源、完整性以及保密性的验证方面的密码要求。

9.3.5.2 FCS_COP.1/SC_02_CBC 密码操作

FCS_COP.1.1/SC_02-CBC TSF 应根据符合标准 FIPS PUB 46-3，ANSI X9.52 以及 ISO/IEC 10116：2006 的特定的 CBC 模式 Triple DES 算法和密钥长度 112 位来执行会话密钥的导出以及通过 GlobalPlatform 的安全信道交换的消息的数据字段的解密。

9.3.5.3 FCS_COP.1/SC_02-ECB 密码操作

FCS_COP.1.1/SC_02/ECB TSF 应根据符合标准 FIPS PUB 46-3，ANSI X9.52 以及 ISO/IEC 10116:2006 的特定的 ECB 模式 Triple DES 算法和密钥长度 112 位来执行密钥的加解密以及 DES 密钥校验和的生成。

9.3.5.4 FCS_COP.1/SC_02 密码操作

FCS_COP.1.1/SC_02 TSF 应根据符合标准 FIPS PUB 46-3 以及 ISO/IEC 9797-1:2011 的特定的 Triple DES 算法和密钥长度 16 字节来执行鉴别密码的生成、验证以及通过安全信道交换的消息的 MAC 码验证。

9.3.5.5 FCS_COP.1/SC_02-ICV 密码操作

FCS_COP.1.1/SC_02-ICV　TSF 应根据符合标准 FIPS PUB 46-2 的特定的 ECB 模式 DES 算法和密钥长度 56 位来执行消息完整性 ICV 的加密和解密。

9.3.5.6 FCS_COP.1/SC_02-FINAL 密码操作

FCS_COP.1.1/SC_02-FINAL　TSF 应根据符合标准 FIPS PUB 46-3，ISO/IEC 9797-1:2011 的特定的 Single DES plus final Triple DES 算法和密钥长度 16 字节来执行通过安全信道交换的消息的 MAC 码验证。

9.3.6 安全信道——密钥装载服务

9.3.6.1 概述

安装或者替换用于实现安全信道的静态密钥的要求，主要关注安全域的 PUT KEY 命令的处理

9.3.6.2 FCS_CKM.3/SC-KL 密钥访问

FCS_CKM.3.1/SC-KL　TSF 应当按照 GP 规范指定的密码访问方法(PUT KEY 或者 STORE DATA 命令)完成安全域密钥的安装以及下载操作

9.3.6.3 FPT_TDC.1/SC-KL TSF 间基本 TSF 数据一致性

FPT_TDC.1.1/SC-KL　当 TSF 与其他可信 IT 产品共享 TSF 数据时，TSF 应提供对安全域密钥进行一致性解释的能力。

FPT_TDC.1.2/SC-KL　当解释来自其他可行 IT 产品的 TSF 数据时，TSF 应使用如下规则：

a) 应当使用安全信道加密会话密钥解密收到的命令的数据字段；
b) 设置之前，应当使用数据加解会话密钥解密导入的 DES 密钥值。

9.3.6.4 FDP_ITC.1/SC-KL 不带安全属性的用户数据输入

FDP_ITC.1.1/SC-KL　在 SFP 控制下从 TSC 之外输入用户数据时，TSF 应执行安全信道协议(SCP)。

FDP_ITC.1.2/SC-KL　从 TSC 外部输入用户数据时，TSF 应略去任何与用户数据相关的安全属性。

FDP_ITC.1.3/SC-KL　在 SFP 控制下从 TSC 之外输入用户数据时，TSF 应执行下面规则：如果输入的数据是安全域的密钥组时，那么：

a) 如果命令指定密钥组替换，指定密钥组应在智能卡内存在，命令提供的密钥和智能卡内要替换的密钥要有相同的密钥组件个数，且每个组件要有相同的类型和长度；
b) 导入密钥的类型应被 GP 配置所支持；
c) 命令的数据字段应使用数据加密密钥解密；
d) 如果指定的密钥是 DES 密钥，附加的校验和应是正确的。

9.3.7 安全信道——密钥生成

9.3.7.1 概述

用于建立安全信道的会话密钥的生成以及分发的要求。

9.3.7.2 FMT_MSA.2/SC-KEYS 安全的安全属性

FMT_MSA.2.1/SC-KEYS　TSF 应确保安全属性只接受安全的值。

应用说明：

使用密钥之前，平台应当检测要完成的密钥操作符合其安全属性，如长度、关联的算法（DES、RSA等）以及密钥的类型（公开的、秘密的）。

9.3.8 安全信道——密钥销毁服务

当删除用于智能卡管理的密钥时要满足的要求。

9.3.9 全局智能卡持有者核对方法

9.3.9.1 概述

智能卡持有者核对方法的安全要求，该策略控制已安装应用通过 GP API 对 CVM 的内部数据结构的修改。

9.3.9.2 FIA_AFL.1/CVM 鉴别失败处理

FIA_AFL.1.1/CVM　TSF 应当检测何时发生，管理员可配置的 1～255 范围内一个正整数次与智能卡持有者鉴别相关的不成功尝试鉴别尝试。

FIA_AFL.1.2/CVM　当达到或超过所定义的未成功鉴别尝试次数时，TSF 应采取临时锁定智能卡持有者鉴别服务，直到特权用户进行了成功解锁。

应用说明：

应用实例创建的 PIN 服务保存锁定状态，直到拥有 PIN 对象的 Applet 通过 Java Card API 复位它的状态。

9.4 运行环境安全功能要求

9.4.1 概述

有关执行 Applet 的运行环境的安全功能要求，收集的要求分为以下几类：

a) 核心要求，对应[PP-JCS]指定 CoreG 组要求；

b) 操作系统要求，对应[PP-JCS]的安全的智能卡平台组的子集的要求。

9.4.2 防火墙

9.4.2.1 FDP_ACC.2 完全访问控制

FDP_ACC.2.1/FIREWALL　TSF 应对 S.PACKAGE，S.JCRE，O.JAVAOBJECT 及 SFP 所涵盖主体和客体之间得所有操作执行防火墙访问控制 SFP。

表 7 是 FDP_ACC.2 的主体、客体描述，表 8 是 FDP_ACC.2 的操作。

表 7 FDP_ACC.2.1/FIREWALL 的主体和客体

主体/客体	描述
S.PACKAGE	任何包，防火墙策略的安全单元
S.JCRE	JCRE，管理 Applet 的选择和取消选择，发送和接收 APDU，这个主体是唯一的
O.JAVAOBJECT	任何对象，密钥、PIN 以及 Applet 实例都是特定对象

表 8　FDP_ACC.2.1/FIREWALL 的操作

操作	描述
OP.ARRAY_ACCESS(OB.JAVAOBJECT, field)	读写数组的组件
OP.INSTANCE_FIELD(OB.JAVAOBJECT, field)	读写类实例的字段
OP.INVK_VIRTUAL(OB.JAVAOBJECT, method, arg1 ,…)	调用类实例或者数组对象的虚方法
OP.INVK_INTERFACE(OB.JAVAOBJECT, method, arg1 ,…)	调用接口方法
OP.THROW(OB.JAVAOBJECT)	抛出例外对象
OP.TYPE_ACCESS(OB.JAVAOBJECT, class)	调用对象的 checkcast 和 instanceof 方法
OP.JAVA(…)	代表以下操作之一： OP.ARRAY_ACCESS、OP.INSTANCE_FIELD、 OP.INVK_VIRTUAL、OP.INVK_INTERFACE、 OP.THROW、OP.TYPE_ACCESS
OP.CREATE(Sharing, LifeTime)	创建对象(new 或者 makeTransient)

FDP_ACC.2.2/FIREWALL　TSF 应确保 TSC 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。

9.4.2.2　FDP_ACF.1/FIREWALL 基于安全属性的访问控制

FDP_ACF.1.1/FIREWALL　TSF 应对客体执行防火墙访问控制 SFP，基于以下安全属性：

表 9 是 FDP_ACF.1 的安全属性，表 10 是安全属性的取值范围。

表 9　SFP 对应的安全属性

主体/客体	安全属性
S.PACKAGE	逻辑通道选择状态
S.JCVM	激活应用、当前激活应用
S.JCRE	选中的应用、选中的上下文
O.JAVAOBJECT	共享、上下文、生命周期

表 10　每个安全属性的可能值

名称	描述
Context	Package AID 或者“JCRE”
Sharing	Standard, SIO, JCRE entry point 或者 global array
LifeTime	CLEAR_ON_DESELECT 或者 PERSISTENT
Currently Active Context	Package AID 或者 “JCRE”
Selected Applet Context	Package AID 或者 “None”
Active Applets	活动 Applet 的 AID，一个活动 Applet 是在至少一个逻辑信道被选择的 Applet
LC Selection Status	Multiselectable，Non-multiselectable 或者“None”

FDP_ACF.1.2/FIREWALL　TSF 应执行以下规则，以决定在受控主体与受控客体间的一个操作是否被允许：

R.JAVA.1：S.PACKAGE 可以自由地对 Sharing 属性有值"JCRE entry point"或者"global array"的客体 O.JAVAOBJECT 执行 OP.ARRAY_ACCESS、OP.INSTANCE_FIELD、OP.INVK_VIRTUAL、OP.INVK_INTERFACE、OP.THROW 或者 OP.TYPE_ACCESS 操作。

R.JAVA.2　S.PACKAGE 可以自由地对任何 Sharing 属性有值"Standard"，Lifetime 属性有值"PERSISTENT"的 O.JAVAOBJECT，完成 OP.ARRAY_ACCESS、OP.INSTANCE_FIELD、OP.INVK_VIRTUAL、OP.INVK_INTERFACE 或者 OP.THROW 操作，仅当客体 O.JAVAOBJECT 的上下文属性和活动上下文有相同的值。

R.JAVA.3　S.PACKAGE 可以对 Sharing 属性有值"SIO"的客体 O.JAVAOBJECT 进行 OP.TYPE_ACCESS 操作，仅当客体 O.JAVAOBJECT 被转换为(checkcast)或者验证是(instanceof)一个共享接口的实例。

R.JAVA.4　S.PACKAGE 可以对 Sharing 属性有值"SIO"，Context 属性有值"Package AID"的客体 O.JAVAOBJECT 进行 OP.INVK_INTERFACE 操作，仅当调用的接口方法扩展至 Shareable 接口，并且适用下列条件之一：

AID 是"Package AID"的包的 Selection Status 属性是"Multiselectable"；

AID 是"Package AID"的包的 Selection Status 属性是"Non-multiselectable"，并且要么"Package AID"是当前选择的 Applet，要么"Package AID"没有在 Active Applets 属性中出现。

R.JAVA.5　主体 S.PACKAGE 可以执行 OP.CREATE 操作，仅当 Sharing 参数的值是"Standard"。

FDP_ACF.1.3/FIREWALL　TSF 应基于以下附加规则，明确授权主体访问客体：

a) 主体 S.JCRE 可以自由地完成 OP.JAVA(…)和 OP.CREATE 操作，FDP_ACF.1.4/FIREWALL 给定的要求例外，假如它是当前活动上下文；

b) 主体 S.JCVM 提供一个应用执行本地代码的唯一方法调用 Java Card 的 API 方法(通过 OP.INVK_INTERFACE or OP.INVK_VIRTUAL)。

FDP_ACF.1.4/FIREWALL　TSF 应基于以下规则，明确地拒绝主体访问客体：

a) 任何主体对一个 LifeTime 属性有值"CLEAR_ON_DESELECT"的客体 O.JAVAOBJECT 进行 OP.JAVA 操作，如果 O.JAVAOBJECT 的上下文属性不同于选择的 Applet 上下文；

b) 任何主体使用"CLEAR_ON_DESELECT"LifeTime 参数进行 OP.CREATE 操作，如果活动上下文不同于选择的 Applet 上下文。

9.4.2.3　FDP_IFC.1 子集信息流控制

FDP_IFC.1.1/JCVM　TSF 应对以下主体、信息以及操作。

主体：S.LOCAL，S.MEMBER。

信息：I.DATA。

操作：OP.PUT(S1，S2，I)。

执行 JCVM 信息流控制 SFP。

表 11 是 FDP_IFC.1 的消息描述，表 12 是 FDP_IFC.1 的操作描述。

表 11 主体消息描述

主体/消息	描述
S.LOCAL	JCVM 栈帧的操作数栈或者包含一个对象和数组引用 JCVM 栈帧的局部变量
S.MEMBER	任何对象的字段、静态字段或数组位置
I.DATA	JCVM 引用数据，临时 JCRE 入口点对象以及全局数组的对象引用地址

表 12 FDP_IFC.1 操作描述

操作	描述
OP.PUT(S1，S2，I)	从 S1 传输一条信息 I 到 S2

9.4.2.4 FDP_IFF.1 简单安全属性

FDP_IFF.1.1/JCVM TSF 应基于下列类型主体和信息的安全属性：当前活动上下文，执行 JCVM 信息流控制 SFP。

FDP_IFF.1.2/JCVM 如果支持下列规则：

a) 操作 OP.PUT(S1，S.MEMBER ，I.DATA)被允许，当且仅当活动上下文是“JCRE”；

b) 其他 OP.PUT 操作和上下文的值无关。

TSF 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。

FDP_IFF.1.3/JCVM TSF 应执行[赋值：附加的信息流控制 SFP]。

FDP_IFF.1.4/JCVM TSF 应提供下列[赋值：附加的 SFP 能力列表]。

FDP_IFF.1.5/JCVM TSF 应根据下列规则：[赋值：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。

FDP_IFF.1.6/JCVM TSF 应根据下列规则：[赋值：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。

9.4.2.5 FDP_RIP.1 子集残余信息保护

FDP_RIP.1.1/OBJECTS TSF 应确保一个资源的任何先前信息内容，在分配资源到下列客体类实例或数组时不再可用。

9.4.2.6 FMT_MSA.1 安全属性管理

FMT_MSA.1.1/JCRE TSF 应执行 FIREWALL 访问控制 SFP，以仅限于 JCRE 能够对安全属性：选择的 Applet 上下文，进行修改。

FMT_MSA.1.1/JCVM TSF 应执行 FIREWALL 访问控制 SFP 以及 JCVM 信息流控制 SFP，以仅限于 JCVM(S.JCVM)能够对安全属性：当前活动上下文以及活动 Applets，进行修改。

9.4.2.7 FMT_MSA.2/FIREWALL_JCVM 安全的安全属性

FMT_MSA.2.1/FIREWALL_JCVM TSF 应确保 FIREWALL 访问控制 SFP 以及 JCVM 信息流控制 SFP 定义的所有安全属性只接受安全的值。

9.4.2.8 FMT_MSA.3/FIREWALL 静态属性初始化

FMT_MSA.3.1/ FIREWALL　TSF 应执行 FIREWALL 访问控制 SFP，以便为用于执行 SFP 的安全属性提供受限的默认值。

FMT_MSA.3.2/FIREWALL　TSF 应不允许任何角色在创建客体或者信息时指定替换性的初始值以代替原来的默认值。

9.4.2.9 FMT_MSA.3/JCVM 静态属性初始化

FMT_MSA.3.1/JCVM　TSF 应执行 JCVM 信息流控制 SFP，以便为用于执行 SFP 的安全属性提供受限的默认值。

FMT_MSA.3.2/JCVM　TSF 应不允许任何角色在创建客体或者信息时指定替换性的初始值以代替原来的默认值。

9.4.2.10 FMT_SMF.1 管理功能规范

FMT_SMF.1.1　TSF 应能够执行如下安全管理功能：

修改当前活动上下文、选择的 Applet 上下文以及活动的 Applet。

9.4.2.11 FMT_SMR.1/JCRE 安全角色

FMT_SMR.1.1/JCRE　TSF 应维护以下角色：

a) Java Card RE (JCRE)；

b) Java Card VM (JCVM)。

FMT_SMR.1.2/JCRE　TSF 应能够把用户和角色关联起来。

9.4.3 应用编程接口-应用密码服务

9.4.3.1 概述

下面要求描述 Java Card API 提供的密码服务

9.4.3.2 FCS_COP.1/APP-RSA 密码操作

FCS_COP.1.1/APP-RSA　TSF 应当完成对应用实例数据的签名生成、签名验证、加密以及解密，使用指定的密码算法(RSA)以及密钥大小(32 位的倍数，从 1 024 位～2 048 位)符合 PKCS#1.5 规范要求。

9.4.3.3 FCS_RND.1/APP 随机数的质量度量

FCS_RND.1.1/APP　TSF 应当提供符合[AIS31]指定的标准级要求的生成随机数的机制，并满足密码行业标准 GM/T 0005—2012 对随机数质量及检测的要求。

9.4.3.4 FIA_AFL.1/KEYS 鉴别失败处理

FIA_AFL.1.1/KEYS　TSF 应当检测何时发生，管理员可配置的 1～255 范围内一个正整数次与给定密钥关联的签名验证相关的不成功尝试鉴别尝试。

FIA_AFL.1.2/KEYS　当达到或超过所定义的未成功鉴别尝试次数时，TSF 应当用管理员设置的因子乘以下一个签名验证操作的响应时间。

应用说明：

这个机制目的是阻止暴力攻击，智能卡初始化阶段可以被激活，一旦激活适用智能卡提供的所有的签名验证服务，包括 Applet 通过 Java Card API 创建的这些服务。

9.4.4 应用编程接口-密钥生成

9.4.4.1 概述

TOE 应当指出不同类型的密钥智能卡内生成。

9.4.4.2 FCS_CKM.1/APP-RSA 密钥生成

FCS_CKM.1.1/APP-RSA TSF 应根据符合下列标准[信息删除]的一个特定的密钥生成算法[信息删除]和规定的密钥长度(1 024 位～2 048 位)来生成密钥。

应用说明：

IEEE P1363—2000 标准的附录 A(数论背景)指定米勒-罗宾的测试应当用于确定是否随机数生成器产生的密钥部件是素数，具有任意小的错误概率。对于指定的长度，生成的密钥应是 RSA-CRT 格式。

9.4.4.3 FCS_CKM.1/APP-EC 密钥生成

FCS_CKM.1.1/APP-EC TSF 应根据符合下列标准[ISO/IEC 15946-1：2008，ISO/IEC 15946-3：2002]的一个特定的密钥生成算法[符合一个给定的 EC 域和曲线的椭圆曲线私钥]和规定的密钥长度(160，192，224 或 256 位)来生成密钥。

9.4.4.4 FCS_CKM.1/APP-DH 密钥生成

FCS_CKM.1.1/APP-DH TSF 应根据符合下列标准[PKCS＃3]的一个特定的密钥生成算法[使用随机数生成 Diffie-Hellman 密钥，根据给定域完成模幂运算]和规定的密钥长度(1 024 位～2 048 位)来生成密钥。

9.4.5 应用编程接口-残留信息保护

9.4.5.1 概述

下列要求涉及可以留在 Java Card 对象的敏感残留信息的保护。

9.4.5.2 FDP_RIP.1 子集残余信息保护

FDP_RIP.1.1/APDU TSF 应确保一个资源的任何先前信息内容，在分配资源到下列客体：APDU 缓冲区。

FDP_RIP.1.1/bArray TSF 应确保一个资源的任何先前信息内容，在分配资源到下列客体：bArray。

FDP_RIP.1.1/TRANSIENT TSF 应确保一个资源的任何先前信息内容，在分配资源到下列客体：任何 transient 对象。

FDP_RIP.1.1/ABORT TSF 应确保一个资源的任何先前信息内容，在释放资源自下列客体：一个中止的事务期间创建的一个对象实例的任何引用。

FDP_RIP.1.1/KEYS TSF 应确保一个资源的任何先前信息内容，在释放资源自下列客体：用于密码计算的缓冲区(D.CRYPTO)。

9.4.5.3 FDP_ROL.1 基本回退

FDP_ROL.1.1/FIREWALL TSF 应执行 FIREWALL 访问控制 SFP 以及 JCVM 信息流控制 SFP，以

	允许对客体 O.JAVAOBJECTs 的 OP.JAVA，OP.CREATE 操作进行回退。
FDP_ROL.1.2/FIREWALL	TSF 应允许在 select()，deselect()，process() or install()调用范围内，尽管有[JCRE222]，§7.7 给定的限制，并且位于提交能力的界限之内，进行回退操作。

9.4.6 智能卡安全管理

9.4.6.1 概述

以下要求和整张智能卡的安全性相关，对照前面的安全要求，只是单独对运行时环境的功能进行些限制。比如，由虚拟机检测到的一个潜在的安全违反可能需要的反应，不仅涉及虚拟机，而且请求的适当的有能力的安全单元阻止智能卡执行该操作。

9.4.6.2 FAU_ARP.1 安全告警

FAU_ARP.1.1 当检测到潜在的安全侵害时，TSF 应进行以下动作之一：

a) TSF 应进行抛出例外；
b) 锁定智能卡会话；
c) 初始化 Java Card 系统以及它的数据；
d) [赋值：其他动作列表]。

应用说明：

潜在的安全侵害细化下列事件之一：

a) CAP 文件不一致；
b) 字节码的操作数类型错误；
c) Applet 生命周期不一致；
d) 智能卡拔出(突然从 CAD 移出 CAD)以及电源失效；
e) 意外的上下文事务的中止；
f) 防火墙或者 JCVM SFP 的违反；
g) 资源不可用；
h) 数组上溢；
i) 与 Applet 失败相关的其他运行时错误(如未捕获的例外)。

这个要求适用于整个 TOE，应由基本的 OS 的破坏性活动完成。

9.4.6.3 FDP_SDI.2 存储数据完整性监视和反应

FDP_SDI.2.1 TSF 应基于下列属性：[赋值：用户数据属性]对所有的客体，监视存储在 TOE 内的用户数据是否存在[赋值：完整性错误]。

FDP_SDI.2.2 检测到完整性错误时，TSF 应[赋值：采取的动作]。

9.4.6.4 FPT_TDC.1 TSF 间基本的 TSF 数据一致性

FPT_TDC.1.1 当 TSF 与其他可信 IT 产品共享 TSF 数据时，TSF 应提供对 CAP 文件(在智能卡管理器和 TOE 间共享)、字节码以及它的数据参数(与 Applet 和 API 包共享)进行一致性解释的能力。

FPT_TDC.1.2 当解释来自其他可行 IT 产品的 TSF 数据时，TSF 应使用如下规则：

a) [JCVM222] 规范；
b) 引用输出文件；
c) ISO/IEC 7816-6:2004 规则；
d) EMV 规范。

9.4.6.5 FPT_FLS.1 失效即保存安全状态

FPT_FLS.1.1 TSF 在下列失效发生时应保持一种安全状态：和 FAU_ARP.1 描述的安全违反相关的失效。

9.4.6.6 FPR_UNO.1 不可观察性

FPR_UNO.1.1 TSF 应确保 S.Package 不能观察由[其他 S.Package]对[Key 值/PIN 值]进行的[密码计算/比较]操作。

9.4.7 AID 管理

9.4.7.1 FMT_MTD.1/AID TSF 数据的管理

FMT_MTD.1.1/AID TSF 应仅限于 JCRE 能够对注册的 Applet 的 AID 进行修改操作。

9.4.7.2 FMT_MTD.3/AID 安全的 TSF 数据

FMT_MTD.3.1/AID TSF 应确保注册的 Applet 的 AID 只接受安全的值。

9.4.7.3 FIA_ATD.1/AID 用户属性定义

FIA_ATD.1.1/AID TSF 应维护属于单个用户的下列安全属性列表：
a) 每个包的 AID；
b) Applet 的版本号；
c) 每个注册的 Applet 的 AID；
d) Applet 选择状态。

9.4.7.4 FIA_UID.2/AID 任何动作前的用户标识

FIA_UID.2.1/AID 在允许执行代表该用户的任何其他 TSF 介导动作之前，TSF 应要求每个用户识别它自己。

9.4.7.5 FIA_USB.1/AID 用户主体绑定

FIA_USB.1.1/AID TSF 应将适当的用户安全属性与代表用户活动的主体相关联。

9.4.8 Applet 安装

9.4.8.1 FDP_ITC.2/Installer 带有安全属性的用户数据输入

FDP_ITC.2.1/Installer 在 SFP 控制下从 TOE 外部输入用户数据时，TSF 应执行包装载信息流控制 SFP。
FDP_ITC.2.2/Installer TSF 应使用与所输入数据相关的安全属性。
FDP_ITC.2.3/Installer TSF 应确保所使用的协议在安全属性和接收的用户数据之间提供了明确的关联。
FDP_ITC.2.4/Installer TSF 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。

FDP_ITC.2.5/Installer　在 SFP 控制下从 TOE 外部输入用户数据时，TSF 应执行下述规则：

包装载被容许，仅当，对每个依赖包，其 AID 属性等于驻留包 AID 属性，依赖包的版本小于或等于驻留包的版本。

9.4.8.2　FMT_SMR.1/Installer 安全角色

FMT_SMR.1.1/Installer　TSF 应维护角色：Installer。

FMT_SMR.1.2/Installer　TSF 应能把角色和用户关联。

9.4.8.3　FPT_FLS.1/Installer 失效即保持安全状态

FPT_FLS.1.1/Installer　TSF 在下列失效发生时应保持一种安全状态：

安全域未能按[JCRE222]，Section11.3.4 描述装载一个可执行文件/安装一个应用实例。

9.4.8.4　FPT_RCV.3/Installer 无过度损失的自动恢复

FPT_RCV.3.1/Installer　当不能从失效或服务中断自动恢复时，TSF 应进入一种维护模式，该模式提供将 TOE 返回到一个安全状态的能力。

FPT_RCV.3.2/Installer　可执行下载文件安装处理的失败，可执行下载文件传输到智能卡的过程中检测到完整性可能损失，可执行装入文件和智能卡内已安装的可执行装入文件链接过程中发生的任何致命错误，TSF 应当确保通过自动化过程使 TOE 返回到安全一个安全状态。

FPT_RCV.3.3/Installer　TSF 提供的从失效或服务中断状态恢复的功能，应确保在所损失的 TSC 内 TSF 数据或客体不超出正在安装的可执行文件的损失情况下，恢复到安全初始状态。

FPT_RCV.3.4/Installer　TSF 应提供确定客体能否被恢复的能力。

9.4.9　Applet 删除

9.4.9.1　概述

本节描述删除可执行文件(ELF)和 Applet 实例的安全功能要求。

9.4.9.2　FDP_ACC.2/ADEL 完全访问控制

FDP_ACC.2.1/ADEL　TSF 应对 S.ADEL，O.JAVAOBJECT，O.APPLET 和 O.CODE_PKG 及 SFP 所涵盖主体和客体之间得所有操作执行 ADEL 访问控制 SFP。

S.ADEL，Applet 删除管理器，可以是一个 Applet，但它的角色从安全观点看要求特定的处理，这个主体是唯一的。

O.CODE_PKG，包的代码，包括所有的链接信息，对于 Java Card 平台，包是安装单元。

O.APPLET，任何已安装的 Applet，它的代码和数据。

O.JAVAOBJECT ，Java 类实例或数组。

操作：

OP.DELETE_APPLET(O.APPLET，…) 逻辑上或物理上删除一个已安装的 Applet 和它的对象。

OP.DELETE_PCKG(O.CODE_PKG，…) 逻辑上或物理上删除一个包。

OP.DELETE_PCKG_APPLET(O.CODE_PKG，…) 逻辑上或物理上删除一个包以及它的已安装的 Applet。

FDP_ACC.2.2/ADEL　TSF 应确保 TSC 内的任何主体和客体之间得所有操作都被一个访问控制 SFP 涵盖。

9.4.9.3　FDP_ACF.1/ADEL 基于安全属性的访问控制

FDP_ACF.1.1/ADEL　TSF 应基于以下信息对客体执行 ADEL 访问控制 SFP：

a）　涵盖的主体或客体的安全属性；

b）　智能卡内已注册的 Applet 实例的 AID 列表；

c）　ResidentPackages 属性日志智能卡内已下载包的 AID 列表；

d）　ActiveApplets 属性，活动 Applet 的 AID 列表。

FDP_ACF.1.2/ADEL　TSF 应执行以下规则，已决定在受控主体与受控客体间的一个操作是否被 ADEL SFP 允许：

R.JAVA14　Applet 实例删除，S.ADEL 可以对 O.APPLET 执行 OP.DELETE_APPLET 操作，仅当

a）　S.ADEL 被当前选择；

b）　O.APPLET 被取消选择；

c）　没有 O.APPLET 拥有的 O.JAVAOBJECT，这些 O.JAVAOBJECT 或者从一个不同于 O.APPLET 可达或者 O.JAVAOBJECT 从包 P 可达，或者 O.JAVAOBJECT 是远程可达。

R.JAVA.15　多重 Applet 实例删除，S.ADEL 可以对多个 O.APPLET 执行 OP.DELETE_APPLET 操作，仅当

a）　S.ADEL 被当前选择；

b）　每个 O.APPLET 被取消选择；

c）　没有任何要被删除 O.APPLET 拥有的这些 O.JAVAOBJECT，或者从一个不同于O.APPLET 可达或者 O.JAVAOBJECT 从包 P 可达，或者 O.JAVAOBJECT 是远程可达。

R.JAVA. 16　Applet/库包删除，S.ADEL 可以对 O.CODE_PCKG 执行 OP.DELETE_PCKG 操作，仅当

a）　S.ADEL 被当前选择；

b）　没有从不同于 O.CODE_PCKG 的包可达，且属于 O.CODE_PCKG 包中的类的一个实例的 O.JAVAOBJECT 在智能卡内存在；

c）　智能卡上没有包依赖 O.CODE_PCKG。

R.JAVA.17　Applet 包以及包含的实例删除

S.ADEL 可以对 O.CODE_PCKG 执行 OP.DELETE_PCKG_APPLET 操作，仅当

a）　S.ADEL 被当前选择；

b）　没有从不同于 O.CODE_PCKG 的包可达，且属于 O.CODE_PCKG 包中的类的一个实例的 O.JAVAOBJECT 在智能卡内存在；

c）　智能卡上没有包依赖 O.CODE_PCKG；

d）　要被删除的每个 O.APPLET 保持(i)O.APPLET 取消选择，(ii)没有 O.APPLET 拥有这些 O.JAVAOBJECT，要么从未删除的 Applet 实例可达，要么从未删除的包可达。

FDP_ACF.1.3/ADEL　TSF 应基于以下附加规则，明确授权主体访问客体，无

FDP_ACF.1.4/ADEL　TSF 应明确地拒绝任何主体访问，除 S.ADEL 对 O.CODE_PKG 或者 O.APPLET 的访问，为从智能卡内删除它的目的。

9.4.9.4 FMT_MSA.1/ADEL 安全属性管理

FMT_MSA.1.1/ADEL TSF 应执行 ADEL 访问控制 SFP，以仅限于 JCRE 能够对安全属性：活动 Applet 安全属性，进行修改。

9.4.9.5 FMT_MSA.3/ADEL 静态属性初始化

FMT_MSA.3.1/ADEL TSF 应执行 ADEL 访问控制 SFP，以便为用于执行 SFP 的安全属性提供受限的默认值。

FMT_MSA.3.2/ADEL TSF 应允许下列角色在创建客体或者信息时指定替换性的初始值以代替原来的默认值：无。

9.4.9.6 FMT_SMR.1/ADEL 安全角色

FMT_SMR.1.1/ADEL TSF 应当维护角色：Applet 删除管理器。

FMT_SMR.1.2/ADEL TSF 应当能够把用户和角色关联。

9.4.9.7 FDP_RIP.1/ADEL 子集残留信息保护

FDP_RIP.1.1/ADEL TSF 应确保一个资源的任何先前信息内容，在释放资源自下列客体：
当 DP_ACC.2.1/ADEL 描述的删除之一被执行时，Applet 实例和/或者包。

9.4.9.8 FPT_FLS.1/ADEL 失效即保持安全状态

FPT_FLS.1.1/ADEL TSF 在下列失效发生时应保持一种安全状态：
Applet 删除管理器未能按[JCRE22]，§11.3.4 描述删除一个包/Applet。

9.4.10 垃圾回收

9.4.10.1 概述

本组的要求涉及按需垃圾收集不可达的对象，Java Card 的 2.2.x 的版本中引入的机制，它们对应的 ODEL 组要求[PP-JCS]。

9.4.10.2 FDP_RIP.1/ODEL 子集残留信息保护

FDP_RIP.1.1/ODEL TSF 应确保一个资源的任何先前信息内容，在释放资源自下列客体：Applet 实例上下文拥有的对象，该实例触发方法 Javacard.framework.JCSystem.requestObjectDeletion()的执行。

9.4.10.3 FPT_FLS.1/ODEL 失效即保持安全状态

FPT_FLS.1.1/ODEL TSF 在下列失效发生时应保持一种安全状态：
对象删除功能未能删除请求这个方法执行的 Applet 所拥有的所有引用的对象。

9.5 平台安全功能要求

9.5.1 FPT_RCV.3/SCP 无过度损失的自动恢复

FPT_RCV.3.1/SCP 当不能检从检测出的 D_APP_CODE、D.APP_I_DATAD、PIND.APP_KEYs 完整性错误自动恢复时，TSF 应进入一种维护模式，该模式提供将 TOE 返回到一

个安全状态的能力。

FPT_RCV.3.2/SCP　对电源失效，TSF 应确保通过自动化过程是 TOE 返回到一个安全状态。

FPT_RCV.3.3/SCP　TSF 提供的从失效或服务中断状态恢复的功能，应确保在所损失的 TSF 控制下的 TSF 数据或客体不超出下述情况下，恢复到安全初始状态：

a) 事务内 Java Card 的静态字段、实例字段以及数组成员的内容；

b) 事务内分配的 Java Card 对象；

c) Java Card 临时对象的内容；

d) 当失效发生时任何可能的可执行装入文件。

FPT_RCV.3.4/SCP　TSF 应提供确定客体能否被恢复的能力。

9.5.2 FPT_RCV.4/SCP 功能恢复

FPT_RCV.4.1/SCP　TSF 应确保读写静态以及对象字段由于掉电中断，有如下特性，即 SF 或者成功完成，或者针对指明的失效情景恢复到一个前后一致的且安全的状态。

应用说明：

这个要求来自 Java Card 平台的要求，但显然地被智能卡底层机制的实现所支持。

9.6 安全功能要求对应关系

说明了安全要求的充分必要性，即每个安全目的都至少有一个安全（包括功能要求和保证要求）组件与其对应，每个安全要求都至少解决了一个安全目的，因此安全要求对安全目的而言是充分和必要的。

表 13 是安全功能要求与安全目的的对应关系。

表 13　安全功能要求与安全目的的对应关系

安全功能组件	安全目的																								
	O.REQUEST	O.INFO-ORIGIN	O.INFO-INTEGRITY	O.INFO-CONFIDENTIALITY	O.INSTALL	O.LOAD	O.DELETION	O.SID	O.FIREWALL	O.GLOBAL_ARRAYS_CONFID	O.GLOBAL_ARRAYS_INTEG	O.NATIVE	O.OPERATE	O.REALLOCATION	O.RESOURCES	O.ALARM	O.CIPHER	O.KEY-MNGT	O.PIN-MNGT	O.TRANSACTION	O.OBJ-DELETION	O.SCP.RECOVERY	O.SCP.SUPPORT	O.PROT-INF-LEAK	O.PROT-PHYS-TAMPER	O.PROT-MALFUNCTION	O.RND
FAU_ARP.1													√		√	√											
FCS_RND.1/APP																											√
FCS_CKM.1/APP-RSA FCS_CKM.1/APP-EC FCS_CKM.1/APP-DH																	√	√									
FCS_CKM.3/SC-KL		√	√	√	√	√	√										√										

表 13（续）

安全功能组件	安全目的																										
	O.REQUEST	O.INFO-ORIGIN	O.INFO-INTEGRITY	O.INFO-CONFIDENTIALITY	O.INSTALL	O.LOAD	O.DELETION	O.SID	O.FIREWALL	O.GLOBAL_ARRAYS_CONFID	O.GLOBAL_ARRAYS_INTEG	O.NATIVE	O.OPERATE	O.REALLOCATION	O.RESOURCES	O.ALARM	O.CIPHER	O.KEY-MNGT	O.PIN-MNGT	O.TRANSACTION	O.OBJ-DELETION	O.SCP.RECOVERY	O.SCP.SUPPORT	O.PROT-INF-LEAK	O.PROT-PHYS-TAMPER	O.PROT-MALFUNCTION	O.RND
FCS_COP.1/DAP FCS_COP.1/SC_02_CBC FCS_COP.1/SC_02-ECB FCS_COP.1/SC_02 FCS_COP.1/SC_02-ICV FCS_COP.1/SC_02-FINAL FCS_COP.1/APP-RSA FCS_COP.1/IC		√	√	√	√	√	√										√	√									
FCO_NRO.2/SC		√																									
FDP_ACC.1/SD	√				√	√	√																				
FDP_ACC.2/FIREWALL FDP_ACC.2/ADEL							√		√				√						√								
FDP_ACF.1/FIREWALL FDP_ACF.1/ADEL FDP_ACF.1/SD	√				√	√	√		√			√	√						√								
FDP_IFC.1/JCVM FDP_IFC.1/IC									√	√	√													√			
FDP_IFC.2/SC		√	√	√																							
FDP_IFF.1/JCVM FDP_IFF.1/SC		√	√	√	√	√	√		√	√	√																
FDP_ITC.1/SC-KL		√	√	√																							
FDP_ITC.2/Installer					√			√	√				√														
FDP_ITT.1/IC																								√		√	
FDP_RIP.1							√			√				√				√	√	√	√						
FDP_ROL.1/FIREWALL FDP_ROL.1/CCM				√	√	√							√		√				√	√							
FDP_SDI.2																		√	√								

表 13（续）

安全功能组件	安全目的																									
	O.REQUEST	O.INFO-ORIGIN	O.INFO-INTEGRITY	O.INFO-CONFIDENTIALITY	O.INSTALL	O.LOAD	O.DELETION	O.SID	O.FIREWALL	O.GLOBAL_ARRAYS_CONFID	O.GLOBAL_ARRAYS_INTEG	O.NATIVE	O.OPERATE	O.REALLOCATION	O.RESOURCES	O.ALARM	O.CIPHER	O.KEY-MNGT	O.PIN-MNGT	O.TRANSACTION	O.OBJ-DELETION	O.SCP.RECOVERY	O.SCP.SUPPORT	O.PROT-INF-LEAK	O.PROT-PHYS-TAMPER	O.PROT-MALFUNCTION	O.RND
FDP_UIT.1/CCM				√	√	√																					
FIA_AFL.1/KEYS FIA_AFL.1/SC FIA_AFL.1/CVM		√	√	√	√	√	√																				
FIA_ATD.1/AID								√					√														
FIA_UID.2/AID								√																			
FIA_USB.1/AID								√					√														
FMT_MSA.1/JCRE FMT_MSA.1/JCVM FMT_MSA.1/ADEL FMT_MSA.1/SD				√	√	√	√	√	√															√			
FMT_MSA.2/FIREWALL_JCVM FMT_MSA.2/SC-KEYS		√	√	√					√															√			
FMT_MSA.3/ FIREWALL FMT_MSA.3/JCVM FMT_MSA.3/ADEL FMT_MSA.3/SD FMT_MSA.3/SC		√	√	√	√	√	√	√	√															√			
FMT_SMF.1 FMT_SMF.1/SD					√	√	√	√	√						√									√			
FMT_SMR.1/JCRE FMT_SMR.1/ADEL FMT_SMR.1/Installer FMT_SMR.1/SD FMT_SMR.1/CA		√	√	√	√	√	√		√						√												
FMT_MTD.1/JCRE									√						√									√			
FMT_MTD.3/JCRE									√						√												
FPR_UNO.1																	√	√	√					√			

表 13（续）

安全功能组件	安全目的																									
	O.REQUEST	O.INFO-ORIGIN	O.INFO-INTEGRITY	O.INFO-CONFIDENTIALITY	O.INSTALL	O.LOAD	O.DELETION	O.SID	O.FIREWALL	O.GLOBAL_ARRAYS_CONFID	O.GLOBAL_ARRAYS_INTEG	O.NATIVE	O.OPERATE	O.REALLOCATION	O.RESOURCES	O.ALARM	O.CIPHER	O.KEY-MNGT	O.PIN-MNGT	O.TRANSACTION	O.OBJ-DELETION	O.SCP.RECOVERY	O.SCP.SUPPORT	O.PROT-INF-LEAK	O.PROT-PHYS-TAMPER	O.PROT-MALFUNCTION	O.RND
FPT_FLS.1 FPT_FLS.1/ADEL FPT_FLS.1/IC FPT_FLS.1/Installer FPT_FLS.1/ODEL						√	√						√		√	√					√	√					
FPT_ITT.1/IC																	√							√			
FPT_PHP.3/IC																									√		
F PT_RCV.3/Installer FPT_RCV.3/ SCP							√							√	√							√	√				
FPT_RCV.4/ SCP																							√				
FPT_TDC.1 FPT_TDC.1/SC-KL		√	√	√	√	√	√						√														
FTP_ITC.1/SC		√	√	√	√	√	√																				
FRU_FLT.2/IC																	√					√				√	

表 14、表 15 和表 16 说明了安全要求的充分必要性，即每个安全目的都至少有一个安全（包括功能要求和保证要求）组件与其对应，每个安全要求都至少解决了一个安全目的，因此安全要求对安全目的而言是充分和必要的。

表 14　安全目的与安全要求的对应关系

安全目的	对应的安全要求组件
O.Log_Prot	FAU_ARP.1，FDP_RIP.1，FMT_MSA.2，FPT_FLS.1，FPT_ITT.1，FPT_RCV.4，FPT_RVM.1，FPT_SEP.1，ADV_IMP.1，AVA_VLA.3
O.I_Leak	FPT_PHP.3，AVA_VLA.3
O.Init	FDP_RIP.1，FPT_RCV.4
O.Flt_Ins	FDP_ACC.1，FDP_ACF.1，FDP_IFC.1，FDP_IFF.1，FDP_ITC.1，AVA_VLA.3
O.Reuse	FIA_AFL.1，FIA_UAU.4，FPT_RPL.1

表 14（续）

安全目的	对应的安全要求组件
O.Set_Up	FDP_ACC.1，FDP_ACF.1，FIA_UAU.1，FMT_MSA.3，ADV_IMP.1
O.DAC	FDP_ACC.1，FDP_ACF.1，FDP_ETC.1，FDP_IFC.1，FDP_IFF.1，FDP_ITC.1，FIA_ATD.1，FIA_UAU.1，FIA_UID.1，FMT_MOF.1，FMT_MSA.1
O.D_Read	FPT_ITT.1，AVA_VLA.3
O.Life_Cycle	FDP_IFC.1，FDP_IFF.1，FPT_SEP.1，ADV_IMP.1，AVA_VLA.3
O.Phys_Prot	FPT_PHP.3，ADV_IMP.1，AVA_VLA.3
O.Crypt	FCS_CKM.2，FCS_CKM.4，FCS_COP.1
O.Unlink	FDP_ACC.1，FDP_ACF.1，FDP_ETC.1，FDP_IFC.1，FDP_IFF.1，FDP_ITC.1
O.Ident	FAU_SAS.1，ACM_CAP.4，ADV_IMP.1
O.Env_Strs	FAU_ARP.1，FAU_SAA.1，FPT_PHP.3，FRU_FLT.2，FPT_FLS.1，AVA_VLA.3
O.Sec_Com	FDP_ETC.1，FDP_ITC.1
O.RND	FCS_RNG.1
OE.Role_Man	FMT_SMR.1
OE.Key_Supp	FCS_CKM.2，FCS_CKM.4

表 15　安全功能要求与安全目的的对应关系

安全功能要求组件	对应的安全目的
FAU_ARP.1	O.Log_Prot
FAU_SAA.1	O.Log_Prot
FAU_SAS.1	O.Ident
FCS_CKM.2	O.Crypt
FCS_CKM.4	O.Crypt
FCS_COP.1	O.Crypt
FDP_ACC.1	O.Flt_Ins，O.Set_Up，O.DAC
FDP_ACF.1	O.Flt_Ins，O.Set_Up，O.DAC，O.Unlink
FDP_ETC.1	O.DAC，O.Unlink
FDP_IFC.1	O.Flt_Ins，O.DAC，O.Life_Cycle
FDP_ITC.1	O.Flt_Ins，O.DAC，O.Unlink
FDP_ITT.1	O.I_Leak，O.Unlink
FDP_RIP.1	O.Log_Prot
FIA_ATD.1	O.DAC
FIA_UAU.1	O.Set_Up，O.DAC
FIA_UID.1	O.DAC

表 15（续）

安全功能要求组件	对应的安全目的
FMT_MOF.1	O.DAC，OE.Role_Man
FMT_MSA.1	O.DAC，OE.Role_Man
FMT_MSA.2	O.Log_Prot，O.Set_Up
FMT_MSA.3	O.Set_Up
FMT_SMR.1	OE.Role_Man
FPT_FLS.1	O.Log_Prot
FPT_ITT.1	O.Log_Prot，O.I_Leak，O.Unlink
FPT_PHP.3	O.Log_Prot
FPT_RCV.4	O.Log_Prot，O.Init
FPT_RVM.1	O.Log_Prot
FPT_SEP.1	O.Life_Cycle，O.Log_Prot
FRU_FLT.2	O.DAC，O.Env_Strs
FCS_RNG.1	O.RNG

表 16　安全功能要求的依赖关系

安全功能要求组件	依赖关系
FAU_ARP.1	FAU_SAA.1
FAU_SAA.1	无依赖关系
FAU_SAS.1	无依赖关系
FCS_COP.1	FDP_ITC.1
	FCS_CKM.4
	FMT_MSA.2
	（间接）FCS_CKM.2
	（间接）FDP_ACC.1
	（间接）FDP_ACF.1
	（间接）FDP_IFC.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1
	（间接）ADV_SPM.1

表 16（续）

安全功能要求组件	依赖关系
FDP_ACC.1	FDP_ACF.1
	（间接）FDP_IFC.1
	（间接）FDP_IFF.1
	（间接）FDP_ITT.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1
	（间接）FPT_ITT.1
FDP_ACF.1	FDP_ACC.1
	FMT_MSA.3
	（间接）FDP_IFC.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_SMR.1
FDP_ETC.1	FDP_ACC.1 或 FDP_IFC.1
	（间接）FDP_ACF.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1
FDP_IFC.1	FDP_IFF.1
	（间接）FDP_ACC.1
	（间接）FDP_ACF.1
	（间接）FDP_ITT.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1

表 16（续）

安全功能要求组件	依赖关系
FDP_IFF.1	FDP_IFC.1
	FMT_MSA.3
	（间接）FDP_ACC.1
	（间接）FDP_ACF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_SMR.1
FDP_ITC.1	FDP_ACC.1 或 FDP_IFC.1
	FMT_MSA.3
	（间接）FDP_ACF.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_SMR.1
FDP_ITT.1	无依赖关系
	（间接）FMT_SMR.1
FDP_RIP.1	无依赖关系
FIA_ATD.1	无依赖关系
FIA_UAU.1	FIA_UID.1
FIA_UID.1	无依赖关系
FMT_MOF.1	（间接）FIA_UID.1
	（间接）FMT_SMR.1
FMT_MSA.1	FDP_ACC.1 或 FDP_IFC.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1
FMT_MSA.2	FDP_ACC.1 或 FDP_IFC.1
	FMT_MSA.1
	（间接）FMT_SMR.1
	ADV_SPM.1
	（间接）FDP_ACF.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.3

表 16（续）

安全功能要求组件	依赖关系
FMT_MSA.3	FMT_MSA.1
	（间接）FMT_SMR.1
	（间接）FDP_ACC.1
	（间接）FDP_ACF.1
	（间接）FDP_IFC.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
FPT_FLS.1	ADV_SPM.1
FPT_ITT.1	无依赖关系
FPT_PHP.3	无依赖关系
FPT_RCV.4	ADV_SPM.1
FPT_RVM.1	无依赖关系
FPT_SEP.1	无依赖关系
FRU_FLT.2	无依赖关系
FCS_CKM.2	FDP_ITC.1
	FCS_CKM.4
	FMT_MSA.2
	（间接）FCS_COP.1
	（间接）FDP_ACC.1
	（间接）FDP_ACF.1
	（间接）FDP_IFC.1
	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1
	（间接）ADV_SPM.1
FCS_CKM.4	FDP_ITC.1
	FMT_MSA.2
	（间接）FCS_CKM.2
	（间接）FCS_COP.1
	（间接）FDP_ACC.1
	（间接）FDP_ACF.1
	（间接）FDP_IFC.1

表 16（续）

安全功能要求组件	依赖关系
FCS_CKM.4	（间接）FDP_IFF.1
	（间接）FIA_UID.1
	（间接）FMT_MSA.1
	（间接）FMT_MSA.3
	（间接）FMT_SMR.1
	（间接）ADV_SPM.1
FMT_SMR.1	FIA_UID.1

10 安全保证要求

10.1 概述

安全保证要求对应 CC 认证体系的级别 EAL4+（参数为：AVA_VAN.5、ALC_DVS.2）。

表 17 是安全保证要求汇总表。

表 17 安全保证要求组件

安全保证要求组件	组件名称	依赖性
ACM 类：配置管理		
ACM_AUT.1/IC	部分配置管理自动化	
ACM_CAP.4/IC	产生支持和接受过程	
ACM_SCP.2/IC	跟踪配置管理范围问题	
ADO 类：交付和运行		
ADO_DEL.2/IC	修改监测	
ADO_IGS.1/IC	安装、生成和启动过程	
ASE 类：安全目标评估		
ASE_INT.1	安全目标介绍	
ASE_CCL.1	一致性声明	
ASE_SPD.1	安全问题定义	
ASE_OBJ.2	安全目的	
ASE_ECD.1	扩展组件定义	
ASE_REQ.2	安全要求	
ASE_TSS.1	TOE 实现概述	
ADV 类：开发		
ADV_ARC.1	安全架构描述	（ADV_FSP.1）与（ADV_TDS.1）

表 17（续）

安全保证 要求组件	组件名称	依赖性
ADV_FSP.4	功能规范	(ADV_TDS.1)
ADV_FSP.2/IC	完全定义的外部接口	
ADV_HLD.2/IC	安全加强的高层设计	
ADV_IMP.1	TSF 实现的子集	(ADV_TDS.3) 与(ALC_TAT.1)
ADV_TDS.3	基本模块设计	(ADV_FSP.4)
AGD 类:指南文档		
AGD_OPE.1	操作用户指南	(ADV_FSP.1)
AGD_PRE.1	准备流程	无
ALC 类:生命周期支持		
ALC_CMC.4	生产支持,接受步骤以及自动化	无
ALC_CMS.4	问题跟踪 CM 覆盖	无
ALC_DEL.1	交付过程	无
ALC_DVS.2	安全措施的充分性	无
ALC_LCD.1	开发者定义的生命周期模型	无
ALC_TAT.1	明确定义的开发工具	(ADV_IMP.1)
ATE 类:测试		
ATE_COV.2	范围分析	(ADV_FSP.2) 与 (ATE_FUN.1)
ATE_DPT.1	测试:基本设计	(ADV_ARC.1) 与(ADV_TDS.2) 与 (ATE_FUN.1)
ATE_FUN.1	功能测试	(ATE_COV.1)
ATE_IND.2	独立性测试-抽样	(ADV_FSP.2) 与 (AGD_OPE.1)与 (AGD_PRE.1) 与 (ATE_COV.1) 与 (ATE_FUN.1)
AVA 类:脆弱性评估		
AVA_VAN.5	高级的系统性脆弱性分析	(ADV_ARC.1) 与(ADV_FSP.4) 与 (ADV_IMP.1) 与 (ADV_TDS.3) 与 (AGD_OPE.1) 与 (AGD_PRE.1)与 (ATE_DPT.1)

10.2 智能卡芯片安全保证要求

10.2.1 概述

智能卡芯片需要满足表 18 中给出的安全保证要求。

表 18　安全保证要求组件

保证要求组件	组件名称
ACM_AUT.1	部分配置管理自动化
ACM_CAP.4	产生支持和接受过程
ACM_SCP.2	跟踪配置管理范围问题
ADO_DEL.2	修改监测
ADO_IGS.1	安装、生成和启动过程
ADV_FSP.2	完全定义的外部接口
ADV_HLD.2	安全加强的高层设计
ADV_IMP.1	安全功能实现的子集
ADV_INT.1	模块化
ADV_LLD.1	描述性低层设计
ADV_RCR.1	非形式化对应性论证
ADV_SPM.1	非形式化智能卡安全策略模型
AGD_ADM.1	管理者指南
AGD_USR.1	用户指南
ALC_DVS.1	安全措施标识
ALC_LCD.1	开发者定义的生命周期模型
ALC_TAT.1	明确定义的开发工具
ATE_COV.2	范围分析
ATE_DPT.1	测试：高层设计
ATE_FUN.1	功能测试
ATE_IND.2	独立性测试—抽样
AVA_MSU.2	分析确认
AVA_SOF.1	安全功能强度评估
AVA_VLA.4	高级抵抗力

TOE 的安全保证要求级别是 EAL4＋，增加了保证要求 ADV_INT.1，增强 AVA_VLA..4，增加的安全保证组件是从 EAL4 中继承而来。安全保证组件描述如下。

10.2.2　ACM_AUT.1 部分配置管理自动化

依赖组件

ADV_CAP.1　授权控制

开发者行为要素

ACM_AUT.1.1D　开发者应该使用配置管理系统。

ACM_AUT.1.2D　开发者应该提供配置管理计划。

证据内容和形式要素

ACM_AUT.1.1C　配置管理系统应该能够提供一种自动方式，通过该方式确保只能对智能卡芯片的实

现表示进行已授权的改变。

ACM_AUT.1.2C　配置管理系统应该能够提供一种自动方式来支持智能卡芯片的生成。

ACM_AUT.1.3C　配置管理计划应该描述在配置管理系统中使用的自动工具。

ACM_AUT.1.4C　配置管理计划应该描述在配置管理系统中如何使用自动工具。

评估者行为要素

ACM_AUT.1.4E　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。

10.2.3　ACM_CAP.4 产生支持和接受程序

依赖组件

ALC_DVS.1　安全措施标识

开发者行为要素

ACM_CAP.4.1D　开发者应为智能卡芯片提供一个参照号。

ACM_CAP.4.2D　开发者应使用配置管理系统。

ACM_CAP.4.3D　开发者应提供配置管理文档。

证据内容和形式要素

ACM_CAP.4.1C　智能卡芯片参照号对每个版本应是唯一的。

ACM_CAP.4.2C　应该给智能卡芯片标记上其参照号。

ACM_CAP.4.3C　配置管理文档应包括配置清单、配置管理计划和接受计划。

ACM_CAP.4.4C　配置清单应描述组成智能卡芯片的配置项。

ACM_CAP.4.5C　配置管理文档应描述对配置项进行唯一标识的方法。

ACM_CAP.4.6C　配置管理系统应唯一的标识所有配置项。

ACM_CAP.4.7C　配置管理计划应描述配置管理系统是如何使用的。

ACM_CAP.4.8C　证据应该证明配置管理系统的运作与配置管理计划相一致。

ACM_CAP.4.9C　配置管理文档应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。

ACM_CAP.4.10C　配置管理系统应提供方法保证对配置项只进行授权修改。

ACM_CAP.4.11C　配置管理系统应支持智能卡芯片的产生。

ACM_CAP.4.12C　接受计划应描述用来接受修改过的或新建的作为智能卡芯片一部分的配置项的程序。

评估者行为要素

ACM_CAP.4.1E　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。

10.2.4　ACM_SCP.2 跟踪配置管理范围问题

依赖组件

ALC_CAP.3　授权控制。

开发者行为要素

ACM_SCP.2.1D　开发者应提供配置管理文档。

证据内容和形式要素

ACM_SCP.2.1C　配置管理文档应说明配置管理系统至少能跟踪以下几项：智能卡芯片实现表示，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。

应用说明：

开发环境被定义为包括开发和制造智能卡芯片的所有的活动。

智能卡芯片的实现表示包括直接与智能卡芯片相关的以下信息：

a） 集成电路制造日期和序列号；

b） 操作软件标识和发布日期。

以下信息也是可确定的：

a） 微处理器的详细说明和制造者；

b） 存储器大小和分配(FLASH，RAM 等)；

c） 有关版图和工艺几何参数的集成电路设计的物理具体实现；

d） 集成电路的所有硬件安全特征，即它们最初是否是使能的；

e） 所有使能的硬件安全特征；

f） 软件标识和发布日期；

g） 所有软件安全特征表现，即它们最初是否是使能的；

h） 所有使能软件安全特征；

i） 工作参数，包括电压和频率范围；

j） 集成电路模块制作者和封装日期；

k） 智能卡制造者和制造日期；

l） 集成电路预个人化设备和日期。

配置管理文档应描述配置管理系统是如何跟踪配置项的。

评估者行为要素

ACM_SCP.2.1E 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。

10.2.5 ADO_DEL.2 修改检测

依赖组件

无

开发者行为要素

ACM_DEL.2.1D 开发者应将把智能卡芯片或其部分交付给用户的程序文档化。

ACM_DEL.2.2D 开发者应使用交付过程。

证据内容和形式要素

ACM_DEL.2.1C 交付文档应描述在给用户方分配智能卡芯片的版本时，用以维护安全所必需的所有程序。

ACM_DEL.2.2C 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方收到的版本之间的任何差异。

ACM_DEL.2.3C 交付文档应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付智能卡芯片。

评估者行为要素

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。

10.2.6 ADO_IGS.1 安装、生成和启动过程

依赖组件

AGD_ADM.1 管理员指南

开发者行为要素

ADO_IGS.1.1D 开发者应将智能卡芯片安全地安装、生成和启动所必要的程序文档化。

证据内容和形式要素

ADO_IGS.1.1C　文档中应描述智能卡芯片的安全安装、生成和启动所必要的步骤。

评估者行为要素

ADO_IGS.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

ADO_IGS.1.2E　评估者应确定安装、生成和启动程序最终产生了安全的配置。

10.2.7　ADV_FSP.2 完全定义的外部接口

依赖组件

ADV_RCR.1　非形式化对应性证实。

开发者行为要素

ADV_FSP.2.1D　开发者应当提供功能规范。

证据内容和形式要素

ADV_FSP.2.1C　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。

ADV_FSP.2.2C　功能规范应当是内在一致的。

ADV_FSP.2.3C　功能规范应当描述使用所有外部安全功能接口的用途与使用方法，要提供所有的影响、例外情况和错误消息的全部细节。

ADV_FSP.2.4C　功能规范应当完备地表示安全功能。

ADV_FSP.2.5C　功能规范应当包括安全功能是完备地表示的基本原理。

评估者行为要素

ADV_FSP.2.1E　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。

ADV_FSP.2.2E　评估者应决定功能规范是智能卡芯片安全功能要求的精确和完备的实例化。

10.2.8　ADV_HLD.2 安全加强的高层设计

依赖组件

ADV_FSP.1　非形式化功能规范。

ADV_RCR.1　非形式化对应性证实。

开发者行为要素

ADV_HLD.2.1D　开发者将提供安全功能的高层设计。

证据内容和形式要素

ADV_HLD.2.1C　高层设计的表示应当是非形式化的。

ADV_HLD.2.2C　高层设计应当是内在一致的。

ADV_HLD.2.3C　高层设计应当按子系统来描述安全功能的结构。

ADV_HLD.2.4C　高层设计应当描述安全功能的每个子系统所提供的安全功能。

ADV_HLD.2.5C　高层设计应当标识安全功能要求的任何基础的硬件、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。

ADV_HLD.2.6C　高层设计应当标识安全功能子系统的所有接口。

ADV_HLD.2.7C　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。

ADV_HLD.2.8C　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、例外情况和错误消息的细节。

ADV_HLD.2.9C　高层设计应当描述把智能卡芯片分成安全策略实施和其他子系统的这种分离。

评估者行为要素

ADV_HLD.2.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ADV_HLD.2.2E　评估者应当决定功能规范是智能卡芯片安全功能要求的精确且完备的示例。

10.2.9　ADV_IMP.1 安全功能实现的子集

依赖组件

ADV_LLD.1　描述性低层设计。

ADV_RCR.1　非形式化对应性证实。

ALC_TAT.1　明确定义的开发工具。

开发者行为要素

ADV_IMP.1.1D　开发者应当为所选的安全功能子集提供实现表示。

应用说明：

芯片的安全功能子集包括：

a）　与智能卡芯片物理结构相关的子集：

1）　结构大小，组成和版图；

2）　互连和数据总线版图；

3）　熔丝部位；

4）　包括防护层和封装的物理结构；

5）　FLASH 处理；

6）　RAM 存取。

b）　与智能卡芯片逻辑结构相关的子集：

1）　中断和复位功能；

2）　安全数据的检查和处理。

c）　与智能卡芯片结构不可改变性相关的子集：

序列号和其他生命周期标识。

证据内容和形式要素

ADV_IMP.1.1C　实现表示应当无歧义而且详细的定义 TSF，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。

评估者行为要素

ADV_IMP.1.1E　评估者应该确认所提供的信息满足证据的内容和形式的所有要求。

ADV_IMP.1.1E　评估者应该决定所提供的最不抽象安全功能表示是智能卡芯片安全功能要求的一个精确且完备的实例化。

10.2.10　ADV_INT.1 模块化

依赖组件

ADV_IMP.1　安全功能实现的子集。

ADV_LLD.1　描述性低层设计。

开发者行为要素

ADV_INT.1.1D　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。

ADV_INT.1.2D　开发者应当提供一种结构化描述。

证据内容和形式要素

ADV_INT.1.2C　结构化描述应当标识 TSF 的模块。
ADV_INT.1.2C　结构化描述应当描述每一个 TSF 模块的用途、接口、参数和影响。
ADV_INT.1.3C　结构化描述应当描述 TSF 设计是如何使得独立的模块之间避免不必要的交互作用。
评估者行为要素
ADV_INT.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV_INT.1.2E　评估者应该确认低层设计和实现表示都遵循结构化描述。

10.2.11　ADV_LLD.1 描述性低层设计

依赖组件
ADV_HLD.2　安全加强的高层设计。
ADV_RCR.1　非形式化对应性证实。
开发者行为要素
ADV_LLD.1.1D　开发者应当提供安全功能的低层设计。
证据内容和形式要素
ADV_LLD.1.1C　低层设计的表示应当是非形式化的。
ADV_LLD.1.2C　低层设计应当是内在一致的。
ADV_LLD.1.3C　低层设计应当以模块方式来描述安全功能。
ADV_LLD.1.4C　低层设计应当描述每个模块的用途。
ADV_LLD.1.5C　低层设计应当依据所提供的安全功能性和对其他模块的依赖性关系两方面来定义模块间的相互关系。
ADV_LLD.1.6C　低层设计应当描述每个安全策略实施功能是如何被提供的。
ADV_LLD.1.7C　低层设计应当标识安全功能模块的所有接口。
ADV_LLD.1.8C　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。
ADV_LLD.1.9C　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、例外情况和错误消息的细节。
ADV_LLD.1.10C　低层设计应当描述如何将智能卡芯片分离成安全策略实施模块和其他模块。
评估者行为要素
ADV_LLD.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV_LLD.1.2E　评估者应当决定低层设计是智能卡芯片安全功能要求的一个精确且完备的实例化。

10.2.12　ADV_RCR.1 非形式化对应性论证

依赖组件
无
开发者行为要素
ADV_RCR.1.1D　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。
证据内容和形式要素
ADV_RCR.1.1C　对于所提供的安全功能表示的每个相邻对，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且完备地细化。
评估者行为要素
ADV_RCR.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

10.2.13 ADV_SPM.1 非形式化安全策略模型

依赖组件

ADV_FSP.1 非形式化功能规范。

开发者行为要素

ADV_SPM.1.1D 开发者应提供安全策略模型。

ADV_SPM.1.2D 开发者应阐明功能规范和安全策略模型之间的对应性。

证据内容和形式要素

ADV_SPM.1.1C 安全策略模型应当是非形式化的。

ADV_SPM.1.2C 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。

ADV_SPM.1.3C 安全策略模型应当包括基本原理，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，而且是完备的。

ADV_SPM.1.4C 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，而且是完备的。

评估者行为要素

ADV_SPM.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

10.2.14 AGD_ADM.1 管理员指南

依赖组件

ADV_FSP.1 非形式化功能规范。

开发者行为要素

AGD_ADM.1.1D 开发者应当提供智能卡芯片管理员指南。

证据内容和形式要素

AGD_ADM.1.1C 管理员指南应当描述管理员可使用的管理功能和接口。

AGD_ADM.1.2C 管理员指南应当描述如何以安全的方式管理智能卡芯片。

AGD_ADM.1.3C 管理员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。

AGD_ADM.1.4C 管理员指南应当描述所有与智能卡芯片的安全运行有关的用户行为的假定。

AGD_ADM.1.5C 管理员指南应当描述所有受管理员控制的安全参数，合适时，应指明安全值。

AGD_ADM.1.6C 管理员指南应当描述每种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制的改变实体的安全特性。

AGD_ADM.1.7C 管理员指南应当与为评估所提供的其他所有文档保持一致。

AGD_ADM.1.8C 管理员指南应当为管理员描述与管理员有关的信息技术环境的所有的安全要求。

评估者行为要素

AGD_ADM.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

10.2.15 AGD_USR.1 用户指南

依赖组件

ADV_FSP.1 非形式化功能规范。

开发者行为要素

AGD_USR.1.1D 开发者应当提供用户指南。

证据内容和形式要素

AGD_USR.1.1C　用户指南应该描述智能卡芯片的非管理员用户可用的功能和接口。
AGD_USR.1.2C　用户指南应该描述智能卡芯片提供的用户可访问的安全功能的用法。
AGD_USR.1.3C　用户指南应该包含受安全处理环境中所控制的用户可访问的功能和权限的警告。
AGD_USR.1.4C　用户指南应该清楚地阐述智能卡芯片安全运行中的用户所必须负的职责，包括有关在智能卡芯片安全环境阐述中找得到的用户行为的假设。
AGD_USR.1.5C　用户指南应该与为评估提供的其他所有文档保持一致。
AGD_USR.1.6C　用户指南应该为用户描述与用户有关的信息技术环境的所有安全要求。
评估者行为要素
AGD_USR.1.1E　评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

10.2.16　ALC_DVS.1 安全措施标识

依赖组件
无
开发者行为要素
ALC_DVS.1.1D　开发者应当提供开发安全文档。
证据内容和形式要素
ALC_DVS.1.1C　开发安全文档应当描述在智能卡芯片的开发环境中，用以保护智能卡芯片的设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施。
应用说明：
开发环境被定义为包括所有的设备，也就是对智能卡芯片开发和制造所需的设备之间的运输和交付。
智能卡芯片设计和实现至少包括以下信息：

a）　设计信息：
　　1）　集成电路的详细说明和技术；
　　2）　集成电路设计；
　　3）　集成电路硬件的安全机制；
　　4）　集成电路软件的安全机制；
　　5）　光掩模；
　　6）　开发工具；
　　7）　初始化程序；
　　8）　访问控制机制；
　　9）　鉴别系统；
　　10）　数据保护系统；
　　11）　存储器分离；
　　12）　加密程序。
b）　数据：
　　1）　初始化数据；
　　2）　个人化数据；
　　3）　口令；
　　4）　加密密钥。
c）　测试信息：
　　1）　测试工具；

2） 测试程序；
3） 测试计划；
4） 测试结果。

d） 物理实例：
1） 硅样品；
2） 封装后的芯片；
3） 初始化前的智能卡；
4） 个人化前的智能卡；
5） 个人化后但未发行的智能。

开发安全文档应提供在智能卡芯片的开发和维护过程中执行安全措施的证据。

评估者行为要素

ALC_DVS.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ALC_DVS.1.2E 评估者应当确认应用了安全措施。

10.2.17 ALC_LCD.1 开发者定义的生命周期模型

依赖组件

无

开发者行为要素

ALC_LCD.1.1D 开发者应建立生命周期模型用于开发和维护智能卡芯片。

ALC_LCD.1.2D 开发者应提供生命周期定义文档。

证据内容和形式要素

ALC_LCD.1.1C 生命周期定义文档应描述用于开发和维护 TOE 的模型。

ALC_LCD.1.2C 生命周期模型应提供对智能卡芯片开发和维护的必要的控制。

评估者行为要素

ALC_LCD.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

10.2.18 ALC_TAT.1 明确定义的开发工具

依赖组件

ADV_IMP.1 安全功能实现的子集。

开发者行为要素

ALC_TAT.1.1D 开发者应描述用于开发智能卡芯片的工具。

ALC_TAT.1.2D 开发者应以文档的形式描述已选择的依赖实现的开发工具的选项。

证据内容和形式要素

ALC_TAT.1.1C 所有用于实现的开发工具都应有明确定义。

ALC_TAT.1.2C 开发工具文档应无歧义地定义实现中的每个语句的含义。

ALC_TAT.1.3C 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。

评估者行为要素

ALC_TAT.1.1E 评估者应确认所提供的信息都满足证据的内容和形式的所有要求。

10.2.19 ATE_COV.2 范围分析

依赖组件

ADV_FSP.1　非形式化功能规范。
ATE_FUN.1　功能测试。
开发者行为要素
ATE_COV.2.1D　开发者应提供对测试覆盖范围的分析。
证据内容和形式要素
ATE_COV.2.1C　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。
ATE_COV.2.2C　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。
评估者行为要素
ATE_COV.2.1E　评估者应确认提供的信息满足证据的内容和形式的要求。

10.2.20　ATE_DPT.1 测试：高层设计

依赖组件
ADV_HLD.1　描述性高层设计。
ATE_FUN.1　功能测试。
开发者行为要素
ATE_DPT.1.1D　开发者将提供对测试深度的分析。
证据内容和形式要素
ATE_DPT.1.1C　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。
评估者行为要素
ATE_DPT.1.1E　评估者应当确定提供的信息满足证据的内容和形式的要求。

10.2.21　ATE_FUN.1 功能测试

依赖组件
无
开发者行为要素
ATE_FUN.1.1D　开发者应当测试安全功能，并文档化结果。
ATE_FUN.1.1D　开发者应提供测试文档。
证据内容和形式要素
ATE_FUN.1.1C　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。
ATE_FUN.1.2C　测试计划应当标识要测试的安全功能，描述要执行的测试目标。
ATE_FUN.1.3C　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他测试结果的顺序依赖性。
ATE_FUN.1.4C　期望的测试结果应当表明成功测试运行后的预期输出。
ATE_FUN.1.5C　开发者执行的测试的结果应当论证了每个被测试的安全性功能按照规定进行运作了。
评估者行为要素
ATE_FUN.1.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

10.2.22 ATE_IND.2 独立性测试—抽样

依赖组件

ADV_FSP.1 非形式化功能规范。

AGD_ADM.1 管理员指南。

AGD_USR.1 用户指南。

ATE_FUN.1 功能测试。

开发者行为要素

ATE_IND.2.1D 开发者要提供被测试的智能卡芯片。

证据内容和形式要素

ATE_IND.2.1C 智能卡芯片要与测试相适应。

ATE_IND.2.2C 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。

评估者行为要素

ATE_IND.2.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

ATE_IND.2.2E 评估者应当适当测试一个安全功能子集，以确认智能卡芯片按照规范运行。

ATE_IND.2.3E 评估者应抽样执行测试文档里的测试样本，以验证开发者测试的结果。

10.2.23 AVA_MSU.2 分析确认

依赖组件

ADO_IGS.1 安装、生成和启动过程。

ADV_FSP.1 非形式化功能规范。

AGD_ADM.1 管理员指南。

AGD_USR.1 用户指南。

开发者行为要素

AVA_MSU.2.1D 开发者应提供指导性文档。

AVA_MSU.2.2D 开发者应当文档化对指导性文档的分析。

证据内容和形式要素

AVA_MSU.2.1C 指导性文档应该确定对智能卡芯片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。

AVA_MSU.2.2C 指导性文档应该是完整的、清晰的、一致的、合理的。

AVA_MSU.2.3C 指导性文档应该列出所有对目标环境的假定。

AVA_MSU.2.4C 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。

AVA_MSU.2.5C 分析文档应该论证指导性文档是完备的。

评估者行为要素

AVA_MSU.2.1E 评估者应当确认提供的信息满足证据的内容和形式的所有要求。

AVA_MSU.2.2E 评估者应该重复所有配置与安装过程以及其他选择性过程，以确认只使用所提供的指导性文档就可以让智能卡芯片安全配置和使用。

AVA_MSU.2.3E 评估者应该决定使用指导性文档能检测到所有不安全状态。

AVA_MSU.2.4E 评估者应该决定分析文档说明了对于智能卡芯片的所有运行方式提供了安全运行指南。

10.2.24 AVA_SOF.1 安全功能强度评估

依赖组件

ADV_FSP.1 非形式化功能规范。

ADV_HLD.1 描述性高层设计。

开发者行为要素

AVA_SOF.1.1D 开发者应对 ST 中标识的具有安全功能强度的安全机制进行智能卡芯片安全功能强度的分析。

证据内容和形式要素

AVA_SOF.1.1C 对于具有安全功能强度申明的安全机制，智能卡芯片安全功能强度分析应说明该机制达到或超过 PP/ST 定义的最低强度。

AVA_SOF.1.2C 对于具有特定安全功能强度申明的安全机制，智能卡芯片安全功能强度分析应证明该机制达到或超过 PP/ST 定义的特定功能强度。

评估者行为要素

AVA_SOF.1.1E 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_SOF.1.2E 评估者应确认强度声明是正确的。

10.2.25 AVA_VLA.4 高级抵抗力

依赖组件

ADV_FSP.1 非形式化功能规范。

ADV_HLD.2 安全加强的高层设计。

ADV_IMP.1 安全功能实现的子集。

ADV_LLD.1 描述性低层设计。

AGD_ADM.1 管理员指南。

AGD_USR.1 用户指南。

开发者行为要素

AVA_VLA.4.1D 开发者应当分析智能卡芯片可交付材料，以寻找用户违反智能卡芯片安全策略的途径，并将分析结果文档化。

AVA_VLA.4.2D 开发者应当文档化已表示的脆弱性的分布。

证据内容和形式要素

AVA_VLA.4.1C 对所有已标识的脆弱性，文档应当能说明在所期望的智能卡芯片环境中无法利用这些脆弱性。

AVA_VLA.4.2C 文档应当证明对于已标识脆弱性的智能卡芯片可以抵御明显的穿透性攻击。

AVA_VLA.4.3C 证据应当能说明对脆弱性的搜索是系统化的。

AVA_VLA.4.4C 分析文档应当提供完备地分析表述 TOE 可交付材料的证明。

评估者行为要素

AVA_VLA.4.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

AVA_VLA.4.2E 评估者应当在开发方脆弱性分析的基础上实施穿透性测试，确保已经表述了标识明显的脆弱性。

AVA_VLA.4.3E 评估者应当实施独立的脆弱性分析。

AVA_VLA.4.4E 基于独立的脆弱性分析，评估者将应当实施独立的穿透性测试以决定在所期望环境

下额外标识的脆弱性的可利用性。

AVA_VLA.4.5E 评估者应当决定可以抵御具有中等攻击潜力的攻击者发起的对智能卡芯片的穿透性攻击。

10.3 开发过程

10.3.1 ADV_ARC.1 安全架构描述

依赖组件

ADV_FSP.1 完全功能规范。

ADV_TDS.1 基本设计。

开发者行为要素

ADV_ARC.1.1D 开发者应当设计和实现 TOE，以便 TSF 的安全特征不能被旁路。

ADV_ARC.1.2D 开发者应当设计和实现 TSF，以便它能够保护自己不受到非信任的主动体的篡改。

ADV_ARC.1.3D 开发者应当提供 TSF 的安全架构描述。

证据内容和形式要素

ADV_ARC.1.1C 安全架构描述的详细程度应当与 TOE 设计文档中所提取的 SFR 执行的描述是相当的。

ADV_ARC.1.2C 安全架构描述应当描述与 SFR 相对应的 TSF 所提供的安全域。

ADV_ARC.1.3C 安全架构描述应当描述 TSF 初始化过程是如何可靠的。

ADV_ARC.1.4C 安全架构描述应当论证 TSF 保护自己不受到篡改。

ADV_ARC.1.5C 安全架构描述应当论证 TSF 阻止 SFR 执行功能性的旁路。

评估者行为要素

ADV_ARC.1.1E 评估者应当确认所提供的信息满足证据的内容和形式的所有要求。

10.3.2 ADV_FSP.4 完全功能规范

依赖组件

ADV_TDS.1 基本设计。

开发者行为要素

ADV_FSP.4.1D 开发者应当提供功能规范。

ADV_FSP.4.2D 开发者应当提供由功能规范可追溯到 SFR。

证据内容和形式要素

ADV_FSP.4.1C 功能规范应当完备地表示 TSF。

ADV_FSP.4.2C 功能规范应当描述所有 TSFI 的用途与使用方法。

ADV_FSP.4.3C 功能规范应当描述与每一个 TSFI 相关的所有参数。

ADV_FSP.4.4C 功能规范应当描述与每一个 TSFI 相关的所有行为。

ADV_FSP.4.5C 功能规范应当描述由每一个 TSFI 引起的所有直接的错误消息。

ADV_FSP.4.6C 功能规范应当论证 SFR 能够追朔 TSFI。

评估者行为要素

ADV_FSP.4.1E 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。

ADV_FSP.4.2E 评估者应决定功能规范是 SFR 的一个精确且完备的实例化。

10.3.3 ADV-IMP.1 TSF 的实现表示

依赖组件

ADV-TDS.3　基本模块设计。
ALC-TAT.1　明确定义的开发工具。
开发者行为要素
ADV-IMP.1.1D　开发者应当为整个 TSF 提供实现表示。
ADV-IMP.1.2D　开发者应当为 TOE 设计描述与实现表示的样品之间提供一个映射关系。
证据内容和形式要素
ADV_IMP.1.1C　实现表示应当详细地定义 TSF，使得无须进一步设计就能生成 TSF。
ADV_IMP.1.2C　实现表示应当以开发人员使用的形式。
ADV_IMP.1.3C　TOE 设计描述与实现表示的样品之间的映射关系应当论证它们之间的对应性。
评估者行为要素
ADV_IMP.1.1E　评估者应当确认来源于被选择的实现表示的样品，以及提供的信息满足证据的内容和形式的所有要求。

10.3.4　ADV_TDS.3 基本模块设计

依赖组件
ADV_FSP.4　完全功能规范。
开发者行为要素
ADV_TDS.3.1D　开发者应当提供 TOE 设计。
ADV_TDS.3.2D　开发者应当为功能规范的 TSFI 与设计中不可再分解的模块之间提供一个映射关系。
证据内容和形式要素
ADV_TDS.3.1C　模块设计应当描述子系统的结构。
ADV_TDS.3.2C　模块设计应当描述模块的 TSF。
ADV_TDS.3.3C　模块设计应当识别 TSF 的所有子系统。
ADV_TDS.3.4C　模块设计应当提供 TSF 的每个子系统的描述。
ADV_TDS.3.5C　模块设计应当提供 TSF 的所有子系统之间的相互作用。
ADV_TDS.3.6C　模块设计应当提供 TSF 的子系统与模块之间的映射关系。
ADV_TDS.3.7C　模块设计应当描述每一个 SFR 执行模块的目的和与其他模块的关系。
ADV_TDS.3.8C　模块设计应当描述每一个 SFR 执行模块的接口，从接口的返回值，与其他模块的相互作用以及与其他 SFR 执行模块之间的接口。
ADV_TDS.3.9C　模块设计应当描述每一个支持的 SFR 或 SFR 非妨碍模块的目的以及与其他模块之间的相互作用。
ADV_TDS.3.10C　映射关系应当论证所有 TSFI 可以追朔 TOE 设计文档中描述的行为。
评估者行为要素
ADV_TDS.3.1E　评估者应当确认所提供的信息满足证据的内容和形式的所有要求。
ADV_TDS.3.2E　评估者应当决定设计文档是安全功能要求的一个精确且完备的实例化。

10.4　指导性文档

10.4.1　AGD_OPE.1 用户指南

依赖组件
ADV-FSP.1　基本功能规范。

开发者行为要素

AGD_OPE.1.1D　开发者应当提供用户指南。

证据内容和形式要素

AGD_OPE.1.1C　用户指南应当描述每一个用户角色，以及受安全处理环境中所控制的用户可访问的功能和权限的警告。

AGD_OPE.1.2C　用户指南应当描述每一个用户角色如何以安全的方式使用可用接口。

AGD_OPE.1.3C　用户指南应当描述每一个用户角色可用的功能和接口，特别是所有受用户控制的安全参数，合适时，应指明安全值。

AGD_OPE.1.4C　用户指南应当描述每一种与需要执行的用户可用功能有关的安全相关事件，包括改变 TSF 所控制的实体的安全特性。

AGD_OPE.1.5C　用户指南应当识别 TOE 的所有可操作的模块，它们的结果和维持安全操作的含义。

AGD_OPE.1.6C　用户指南应当描述每一个用户角色的安全措施，以履行 ST 中描述的可操作环境的安全目的。

AGD_OPE.1.7C　用户指南应当清晰、合理。

评估者行为要素

AGD_OPE.1.1E　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。

10.4.2　AGD_PRE.1 预备程序

依赖关系

无

开发者行为要素

AGD_PRE.1.1D　开发者应当提供包含预备程序的 TOE。

证据内容和形式要素

AGD_PRE.1.1C　预备程序应当描述被交付的 TOE 的所有必须的步骤，并且与开发者交付程序保持一致。

AGD_PRE.1.2C　预备程序应当描述 TOE 安装的所有必须的步骤，并且与 ST 中描述的可操作环境的安全目的保持一致。

评估者行为要素

AGD_PRE.1.1E　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。

AGD_PRE.1.2E　评估者应提供预备程序，以确认 TOE 为了操作能够被安全地准备。

10.5　生命周期支持

10.5.1　ALC_CMC.4 产品支持，接受程序和自动化

依赖组件

ALC_CMS.1　TOE CM 范围。

ALC_DVS.1　安全措施的识别。

ALC_LCD.1　生命周期模型中定义的开发者。

开发者行为要素

ALC_CMC.4.1D　开发者应当提供 TOE 和 TOE 的参照号。

ALC_CMC.4.2D　开发者应当提供 CM 文档。

ALC_CMC.4.3D　开发者应当使用 CM 系统。

证据内容和形式要素

ALC_CMC.4.1C　TOE 应当被标记上唯一的参照号。

ALC_CMC.4.2C　CM 文档应当描述用以唯一标识配置项的方法。

ALC_CMC.4.3C　CM 系统应当唯一标识所有配置项。

ALC_CMC.4.4C　CM 系统应当提供一种自动方式，通过该方式确保只能对 TOE 的实现表示进行已授权的改变。

ALC_CMC.4.5C　CM 系统应当提供一种自动方式来支持 TOE 的生成。

ALC_CMC.4.6C　CM 文档应当包括 CM 计划。

ALC_CMC.4.7C　CM 计划应当描述在 CM 系统中如何使用自动工具。

ALC_CMC.4.8C　CM 计划应当描述一个程序，用于被授权修改或者作为 TOE 一部分的最新建立的配置项。

ALC_CMC.4.9C　证据应当论证所有的配置项被 CM 系统支撑着。

ALC_CMC.4.10C　证据应当论证 CM 系统遵循 CM 计划被操作。

评估者行为要素

ALC_CMC.4.1E　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。

10.5.2　ALC_CMS.4 问题追踪 CM 范围

依赖关系

无

开发者行为要素

ALC_CMS.4.1D　开发者应当提供一个配置清单。

证据内容和形式要素

ALC_CMS.4.1C　配置清单应当包括：TOE；SAR 的评估证据；TOE 的组成部分；实现表示；安全缺陷报告和解决状况。

ALC_CMS.4.2C　配置清单应当唯一地标识配置项。

ALC_CMS.4.3C　对于每一个 TSF 相关的配置项，配置清单应当指出配置项的开发者。

评估者行为要素

ALC_CMS.4.1E　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。

10.5.3　ALC_DEL.1 交付过程

依赖关系

无

开发者行为要素

ALC_DEL.1.1D　开发者应将把 TOE 及其部分交付给用户的程序文档化。

ALC_DEL.1.2D　开发者应使用交付程序。

证据内容和形式要素

ALC_DEL.1.1C　交付文档应描述，在给用户方分配 TOE 的版本时，用以维护安全所必须的所有程序。

评估者行为要素

ALC_DEL.1.1E　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。

10.5.4　ALC_DVS.2 安全措施的充分性

依赖关系

无

开发者行为要素

ALC_DVS.2.1D　开发者应当生成并提供开发安全文档。

证据的内容和形式要素

ALC_DVS.2.1C　开发安全文档应描述在 TOE 的开发环境中，用以保护 TOE 设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施。

ALC_DVS.2.2C　开发安全文档应证明安全措施提供必要的保护级以维护 TOE 的保密性和完整性。

评估者行为要素

ALC_DVS.2.1E　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。

ALC_DVS.2.2E　评估者应确认应用了安全措施。

10.5.5　ALC_LCD.1 开发者定义的生命周期模型

依赖组件

无

开发者行为要素

ALC_LCD.1.1D　开发者应建立生命周期模型用于开发和维护 TOE。

ALC_LCD.1.2D　开发者应提供生命周期定义文档。

证据内容和形式要素

ALC_LCD.1.1C　生命周期定义文档应描述用于开发和维护 TOE 的模型。

ALC_LCD.1.2C　生命周期模型应提供对 TOE 开发和维护所必要的控制。

评估者行为要素

ALC_LCD.1.1E　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。

10.5.6　ALC_TAT.1 明确定义的开发工具

依赖组件

ADV_IMP.1　TSF 的实现表示。

开发者行为要素

ALC_TAT.1.1D　开发者应提供文档以标识用于开发 TOE 的工具。

ALC_TAT.1.2D　开发者应文档化已选择的依赖实现的开发工具的选项。

证据内容和形式要素

ALC_TAT.1.1C　所有用于实现的开发工具都应有明确定义。

ALC_TAT.1.2C　开发工具文档应无歧异地定义实现中每个语句的含义。

ALC_TAT.1.3C　开发工具文档应无歧异地定义所有基于实现的选项的含义。

评估者行为要素

ALC_TAT.1.1E　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。

10.6　测试过程

10.6.1　ATE_COV.2 范围分析

依赖组件

ADV_FSP.2　安全执行的功能规范。

ATE_FUN.1　功能测试。

开发者行为要素

ATE_COV.2.1D　开发者应当提供测试范围分析。

证据内容和行为要素

ATE_COV.2.1C　测试范围分析应当论证测试文档中标识的测试和功能规范中所描述的 TSFI 之间的对应性。

ATE_COV.2.2C　测试范围分析应当论证功能规范中所描述的所有 TSFI 已被测试。

评估者行为要素

ATE_COV.2.1E　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。

10.6.2　ATE_DPT.1 测试：基本设计

依赖组件

ADV_ARC.1　安全架构描述。

ADV_TDS.2　架构设计。

ATE_FUN.1　功能测试。

开发者行为要素

ATE_DPT.1.1D　开发者应当提供测试深度分析。

证据内容和形式要素

ATE_DPT.1.1C　深度分析应当论证测试文档中所标识的测试和 TOE 设计文档中子系统之间的对应性。

ATE_DPT.1.2C　深度分析应当论证 TOE 设计文档中所描述的所有子系统已被测试。

评估者行为要素

ATE_DPT.1.1E　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。

10.6.3　ATE_FUN.1 功能测试

依赖组件

ATE_COV.1　范围证据

开发者行为要素

ATE_FUN.1.1D　开发者应当测试 TSF，并文档化结果。

ATE_FUN.1.2D　开发者应提供测试文档。

证据内容和形式要素

ATE_FUN.1.1C　测试文档应当包括测试计划、预期的测试结果和实际的测试结果。

ATE_FUN.1.2C　测试计划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他测试结果的顺序依赖性。

ATE_FUN.1.3C　预期的测试结果应当表明成功测试运行后的预期输出。

ATE_FUN.1.4C　实际的测试结果与预期的测试结果是一致的。

评估者行为要素

ATE_FUN.1.1E　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。

10.6.4　ATE_IND.2 独立性测试——抽样

依赖组件

ADV_FSP.2　安全执行的功能规范。

AGD_OPE.1　用户指南。
AGD_PRE.1　预备程序。
ATE_COV.1　范围证据。
ATE_FUN.1　功能测试。
开发者行为要素
ATE_IND.2.1D　开发者应当提供用于测试的 TOE。
证据内容和形式要素
ATE_IND.2.1C　TOE 应与测试相适应。
ATE_IND.2.2C　开发者应提供一个与开发者的 TSF 功能测试中使用的资源相当的集合。
评估者行为要素
ATE_IND.2.1E　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。
ATE_IND.2.2E　评估者应抽样执行测试文档里的测试样本，以验证开发者测试的结果。
ATE_IND.2.3E　评估者应当适当测试一个 TSF 子集，以确认 TOE 相应的按照规范运行。

10.7　脆弱性评估

AVA_VAN.5 高级系统化地脆弱性分析
依赖组件
ADV_ARC.1　安全架构描述。
ADV_FSP.4　完全功能规范。
ADV_TDS.3　基本模块设计。
ADV_IMP.1　TSF 的实现表示。
AGD_OPE.1　操作用户指南。
AGD_PRE.1　预备程序。
ATE_DPT.1　测试：基本设计。
开发者行为要素
AVA_VAN.5.1D　开发者应当提供用于测试的 TOE。
证据内容和形式要素
AVA_VAN.5.1C　TOE 应与测试相适应。
评估者行为要素
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　评估者应执行公开领域来源的搜索已标识 TOE 潜在的脆弱性。
AVA_VAN.5.3E　评估者应针对指导文档、功能规范、TOE 设计、安全架构描述和实现表示中被标识的脆弱性，执行独立的、系统化的测试。
AVA_VAN.5.4E　评估者应当基于已标识的潜在脆弱性的基础上实施穿透性测试，以决定 TOE 有能力抵抗具有高攻击潜力的攻击者的攻击。

10.8　安全保证要求对应关系

表 19 是安全保证要求与安全目的的对应关系。

表 19　安全保证要求与安全目的的对应关系

安全保证要求	对应的安全目的
ACM_AUT.1	O.Ident
ACM_CAP.4	O.Ident
ACM_SCP.2	O.Ident
ADO_IGS.1	EAL4 的要求
ADV_FSP.2	EAL4 的要求
ADV_HLD.2	EAL4 的要求
ADV_IMP.1	O.Log_Prot,O.Set_Up,O.Life_Cycle
ADV_INT.1	O.IT_Std
ADV_LLD.1	EAL4 的要求
ADV_RCR.1	EAL4 的要求
ADV_SPM.1	EAL4 的要求
AGD_ADM.1	EAL4 的要求
AGD_USR.1	EAL4 的要求
ALC_DVS.1	OE.Init_Acs, O.Life_Man
ALC_LCD.1	O.IT_Std ,O.Life_Man
ALC_TAT.1	O.IT_Std ,O.Life_Man
ATE_COV.2	EAL4 的要求
ATE_DPT.1	EAL4 的要求
ATE_FUN.1	EAL4 的要求
ATE_IND.2	EAL4 的要求
AVA_MSU.2	EAL4 的要求
AVA_SOF.1	EAL4 的要求
AVA_VLA.3	O.Log_Prot,O.I_Leak,O.Flt_Ins,O.Search,O.Life_Cycle, O.Unlink
FCS_CKM.2	O.Crypt
FCS_CKM.4	O.Crypt

O.Log_Prot 是当检测到潜在的侵害时 FAU_ARP.1 提供一个响应。当包含信息的资源不再使用时 FDP_RIP.1 对信息提供保护。在失败情况下 FPT_FLS.1 和 FPT_RCV.4 提供可接收的安全操作。FPT_RVM.1 连同 FPT_SEP.1 使智能卡芯片安全功能提供必要的分离和保护以保证要求的智能卡芯片安全策略能够成功执行。ADV.IMP.1 为智能卡芯片针对逻辑攻击所执行的特殊抵抗所选子集提供回顾和评估,同时 AVA_VLA.3 回顾了已确定的缺陷,包括那些涉及关于智能卡芯片的逻辑操作。

O.I_Leak 是由 FPT_PHP.3 通过智能卡芯片用来掩饰这些泄露所采取的行动得到部分的保证。另外一部分由 AVA_VLA.3 确保。此安全目的回顾了已确定的缺陷,包括那些涉及来自智能卡芯片的信息泄露。

O.Init 是当包含信息的资源不再使用时,FDP_RIP.1 提供对信息的保护,它对几乎所有即时运行

参数提供保护。FPT_RCV.4 在错误发生时提供可接收的安全操作。

O.Flt_Ins 是由 FDP_ACC.1 和 FDP_IFC.1 中定义的访问控制安全功能策略和信息路程序控制安全功能策略保证，同时在 FDP_ACF.1 和 FDP_IFF.1 中详细地进行了阐述。FDP_ITC.1 明确陈述了对接收数据的要求。此安全目的由 AVA_VLA.3 确保，它回顾了已确定的缺陷，包括那些涉及对智能卡芯片的逻辑探测。

O.Set_Up 是由 FDP_ACC.1 中定义的访问控制安全功能策略提供保证，同时 FDP_ACF.1 进行了详细描述。这些要求在智能卡芯片中的执行由 ADV_IMP.1 确保，特别是在第一次使用指示的执行时。

O.DAC 是由 FDP_ACF.1 和 FDP_IFF.1 设置了基本规则通过在 FDP_ACC.1 和 FDP_IFC.1 指定的访问控制安全功能策略和信息流程控制安全功能策略。用户数据的输入输出是由 FDP_ETC.1 和 FDP_ITC.1 控制的。

O.D_Read 是由 FDP_ITT.1 确保，当用户数据基于访问控制安全功能策略和智能卡信息流程控制安全功能策略中所描述的策略在智能卡芯片的各个部分间传递时，FDP_ITT.1 为用户数据提供一种避免泄露的保护方式。FPT_ITT.1 更进一步特别保护了智能卡芯片安全功能数据免遭泄露。此安全目的也被 AVA_VLA.3 确保，AVA_VLA.3 回顾了确定的缺陷，包括那些对智能卡芯片的探测。

O.Life_Cycle 是由 FDP._IFF.1 和在 FDP_IFC.1 中定义的信息流程控制安全功能策略的规范提供保证。FPT_SEP.1 为测试模式的功能和运行模式的功能在智能卡芯片安全功能方面提供必须的分离以便智能卡芯片安全策略能够成功执行。在智能卡芯片中这些要求的执行是通过 ADV_IMP.1 和 AVA_VLA.3 回顾了已确定的缺陷，包括那些设计已定义临界条件之外的操作和对所有逻辑指令的安全响应的确保来保证的。

O.Phys_Prot 是通过智能卡芯片针对物理攻击的相应由 FPT_PHP.3 部分保证。此外的覆盖由要求 ADV_IMP.1 和 AVA_VLA.3 提供。ADV_IMP.1 为智能卡芯片针对物理攻击所执行的特殊抵抗所选子集提供回顾和评估，AVA_VLA.3 回顾了已确定的缺陷，包括那些涉及关于 IC 的解构和操作。

O.Crypt 是由 FCS_COP.1 提供保证，它从用于产生和确认相关保密信息的 FCS_CKM.2 和 FCS_CKM.4 处得到支持。

O.Unlink 是由 FDP_ACF.1 和 FDP_IFF.1 通过在 FDP_ACC.1 和 FDP_IFC.1 中定义的访问控制安全功能策略和信息流程控制安全功能策略位数据的访问设置基本的规则。用户数据的输出通过 FDP_ETC.1 被控制。

O.Ident 是由 FAU_SAS.1 保证，保存一些用于智能卡芯片认证的与审计相关的信息。另外的覆盖由保证要求 ACM_CAP.4 提供，它要求开发者描述并保持那些用于唯一确定配置项的方法，这些方法包括智能卡芯片本身。此目的更进一步地由 ADV_IMP.1 支持，特别在序列号和其他一些生命周期标志符的使用时。

O.Env_Strs 是由 FPT_PHP.3 和 FPT_FLS.1 保证。此安全目的由 AVA_VLA.3 确保。这个要求回顾了已确定的缺陷，包括那些涉及在定义运行临界之外的操作。

O.Sec_Com 是由 FDP_ETC.1 和 FDP_ITC.1 提供了一种控制信息的方法，这些信息能够通过强制执行访问控制安全功能策略和信息流控制安全功能策略进行交换。

OE.Key_Supp 是一个针对智能卡芯片非 IT 环境的目的用来为智能卡芯片提供密钥支持。它由 FCS_CKM.2 和 FCS_CKM.4 保证。这些要求确保了密钥的分配和销毁以一种可接受的安全方式被完成。这些要求设计的密钥是那些在运行的智能卡芯片中存在的密钥。这些密钥可能被伪造或在智能卡芯片的安全的加密操作是必要的。应该注意到也许会有额外的要求针对非 IT 环境中基于加密密钥的产生，加密操作和其他密码功能。这些，在 A.Key_Supp 之中包含的都是假设存在的。

参 考 文 献

[1] AIS31 A proposal for:Functionality classes and evaluation methodologyfor true (physical) random number generators, Version 3.1, 25.09.2001

[2] AIS31 A proposal for: Functionality classes for random number generators,Version 2.0, September 18, 2011

[3] JCVM222 Java Card Platform Virtual Machine Specification,Version 2.2.2,March 2006. Sun Microsystems, Lnc.

[4] JCRE222 Java Card Platform Runtime Environment Specification,Version 2.2.2,March 2006. Sun Microsystems, Lnc.

[5] JCAPI222 Java Card Platform Application Programming Interface,Version 2.2.2,March 2006. Sun Microsystems, Lnc.

[6] GPCSRS GlobalPlatform Card Security Requirements Specification, Version 1.0, May 2003

[7] GP-SE GlobalPlatform Card—Secure Element Configuration, Version 1.0,October 2012

[8] GP-UICC GlobalPlatformCard,UICC Configuration , Version 1.0.1, January 2011

[9] GP-AmdA GlobalPlatformCard Confidential Card Content Management, Card specification v2.2—Amendment A, Version 1.0.1,January 2011

[10] GP-AmdB GlobalPlatformCard, Remote Application Management over HTTP, Card Specification v 2.2—Amendment B, v1.1.1,March 2012

[11] GP-AmdC GlobalPlatformCard, Contactless Service, Card Specification v2.2—Amendment A, Version 1.0.1,February 2012

[12] PP-JCS Java Card System Protection Profile—Open Configuration,Version 2.6, April 2010. ANSSIPP/0304

[13] TS102.225 ETSI 3GPP TS 102.225 Smart Cards,Secured packet structure for UICC based applications, Release 6

[14] ANSI X9.52:1998 Triple Data Encryption Algorithm Modes of Operation

[15] AIS31:2001 Functionality Classes and Evaluation Methodology for Physical Random Number Generators

[16] FIPS PUB 46-2:1993 Date Encruption Standard

[17] FIPS PUB 46-3:1999 Date Encruption Standard

[18] PKCS#1.5 RSA Encryption

[19] PKCS#3 Diffie—Hellman Key—Agreement Standard