

ICS 33.060.99

M 36



中华人民共和国通信行业标准

YD/T 2501-2013

手机支付 智能卡和内置安全模块安全技术要求

Mobile payment
Technical requirements for
UICC and embedded security element security

2013-04-25 发布

2013-04-25 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	III
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 智能卡和内置安全模块安全技术要求概述	3
4.1 概述	3
4.2 安全架构	4
4.3 内置安全模块安全要求	4
5 芯片安全技术要求	4
5.1 基本安全要求	4
5.2 密码算法安全要求	4
5.3 密钥安全保护要求	5
5.4 固件安全要求	6
5.5 对芯片攻击的削弱与防护要求	6
5.6 芯片的生命周期保证要求	7
6 卡上操作系统 COS 安全要求	8
6.1 导入	8
6.2 存储	8
6.3 安全状态	8
6.4 认证	8
6.5 命令	8
7 数据安全要求	8
7.1 数据存储安全要求	8
7.2 数据传输安全要求	9
7.3 数据安全恢复要求	9
8 访问控制安全要求	9
8.1 卡片系统对数据的访问控制安全要求	9
8.2 基于安全属性的访问控制安全要求	9
8.3 文件访问控制安全要求	10
8.4 特殊数据访问要求	10
8.5 智能卡访问控制口令的特征	10
9 多应用管理安全要求	10

9.1 智能卡对多应用管理安全规范的支持.....	10
9.2 智能卡的多应用生命周期的安全要求.....	10
9.3 安全域管理.....	11
9.4 安全域密钥管理.....	12
9.5 应用管理.....	18
9.6 智能卡和远程管理服务器之间的通信的安全要求.....	19

前 言

本标准按照 GB/T 1.1-2009给出的规则编写。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准主要依据手机支付系列相关标准制订，并结合国内外智能卡制造商的安全技术方案。

本标准是手机支付系列标准之一。该系列标准的名称预计如下：

- 1、手机支付 术语和定义
- 2、手机支付 总体技术要求
- 3、手机支付 基于13.56MHz近场通信技术的移动终端技术要求
- 4、手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块技术要求
- 5、手机支付 基于2.45GHz射频技术的智能卡技术要求
- 6、手机支付 基于 13.56MHz 近场通信技术的非接触式销售点终端技术要求
- 7、手机支付 基于2.45GHz射频技术的非接触式销售点终端技术要求
- 8、手机支付 基于 13.56MHz 和 2.45GHz 双频的非接销售点终端技术要求
- 9、手机支付 基于13.56MHz 近场通信技术的非接触式射频接口技术要求
- 10、手机支付 基于2.45GHz 射频技术的非接触式射频接口技术要求
- 11、手机支付 智能卡和内置安全模块安全技术要求
- 12、手机支付 移动终端安全技术要求
- 13、手机支付 多应用管理技术要求
- 14、手机支付 基于13.56MHz近场通信技术的移动终端测试方法
- 15、手机支付 基于13.56MHz近场通信技术的智能卡和内置安全模块测试方法
- 16、手机支付 基于2.45GHz射频技术的智能卡测试方法
- 17、手机支付 基于13.56MHz近场通信技术的非接触式销售点终端测试方法
- 18、手机支付 基于2.45GHz射频技术的非接触式销售点终端测试方法
- 19、手机支付 基于13.56MHz和2.45GHz的双频非接销售点终端测试方法
- 20、手机支付 基于13.56MHz的非接触式射频接口测试方法
- 21、手机支付 基于2.45GHz的非接触式射频接口测试方法
- 22、手机支付 智能卡和内置安全模块安全测试方法
- 23、手机支付 移动终端安全测试方法
- 24、手机支付 多应用管理测试方法

本标准由网络互联互通技术标准工作组提出。

本标准由中国通信标准化协会归口。

本标准起草单位：工业和信息化部电信研究院、中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团公司。

本标准主要起草人：孙宇涛、潘 娟、袁 琦、戴任飞、李 琳、俞海宏、赵尽晖、乐祖晖、马 丽。

手机支付

智能卡和内置安全模块安全技术要求

1 范围

本标准规定了手机支付智能卡和内置安全模块安全技术要求,包括芯片安全技术要求、卡上操作系统 COS 安全技术要求、数据安全技术要求、访问控制安全技术要求、多应用管理安全技术要求等。

本标准适用于支持手机支付业务的智能卡和内置安全模块设备。

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,仅所注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ETSI TS 102 225 智能卡:基于UICC应用的安全包结构

ETSI TS 102 226 智能卡:基于UICC应用的远程APDU结构

Global Platform Card Specification V2.2 全球平台卡片规范V2.2版本

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件:

3.1.1

安全芯片 Security IC

实现了一种或多种密码算法,直接或间接地使用密码技术来保护密钥或敏感信息安全的集成电路,包括集成电路硬件实体及依附于该硬件实体运行的固件。

3.1.2

版图 Layout

在一定工艺条件下,依据相关设计规则,为实现集成电路功能和性能要求而设计出的一套多层次几何图形,包含电路中每个元器件的图形结构和尺寸,以及元器件相互间的位置和连接等物理信息。

3.1.3

错误诱导攻击 Fault Attack

在外界干扰下,安全芯片的运算过程中可能出现硬件故障或运算错误,利用这些故障行为或错误信息分析和破译密码算法的各种有效信息的一种攻击方式。

3.1.4

固件 Firmware

固化在芯片硬件里的嵌入式软件。

3.1.5

接口 Interface

安全芯片的输入点或输出点,该点为表征物理信号的逻辑信息流提供了进入模块的入口。

3.1.6

逻辑接口 Logic Interface

相对物理接口而言，能够实现数据交换功能但在物理上不存在、需要通过配置来建立的接口。

3.1.7**能耗攻击 Power Attack**

通过采集安全芯片在进行密码运算时产生的能量消耗信息，利用密码学、统计学等原理分析和破译密码算法的各种有效信息的一种攻击方式。

3.1.8**凭证 Receipt**

凭证为由智能卡提供的经过加密的数据，用于作为已经发生的智能卡托管操作的证据。

3.1.9**显式选择 Explicit Selection**

显式选择是通过在SELECT命令中指定要选择的应用的AID，或者在SELECT FILE命令中指定要选择的文件的FID，然后将SELECT或者SELECT FILE命令发送给智能卡以选择对应的应用或者文件。

3.1.10**时序攻击 Timing Attack**

根据密码算法在安全芯片中运行时的执行时间差异，分析和破译密码算法的各种有效信息的一种攻击方式。

3.1.11**物理接口 Physical Interface**

涉及各种传输介质或传输设备的接口。

3.1.12**隐式选择 Implicit Selection**

隐式选择智能卡中的文件是通过短FID选择的，它作为一个参数由实际对文件进行访问的命令来传送。一系列限制施加于隐式选择的使用。它只是在当前被选的目录范围内有效，不能跨目录区域隐含地选择一个文件。隐式选择只可能用于某些存取命令，这些命令允许短FID作为参数传送（诸如：READ BINARY、UPDATE BINARY、READ RECORD和UPATERECORD）

3.2 缩略语

下列缩略语适用于本文件：

ADF	Application Dedicated File	应用专用文件
AID	Application IDentity	应用标识
APDU	Application Protocol Data Units	应用协议数据单元
ATR	Answer To Reset	响应复位（命令）
BIP	Bearer Independent Protocol	承载无关协议
CLA	CLass byte of the command message	命令消息中的Class字节
COS	Chip Operating System	智能卡操作系统
DFA	Differential Fault Analysis	差分错误分析
DPA	Differential Power Analysis	微分功率分析

EMA	Electro-Magnetic Analysis	电磁分析
eNFC	Enhanced Near Field Communication	增强型近场通信
FID	File IDentity	文件标识
GP	Global Platform	全球平台
IC	Integrated Circuit	集成电路
ICV	Integrity Check Value	完整性检验值
JSR	Java Specification Request	Java规范要求
MAC	Message Authentication Code	报文的鉴别码
UICC	Universal Integrated Circuit Card	通用集成电路卡
UIM	Universal Identity Module	通用识别模块
USIM	Universal Subscriber Identity Module	全球用户识别卡
OTA	Over the Air Technology	空中下载技术
PIN1	Personal Identification Number1	个人识别码1
PIN2	Personal Identification Number2	个人识别码2
PKI	Public Key Infrastructure	公钥基础设施
SCP02	Security Channel Protocol 02	02型安全通道协议
SCP10	Security Channel Protocol 10	10型安全通道协议
SIM	Subscriber Identity Module	用户识别卡
SPA	Simple Power Analysis	简易功率分析
STK	SIM Tool Kit	用户识别应用发展工具

4 智能卡和内置安全模块安全技术要求概述

4.1 概述

智能卡作为实现支付应用相关的存储、执行模块以及实现电信应用相关的身份验证和功能模块，应在满足电信智能卡的安全技术要求的同时，又需要提供措施实现支付应用相关的安全，智能卡应能够保证存储在智能卡中的用户数据、系统数据、系统参数、各种密钥和口令、安全算法等信息的完整性和机密性。

智能卡基本安全要求如下：

- 支持电信智能卡本身的安全机制：电信智能卡本身的安全机制为存储在卡中的手机支付应用和电信类应用提供了一个安全的运行环境；
- 支持多应用管理规范：这种架构保证了在卡中可以按照一套完整的安全标准创建多个独立的安全域，以存储多种完全不同的应用，并实现不同应用之间的隔离，有效防止未授权的恶意攻击行为；同时保证了卡上手机支付应用的安全性以及通过移动网络进行应用和密钥的空中下载的安全性；
- 支持安全域及其密钥管理：保证智能卡内部信息在存储和手机支付全过程中的机密性、完整性、有效性和真实性。
- 芯片要求：智能卡芯片应具备安全防护设计和掉电保护设计，应具有低频检测、温度检测、高低压检测的功能，可以抵御物理攻击，避免因物理攻击造成信息泄漏；

- 卡上操作系统 COS 要求：智能卡操作系统应具备抵抗逻辑操纵或者修改的结构和能力，以抵抗软件逻辑攻击；
- 数据安全要求：智能卡应能保证数据在智能卡内存储的安全，智能卡与卡外实体进行数据传输时应能支持数据传输的安全。

4.2 安全架构

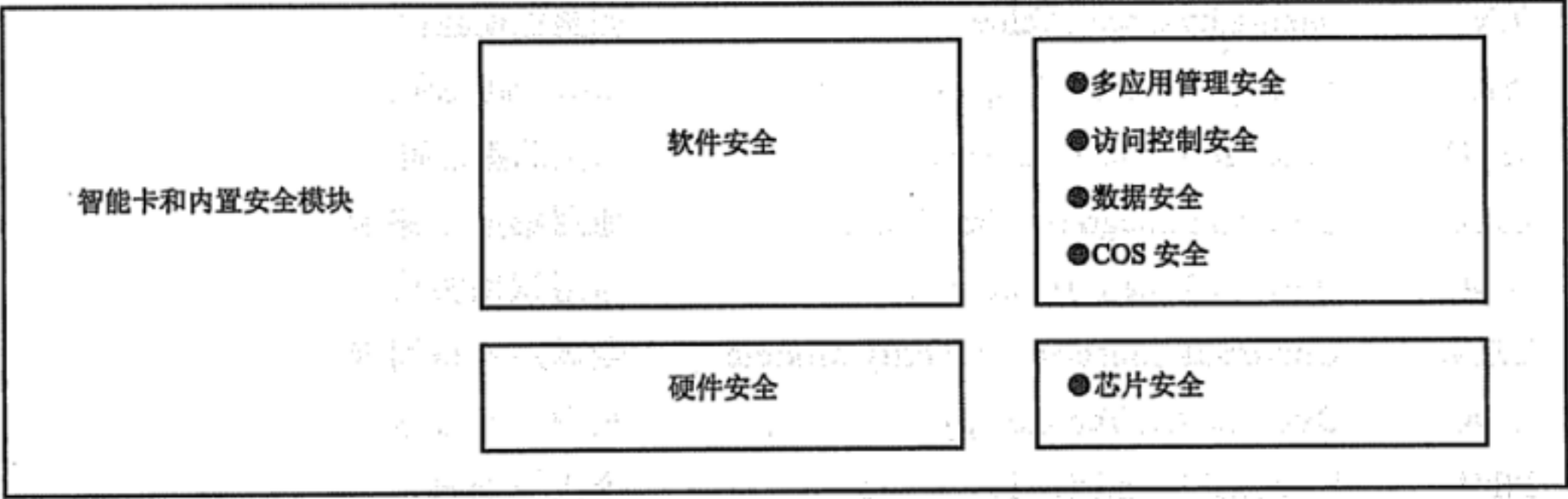


图1 智能卡和内置安全模块安全架构

智能卡和内置安全模块安全架构如图1所示。

本标准的安全技术要求包括以下部分：

- 芯片安全要求；
- 卡上操作系统 COS 安全要求；
- 数据安全要求；
- 访问控制安全要求；
- 多应用管理安全要求。

4.3 内置安全模块安全要求

对于全终端方案的内置安全模块安全技术要求，做与智能卡安全技术要求等同处理。

内置安全模块和智能卡在支持的通信接口方面存在区别：内置安全模块支持的通信接口包括与移动终端主处理器的通信接口和用于现场支付的与近距离通信芯片的通信接口，智能卡支持的接口包括ISO 7816接口和与近距离通信芯片的通信接口。通过上述通信接口对内置安全模块或智能卡进行访问，应符合本标准8.1节~8.3节的规定。

5 芯片安全技术要求

5.1 基本安全要求

智能卡所部署的外部运行环境通常不能够提供芯片自身的物理安全和输入输出的信息的安全，并且芯片在该环境下往往面临各种攻击的风险。为了适用于上述应用场合，智能卡的芯片应当达到如下基本安全要求：

- a) 芯片的安全功能实现正确，且芯片的安全能力满足应用的要求；
- b) 芯片具有逻辑或物理的安全措施，能够对密钥和敏感信息提供完整的主动和被动保护；
- c) 芯片具有对抗和防御各种攻击的逻辑或物理上的安全措施，并且开发者能够证明这些措施的有效性；
- d) 芯片具有全面的生命周期保障。

5.2 密码算法安全要求

5.2.1 密码算法实现

密码算法实现应符合如下要求:

- a) 智能卡和内置安全模块原则上应选择国家密码主管部门认可的密码算法;
- b) 芯片支持的密码算法实现正确, 运算结果与相应的标准运算结果相符;
- c) 芯片支持的密码算法可以采用硬件实现或软硬件结合的方式实现;
- d) 芯片的密码模块具有防错误注入的功能。

5.2.2 随机数生成

随机数生成应符合如下要求:

- a) 安全芯片内应由 3 个或 3 个以上的物理随机源生成随机数;
- b) 随机组合电压、频率、温度等多种可能影响生成的随机数质量的工作条件, 在每一种组合下安全芯片生成的随机数都能够通过随机性检测。

5.3 密钥安全保护要求

5.3.1 密钥生成

密钥生成应符合如下要求:

- a) 安全芯片能够生成正确有效的密钥, 且生成的密钥不可预测、不可倒推;
- b) 如果安全芯片具有随机数模块, 则在安全芯片密钥生成过程中需要使用的随机数必须由芯片内部产生。

5.3.2 密钥存储

密钥存储应符合如下要求:

- a) 安全芯片密钥以密文的形式存储;
- b) 存储密钥的解密密钥应与存储内容分开存放, 且有安全措施来保证解密密钥的安全性。

5.3.3 密钥使用

密钥使用应符合如下要求:

- a) 安全芯片能够正确有效地使用密钥, 且对密钥的使用有着相应的权限要求;
- b) 密钥使用过程中具有安全的防护措施, 不会泄露或者被读出到芯片外。

5.3.4 密钥更新

密钥更新应符合如下要求:

- a) 安全芯片能够正确有效地更新密钥, 且对密钥的更新有着相应的权限要求;
- b) 密钥更新过程不会泄露原密钥和更新的密钥。应有安全的身份认证机制与密钥协商机制来保证更新过程的安全, 更新过程中传输的原密钥和更新的密钥应是密文形式。

5.3.5 密钥导入

密钥导入应符合如下要求:

- a) 安全芯片支持以密文形式导入密钥, 且有着相应的权限要求;
- b) 密钥导入过程不会泄露密钥, 若导入过程需要经过开放信道则密钥在开放信道中传输时应是密文的形式。

5.3.6 密钥销毁

密钥销毁应符合如下要求:

- a) 安全芯片能够根据需要有效地销毁密钥, 且对密钥的销毁有着相应的权限要求;
- b) 密钥在销毁过程中不会被泄露, 密钥销毁操作与被销毁的密钥内容无关;
- c) 具有安全的密钥销毁机制 (例如, 对密钥的存储空间使用随机数重写 8 次以上等)。

5.4 固件安全要求

5.4.1 存储

固件的存储应符合如下要求:

- a) 安全芯片中的固件加密存储, 且不可通过物理接口被读出到芯片外;
- b) 有安全机制保证芯片任何区域的代码不能读取程序存储区的数据;
- c) 有安全机制保证程序数据区不能读取程序代码区内容。

5.4.2 执行

固件的执行应符合如下要求:

- a) 安全芯片固件能够正确地实现设计的目标功能;
- b) 固件不得支持任何非设计的目标功能;
- c) 有相应的措施来保证固件的健壮性和安全性。

5.4.3 权限

固件的权限应符合如下要求:

- a) 对芯片功能等级进行划分, 不同的等级需要不同的权限;
- b) 有相应的角色划分, 每种角色有相应的权限范围;
- c) 有实时的状态列表保证当前权限的合法性与正确性。

5.4.4 导入

固件的导入应符合如下要求:

- a) 安全芯片能够正确有效地导入固件;
- b) 安全芯片导入固件前能够报告芯片导入环境的安全性;
- c) 安全芯片有锁定机制以防止未经授权的二次导入。

5.5 对芯片攻击的削弱与防护要求

5.5.1 版图保护

版图保护应符合如下要求:

- a) 版图采取混合布线, 版图上各模块间没有明显的独立通信链路;
- b) 版图上没有明显独立的逻辑单元;
- c) 同一个模块的布线分多层实现。

5.5.2 时序攻击的防护

时序攻击的防护应符合如下要求:

- a) 特定模块有着良好的时序攻击防御措施;
- b) 有相应的软件或硬件措施保证模块时序特征不明显;
- c) 运算操作执行时间不带有明显的运算特征。

5.5.3 能耗攻击的防护

能耗攻击的防护应符合如下要求:

- a) 特定模块有着良好的功耗分析防御措施;
- b) 有相应的软件或硬件措施保证模块功耗特征不明显;
- c) 功耗曲线没有明显的运算轮廓特征;
- d) 能抵御一定强度的 SPA 与 DPA 攻击。

5.5.4 错误诱导攻击的防护

错误诱导攻击的防护应符合如下要求:

- a) 当安全芯片工作条件中的电压、频率改变使安全芯片处于易受攻击状态时, 安全芯片具有相应的软件或硬件措施来发现并报告这些改变, 并采取相应的防御措施保护密钥和敏感参数不泄露;
- b) 当安全芯片工作条件中的温度、自然光照强度的改变使安全芯片处于易受攻击状态时, 安全芯片具有相应的软件或硬件措施来发现并报告这些改变, 并采取相应的防御措施保护密钥和敏感参数不泄露;
- c) 当芯片受到电压毛刺、频率毛刺以及激光攻击时, 安全芯片具有相应的软件或硬件措施来发现并报告, 并采取相应的防御措施保护密钥和敏感信息不泄露。

5.5.5 侵入式攻击的防护

侵入式攻击的防护应符合如下要求:

- a) 当安全芯片内部逻辑和模拟模块受到物理探测时, 安全芯片具有相应的硬件措施来发现并报告, 并采取相应的防御措施保护密钥和敏感信息不泄露;
- b) 安全芯片设计有相应的硬件措施, 能够防御对芯片内部存储介质的非法读取;
- c) 安全芯片设计有相应的硬件措施, 能够防御移除芯片安全传感器的攻击。

5.5.6 自毁

自毁应符合如下要求:

- a) 安全芯片在检测到侵入式攻击时能够自毁;
- b) 安全芯片自毁过程如果被掉电中断, 下次上电时能够继续完成自毁。

5.6 芯片的生命周期保证要求

5.6.1 芯片标识

芯片标识应符合如下要求:

- a) 同一厂家生产的安全芯片具有唯一标识;
- b) 安全芯片标识在整个生命周期不可更改。

5.6.2 生命周期标识

芯片的生命周期标识应符合如下要求:

- a) 安全芯片在生命周期的各个阶段都有相应的标识;
- b) 有相应的文档跟踪记录芯片所处的生命周期状态;
- c) 有专人负责管理芯片的生命周期。

5.6.3 开发环境

开发环境应符合如下要求:

- a) 开发者对开发环境有相应的安全管理制度;
- b) 对于开发环境的访问有着严格的人员控制和访问记录;
- c) 开发环境与外网物理隔离;

- d) 开发者有明确的保密规定。

5.6.4 代码

代码应符合如下要求:

- a) 安全芯片源代码应安全存放;
- b) 安全芯片源代码的设计有规范的格式;
- c) 安全芯片有详细的开发设计文档;
- d) 开发者应当使用代码检查工具以检测代码的规范性。

6 卡上操作系统 COS 安全要求

6.1 导入

COS的导入应符合如下要求:

- a) COS 能够正确有效地导入到芯片中;
- b) COS 导入前能够获知芯片导入环境的安全性;
- c) COS 导入后可防止未经授权的二次导入。

6.2 存储

COS的存储应符合如下要求:

- a) COS 存储具备锁定机制, 不容许未经授权的修改; 且不可通过物理接口被读出到芯片外;
- b) COS 要保证程序区和数据区的隔离, 不允许互相读取。

6.3 安全状态

COS的安全状态应符合如下要求:

- a) COS 状态应具备安全状态, 并具备明确的进入和退出条件;
- b) COS 能够划分智能卡全局、应用、文件和命令的安全状态, 并进行管理;
- c) COS 安全状态和操作权限有明确的对应。
- d) 安全操作要有记录, 并且该记录不能被修改;

6.4 认证

COS支持认证应符合如下要求:

- a) COS 能够对读写器进行身份认证;
- b) COS 能够对持卡人进行身份认证。

6.5 命令

COS支持命令应符合如下要求:

- a) COS 不得支持任何非设计的命令;
- b) COS 能够防止非法命令的探测访问;
- c) COS 能够保证命令的完整性。

7 数据安全要求

7.1 数据存储安全要求

智能卡数据存储应符合如下要求:

- 对于敏感数据, 如密钥、数字证书、安全算法等应存储在卡上非易失性存储器中。

- 在卡上，每个应用应该放在一个独立的芯片存储空间内，每个应用的逻辑和数据相互不影响。
- 智能卡应能对不同安全属性的数据提供不同访问权限的保护，不同访问权限的用户只能读取其访问权限范围内所指定的数据，如果访问超出其规定的权限，智能卡应能及时检测出，并阻止该访问指令的继续执行并进行安全告警。
- 智能卡应根据数据访问权限的设置控制对数据的访问，并能检测存储在智能卡中的数据是否被未经授权地修改，以防止诸如非法存储数据等引起的逻辑攻击。当检测到有破坏卡内存储数据完整性的操作后，智能卡应发出数据完整性破坏的告警或恢复被破坏的数据。
- 智能卡应提供硬件控制机制保证数据都存储在设定的存储边界内。

7.2 数据传输安全要求

数据传输安全应符合如下要求：

- 身份认证：为保护卡上数据传输的安全，应支持卡外实体与卡的相互认证，相互确认对方的合法性；认证通过后，卡外实体和智能卡在认证过程中确定用于数据传输安全的密钥，包括数据加解密密钥和完整性保护密钥。
- 数据机密性保护：为了实现传输数据的安全，敏感数据等需要保护的数据需要采用加密密钥进行加密后再进行发送。
- 数据完整性保护：使用安全报文传输的目的是保证数据的完整性以及对发送方的认证，一般可以通过在传输报文后加上 MAC 码来保证。为了保证命令中明文数据的保密性，可以对数据加密，来掩盖真实信息，达到保密的目的。

7.3 数据安全恢复要求

智能卡应能保证安全数据的备份和恢复，以及应具有防插拔处理能力。

智能卡应具备安全功能数据的冗余备份与恢复功能，以防止这些安全功能数据在收到非法操作的损害或者是存储发生完整性错误时，能够快速可靠的从备份功能数据中恢复，从而增强智能卡系统的安全性能。备份的安全功能数据包括：访问口令、PIN码验证尝试次数、PIN码解锁尝试次数、密钥、密钥的属性（有效期、用途）、安全域信息及其相关的密钥、以及一些应用需要的证书等。

当智能卡在运行过程中遇到异常、中断、重启等操作时，应能保证智能卡恢复到一个安全、有效的状态。

当智能卡在执行过程中发生意外断电或者突然取卡并再次上电后，应确保返回到某一个安全状态。

8 访问控制安全要求

8.1 卡片系统对数据的访问控制安全要求

除开发阶段，不应提供智能卡操作系统（COS）代码读写的权限；

8.2 基于安全属性的访问控制安全要求

支持手机支付应用的智能卡应当支持以下数据访问控制策略，以决定访问操作是否被允许：

- a) 对数据及与数据有关的操作控制：定义访问数据文件的权限，只有获得相应的访问权限才可以对数据文件进行相应的操作，如读、写、更新、删除、删除恢复等操作。
- b) 应用及数据装载控制：在卡发行和应用安装阶段，所有载入智能卡的数据都要求有授权管理者的授权；在用户使用阶段，应用及数据的装载应获得用户的授权。

c) 卡上数据文件的控制: 建立文件结构的过程和指令, 包括文件访问条件, 都应受文件访问控制规则的约束。

d) 访问级别: 应当对智能卡上的数据设定安全等级, 应当对不同的用户或应用设定安全等级, 以使得不同级别的授权用户或应用对智能卡不同级别的数据进行合法访问, 以此形成的数据访问等级策略一旦确定, 将适用于所有访问操作且不能进行修改。

e) 保密: 支持手机支付应用的智能卡应保证口令、密钥等保密数据的安全存储, 不应向用户提供密钥和算法数据的访问权限。

8.3 文件访问控制安全要求

在支持手机支付应用的智能卡中, 以文件形式存储的数据通过智能卡指令系统提供的接口供外界访问。在支持手机支付应用的智能卡中, 每个文件对于每个指令都有特定的访问条件。任何指令在开始执行前, 应满足最近选择的文件的相关访问条件。

各级访问条件是独立的。对于基于UICC平台建立的支持本规范的手机支付应用智能卡中, 即使有正确的PIN2码, 也不允许执行需要PIN1码支持的操作。满足访问条件的操作, 其有效性在整个过程中都将保持。

8.4 特殊数据访问要求

这里的特殊数据主要是一些安全功能数据, 包括密钥、算法等。除授权管理者外, 智能卡COS不向用户提供访问此类数据的权限, 只有COS才可以调用该数据。

8.5 智能卡访问控制口令的特征

智能卡规定口令字符只能取自阿拉伯数字集0~9, 建议口令数据长度位数为8位。对不符合规定的口令输入, 智能卡应向卡外终端返回一个错误告警。

9 多应用管理安全要求

9.1 智能卡对多应用管理安全规范的支持

Global Platform发布的Global Platform Card Specification V2.2规定了支持多应用的智能卡的技术规范。该规范的内容包括智能卡的架构、安全架构、生命周期模型、Global Platform环境 (OPEN)、安全域、全局平台服务、卡和应用的管理、安全通信等。

支持Global Platform Card Specification V2.2规范的智能卡可以安装多个应用, 这些应用被放置在若干个独立的安全域, 用来保证各个应用之间的隔离及应用之间的独立性; 卡片发行商管理卡片以及卡片发行商自己的和受委托管理的应用, 应用提供商管理自己的应用和应用数据。

在标准中, 智能卡符合Global Platform Card Specification V2.2规范的要求。

9.2 智能卡的多应用生命周期的安全要求

Global Platform Card Specification V2.2规范5.1节规定了智能卡在其生命周期内所经历的5种状态, 每种状态都有其对应的安全要求。卡发行商在发行和管理智能卡时, 应记录每张智能卡的生命周期状态并符合每种生命周期状态下的安全要求。

智能卡的生命周期状态包括: OP_READY、INITIALIZED、SECURED、CARD_LOCKED、TERMINATED, 其中, 前两个用于卡发行前, 后面三个用于卡发行后。各生命周期状态的安全要求如下:

- **OP_READY**: 这个状态表明, 运行时环境已准备好运行; 主安全域, 将准备接收、执行以及响应 APDU 命令; 主安全域中应有一个可用的初始密钥。在这个状态, 卡外实体可以执行辅助安全域的装载和安装; 为了保持与主安全域密钥的隔离, 辅助安全域密钥可以被加入。
- **INITIALIZED**: 这个状态表明一些初始数据 (例如, 主安全域密钥和数据) 已经存在卡中, 但是卡还不能发给卡持有者。
- **SECURED**: 这个状态可以被安全域和应用用于实施他们各自的安全策略, 这个状态同时向卡外实体表明, 主安全域包含所有必需的密钥和安全元素。
- **CARD_LOCKED**: 在这个状态不能进行安全域和应用的选择; 不允许卡内容改变包括任何类型的数据管理 (尤其是安全域密钥和数据); 卡仅允许选择具有 Final Application 特权的应用。
- **TERMINATED**: 这个状态表示卡生命周期和卡的结束, 用于永久地禁止卡的所有功能, 包括任何卡内容管理及卡生命周期的改变。这个状态作为一个机制用于为应用从逻辑上“毁坏”卡, 例如, 当检测到对卡有严重安全威胁时。

9.3 安全域管理

9.3.1 安全域要求及其生命周期状态

安全域扮演卡外权力在卡上的代表, 它负责实施卡外实体安全域提供者的安全策略。安全域的安全要求包括:

- 依据安全域提供者的安全策略, 与卡外实体通信;
- 安全地管理卡上的数据;
- 在个人化及后续操作期间, 为应用提供密码保护服务;
- 请求多应用管理规范运行时环境装载、安装、托管(Extradite)以及删除卡内容;
- 为装载、安装、托管以及删除卡内容生成凭证 (Receipt), 并返回凭证给卡外实体;
- 验证卡内容改变的授权;
- 当多应用管理规范运行时环境请求时, 验证装载文件数据块签名。

安全域的生命周期状态包括: **INSTALLED**、**SELECTABLE**、**PERSONALIZED**、**LOCKED**。主安全域不具有安全域的生命周期状态, 它继承了卡的生命周期状态。

- **INSTALLED**: 在这个状态, 安全域被登记在多应用管理规范注册表中, 但此时它还不能被选择, 还不能跟应用关联, 它的安全域服务还不能被应用使用。
- **SELECTABLE**: 在这个状态, 安全域能从卡外实体接收命令 (尤其是个人化命令)。因为仍然没有密钥, 安全域还不能与应用关联, 它的安全域服务还不能被应用使用。
- **PERSONALIZED**: 当安全域被写入所有必需的个人化数据和密钥后, 它处于 **PERSONALIZED** 状态, 在这个状态, 安全域和应用关联, 并且它的服务可被关联的应用所使用。
- **LOCKED**: 这个状态作为一个安全管理机制, 用于阻止安全域的选择和执行。如果检测到一个卡内部的威胁并且确定这个威胁跟特定的安全域相关, 那么安全域通过设置到 **LOCKED** 状态来阻止对安全域的进一步操作; 卡外实体可以基于商业或者安全原因决定安全域是否需要被锁定。一旦安全域处于这个状态, 仅有具有 Global Lock 特权的应用或者具有 Global Lock 特权的安全域允许解锁它。

9.3.2 安全域创建

安全域是一种特殊的密钥和安全管理应用，通过创建安全域来保证卡片发行商和多个应用提供商之间的密钥的完全分离。

主安全域在卡片出厂前预置。

辅助安全域的创建由主安全域控制、由智能卡应用下载请求触发，可通过短消息通道或者分组数据业务通道等，创建的渠道可以通过移动网络或者业务终端进行。

智能卡中需要下载应用提供商的应用但智能卡中还不存在该应用提供商的辅助安全域时，应用提供商管理平台可以向卡片发行商管理平台发送创建辅助安全域的请求；辅助安全域由卡片发行商管理平台指示智能卡中的主安全域创建，并且为该辅助安全域分配初始密钥；卡片发行商管理平台将辅助安全域基本信息及初始密钥信息发送给应用提供商管理平台，并通知应用提供商进行安全域密钥更新；应用提供商管理平台选择辅助安全域，并且与智能卡相互认证后，对辅助安全域密钥进行更新。

在完成辅助安全域的个人化操作之后，辅助安全域的状态应为“PERSONALIZED”；智能卡应登记辅助安全域创建的结果。

9.3.3 安全域删除

主安全域不能被删除。

辅助安全域的删除可以在安全域生命周期状态的任何时刻进行，可以由应用提供商管理平台获得卡片发行商管理平台的授权后发起，删除辅助安全域时，要求已无任何应用与之关联。应用提供商管理平台保存和维护应用及其相关联的辅助安全域的记录，卡片发行商管理平台保存应用及其相关联的辅助安全域的记录。

辅助安全域的删除可通过短消息通道或者分组数据业务通道，删除的渠道可以通过移动网络或者业务终端进行。

安全域被删除后，智能卡上先前用于物理存储这个安全域的空间被收回并且可以被重用。

9.3.4 安全域更新

安全域的更新包括安全域本身的设置参数等信息的更新，对安全域的更新可以由应用提供商管理平台在取得卡片发行商管理平台的授权后对智能卡中与其对应的安全域执行更新操作，安全域本身的更新应不能影响到该安全域中的支付应用。更新完成后，应用提供商管理平台和卡片发行商管理平台保存安全域更新的操作记录。

9.3.5 安全域锁定和解锁

卡片发行商管理平台或者智能卡中的某个安全域所对应的应用提供商管理平台根据业务需要或者检测到智能卡中的安全域存在安全威胁时，可以指示智能卡将该安全域进行锁定。智能卡检测到某个安全域出现异常后，智能卡应将该安全域锁定，同时将异常上报给卡片发行商管理平台。安全域被锁定后处于锁定状态，智能卡不允许选择该安全域进行访问等操作，该安全域中的支付应用不能再用于支付。

安全域被锁定后，卡片发行商管理平台或者该安全域所对应的应用提供商管理平台可以将该安全域解锁。安全域解锁后，智能卡将该安全域恢复到锁定前的状态。

9.4 安全域密钥管理

9.4.1 密钥管理总体要求

密钥管理包括对智能卡安全域密钥和电子支付应用密钥的管理。安全域的密钥可以采用对称密钥或者非对称密钥体制。在本节中对密钥的生成、分发、更新和存储作了规定。

9.4.2 对称密钥管理

9.4.2.1 安全域密钥

9.4.2.2 安全域及安全域密钥

安全域是卡外实体在卡上的代表，它们包含用于支持安全通道协议运作以及卡内容管理的安全域密钥。安全域负责它们自己的密钥管理，这保证了来自不同应用提供者的应用和数据可以共存于同一个卡上。主要包含两种类型的安全域：

- 主安全域 (Issuer Security Domain, ISD)：又称为发行者安全域，是卡片发行商的主要的、强制的卡上代表，负责对卡片发行商或其应用提供商提供的应用进行装载、安装、删除；主安全域可增加或删除辅助安全域。
- 辅助安全域 (Supplementary Security Domain, SSD)：是应用提供商或者卡片发行商或者他们的代理的附加的、可选的卡上代表，存放应用提供商自主管理的应用以及应用提供商委托卡片发行商管理的应用，该安全域的控制方可以对存放的应用进行操作和维护，如下载新应用、应用升级和删除。

安全域密钥存放在卡上的安全区域内，由 COS 统一管理。

9.4.2.3 主安全域密钥管理

主安全域密钥管理包括主安全域密钥的生成、分发、更新和存储。卡发行商管理平台的密钥管理系统负责智能卡主安全域密钥的生成、分发、更新及存储。

9.4.2.3.1 密钥生成

智能卡的主安全域密钥由卡发行商管理平台采用种子密钥和分散算法分散生成。

9.4.2.3.2 密钥分发

密钥分发是将生成的智能卡主安全域密钥安全的导入对应的智能卡的过程。因采用的智能卡的形态存在多种形式以及密钥分发的策略有多种，密钥分发的方法可以包括：

- 智能卡为 SIM/USIM 和智能卡时，卡发行商管理平台将生成的主安全域密钥交给卡生产商，由卡生产商将主安全域密钥写入智能卡，以及由卡生产商完成智能卡的初始化。
- 智能卡为 SIM/USIM 和智能卡时，由卡发行商写入智能卡的主安全域密钥。卡生产商生产智能卡时，在生产的智能卡中写入智能卡生产商密钥。卡生产商将智能卡交付给卡发行商时，将智能卡生产商密钥也交付给卡发行商。卡发行商使用卡生产商密钥与智能卡建立安全通信信道，将智能卡主安全域密钥写入智能卡。
- 智能卡为集成在移动终端上的 IC 芯片时，由卡发行商写入智能卡的主安全域密钥。移动终端生产商在生产移动终端时，将设备生产商密钥写入终端上的 IC 芯片。移动终端生产商将密钥交付给卡发行商时，将设备生产商密钥也交付给卡发行商。卡发行商使用设备生产商密钥与移动终端建立安全通信信道，将智能卡安全域密钥写入移动终端上的 IC 芯片。

9.4.2.3.3 密钥更新

主安全域的密钥更新包括按计划更新和强制更新。按计划更新是指，按照设置的主安全域的更新周期，在主安全域密钥即将过期之前，对主安全域密钥进行更新；强制更新是指主安全域密钥出现泄露或者经过评估确认密钥存在泄漏风险的情况下决定对主安全域密钥进行强制更新。

按照安全域更新的渠道划分,主安全域的密钥更新包括:通过移动通信网络进行密钥更新、通过卡片发行商的业务终端进行密钥更新。从安全性方面考虑,安全域密钥的强制更新通过卡片发行商的业务终端进行。

9.4.2.3.4 密钥存储

主安全域种子密钥存储在卡发行方密钥管理系统,在卡发行商密钥管理系统内进行密钥分散,产生主安全域密钥;主安全域密钥存储在卡片主安全域内,密钥只能更新,不能被读取,由智能卡COS实现存储安全。

9.4.2.4 辅助安全域密钥管理

辅助安全域密钥管理包括辅助安全域密钥的生成、分发、更新和存储。创建辅助安全域时,需要首先设置辅助安全域初始密钥,辅助安全域初始密钥包括加解密密钥,完整性密钥和DAP校验密钥,其中加解密密钥又包括密钥S-ENC、密钥密钥DEK;完整性密钥包括S-MAC。DAP校验密钥可以为长度为1024bit的应用提供者的RSA公钥,或者是长度为160bit的应用提供者的ECC公钥,或者对称密钥算法的最小长度128bit的对称密钥,用于应用程序数据块或文件数据块签名的校验。卡片发行商管理平台的密钥管理系统负责卡片辅助安全域初始密钥的生成、分发及存储。当针对应用提供商创建新的辅助安全域完成之后,应用提供商可以通过应用提供商管理平台对辅助安全域密钥进行更新,保证应用提供商自有电子支付应用的安全性。

9.4.2.4.1 辅助安全域的密钥生成

卡片发行商管理平台在创建新的辅助安全域时应首先设置所创建的辅助安全域的初始密钥。如果是卡片发行商自己管辖的辅助安全域,则该辅助安全域的初始密钥即为辅助安全域密钥。如果是应用提供商管辖的辅助安全域,在辅助安全域创建完成后,应用提供商将通过辅助安全域密钥更新流程把该辅助安全域初始密钥更新为应用提供商的辅助安全域密钥。

智能卡的辅助安全域初始密钥由卡发行商管理平台使用种子密钥和分散算法分散生成。对于应用提供商管理的辅助安全域,辅助安全域密钥由应用提供商管理平台使用种子密钥和分散算法分散生成。卡发行商管理平台和应用提供商管理平台的种子密钥包括S-ENC、S-MAC和DEK的种子密钥,长度为128bit。分散算法可以采用AES、3DES等算法。分散计算中使用的分散参数可以采用随机数或将随机数与智能卡有关的数据进行某种计算后得出的结果作为分散参数。

智能卡辅助安全域密钥由卡发行商管理平台或应用提供商管理平台维护和管理,卡发行商管理平台或应用提供商管理平台可以设置辅助安全域密钥更新时间周期,也可以根据安全需要对辅助安全域密钥进行强制更新。

9.4.2.4.2 辅助安全域初始密钥分发

辅助安全域由卡片发行商管理平台负责创建,并且为该辅助安全域分配初始密钥。辅助安全域初始密钥的分发可以通过移动通信网络采用OTA方式进行,也可以通过卡发行商业务终端的方式进行。

一种辅助安全域密钥的分发过程为:

1) 分发过程中,用户通过智能卡程序或卡发行商业务终端客户端程序触发应用下载请求,并将应用下载请求信息发送给卡发行商管理平台,应用下载请求信息中包括智能卡标识、应用标识及应用提供商身份信息。

2) 卡发行商管理平台收到应用下载请求信息后,与智能卡主安全域建立安全信道。

3) 卡发行商管理平台还需要进一步根据应用下载请求信息或智能卡状态信息, 判断是否创建辅助安全域。如果需要创建辅助安全域, 卡发行商管理平台则进一步创建辅助安全域并生成辅助安全域初始密钥。

4) 辅助安全域初始密钥通过上述安全信道导入到新创建的智能卡辅助安全域。

9.4.2.4.3 辅助安全域密钥更新

辅助安全域密钥需要定期或强制更新以保证其安全性。对于卡发行商管理的辅助安全域, 由卡发行商管理平台设定辅助安全域密钥的更新周期并触发辅助安全域密钥更新操作; 对于由应用提供商管理的辅助安全域, 由应用提供商管理平台设定辅助安全域密钥更新周期, 并由应用提供商管理平台触发辅助安全域密钥更新操作。

9.4.2.4.4 辅助安全域密钥存储

卡发行商的辅助安全域种子密钥存储在卡发行商密钥管理系统, 应用提供商的辅助安全域种子密钥存储在应用提供商密钥管理系统。辅助安全域种子密钥在密钥管理子系统内进行密钥分散, 产生辅助安全域初始密钥和辅助安全域密钥。辅助安全域初始密钥和辅助安全域密钥存储在卡片安全区域内, 由COS统一管理。

9.4.3 非对称密钥管理

9.4.3.1 安全域非对称密钥

安全域的密钥采用非对称密钥时, 安全域中存储的密钥和证书至少包括:

- 一个用于外部认证的信任根的公钥 (PK.TP_EX.AUT);
- 一个安全域私钥 (SK.SD.AUT);
- 一个安全域公钥 (PK.SD.AUT);
- 根据安全域公钥, 由安全域密钥机构签发的一个安全域证书 (CERT.SD.AUT)。

安全域还可以包含:

- 用于外部认证的被验证过的卡外实体公钥 (PK.OCE.AUT);
- 在从外部认证信任根到卡外实体的有效证书链中的用于外部认证的密钥认证机构公钥 (PK.KA_EX.AUT);
- 在从内部认证信任根到安全域的有效证书链中的用于内部认证的密钥认证机构公钥 (CERT.KA_IN.AUT)。

卡外实体 (OCE) 可用的密钥和证书至少包括:

- 一个用于内部认证信任根的公钥 (PK.TP_IN.AUT);
- 一个卡外实体公钥 (PK.OCE.AUT);
- 根据卡外实体公钥, 由卡外实体密钥机构签发的一个卡外实体证书 (CERT.OCE.AUT)。
- 参与证书链下载到安全域公钥的卡外实体信任根证书公钥 (PK.TP_OCE.AUT)。
- 卡外实体还可以包含:
- 在从外部认证信任根到卡外实体的有效证书链中的用于外部认证的密钥机构证书 (CERT.KA_EX.AUT)。

安全域的拥有者可以是应用提供商 (对于辅助安全域) 或者卡片发行商 (对于主安全域)。

在安全通道的初始化过程中使用非对称加密和公钥基础设施 (PKI)，安全通道会话使用对称会话密钥，在安全通道初始化过程中，安全域从卡外实体接收会话密钥用于安全通道会话，即密钥传送 (key transport)。

9.4.3.2 认证中心 (CA)

认证中心CA根据用途包括为卡发行商和应用提供商签发证书的CA、为智能卡上的主安全域和辅助安全域颁发证书的CA。

可以只选择一个CA为卡发行商和应用提供商签发证书，该CA可以作为可信的第三方，在智能卡上拥有自己的Controlling Authority辅助安全域，为应用提供商辅助安全域提供可信的服务。

为主安全域和辅助安全域签发证书的CA可以由卡发行商和应用提供商自己选择。

9.4.3.3 主安全域密钥管理

主安全域非对称密钥管理指的是主安全域非对称密钥和证书的生成、分发、更新和存储。主安全域非对称密钥指的是主安全域公钥和私钥对。卡片发行方密钥管理系统负责卡片主安全域非对称密钥的生成、分发、更新及存储。

9.4.3.3.1 密钥和证书生成

主安全域的公私密钥对和证书由卡发行商生成，在发卡时由卡发行商将主安全域的公私密钥对和证书预置在智能卡上。在密钥和证书的生成过程中，首先需要产生主安全域的公私密钥对，然后由卡发行商的CA根据产生的公钥签发主安全域的证书。

公私密钥的长度在支持RSA算法时需要为1024bit，在支持ECC算法时需要为160bit，智能卡的证书格式应满足PKCS (ITU-T X.509) 标准的要求。

9.4.3.3.2 密钥和证书分发

主安全域的公私密钥对和证书需要存储在安全的存储介质，交给卡片制造商，在个人化过程中预置到卡中。

密钥分发是将生成的智能卡主安全域的公私密钥对和证书安全的导入对应的智能卡的过程。因采用的智能卡的形态存在多种形式以及密钥分发的策略有多种，密钥分发的方法可以包括：

1) 智能卡为SIM/USIM和智能卡时，卡发行商管理平台将生成的主安全域公私密钥对和证书交给卡生产商，由卡生产商将主安全域公私密钥对和证书写入智能卡，以及由卡生产商完成智能卡的初始化。

2) 智能卡为SIM/USIM和智能卡时，由卡发行商写入智能卡的主安全域公私密钥对和证书。卡生产商生产智能卡时，在生产的智能卡中写入智能卡生产商密钥。卡生产商将智能卡交付给卡发行商时，将智能卡生产商密钥也交付给卡发行商。卡发行商使用卡生产商密钥与智能卡建立安全通信信道，将智能卡主安全域公私密钥对和证书写入智能卡。

3) 智能卡为集成在移动终端上的IC芯片时，由卡发行商写入智能卡的主安全域公私密钥对和证书。移动终端生产商在生产移动终端时，将设备生产商密钥写入终端上的IC芯片。移动终端生产商将智能卡交付给卡发行商时，将设备生产商密钥也交付给卡发行商。卡发行商使用设备生产商密钥与移动终端建立安全通信信道，将智能卡主安全域公私密钥对和证书写入移动终端上的IC芯片。

9.4.3.4 密钥和证书更新

主安全域的证书更新由卡发行商管理平台中的证书管理系统发起。证书管理系统可以定期扫描系统中保存的主安全域的证书，根据证书更新策略确定需要废止的证书。在进行证书更新时，需要在智能卡

对应的主安全域上将原有的证书删除并重新生成主安全域的公私钥对和证书，然后将公私钥和证书安全的导入到智能卡主安全域中。

在进行证书更新时，主安全域的公私钥对由卡发行商管理平台生成。另外，主安全域的证书和密钥更新可以通过移动通信网络采用OTA的方式完成，也可以通过卡发行商的业务终端完成。

9.4.3.5 密钥和证书存储

主安全域公私钥、证书及用于外部验证的可信根的公钥存储在智能卡上，以密钥文件方式存在，密钥文件是一种内部文件，不可以被读取，其安全性由卡片操作系统保证。

卡发行商管理平台中的证书管理系统保存主安全域的证书；为了智能卡的安全，密钥管理系统只保存主安全域的公钥，不保存主安全域的私钥。

9.4.3.6 辅助安全域密钥和证书管理

9.4.3.6.1 密钥和证书的生成

卡发行商创建辅助安全域后，需要生成辅助安全域的公私钥对和辅助安全域的证书，并将公私钥对和证书安全的导入到辅助安全域。在密钥和证书的生成过程中，首先需要产生辅助安全域的公私钥对，然后由应用提供商的CA根据产生的公钥签发辅助安全域的证书。根据公私钥对的产生方式，可以分为由应用提供商负责生成密钥对和卡上生成公私钥对。

公私钥对的长度在支持RSA算法时需要为1024bit，在支持ECC算法时需要为160bit，智能卡的证书格式应满足ITU-T X.509标准的要求。

公私钥对由应用提供商生成时，应用提供商管理平台的密钥管理系统生成智能卡的公私钥对，然后将公钥和证书申请的其它信息通过应用提供商管理平台的证书管理系统发给应用提供商CA，由CA生成证书并返回给证书管理系统。

公私钥对由智能卡生成时，生成采用RSA算法长度为1024bit的公私钥对或者采用ECC算法长度为160bit的公私钥对的时间不超过30s。智能卡生成公私钥对后，把公私钥对保存在辅助安全域，将公钥发送给应用提供商的密钥管理系统，然后由应用提供商CA生成辅助安全域的证书。

9.4.3.6.2 密钥和证书分发

密钥分发指将辅助安全域的公私钥对和证书等导入到辅助安全域的过程。

公私钥对的生成方式分为应用提供商生成和卡上生成，其对应的密钥分发过程也不同。另外从密钥分发所采用的渠道考虑，密钥分发可以通过移动通信网络采用OTA的方法完成，也可以通过卡发行商的业务终端或者应用提供商的业务终端完成。

9.4.3.6.3 辅助安全域密钥和证书更新

辅助安全域的证书更新由应用提供商管理平台中的证书管理系统发起。证书管理系统可以定期扫描系统中保存的辅助安全域的证书，根据证书更新策略确定需要废止的证书。在进行证书更新时，需要在智能卡对应的辅助安全域上将原有的证书删除并重新生成辅助安全域的公私钥对和证书，然后将公私钥和证书安全的导入到智能卡辅助安全域中。

在进行证书更新时，辅助安全域的公私钥对可以由应用提供商管理平台，也可以由智能卡在卡上生成。另外，辅助安全域的证书和密钥更新可以通过移动通信网络采用OTA的方式完成，也可以通过卡发行商的业务终端及应用提供商的业务终端完成。

9.4.3.6.4 密钥存储

辅助安全域的公私钥、证书及用于外部验证的可信根的公钥保存在辅助安全域中，由智能卡COS实现存储安全。其中辅助安全域的私钥只能更新，不能读取。

应用提供商管理平台中的证书管理系统保存辅助安全域的证书；为了智能卡的安全，密钥管理系统只保存辅助安全域的公钥，不保存辅助安全域的私钥。

9.4.4 支付应用密钥管理

支付应用的密钥需要符合支付应用规范中对密钥的规定和业务安全规范。支付应用的业务密钥总体上分为对称密钥和非对称密钥。智能卡安全域需要正常支持采用对称密钥和非对称密钥的电子支付应用。

支付应用的密钥数据和支付应用个人化数据的准备可以由支付应用管理系统完成。

在进行支付应用的个人化时，由支付应用管理系统和智能卡之间建立SCP02或者SCP10安全信道，然后将支付应用的密钥和个人化数据下载到智能卡中对应的安全域，支付应用进行密钥和数据的存储。支付应用的个人化可以通过OTA方式、卡发行商的业务终端或者应用提供商的业务终端完成。

9.5 应用管理

9.5.1 多应用的安全隔离与共存

应用提供者通过创建它们自己的安全域来管理它们的应用，同时安全域负责它们自己的密钥管理，这保证了来自不同应用提供者的应用和数据之间的安全隔离。

多应用的选择可以在卡上不同的逻辑通道上，互不干扰。逻辑通道是指不同的应用传输数据的通道，卡片支持的通道数要在复位应答(ATR)中表明，一般情况下卡片可支持4个标准逻辑通道0、1、2、3，由APDU命令的CLA的低2位决定，其中逻辑通道0是基本的逻辑通道，在卡会话过程中始终打开并有效。也可支持扩展的逻辑通道4~19，由APDU命令的CLA的低4位决定。非基本的逻辑通道是通过MANAGE CHANNEL命令被打开的，并将一直保持打开状态，除非用MANAGE CHANNEL命令关闭它，或者卡失效自动关闭。

逻辑通道上应用的选择可以在复位应答(ATR)后默认选择，或者，通过SELECT命令显式选择。应用可以在多个通道上同时被选择，但是，一个通道内的命令交互要独立于另一个通道内的命令交互；命令响应对不能在通道之间交叉，在同一时刻，只有一个通道在使用。

在卡上，每个应用放在单独的一个ADF文件中。需要被多个通道访问的文件，应在其文件属性中指明为是可共享的。当从不同通道访问同一个文件时，由应用来保证文件数据的一致性。

9.5.2 支付应用的管理

支付应用的管理包括应用的下载、安装、选择、注册表更新以及应用的删除，这些应用管理操作由特定的APDU命令执行，这些命令执行之前，还需进行安全域选择以及卡外实体与卡片的相互认证。

应用的下载申请由INSTALL[load]命令发起，INSTALL[load]命令一方面提示卡片做好可执行文件装载的准备、完成下载开始前的清理和初始化工作；另一方面，也传入一些相关的信息由卡端进行确认和验证。这些相关信息包括：将要下载的应用标识AID长度和数据、卡内执行下载操作的安全域的AID长度和数据、用来进行可执行文件数据验证的Hash数、以及其他可选的系统参数和应用参数。

接下来，进行应用的可执行文件数据的下载，这些数据被拆分成若干个数据块，用多个LOAD命令发送，每条LOAD命令都带有数据块的序号，执行下载应用的安全域负责把各个数据块按次序组合成完整的可执行文件。一旦成功完成了应用下载，该可执行文件的一个登记条目将被创建在注册表中。

应用的安装由INSTALL[for install]命令发起,它负责策动卡端根据刚下载完成的可执行文件的组件创建应用。

INSTALL[for make selectable]命令用于请求选择先前已安装的应用。选择之后,在注册表中应增加应用生命周期和特权信息。

已经安装在卡上的应用也可以与另一个安全域关联,这个托管过程由命令INSTALL[for extradition]完成。

与应用相关的注册表数据,可以被改变,这个注册表更新过程由一个或多个INSTALL[for registry update]命令完成。

根据卡发行商的政策,应用供应商可以从卡上删除应用,应用的删除包括应用实例的移除以及相关的应用数据的移除。只有未与卡上实体相关联的代码和数据才能被删除,并且,当应用被选择在另一个逻辑通道时,这个应用也不能被删除。当应用被移除后,它的内容不能再被访问。删除应用是由命令DELETE完成的。这个操作完成后,注册表中应用的登记条目将被移除。

当安全域的生命周期状态处于PERSONALIZED,以及卡的生命周期状态不是CARD_LOCKED或者TERMINATED时,才可以执行以上应用管理相关的操作。

9.6 智能卡和远程管理服务器之间的通信的安全要求

智能卡和远程管理服务器进行通信时,远程管理服务器选择智能卡中的某个安全域。安全域被选择后,为了通信安全,安全域和远程服务器之间需要建立安全信道(Secure Channel),智能卡安全域和远程管理服务器之间的通信协议采用Global Platform Card Specification V2.2中对安全信道的规定,建立安全信道的通信协议包SCP02、SCP10和SCP80。

在智能卡安全域密钥采用对称密钥体制时,智能卡和远程管理服务器之间的通信可以采用SCP02通信协议,参见Global Platform Card Specification V2.2 “E Secure Channel Protocol ‘02’” 中的要求。

在智能卡安全域密钥采用非对称密钥和PKI体制时,智能卡和远程管理服务器之间的通信采用SCP10通信协议,参见Global Platform Card Specification V2.2 “F Secure Channel Protocol ‘10’” 中的要求。

智能卡和远程服务器之间通过OTA进行通信时,智能卡和远程管理服务器之间建立安全信道可以采用SCP80通信协议,该通信协议由ETSI TS 102 225和ETSI TS 102 226规范进行了规定,参见ETSI TS 102 225和ETSI TS 102 226规范的要求。智能卡和远程管理服务器之间可以采用短信或者TCP等方式实现OTA。

中 华 人 民 共 和 国
通 信 行 业 标 准
手机支付
智能卡和内置安全模块安全技术要求
YD/T 2501-2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座

邮政编码：100061

宝隆元（北京）印刷技术有限公司印刷

版权所有 不得翻印

*

开本：880×1230 1/16

2013年5月第1版

印张：1.75

2013年5月北京第1次印刷

字数：41千字

15115·170

定价：25元

本书如有印装质量问题，请与本社联系 电话：(010)67114922