ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0101—2020

近场通信密码安全协议检测规范

Test specification for cryptography and security protocol of near field communication

2020-12-28 发布　　2021-07-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、国家密码管理局商用密码检测中心、无线网络安全技术国家工程实验室、国家无线电监测中心检测中心、鼎铉商用密码测评技术(深圳)有限公司、国家信息技术安全研究中心、中国通用技术研究院、天津市电子机电产品检测中心、广州广电计量检测股份有限公司、北京计算机技术及应用研究所、工业和信息化部宽带无线IP标准工作组。

本文件主要起草人：杜志强、李琴、李国友、张国强、黄振海、李冬、潘琪、彭潇、李大为、颜湘、段亮、吕春梅、周涛、赵旭东、于光明、林德欣、李楠、傅强、熊克琦、房骥、张璐璐、郑骊、朱正美、赵慧。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及到与第6章～第8章相关的CN201410255349.X、US15/309861、JP2016-567036、EP15807391.6、KR10-2016-7034816等专利的使用。

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且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发布机构备案。相关信息可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：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

近场通信密码安全协议检测规范

1 范围

本文件规定了符合GB/T 33746系列标准的近场通信(NFC)设备的密码算法与NFC安全协议(NEAU)检测方法,包括如下内容:

a) 密码算法的性能和工程实现的正确性的检测方法及要求;

b) NEAU协议实现的一致性和互操作性的检测方法及要求。

本文件适用于符合GB/T 33746系列标准的NFC设备,用于检测其密码算法及NEAU安全协议实现是否符合要求。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 32907 信息安全技术 SM4分组密码算法

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分:数字签名算法

GB/T 32918.3 信息安全技术 SM2椭圆曲线公钥密码算法 第3部分:密钥交换协议

GB/T 33746.1 近场通信(NFC)安全技术要求 第1部分:NFCIP-1安全服务和协议

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

GB/T 35276 信息安全技术 SM2密码算法使用规范

GB/T 37092 信息安全技术 密码模块安全要求

GM/T 0042—2015 三元对等密码安全协议测试规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 33746.1、GB/T 33746.2—2017、GM/T 0042—2015、GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

被测设备 tested equipment

声称实现了NEAU协议的被测试的对象。

3.2

测试平台 test platform

收集测试数据,进行分析处理,按照本标准的要求对其进行测试和判断,输出并记录测试结果的硬件平台。

3.3

基准设备 standard equipment

和被测设备协同工作执行NEAU协议交互,在对被测设备开展测试时需要同步使用的来自检测机