ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33746.1—2017

近场通信(NFC)安全技术要求 第1部分:NFCIP-1安全服务和协议

**Technical specification of NFC security—
Part 1: NFCIP-1 security services and protocol**

(ISO/IEC 13157-1:2010, Information technology—Telecommunications and information exchange between systems—NFC Security—Part 1: NFC-SEC NFCIP-1 security services and protocol, MOD)

2017-09-07 发布　　2018-04-01 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 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　数字表示形式和符号 …… 2
4.1　数字表示形式 …… 2
4.2　符号 …… 2
5　缩略语 …… 2
6　符合性 …… 3
7　概要 …… 3
8　服务 …… 4
8.1　概述 …… 4
8.2　共享秘密服务(SSE) …… 4
8.3　安全通道服务(SCH) …… 4
9　协议机制 …… 5
9.1　流程 …… 5
9.2　密钥协商 …… 5
9.3　密钥确认 …… 5
9.4　PDU 安全 …… 5
9.5　终止 …… 5
10　状态和子状态 …… 6
11　NFC-SEC-PDU …… 7
11.1　结构 …… 7
11.2　安全交换协议(SEP) …… 7
11.3　协议标识符(PID) …… 8
11.4　NFC-SEC 有效载荷 …… 8
11.5　终止(TMN) …… 8
11.6　错误(ERROR) …… 8
12　协议规则 …… 8
12.1　协议和服务错误 …… 8
12.2　互通规则 …… 9
12.3　序列完整性 …… 9
12.4　加密处理 …… 9

附录 A（规范性附录） 在 ISO/IEC 18092:2004(NFCIP-1)中使用 NFC-SEC 的附加要求 …… 10
A.1 NFCIP-1 设备表明支持 NFC-SEC 的方法 …… 10
A.2 安全 PDU 介绍 …… 10
A.3 安全 PDU 编号扩展规则 …… 10
A.4 NFCIP-1 修订 …… 10
附录 B（规范性附录） 协议机规范 …… 13
B.1 SDL 符号 …… 13
B.2 请求 SDU …… 13
B.3 确认 SDU …… 14
B.4 SDL 流程 …… 14
B.4.1 空闲状态 …… 14
B.4.2 选择状态 …… 15
B.4.3 建立状态 …… 15
B.4.4 确认状态 …… 16

前　言

GB/T 33746《近场通信(NFC)安全技术要求》分为以下2部分：

——第1部分：NFCIP-1安全服务和协议；

——第2部分：安全机制要求。

本部分为GB/T 33746的第1部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分使用重新起草法修改采用ISO/IEC 13157-1：2010《信息技术　系统间通信及信息交互NFC安全　第1部分：NFC安全NFCIP-1安全服务和协议》。

本部分与ISO/IEC 13157-1：2010的技术性差异及其原因如下：

——将原标准的规范性引用文件中的ISO标准更改为对应的国标；

——删除了两个国标中没有用到的术语LSB和MSB；

——在第7章增加“本部分中涉及的密码算法应遵循国家商用密码的有关规定。”；

——为了避免悬置段的产生调整了8、9、10、11章的章节号；

——附录的顺序按照国标要求，原ISO标准的附录A和附录B，按提及的先后顺序，分别变为本部分的附录B和附录A。

本部分由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本部分起草单位：工业和信息化部电信研究院、西安西电捷通无线网络通信股份有限公司、中国普天信息产业股份有限公司、中国物品编码中心、国家射频识别产品质量监督检验中心。

本部分主要起草人：张琳琳、孙倩、杨军、杜志强、胡亚楠、朱锋、姜国强、鄢若韫、李卓凡、李志敏。

近场通信(NFC)安全技术要求
第1部分:NFCIP-1安全服务和协议

1 范围

GB/T 33746的本部分规定了NFCIP-1的NFC-SEC安全通道服务和共享秘密服务,以及相应服务使用的PDU和协议。

本部分适用于NFCIP-1安全服务和协议的要求。

注1:NFC-SEC专为ISO/IEC 18092中规定的数据交换协议而设计。

注2:本部分不提出与特定应用相关的安全机制(例如:ISO/IEC 7816系列标准中提出的智能卡应用案例需要的安全机制)。NFC-SEC可作为ISO/IEC 7816中应用安全机制的补充。

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 9387.1—1998 信息技术 开放系统互连 基本参考模型 第1部分:基本模型(ISO/IEC 7498-1:1994,IDT)

GB/T 17967—2000 信息技术 开放系统互连 基本参考模型 OSI服务定义约定(ISO/IEC 10731:1994,IDT)

GB/T 25069—2010 信息安全技术 术语

GB/T 33746.2—2017 近场通信(NFC)安全技术要求 第2部分:安全机制要求(ISO/IEC 13157-2:2010,MOD)

ISO/IEC 18092:2004 信息技术 系统间远程通信和信息交换 近场通信 接口和协议 NFCIP-1[Information technology—Telecommunications and information exchange between systems—Near Field Communication—Interface and Protocol (NFCIP-1)]

3 术语和定义

GB/T 17967—2000、GB/T 25069—2010和ISO/IEC 18092:2004界定的以及下列术语和定义适用于本文件。

3.1

连接密钥 link key

保证安全通道安全性的密钥。

3.2

NFC-SEC用户 NFC-SEC user

使用NFC-SEC服务的实体。

3.3

接收者 recipient

接收ACT-REQ命令的NFC-SEC实体。