



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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 约定和记法	1
4.1 级连	1
4.2 十六进制数字	1
5 缩略语	2
6 符合性	3
7 概要	3
8 协议标识符(PID)	3
9 原语	3
9.1 原语的特点概要	3
9.2 密钥协商	4
9.3 密钥导出函数	4
9.4 密钥用途	5
9.5 密钥确认	5
9.6 数据加密	6
9.7 数据完整性	6
9.8 信息序列完整性	6
10 数据转换	7
10.1 整数到字节串的转换	7
10.2 字节串到整数的转换	7
10.3 点到字节串的转换	7
10.4 字节串到点的转换	7
11 SSE 和 SCH 服务调用	7
11.1 概述	7
11.2 前提条件	8
11.3 密钥协商	8
11.4 密钥导出	9
11.5 密钥确认	9
12 SCH 数据交换	10
12.1 概述	10
12.2 准备	11

12.3 数据交换	11
附录 A (规范性附录) SM4-XCBC-PRF-128 和 SM4-XCBC-MAC-96 算法	13
A.1 SM4-XCBC-PRF-128	13
A.2 SM4-XCBC-MAC-96	13
附录 B (规范性附录) 字段长度	14
附录 C (规范性附录) NEAU-A 鉴别机制	15
C.1 NEAU-A 鉴别机制概述	15
C.2 准备	15
C.3 支持可信第三方 TTP 的鉴别流程	16
C.4 不支持可信第三方 TTP 的鉴别流程	17
C.5 密钥推导	18
附录 D (规范性附录) NEAU-S 鉴别机制	19
D.1 NEAU-S 鉴别机制概述	19
D.2 准备	19
D.3 流程	19

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、鄢若韞、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。