ICS 35 220
L 64

YD

中华人民共和国通信行业标准

YD/T 1625-2007

电信智能卡安全技术要求

Security requirements for smart card in telecommunication

2007-04-16 发布　　2007-10-01 实施

中华人民共和国信息产业部　发布

目　录

前　言

本标准根据我国实际国情和各企业实际状况制定，并在制定过程中参考了GB/T 18336《信息技术 安全技术 信息技术安全性评估准则》。

本标准的附录A为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：大唐电信科技产业集团

本标准主要起草人：穆肇骊　赖华添　耿　静

电信智能卡安全技术要求

1 范围

本标准规定了电信智能卡产品在防物理攻击、数据存储、访问控制、应用等方面的安全技术要求。

本标准适用于电信领域中智能卡产品。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 14916 识别卡 物理特性（ISO/IEC 7810，Identification cards - Physical characteristics，IDT）

GB/T 16649.1 识别卡 带触点的集成电路卡 第1部分：物理特性（ISO/IEC 7816-1，Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics，MOD）

GB/T 16649.2 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置（ISO/IEC 7816-2，Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts，IDT）

GB/T 16649.3 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议（ISO/IEC 7816-3，Information cards - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols，IDT）

ETSI GSM 03.48 欧洲数字蜂窝通信系统（第2+阶段）：SIM应用工具包的安全机制

ETSI GSM 11.11 欧洲数字蜂窝通信系统（第2+阶段）：用户识别模块—移动设备（SIM-ME）接口规范（5V）

ETSI GSM 11.14 欧洲数字蜂窝通信系统（第2+阶段）：用户识别模块—移动设备（SIM-ME）接口的SIM应用工具包规范

3 术语和定义

下列术语和定义适用于本标准。

3.1 审计 audit

对指定操作的错误尝试次数或相关安全事件进行记录的过程。

3.2 用户 user

对电信智能卡进行操作的实体，此实体不具有能够影响电信智能卡安全策略执行的特权。

3.3 授权用户 authorized user

依据安全策略可以执行某项操作的用户。

3.4 角色 role

一组预先确定的规则，用于在用户和电信智能卡之间建立许可的交互。

3.5 安全策略 security policy

一组规则，规定了电信智能卡中的资产管理、保护和分配。

3.6 **授权管理者** authorized administrator

具有旁路或绕过电信智能卡安全策略权限的合法组织和个体。

3.7 **安全功能控制范围** security function scope of control

电信智能卡中受安全策略控制的相互作用的集合。

3.8 **访问控制** access control

一种防止资源被未授权用户使用的安全策略。

3.9 **安全事件** security event

一种在电信智能卡资产管理、保护和分配过程中具有直接或潜在危害性的操作或行为。

3.10 **机密性** confidentiality

信息不提供给或不泄露给未授权方的属性。

3.11 **完整性** integrity

信息不被未授权方变更或破坏的属性。

3.12 **数字签名** digital signature

一种非对称加密数据变换，它使得接收方能够验证数据的可靠性和完整性，保护发送和接收的数据不被第三方伪造，同时对于发送方来说，还可用以防止接收方的伪造。

3.13 **私有密钥** private key

一个实体的非对称密钥对中仅供实体自身使用的密钥，在数字签名模式中，私有密钥用于签名功能。

3.14 **公共密钥** public key

一个实体的非对称密钥对中可以公开的密钥，在数字签名模式中，公共密钥用于验证功能。

3.15 **认证中心** certificate authority

一个可信的第三方认证机构，负责向用户签发含公共密钥信息的证书，该证书具有不可伪造性。

3.16 **会话** session

通信双方之间的逻辑连接。

3.17 **应用** application

指电信智能卡上用于实现业务功能的文件组或程序。

3.18 **用户访问认证** user authentication

对用户身份标识的有效性进行验证和测试的过程。

3.19 **安全功能数据** secure function data

与实现电信智能卡安全功能相关的安全元素集合。

4 缩略语

下列缩略语适用于本标准。

ADM	Access condition to an EF which is under the control of the authority which creates this file	智能卡授权管理者所具有的文件访问权限
ALW	Always	没有任何限制的文件访问权限
API	Application Programming Interface	应用程序接口

CHV/CHV2	Card Holder Verification Information	卡持有者的验证信息
COS	Card Operating System	卡操作系统
DF	Dedicated File	专有文件
EF	Elementary File	基本文件
JCAPI	Java Card Application Programming Interface	Java 卡应用程序接口
JCRE	Java Card Runtime Environment	Java 卡运行环境
JCVM	Java Card Virtual Machine	Java 卡虚拟机
MF	Master File	主文件
NEV	Never	禁止访问文件的安全属性标志
OTA	Over The Air	空中下载
PIN/PIN2	Personal Identity Number	用户身份识别号
PIN-G	PIN-General	通用 PIN 码
PIN-NR	PIN-Non Repudiation	用于不可否认交易的 PIN 码
PKI	Public Key Infrastructure	公开密钥基础结构
PUK/PUK2	PIN Unblock Key	PIN 解锁码，分别对应 PIN/PIN2
TLS	Transport Layer Security	传输层安全协议
WAP	Wireless Application Protocol	无线应用协议
WIM	Wireless Identity Module	无线识别模块
WTLS	Wireless Transport Layer Security	无线传输层安全协议

5 概述

电信智能卡是应用于电信领域，集成芯片、软件及应用的通信用存储性安全产品，其主要作用是存储网络或用户个人的安全数据，并配合网络进行身份鉴权及其他安全应用。因此，电信智能卡必须确保数据存储的安全性、可靠性和完整性；同时电信智能卡作为一个独立的实体，也应该加强自身的安全防护技术，以提高数据存储器的可靠性，芯片模块的稳定性、抗干扰性等。

6 与电信智能卡相关的安全威胁

电信智能卡应当考虑以下各类安全威胁：

—对电信智能卡的物理类安全威胁；

—对电信智能卡的逻辑类安全威胁；

—与不充分说明相关的安全威胁；

—有关密码功能的安全威胁；

—监视信息的安全威胁；

—其他安全威胁。

6.1 对电信智能卡的物理类安全威胁

攻击者可能对电信智能卡芯片实施半导体逆向工程技术等物理分析手段获取电信智能卡的设计信息和其所存储的安全信息等内容。

6.2 对电信智能卡的逻辑类安全威胁

6.2.1 用户误操作

一个电信智能卡的授权用户可能因为引入了错误数据或不适当操作等用户误操作而降低了电信智能卡的安全防护能力。

6.2.2 未授权操作

攻击者可能利用对电信智能卡的未授权操作而刺探或修改电信智能卡的安全特性。如攻击者在电信智能卡的几个端口加入不同的脉冲序列，试图使卡的安全功能减弱或进入一种不稳定的状态，从而让卡执行预先设计好的未授权操作，绕过卡的安全措施的保护。

6.2.3 未授权装载

攻击者可能利用未授权程序来刺探或修改电信智能卡的安全功能，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电信智能卡安全功能的未授权装载程序，如病毒程序。

6.2.4 命令操纵

攻击者可能使用智能卡操作指令来揭示存储器内容。这种操纵是基于对指令或功能的正确使用，但指令的要求或格式超出了正常使用范围。例如试图读取超出寄存器限制范围的数据或向受保护的存储区域写入数据，以达到威胁安全性能的目的。

6.2.5 强制重置

攻击者可通过提前中止电信智能卡与读写设备之间的通信、插入中断或选择等手段使电信智能卡进入不安全状态。

6.2.6 缺陷数据输入攻击

攻击者可能针对电信智能卡特定的应用或安全算法输入缺陷数据（特定或错误的数据等），并观察电信智能卡如何对缺陷数据输入做出的响应来获取控制信息和与安全相关的信息。

6.2.7 数据装载故障

攻击者可能在待装载数据中恶意地生成错误来威胁电信智能卡的安全。比如在向电信智能卡中装载应用程序等数据的阶段，数据可能会被攻击者修改或破坏，其中任何一种情况都可能是刺探智能卡的安全功能或暴露安全信息的非法操作。

6.3 与不充分说明相关的安全威胁

6.3.1 对初始使用权的欺骗

电信智能卡的发行过程包括各种标志的设定，这些标志可用在卡的内部或用来向外部发行实体标明该卡生效。如果未经过授权许可而试图使用尚未发行的卡会导致欺骗使用。

6.3.2 身份冒充

电信智能卡应允许特定的角色获取特定的权限。冒充已获得相应权限的用户会导致安全功能或安全信息的暴露。

6.3.3 非法访问

每一个授权角色都有特定的权限来访问电信智能卡中指定的地址区域及其包含的信息，如果访问超出规定权限，会导致安全相关信息的暴露。

6.3.4 数据空间搜索

攻击者可利用对数据空间的重复搜索以确定重要信息。这种威胁的特点是重复采用有效的指令和有

效的要求范围来获取尽可能多的数据空间中的信息。

6.3.5 审计失败

由于审计失败,攻击者可通过重复刺探以揭示存储器内容或改变电信智能卡中安全功能的关键要素。

6.4 有关密码功能的威胁

攻击者可利用编码/解码函数实施密码攻击或穷举攻击来攻破电信智能卡的安全功能。

6.5 监视信息的安全威胁

6.5.1 输入/输出操纵

攻击者可通过操纵集成电路的管脚并监测结果以揭示重要安全信息。该类操作涉及控制 I/O、时钟、电源以直接获取重要安全信息或推导出该类信息。这种威胁的特点是仅仅监视信息或插入选定的符合预期信号特性的错误就可以达到获取安全信息的目的。

6.5.2 信息泄漏

攻击者可对正常使用期间电信智能卡泄漏的信息加以利用。该类泄漏包括功耗、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。这些泄漏信息可通过直接（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。

6.6 其他威胁

6.6.1 联合攻击

攻击者可能会综合利用多种方法来对电信智能卡进行攻击。比如攻击者对不同操作所获取的知识进行综合，获得电信智能卡的相关安全信息；在电信智能卡不稳定或其安全功能的某些方面下降时操纵输入管脚的同时监测输出管脚的变化。

6.6.2 克隆

攻击者可能通过电信智能卡本身的详细说明或者通过非法占有的智能卡设计信息克隆部分或全部电信智能卡的功能以开发进一步的攻击手段。

7 电信智能卡基础安全要求

7.1 安全目的

电信智能卡作为实现电信应用相关的身份验证和功能模块，必须提供措施保证存储在卡中的用户数据、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。

为了实现以上安全要求，电信智能卡必须具有以下基本安全能力：

（1） 电信智能卡应能抵抗探针探测、光学显微镜探测等物理攻击，或应使通过此类攻击难以获得有效信息；

（2） 电信智能卡应具有抵抗逻辑操纵或修改的结构和能力，以抵抗软件逻辑攻击；

（3） 电信智能卡在硬件设计和软件开发上必须使其所储存或运算的机密信息不会通过分析电流波形、频率、能量消耗、功率等表征变化而泄露；

（4） 电信智能卡必须能够基于单个用户或已标识的用户组，为用户提供受控和受限的资源及对象的访问、操作权限；

（5） 电信智能卡必须提供记录所选定安全相关事件的手段，以帮助管理及抵抗潜在攻击；

（6） 电信智能卡必须提供检查存储数据完整性的机制。

7.2 芯片安全属性

在无特殊要求时，电信智能卡的物理特性应满足 GB/T 16649.1 和 GB/T 16649.2 的规定；电信智能卡的触点应该在卡的表面，并且严格遵循 GB/T 14916 的规定。

7.2.1 芯片电路分布要求

电信智能卡芯片电路的版图布线应该采用多层布线，将传输敏感数据的电路和易于分析的成分（尤其是 ROM）尽可能地隐蔽在较低层，而在表面层只布置不传输敏感数据的电路。

在空间允许的情况下，建议添加适量的冗余单元，以增加逆向工程的难度。

7.2.2 总线布线要求

总线不应该在同一层走线。并建议总线不暴露在集成电路金属布线层的最外层，且在不同层有不同的走线顺序，避免呈现出某种规则，以增加逆向工程的难度。

7.2.3 存储器编址要求

电信智能卡操作系统中使用的逻辑存储结构应该随机地映射到物理存储器上，这样可以避免利用存储映射，重构物理存储器的数据而得到卡内关键信息。

7.2.4 芯片的防护设计

卡的微模块在封装的时候应该有对芯片的保护机制，以增加攻击者通过去除芯片表面封装层而探测电路设计或存储器数据的难度，如：

（1） 在芯片周围包围一层与主要的安全逻辑相联系的金属层，如果移走金属层将会导致芯片毁坏；

（2） 在芯片最上层增加不易被腐蚀的金属氧化层（或钝化层），并且使得芯片电路中的活动组件或者连线通过该层，如果破坏该层将导致整个芯片电路失效；

（3） 在芯片电路设计中增加对光的敏感元器件，如果发现芯片被探测，就主动采取措施对存储器中的数据进行保护。

7.2.5 低频检测

电信智能卡的核心芯片必须具有低频监测的功能，以避免攻击者通过观测低频条件下芯片的工作状态进行电路分析。当采用低于芯片正常工作频率时（参见 GB/T 16649.3），芯片应立即发现，并且采取相应措施，如：

（1） 芯片停止正常工作；

（2） 不对外输出有效数字信号；

（3） 如有安全审计功能应记录该低频探测的事件。

7.2.6 温度检测

温度检测要求芯片可以自动探测到环境温度的变化，在正常温度中应不出现芯片不能正常工作或功能混乱现象。当发现温度超出正常工作温度范围时（参见 GSM 11.11），电信智能卡应采取某种机制进行自我保护，这些机制包括：

（1） 主动停止工作，防止自身温度继续升高而损害芯片的性能和功能；

（2） 停止对存储器的访问，防止在异常状况下访问存储器，破坏内部保存的数据。

7.2.7 高低压检测

电信智能卡的核心芯片必须具有高低压检测的功能，以防止攻击者输入智能卡正常工作电压范围（参见 GB/T 16649.3）以外的特殊电压而使智能卡进入测试模式等状态。当智能卡检测到输入电压超过正常

工作电压范围时，应采取相应的安全措施，如停止正常工作等，以避免卡内机密信息的泄露。

7.2.8 测试模式的禁用

测试模式指电信智能卡在研发过程中，预留的特殊输入输出通道，通过特定接口可以观察和使用电信智能卡内部的各种资源。

电信智能卡生产出来后必须禁止电信智能卡进入测试模式，尽可能有效抑制攻击者的重用企图；同时去掉为开发预留的测试点、硬件的跳线、标注等。

7.2.9 电磁场及电磁辐射

卡暴露在79500Ar/m(1000Oe)的磁场中应不会造成集成电路失效。

7.2.10 指令执行电压波动

卡工作的时候，内部电路输出管脚电压应持续保持相对稳定，不能因卡的处理任务不同而显露明显的电压波动特征，以避免外界通过分析电信号而获取卡的工作信息。当采用精密电流电压测试设备对正在正常工作的电信智能卡进行测量的时候，应出现如下特征：

（1） 卡的VCC端口电流波形无明显的特征信息；

（2） 卡片功耗应保持稳定，不因空闲状态还是满负荷运转状态而出现明显不同的测量值。

7.2.11 掉电保护设计

当操作过程中发生意外掉电，对电信智能卡再次上电后，应可按照GB/T 16649.3中的传输协议要求重新启动，不应出现如下的现象：

（1） 卡内数据丢失或混乱；

（2） 卡内文件丢失或操作安全体系受到破坏；

（3） 卡内程序发生混乱；

（4） 直接进入掉电前电信智能卡所处的标志状态；

（5） 卡的电路因电路突然掉电而造成了物理损坏。

7.3 数据安全

7.3.1 数据存储的安全要求

7.3.1.1 存储数据的机密性保护

由于现代半导体逆向工程技术的发展，可以较容易地对集成电路进行解剖及分析。因此对于一些关键数据，如密钥、安全算法等应存储于EEPROM、FLASH等存储器中，以增加通过光学显微镜、电子显微镜等获取存储数据的难度。

电信智能卡应能对不同安全属性的数据提供不同访问权限的机密性保护，不同权限的用户只能读取其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来，并阻止该访问指令的继续执行和进行安全告警。

7.3.1.2 存储数据的完整性保护

电信智能卡应根据数据访问权限的设置控制对数据的访问，并能够检测存储在电信智能卡内的数据是否被未授权的修改，以防止出现非法修改存储数据的逻辑攻击。当检测到有破坏卡内存储数据完整性的操作后，电信智能卡安全功能应发出数据完整性破坏的告警或恢复被破坏数据。

7.3.1.3 数据存储边界的安全保护

电信智能卡应提供硬件控制机制保证数据都能存储在设定的存储边界内。

7.3.2 数据传输的完整性要求

电信智能卡在与外接终端交互过程中，应保证送出数据的完整性，并对读入的具有完整性需求的数据进行完整性校验。当读入数据因为数据错误等原因而不能通过数据完整性校验时，电信智能卡应采取以下相应的动作：

（1） 严格遵循 GB/T 16649.3 的错误检测与数据重传要求；

（2） 对送入该数据的指令不予执行，并产生一个数据不正确或长度有误的告警。

7.4 访问控制要求

7.4.1 基于安全属性的访问控制

电信智能卡必须支持并执行下面的访问控制策略以决定访问的操作是否被允许。

（1） 权限管理：定义各种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对应的操作，如读、更新、删除、删除恢复等操作。

（2） 数据装载：在卡片发行阶段，所有载入电信智能卡的数据都要求有授权管理者的授权，在用户使用阶段所有载入电信智能卡的应用都应该获得用户授权。

（3） 访问级别：数据访问应该根据需要设定一定的等级权限，以应对不同级别的授权用户，数据访问等级策略一旦确定，将适用于所有的访问操作且不允许进行修改（具体规则参见附录 A）。

（4） 文件控制：建立文件结构的过程和指令，包括文件访问条件，都应受其访问控制规则的约束。

（5） 保密：电信智能卡必须保证口令、密钥、算法等保密数据的安全存储。

7.4.2 操作系统的访问控制

除开发、发行阶段以外，不应提供操作系统代码读写的权限。

7.4.3 文件的访问控制

以文件形式存储在智能卡中的数据通过电信智能卡指令系统提供的接口供外界访问。电信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，必须满足最近选择的文件的相关访问条件。

每个文件：

—读操作与寻址定位操作的访问条件是相同的；

—文件体系中按照合法路径选取相匹配的根目录、应用目录或数据文件和获取与当前文件目录（根目录或应用目录）有关信息的指令的访问条件是 ALW。

各级访问条件之间是独立的。例如，即使有正确 PIN2 码，也不允许执行需要 PIN1 码支持的动作。满足访问条件的操作其有效性在整个会话过程中都将保持。

根目录文件信息中应包含 PIN 的状态信息，以决定 PIN 码是否可用，若 PIN 码没有初始化，则关于 PIN 码的指令将不能使用。

7.4.4 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，操作系统不向用户提供访问此类数据的权限，只有操作系统才可以调用该数据，比如只有在 GSM 系统鉴权的时候操作系统内部才调用密钥 KI 来产生鉴权响应。

7.4.5 访问控制口令的特征

电信智能卡规定口令字符仅能取自阿拉伯数字集 0~9，且口令长度位数为 8 位。对于不符合规定的口令输入，智能卡应向外接终端返回一个错误告警。

电信智能卡上的PIN码必须指定一个PUK码作为解锁码，用于PIN码验证错误被锁后的解锁。

PIN码分为PIN1和PIN2，对应于访问控制权限中的CHV1和CHV2。

7.4.6 访问控制口令的操作

7.4.6.1 PIN码的验证

PIN码验证尝试次数的阈值为3，当连续3次验证错误后，PIN码将被锁，先前由这个PIN授予的访问权将立刻失去，但提供PUK码解锁的入口。对于PIN码验证尝试次数记录的操作仅仅包括减操作和置位操作两种，也就是说该记录只可能单向递减，置位操作必须满足的条件是正确的PUK码或者正确的PIN码本身。

在对PIN码进行验证时，如果PIN码错误，电信智能卡应将PIN码验证尝试次数记录减一，并返回验证错误的告警信息，当在阈值范围内输入正确的PIN码并校验通过后，该记录被立即置位。

7.4.6.2 PIN码的解锁

PUK码包括PUK1和PUK2，分别用于PIN1码和PIN2码的解锁。PUK码解锁尝试次数的阈值为10，当连续10次解锁错误后，PUK码将被锁死。对于PUK码解锁尝试次数记录的操作仅仅包括减操作和置位操作两种，也就是说该记录只可能单向递减，置位操作的条件是输入正确的PUK码。

当电信智能卡PIN码被锁时，必须输入正确的PUK码才能解锁。输入PUK码后，电信智能卡验证PUK码的正确性，如果正确则执行解锁操作，将PUK码解锁尝试次数记录置位，否则智能卡将向终端返回一个PUK码解锁错误的告警信息，并将PUK码解锁尝试次数减一。

7.4.6.3 PIN码的修改

PIN码的修改可以通过PIN码修改指令和PIN码解锁指令来实现。

对于PIN码修改指令，电信智能卡应先对旧的PIN码进行验证，旧PIN码的验证要求见7.4.6.1。如果在PIN码验证尝试次数阈值范围内输入正确的旧PIN码，PIN码验证尝试次数记录将被置位，并且新的PIN码生效。

在PIN码被锁的情况下，PIN码的解锁指令中包含一个新的PIN码，如果解锁成功，则新的PIN码生效，PIN码修改成功。

7.4.6.4 PIN1码状态的改变

PIN1码的状态包括使能和不使能两种，相应的，其状态的改变也包括从使能状态改变成不使能状态以及从不使能状态改变成使能状态两种。

在进行状态改变时，电信智能卡应先对PIN1码进行验证，PIN1码的验证要求见7.4.6.1。如果在PIN1码验证尝试次数阈值范围内输入正确的PIN1码，PIN1码验证尝试次数记录将被置位，并且状态的改变生效。

电信智能卡在发行前，必须把PIN1的初始状态设置为使能。

7.5 安全审计

电信智能卡的安全审计是指对指定操作的错误尝试次数及相关安全事件进行记录、分析的过程。通过分析记录结果，电信智能卡可判断发生了哪些安全相关活动，并采取预先设定的安全措施。另外，检查审计记录结果还可以帮助管理者分析潜在攻击，并且使得持卡者对他们所执行的任何与安全相关的操作负责。

电信智能卡必须具备与以下安全操作相关的审计记录生成、存储、分析等能力以及相应的结果处理能力：

（1） PIN 码的验证、解锁、修改；

（2） PIN1 码使能状态的改变；

（3） ADM 口令的验证（只允许在开发和发行阶段存在）。

7.5.1 审计记录生成

电信智能卡应能够第一时间对相关安全事件生成准确客观的审计记录，以标明或间接反映出安全事件的影响程度或当前卡的状态。

7.5.2 潜在侵害分析

电信智能卡应能用一系列的规则，如已知的潜在安全攻击，去分析审计记录，并根据记录指示出这些安全事件对电信智能卡可能造成的潜在危害。

7.5.3 审计记录的存储安全

电信智能卡应保证审计记录存储的完整性，并应对审计记录提供严格的访问权限，可公开的审计记录（如口令验证剩余次数等）用户可以对其进行读取，但没有进行直接修改或删除的操作权限，系统审计记录只能由操作系统进行记录和调用。

7.5.4 安全告警

电信智能卡应该具有根据安全事件的类型，针对那些会对智能卡安全构成威胁的操作不予执行并且向外接终端发出告警的能力。安全告警的内容应包括安全事件的威胁类型以及相应操作的潜在威胁信息。安全告警事件类型主要包括数据的非法访问、数据的完整性检验、PIN 码验证以及 PIN 码解锁等。对此被动操作的电信智能卡应该通过响应指令中的状态字向操作者发出告警行为，另外对于具备主动能力的电信智能卡则建议还需要具备主动告警的能力，使得智能卡具有根据所检测到的安全威胁主动地向外接终端发出此类的告警信息。

7.6 安全功能管理

7.6.1 安全功能行为的管理

电信智能卡仅限于授权管理者对下列安全功能进行修改：

—数据访问规则及级别的设置；

—在安全告警事件中要执行行为的管理；

—密钥属性的管理，密钥属性包括密钥类型、有效期和用途；

—用户访问认证失败所采取行为的管理；

—在用户被认证之前所能采取行为的管理。

7.6.2 安全属性的管理

电信智能卡仅允许授权管理者对电信智能卡中数据的访问控制权限等安全属性进行查询、修改等操作。

7.6.3 安全功能数据管理

电信智能卡仅限于已识别了的授权用户能够对电信智能卡中存储的功能数据进行修改操作。

电信智能卡还必须确保安全功能数据只接收合法的值。

7.6.4 安全功能数据阈值的管理

电信智能卡仅限于授权管理者对 PIN 码验证的尝试次数、PIN 码解锁的尝试次数等安全功能数据阈值进行修改。

7.6.5 密钥管理

对于鉴权密钥，电信智能卡负责安全存储，而针对特殊的应用，电信智能卡将被要求提供一种机制对密钥的类型、有效期、用途等进行安全管理，仅限于授权管理者对这些属性进行查询、修改等操作，对于临时密钥还应负责密钥的动态生成和及时销毁等。

7.7 其他安全要求

7.7.1 安全状态的恢复

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

当电信智能卡在执行过程中发生意外断电或突然取卡并再次上电后，应确保卡返回到某一个安全状态。

7.7.2 安全功能数据的备份与恢复

建议电信智能卡具备安全功能数据的冗灾备份与恢复功能，以防止这些安全功能数据在受到非法操作的损害或者是存储发生完整性错误时，能够快速可靠地从备份功能数据中恢复，从而增强了智能卡系统的安全性能。建议需要增加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、用途等）以及一些特殊应用需要的证书等。

7.7.3 安全功能的不可旁路性

电信智能卡应确保安全策略覆盖范围内的每一项功能在执行前，必要的安全功能都已被成功执行。任何操作都无法旁路系统所定义的安全功能。

8 电信智能卡安全应用要求

8.1 OTA 卡安全应用要求

8.1.1 总体安全要求

OTA 卡应用的实现借助于移动通信网短消息通道，通过数据短消息的形式将相应的服务内容发给用户手机，并将下载数据传递给用户 OTA 卡，OTA 卡对下载内容进行处理，实现 OTA 卡上相应的特定的应用，如菜单下载操作等。

OTA 卡安全应用的目的是抵抗 OTA 业务在通过短消息通道进行传播过程中可能存在的篡改、假冒、重传等攻击，保证业务数据的完整性、可靠性，同时防止未授权用户读取和修改存储在卡中的机密信息及应用数据等。

为了达到以上的安全目的，OTA 的设计应充分满足以下安全策略：

OTA 卡应满足 GSM 11.14 定义的相关要求。

对下载过程中的数据进行安全身份认证、失步处理、加密处理、同步机制。

对卡中的应用代码、密钥、PIN 码等敏感数据进行有效的安全管理。

8.1.2 数据的完整性及机密性要求

OTA 卡应提供一种有效的安全机制对 OTA 业务内容的完整性进行有效的检查，以防止非法攻击者修改业务数据内容、添加异常代码等。

对于涉及敏感数据的 OTA 业务，OTA 卡还应通过安全算法对业务内容进行加密处理，以防止在传播过程中泄露用户的敏感信息。

OTA 卡还应提供措施保证存储在卡中密钥、PIN 码等敏感数据及应用数据的安全可靠，其具体要求

参见 7.3、7.4。

8.1.3 数据的安全认证

OTA 卡应对接收到的业务数据的合法性进行认证，对于非可靠信息源的 OTA 业务数据，OTA 卡不予接受或进行隔离删除，以避免恶意代码对用户 OTA 卡的入侵。

8.1.4 数据的同步处理

OTA 卡应维护一个同步机制以实现和 OTA 业务服务器间的同步，以防止重传攻击对 OTA 应用系统造成损害。同步机制可通过同步计数器实现，其要求可参见 GSM 03.48。

8.1.5 OTA 卡应用管理

8.1.5.1 业务管理

OTA 卡应提供合理完善的用户界面供用户完成 OTA 业务处理。OTA 卡还应提供合理的机制供用户对下载的服务项目进行组织。为了防止恶意攻击，对于卡中已有的应用，OTA 卡不应允许重复下载。

8.1.5.2 远程应用管理

OTA 卡的远程应用管理包括远程文件内容更新、远程业务列表更新、远程业务内容更新、远程删除用户卡中业务、业务禁用、目录删除等。

可被远程更新的文件应限定在预先指定的范围内，指定为不可被 OTA 远程更新的文件应不能被远程文件管理更新。OTA 卡应提供措施对文件的更新属性进行管理。

由于远程应用管理命令一般是通过无线方式进行传播，该命令有可能被外界所窃听、篡改，甚至被恶意攻击者所分析利用，造成卡用户的损失，因此对于特殊的应用必须采用较高级别的安全措施，如下：

（1）必须对远程应用管理命令的特殊字段进行加密处理，以保证命令的机密性。

（2）必须对远程应用管理命令进行校验处理，以防止命令被攻击者所篡改。

（3）有选择的使用源认证、数字签名等安全措施，以进一步保证远程应用管理的安全。

8.1.6 其他安全要求

8.1.6.1 服务使用的安全性

对于用户通过动态申请获取的服务，OTA 卡应采取措施保证服务使用时的安全，如服务的异常中断和失败处理等。同时应用服务应符合 GSM11.14 中 STK 应用规范，不影响外接终端的基本应用。

8.2 Java 卡安全应用要求

8.2.1 总体描述

本节主要是描述 Java 卡系统和 Java 卡应用的通用安全要求，不影响上文对集成电路、电信智能卡操作系统及智能卡专有软件等的安全要求。

Java 卡系统包括 Java 卡虚拟机、Java 卡运行环境、Java 卡应用程序接口等。它建立在电信智能卡操作系统之上，并为 Java 卡应用提供服务。

Java 卡虚拟机（JCVM）指的是嵌入在电信智能卡中并负责规范、描述字节码解释器行为的虚拟机。

Java 卡运行环境（JCRE）负责管理 Java 卡资源、通信、应用的执行、系统与应用的安全等。

Java 卡应用程序接口（JCAPI）负责为 Java 卡应用提供 I/O 管理、获取 JCRE 资源等功能的类和接口，并定义这些类和接口的调用规范。

Java 卡应用指的是 Java 卡上的应用，也称为 Applet。

Java 系统中用户指的是一般使用者、机构（Applet 开发者、卡发行者等）、硬件（如读外接终端）、软件（如安装包、应用程序）等。

8.2.2 安全目的

Java卡安全应用的目的主要是防止未授权对象读取或修改与Java卡系统及应用有关的代码和数据，同时保护密钥、PIN码等敏感数据。

为了达到以上的安全目的，在进行Java应用开发、设计时应充分考虑和提供一系列安全策略，主要如下：

（1）保证不同的Java卡应用及其所使用数据在逻辑上的隔离；

（2）在Java卡上安装Applet之前，应提供安全机制对安装代码的格式等进行静态检查；

（3）对经过静态检查后的安装代码进行完整性、可靠性保护；

（4）对安全算法、密钥、PIN码等敏感数据进行安全管理；

（5）能够识别不同的应用并启用对应的安全策略。

8.2.3 机密性

8.2.3.1 应用数据的机密性

支持Java应用的电信智能卡必须保证应用数据只有授权者可以访问，以防止在运行过程中出现读取其他应用程序数据的逻辑攻击。

8.2.3.2 系统代码的机密性

支持Java应用的电信智能卡必须保证Java系统代码只有授权者可以访问，以防止在运行过程中出现读取系统代码的逻辑攻击。如应用程序在执行的时候试图读取存储系统代码的存储区域。

8.2.3.3 系统数据的机密性

支持Java应用的电信智能卡必须保证Java系统数据只有授权者可以访问，以防止在执行过程中出现读取系统数据的逻辑攻击。Java系统数据包括由Java运行环境管理的有关系统数据以及Java虚拟机和Java API类的内部数据等。

8.2.4 完整性

8.2.4.1 应用代码的完整性

支持Java应用的电信智能卡必须保证应用代码只有授权者可以修改，以防止出现在应用代码存储的区域内修改代码的逻辑攻击。

8.2.4.2 应用数据的完整性

支持Java应用的电信智能卡必须保证应用数据只有授权者可以修改，以防止在运行过程中出现非法修改应用数据的逻辑攻击。

8.2.4.3 系统代码的完整性

支持Java应用的电信智能卡必须保证只有授权者可以修改系统的执行代码，以防止在运行过程中出现修改系统代码的逻辑攻击。

8.2.4.4 系统数据的完整性

支持Java应用的电信智能卡必须保证只有授权者可以修改系统数据，以防止在执行过程中出现修改系统数据的逻辑攻击。Java系统数据包括由Java运行环境管理的有关系统数据以及Java虚拟机和Java API类的内部数据等。

8.2.4.5 会话完整性

支持Java应用的电信智能卡必须保证不会因为会话期间的突然断电等意外而使应用的数据处于未规定的状态，对应用数据的任何修改都能被虚拟机或操作系统隐含的予以保护。

8.2.5 Applet 防火墙

由于支持Java应用的电信智能卡在发行以后支持最终用户动态安装、删除卡上的Applet，而且Applet可由不同的服务提供商提供，它们管理各自的敏感数据和共享一些系统信息，因此必须保证各个应用之间在逻辑上是相互隔离的，任何可能的影响都应该被Java系统或卡操作系统所阻止。

Applet防火墙是实现Java应用逻辑隔离的重要安全措施，它使得不同的应用限制在不同的指定存储区域，不允许在运行过程中扩展到其他Applet所拥有的存储区域或出现读取属于其他Applet对象的操作。

在附加额外安全措施的条件下，Applet防火墙应允许不同的Applet之间可进行受控的通信，以实现某些数据或对象的共享。

Applet防火墙能正确工作的前提是安装或可执行代码的可靠和完整，这可通过字节码验证来保证。字节码验证实现方式和安全要求见8.2.6。

8.2.6 字节码验证

字节码验证是保证Java应用安全的一个主要安全措施，所有的字节码在执行前必须通过验证。字节码验证主要涉及应用程序的安装代码或不需要安装的可执行代码。

字节码验证主要包括字节码的合法性及可靠性检查。

8.2.6.1 字节码合法性验证

字节码的合法性验证主要包括：

（1） 字节码的指令集必须符合Java卡平台所定义的语法及语义规则。

（2） 检查字节码中是否存在引起缓冲区溢出、内存泄漏的指令。

（3） 检查字节码中是否存在伪造内存地址、返回不正确地址等指令。

字节码合法性验证是通过一个字节码验证器来实现的，它是一种对Java字节码进行静态检查的应用程序。字节码验证器的具体实现过程、模型建立、数据流分析方法等不做统一要求。

8.2.6.2 字节码可靠性验证

字节码的可靠性是通过数字签名来实现的，在Java卡应用中，所有的字节码都应以数字签名的形式提供，以避免受控的应用绕过卡内的安全机制。只有通过数字签名验证的字节码，才能被系统所接受。

对于多用途Java卡，Java卡系统应能识别应用的类型，并调用不同的算法对其签名进行认证。

8.2.7 Java卡应用管理

Java卡系统有一个特殊权限的应用——卡管理器，负责Java卡系统及应用的管理，主要包括Java应用的安装、升级、删除管理、安全属性及安全策略的管理、Java卡和外接终端间逻辑信道的管理等。

8.2.7.1 应用的安装管理

Java卡必须确保Java应用安装过程的安全可靠。

Java卡必须保证当应用安装失败或取消后，系统可返回到一个安全状态。

Java卡必须确保安装过程不能旁路Java卡所具有的安全功能，不能影响已有应用的代码、数据、功能和状态等。

Java卡应提供一种机制确保所下载安装代码的完整性及可靠性。

8.2.7.2 应用的删除管理

电信智能卡应提供一种机制可以删除存储在卡中的Java应用，以释放卡的存储器空间。

电信智能卡必须确保卡上应用的删除过程安全可靠。

删除卡上的应用不能影响其他应用的完整性，不能旁路卡所具有的安全功能，不能为系统引入安全

风险。

当卡上的应用被删除后，必须确保应用所拥有的数据同时也被释放掉或不可用。

必须充分考虑在删除过程中发生掉电或其他异常时所可能带来的后果以及对应的解决办法。

8.2.7.3 对象的删除管理

Java 系统必须确保 Applet 实例在删除其所拥有的未被其他 Applet 所共享对象过程的安全可靠。

Applet 在删除指向不再使用或用于其他目的内存区域的对象时，应不能为系统引入新的安全风险或不稳定因素。

Java 系统应确保 Applet 在删除对象时，不能旁路卡所具有的安全功能，如不能删除和其他应用所共享的对象等。

系统应确保已删除对象不能再被应用程序恶意调用，以避免造成系统异常或崩溃。

8.2.7.4 应用的更新管理

Java 系统必须确保 Java 应用更新过程的安全可靠。

更新卡上的应用不能影响其他应用的完整性，不能旁路卡所具有的安全功能，不能为系统引入安全风险。

必须充分考虑在更新过程中发生掉电或其他异常时所可能带来的后果以及对应的解决办法。

8.2.7.5 远程应用管理

远程应用管理指的是通过无线信道远程管理应用的加载、安装、删除、应用的锁定与解锁等。

应用加载、安装、删除、更新应用的安全要求同 8.2.7.1、8.2.7.2、8.2.7.3、8.2.7.4。

应用锁定后，在未被解锁前，该应用就不能被执行或选定。

远程应用管理命令的具体安全要求见 8.1.5.2。

8.2.7.6 逻辑信道管理

Java 系统允许外接终端设备和 Java 卡之间建立多个逻辑信道（会话），通过某一逻辑信道激活的应用只能响应从该条逻辑信道发送过来的指令。Java 系统还应允许一个 Java 应用与外接终端设备之间建立多个逻辑信道。

8.2.7.7 身份及权限管理

Java 系统应能对不同的用户赋予不同的角色，不同的角色对应着不同的访问、管理权限及优先级。

Java 系统应能识别不同的用户及其所对应的角色及权限。

Java 系统应确保用户身份及权限数据不被非法篡改，特别是具有管理员权限的身份。

Java 系统应能检测到用户身份的改变，以防止破坏系统的安全属性和策略。如有的 Applet 可能假冒成 Java 虚拟机身份而获得管理员权限。

8.2.7.8 访问控制管理

外接终端设备必须输入访问控制口令才能访问 Java 系统。

Java 系统应保证 Applet 只能通过 Java 虚拟机或 Java 卡 API 获取系统的资源。

Java 系统应保证应用代码、系统代码只有授权用户可以执行和调用，系统代码包括系统提供的 API 和系统底层代码等。

Java 系统应对不同的应用进行分级并能识别不同的分级，不同级别的应用被赋予不同的资源访问权限，如没有经过数字签名的应用功能受限，不能实现读取系统重要信息或调用重要 API 函数等功能。

8.2.8 其他服务

8.2.8.1 安全告警

当系统在验证、安装或执行过程中检测到一个潜在的安全风险时，必须中止当前的操作，对于具有主动能力的 Java 卡还应向外接终端发出一个告警信息。

8.2.8.2 资源保护

系统负责保护、维持应用所需资源的有效性和可用性，同时还管理一个同时使用资源的限额，以维护系统服务的连续性。

8.2.8.3 加密服务

系统应提供一系列底层的安全算法接口，使得应用可以利用其对一些敏感数据进行加密。这些安全算法必须符合通用的安全策略和标准，同时这些安全算法的使用或设计必须充分考虑功能受限的智能卡特征。

8.2.8.4 边界管理

对于支持下载可执行代码的 Java 卡，必须提供以硬件为基础的存储管理部件，检查运行的代码是否保持在其设定的存储边界内，以防止边界越出，保护卡的安全。

8.3 WIM 卡安全应用要求

8.3.1 概述

WIM 卡是指实现 WAP 安全体系中全部或部分 WIM 功能，并保存用于用户身份识别、认证等相关信息的电信智能卡。它可以是一单独的智能卡，也可以作为一个模块集成在其他电信智能卡中，如 GSM SIM 卡。

WIM 卡安全应用的主要目的是保证与 WTLS/TLS 及应用层安全算法有关证书、密钥、PIN 码、敏感数据等信息的安全。

8.3.2 数据的机密性及完整性要求

WIM 卡作为存储与 WAP 安全功能有关数据的载体，必须提供安全机制保证数据的机密性和完整性。WIM 卡中的安全数据主要有三类：证书、密钥、敏感信息。

证书包括 CA 中心证书和用户证书，WIM 卡不需要保证证书的机密性，但必须提供安全措施防止未授权用户对证书进行修改、删除等。

在 WIM 卡中，存在用于不同安全目的的多种密钥，包括应用层的数字签名密钥、WTLS/TLS 握手阶段的客户端认证密钥、WTLS/TLS 握手阶段产生的主密钥以及由主密钥导出的其他临时密钥，如加密密钥等。对于这些密钥系统应保证只有授权用户才能对其进行读取和修改，同时还应提供安全策略对 WTLS/TLS 握手阶段产生的主密钥及临时密钥的有效性、生存期等进行管理。

敏感信息主要指与应用层程序有关的参数及个人机密信息，WIM 卡一般不提供该信息的访问接口，只有卡内部程序才能对其进行调用。

8.3.3 访问控制要求

在 WIM 卡中，公共密钥、私有密钥、证书、PIN 码等数据对象都是以文件的形式在不同的目录中进行存储，并对应着不同的安全属性和访问控制条件。

WIM 卡中存在两种形式的 PIN 码，PIN-G 码（通用 PIN 码）和 PIN-NR 码（不可否认 PIN 码）。PIN-G 码用来保护除应用层数字签名密钥以外需要由 PIN 码保护的文件安全，而 PIN-NR 码仅对应用层数字签名密钥文件进行读/写保护。系统中可有多个 PIN-NR 码，分别保护不同的应用层数字签名密钥。

系统应确保 WIM 的使用仅限制于一个授权的用户或一些授权的用户。即接入 WIM 或使用 WIM 卡上的应用是受限的，直到 WIM 认证了该用户为止。

当连续三次输入错误 PIN 码（包括 PIN-G、PIN-NR）时，系统应至少能锁定 WIM 卡鉴权功能。当 WIM 卡锁定后，可通过解锁码进行解锁。

8.3.4 应用的逻辑隔离

对于支持 WIM 的多应用卡，必须保证不同应用在功能上互不影响及在逻辑上的隔离。如 WIM/SIM 卡，卡上的 WIM 应用不应影响卡的 GSM 功能，使得不支持 WIM 的 ME，也能在 GSM 网中使用。

对于支持 WIM 的多应用卡，还必须支持逻辑通道。如 WIM/SIM 卡，GSM 应用使用基本的通道 0，WIM 应用使用通道 1、2 或 3。在激活 WIM 应用前，ME 必须首先通过指令打开通道 1、2 或 3。

8.3.5 其他安全要求

对于支持 WIM 功能的多应用卡，还必须符合其他应用所规范的安全要求，如 WIM/SIM 卡必须遵循 GSM 11.11、GSM 11.14 等规定。

附 录 A
（资料性附录）
文件访问条件的级别设置

根据不同操作指令的用途以及文件的重要性，电信智能中的所有文件对于每个操作指令都赋予了特定的访问条件。每个文件的相关访问条件应该在指令请求开始之前获得。

表 A.1 给出了电信智能卡中访问条件的一种级别设置方式。

表 A.1 电信智能卡中访问条件的级别设置方式

级别	访问条件
0	ALW
1	CHV1
2	CHV2
3	保留
4~14	ADM
15	NEV

ALW：无条件执行指令。

CHV1：只有满足下列 3 种条件之一，才可执行指令：

（1）在当前对话期间，一个正确的 CHV1 值已经提供给电信智能卡；

（2）CHV1 使能/不使能指示器已处于“不使能”状态；

（3）当前对话期间已经成功地执行了 UNBLOCK CHV1。

CHV2：只有满足下列两个条件之一，才能执行指令：

（1）在当前会话期间，一个正确的 CHV2 值已经提供给电信智能卡；

（2）当前会话期间已经成功地执行了 UNBLOCK CHV2。

ADM：这是用于智能卡授权管理者所使用的访问级别。

NEVER：在卡与外接终端接口上，不执行请求指令。