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。