ICS 35.040
L 80

中华人民共和国国家标准

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

Technical specification of NFC security—Part 2:Security mechanism requirements

(ISO/IEC 13157-2:2010,Information technology—Telecommunications and information exchange between systems—NFC Security—Part 2:Security mechanism requirements, NFC-SEC cryptography standard using ECDH and AES,MOD)

2017-09-07 发布　　2018-01-01 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

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2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 13157-2：2010《信息技术　系统间通信及信息交互NFC安全　第2部分：安全机制要求，使用ECDH和AES的密码标准》。

本部分与ISO/IEC 13157-2：2010的技术性差异及其原因如下：

——标准的英文名称修改为Technical specification of NFC security—Part 2：Security mechanism requirements；

——增加了3个规范性引用文件；

——增加了5个缩略语；

——删除原资料性附录C，增加了2个规范性附录C和附录D；

——将AES替换为符合国家密码管理相关规定的密码算法。

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、国家射频识别产品质量监督检验中心、中国物品编码中心。

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

引　言

本部分的使用者是通信行业的生产企业、检测机构和科技机构。

本文件的发布机构提请注意，声明符合本文件时，可能涉及附录 C 与“一种实体双向鉴别方法”、附录 D 与“一种基于对称密码算法的实体鉴别方法及系统”等相关的专利的使用。

本文件的发布机构对于上述专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可以通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路 68 号西安软件园秦风阁 A201

联系人：刘长春

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

请注意除上述专利外，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。

近场通信(NFC)安全技术要求
第2部分:安全机制要求

1 范围

GB/T 33746的本部分规定了协议标识符PID为01的消息内容和加密方法。本部分的密码机制是使用SM2密钥交换协议作为密钥协定协议以及SM4分组密码算法用于数据加密和完整性保护。

本部分适用于NFC安全服务建立中的安全机制的要求。

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 17964—2008 信息安全技术 分组密码算法的工作模式

GB/T 28455—2012 信息安全技术 引入可信第三方的实体鉴别及接入架构规范

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(ISO/IEC 13157-1:2010,MOD)

GM/T 0002—2012 SM4分组密码算法

GM/T 0003—2012 SM2椭圆曲线公钥密码算法

ISO/IEC 9798-3:1998/Amd.1:2010 信息技术 安全技术 实体鉴别 第3部分:使用数字签名技术的机制 补篇1(Information technology—Security techniques—Entity authentication—Part 3: Mechanisms using digital signature techniques—Amendment 1)

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)]

ISO/IEC 20009-2:2013 信息技术 安全技术 匿名实体鉴别 第2部分:采用群组公钥技术的机制(Information technology—Security techniques—Anonymous entity authentication—Part 2:Mechanisms based on signatures using a group public key)

3 术语和定义

GB/T 33746.1—2017界定的术语和定义适用于本文件。

4 约定和记法

4.1 级连

A‖B表示字段A和字段B的级联:B内容在A内容之后。

4.2 十六进制数字

(XY)代表XY的十六进制数(即以16为基数),每对字符编码为一个字节。