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。