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

构的设备。

注：基准设备为符合 NEAU 协议的产品。

3.4

辅助设备　support equipment

提供除进行 NEAU 协议交互外的用于辅助测试的数据给测试平台的特殊的基准设备，该设备通常由检测机构提供。

4　缩略语

下列缩略语适用于本文件。

CBC	密文分组链接模式	Cipher Block Chaining
CTR	计算器模式	Counter Operation Mode
NEAU	NFC 实体鉴别	NFC Entity Authentication
NEAU-A	使用非对称密码算法的 NEAU	NFC Entity Authentication using Asymmetric cryptography
NEAU-S	使用对称密码算法的 NEAU	NFC Entity Authentication using Symmetric cryptography
NFC	近场通信	Near Field Communication
TePA	三元对等架构	Tri-element Peer Architecture
TTP	可信第三方	Trusted Third Party

5　总体要求

5.1　密码算法性能及工程实现的正确性的要求

符合 GB/T 33746.2—2017 规定的 NEAU 协议的产品应支持国家密码主管部门核准的密码算法。

密码算法的实现应满足：

a)　NEAU 协议中密码算法性能要求

NEAU 协议中使用的密码算法性能应满足产品应用的特定场景需求。

b)　NEAU 协议中对称密码算法工程实现的正确性的要求

NEAU 协议中使用的对称密码算法及其运算模式(CTR 和 CBC)，其运算结果应与密码算法国家标准中规定的对应算法提供的运算结果一致，包括加密、解密。

c)　NEAU 协议中非对称密码算法工程实现的正确性的要求

NEAU 协议中使用的非对称密码算法，其运算结果应与密码算法国家标准中规定的对应算法提供的运算结果一致，包括密钥交换、签名和验签。

5.2　NEAU 协议实现的一致性和互操作性要求

近场通信 NEAU 安全协议应符合 GB/T 33746.2—2017，涉及的实体主要有发送者(A)、接收者(B)和 TTP。NEAU 包括 NEAU-A 机制和 NEAU-S 机制，其中 NEAU-A 机制基于三元对等架构(TePA)。

5.3　其他要求

产品应考虑自检，且产品可靠性、稳定性应满足产品应用的特定场景需求。

根据协议在产品中的实现可提供密码算法正确性自检以及随机数自检说明。产品中应采用符合国家密码管理主管部门对核准的随机比特生成器。

产品中的密码模块的安全要求应满足 GB/T 37092。

6 测试拓扑

6.1 发送者(A)测试拓扑

发送者(A)测试分两种情况:支持 TTP 和不支持 TTP。其中,被测设备为发送者(A),基准设备为接收者(B)。

被测设备(A)与基准设备(B)连接,测试平台获取被测设备收发的 NEAU 协议交互数据进行测试。获取测试数据的方式是由测试平台通过抓包等方式主动获取,或者是由被测设备(A)将收发的 NEAU 协议交互数据按照 GM/T 0042—2015 中第 7 章的要求主动提供给测试平台。当支持 TTP 时,TTP 为辅助设备,测试平台还需获取辅助设备 TTP 收发的 NEAU 协议交互数据进行测试,获取方式是由测试平台通过抓包等方式主动获取,或者是由辅助设备 TTP 将收发的 NEAU 协议交互数据按照 GM/T 0042—2015 中第 7 章的要求主动提供给测试平台。

在支持 TTP 时,发送者(A)测试拓扑如图 1 所示。在不支持 TTP 时,发送者(A)测试拓扑如图 2 所示。

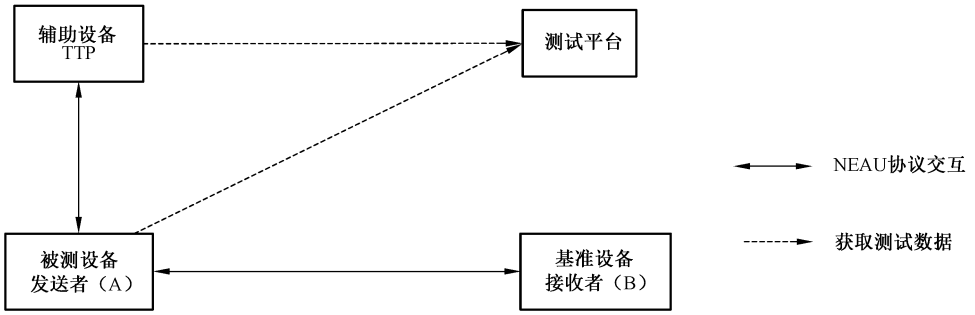

图 1 发送者(A)测试拓扑(支持 TTP)

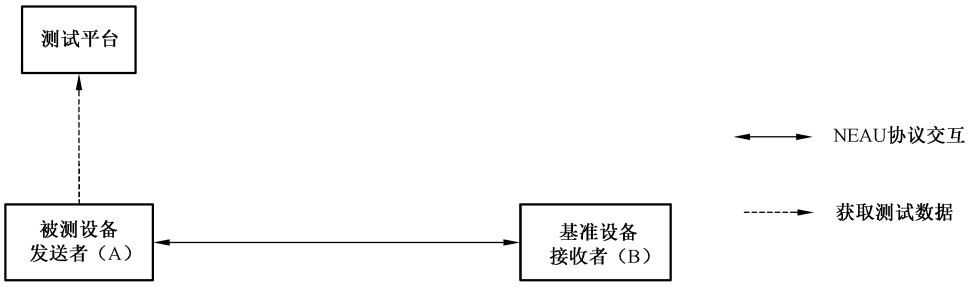

图 2 发送者(A)测试拓扑(不支持 TTP)

6.2 接收者(B)测试拓扑

接收者(B)的测试分两种情况:支持 TTP 和不支持 TTP。其中,被测设备为接收者(B),基准设备为发送者(A)。

被测设备(B)与基准设备(A)连接,测试平台获取被测设备收发的 NEAU 协议交互数据进行测试。

获取测试数据的方式是由测试平台通过抓包等方式主动获取，或者是由被测设备(B)将收发的 NEAU 协议交互数据按照 GM/T 0042—2015 中第 7 章的要求主动提供给测试平台。当支持 TTP 时，TTP 为辅助设备，测试平台必要时还需获取辅助设备 TTP 收发的 NEAU 协议交互数据进行测试，获取方式是由测试平台通过抓包等方式主动获取，或者是由辅助设备 TTP 将收发的 NEAU 协议交互数据按照 GM/T 0042—2015 中第 7 章的要求主动提供给测试平台。

在支持 TTP 时，接收者(B)测试拓扑如图 3 所示。在不支持 TTP 时，接收者(B)测试拓扑如图 4 所示。

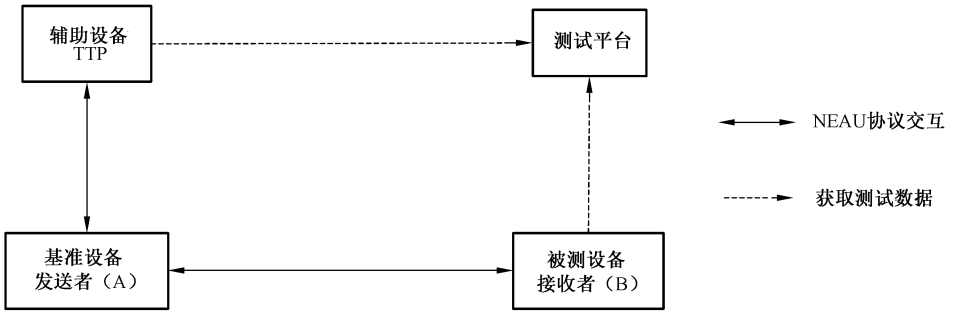

图 3　接收者(B)测试拓扑(支持 TTP)

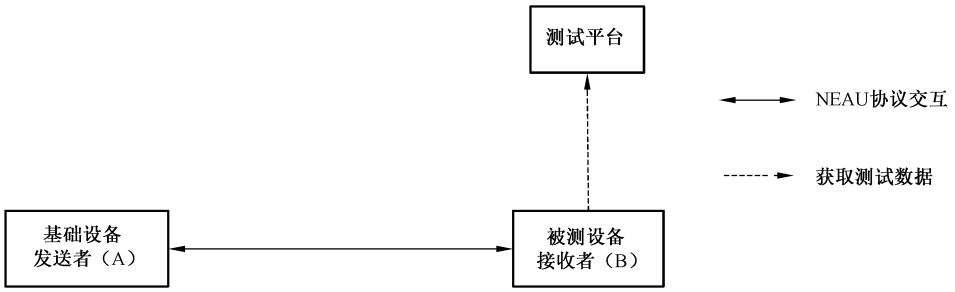

图 4　接收者(B)测试拓扑(不支持 TTP)

7　密码算法性能及工程实现的正确性的测试方法

7.1　密码算法性能测试方法

测试方法如下：

a)　根据测试需求，若被测设备为发送者则按照图 1 或图 2 搭建测试网络，若被测设备为接收者则按照图 3 或图 4 搭建测试网络，被测设备、基准设备和辅助设备执行 NEAU 协议交互。

b)　测试平台获取密码算法性能测试相关数据，包括数据长度、密码操作、重复次数、统计的完成时间等数据。密码操作包括：SM4 加密/解密、SM2 签名/验签。

c)　测试平台利用获得的数据计算对应的密码算法性能。

7.2　对称密码算法工程实现的正确性的测试方法

测试方法如下：

a)　根据测试需求，若被测设备为发送者则按照图 1 或图 2 搭建测试网络，若被测设备为接收者则按照图 3 或图 4 搭建测试网络，被测设备、基准设备和辅助设备执行 NEAU 协议交互。其中，

基准设备应按照 GB/T 32907 给出的运算示例与被测设备进行交互。

b) 测试平台获取对称密码算法测试相关数据，包括被测设备和基准设备执行 GB/T 33746.2—2017 中附录 D.3 中 NEAU-S 协议时涉及的对应算法工作模式、密钥、初始化向量、明文、密文等数据。建议采集 3 组数据。

c) 测试平台利用这些数据开展对称密码算法工程实现的正确性测试，具体遵循 GB/T 32907 和 GB/T 33746.2—2017 中规范的算法工作模式，检测其运算结果的正确性，建议 3 组数据都正确时判定为测试通过，否则判定为测试不通过。

7.3 数字签名算法工程实现的正确性的测试方法

测试方法如下：

a) 根据测试需求，若被测设备为发送者则按照图 1 或图 2 搭建测试网络，若被测设备为接收者则按照图 3 或图 4 搭建测试网络，被测设备、基准设备和辅助设备执行 NEAU 协议交互。其中，基准设备应按照 GB/T 32918.2 给出的数字签名与验证示例和被测设备进行交互；

b) 测试平台获取数字签名算法测试相关数据，包括被测设备和基准设备执行 GB/T 33746.2—2017 中附录 C.3 或附录 C.4 中 NEAU-A 协议时涉及的密钥、待签名数据、签名结果等数据。建议采集 3 组数据；

c) 测试平台利用这些数据开展数字签名算法工程实现的正确性测试，具体遵循 GB/T 32918.2 和 GB/T 35276，检测其运算结果的正确性，建议 3 组数据都正确时判定为测试通过，否则判定为测试不通过。

7.4 密钥交换协议工程实现的正确性的测试方法

测试方法如下：

a) 根据测试需求，若被测设备为发送者则按照图 1 或图 2 搭建测试网络，若被测设备为接收者则按照图 3 或图 4 搭建测试网络，被测设备、基准设备和辅助设备执行 NEAU 协议交互。其中，基准设备应按照 GB/T 32918.3 给出的密钥交换及验证示例与被测设备进行交互。

b) 测试平台获取密钥交换协议测试相关数据，包括被测设备和基准设备执行 GB/T 33746.2—2017 中附录 C.3 或附录 C.4 中 NEAU-A 协议时涉及的公钥算法曲线参数、密码杂凑算法标识、发送者临时公钥、发送者交换公钥、接收者临时公钥、接收者交换公钥、发送者 ID、接收者 ID、密钥交换输出密钥等数据。建议采集 3 组数据。

c) 测试平台利用这些数据开展密钥交换协议工程实现的正确性测试，具体遵循 GB/T 32918.3 和 GB/T 35276，检测其协商结果的正确性，建议 3 组数据都正确时判定为测试通过，否则判定为测试不通过。

7.5 随机数测试方法

测试方法如下：

a) 根据测试需求，若被测设备为发送者则按照图 1 或图 2 搭建测试网络，若被测设备为接收者则按照图 3 或图 4 搭建测试网络，被测设备、基准设备和辅助设备执行 NEAU 协议交互。

b) 测试平台获取随机数测试相关数据，包括被测设备执行 GB/T 33746.2—2017 中附录 C.3 或附录 C.4 或附录 D.3 中 NEAU 协议时所涉及的随机数及被测设备通过随机数测试接口按照 GB/T 32915 要求所采集的随机数样本，建议样本数量 1 000。

c) 测试平台利用这些数据按照 GB/T 32915 的相关要求进行检测。

8 NEAU 协议实现的一致性和互操作性测试方法

8.1 NEAU-A 测试方法

8.1.1 概述

该项测试针对发送者(A)和接收者(B)。

8.1.2 发送者(A)测试方法

当支持 TTP 时,测试拓扑见图 1,需要基准设备接收者(B)、辅助设备 TTP 开展测试:

a) 搭建测试网络,被测设备、基准设备和辅助设备执行 NEAU-A 协议交互;

b) 获取被测设备执行 NEAU-A 协议交互过程中的数据,包括 ACT_REQ(TTP||NA||$Cert_A$)、TAEP_REQ(NA||NB||$Cert_A$||$Cert_B$)和 VFY_REQ(NA||NB||QA||Res_A||Res_B||Sig_{TTP}||Sig_A||$MacTag_A$)等;

c) 检查所获取的被测设备交互的数据是否符合 GB/T 33746.2—2017 中附录 C.3 中规定的发送者(A)应发送的数据。

当不支持 TTP 时,测试拓扑见图 2,需要基准设备接收者(B)开展测试:

a) 搭建测试网络,被测设备和基准设备执行 NEAU 协议交互;

b) 获取被测设备执行 NEAU-A 协议交互过程中的数据,包括 ACT_REQ(TTP||N_A||$Cert_A$)和 VFY_REQ(NA||NB||QA||Sig_A||$MacTag_A$)等;

c) 检查所获取的被测设备交互的数据是否符合 GB/T 33746.2—2017 中附录 C.4 中规定的发送者(A)应发送的数据。

8.1.3 接收者(B)测试方法

当支持 TTP 时,测试拓扑见图 3,需要基准设备发送者(A)、辅助设备 TTP 开展测试:

a) 搭建测试网络,被测设备、基准设备和辅助设备执行 NEAU 协议交互;

b) 获取被测设备执行 NEAU-A 协议交互过程中的数据,包括 ACT_RES(TTP||NB||NA||$Cert_B$||QB|| Sig_B)和 VFY_RES($MacTag_B$)等;

c) 检查所获取的被测设备交互的数据是否符合 GB/T 33746.2—2017 中附录 C.3 中规定的接收者(B)应发送的数据。

当不支持 TTP 时,测试拓扑见图 4,需要基准设备发送者(A)开展测试:

a) 搭建测试网络,被测设备和基准设备执行 NEAU 协议交互;

b) 获取被测设备执行 NEAU-A 协议交互过程中的数据,包括 ACT_RES(TTP||NB||NA||$Cert_B$||QB||Sig_B)和 VFY_RES($MacTag_B$)等;

c) 检查所获取的被测设备交互的数据是否符合 GB/T 33746.2—2017 中附录 C.4 中规定的接收者(B)应发送的数据。

8.2 NEAU-S 测试方法

8.2.1 概述

该项测试针对发送者(A)和接收者(B)。

8.2.2 发送者(A)测试方法

测试拓扑见图 2,需要基准设备接收者(B)开展测试:

a) 搭建测试网络,被测设备和基准设备执行 NEAU 协议交互;

b) 获取被测设备执行 NEAU-S 协议交互过程中的数据,包括 ACT_REQ(NA)和 VFY_REQ(NA||NB||$EncData_A$||MAC_A||$MacTag_A$)等;

c) 检查所获取的被测设备交互的数据是否符合 GB/T 33746.2—2017 中附录 D.3 中规定的发送者(A)应发送的数据。

8.2.3 接收者(B)测试方法

测试拓扑见图 4,需要基准设备发送者(A)开展测试:

a) 搭建测试网络,被测设备和基准设备执行 NEAU 协议交互;

b) 获取被测设备执行 NEAU-S 协议交互过程中的数据,包括 ACT_RES(NB||NA||$EncData_B$||MAC_B)和 VFY_RES($MacTag_B$)等;

c) 检查所获取的被测设备交互的数据是否符合 GB/T 33746.2—2017 中附录 D.3 中规定的接收者(B)应发送的数据。

中华人民共和国密码
行业标准
近场通信密码安全协议检测规范
GM/T 0101—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 0.75 字数 18千字
2021年5月第一版 2021年5月第一次印刷
*
书号:155066·2-35847 定价 18.00 元

GM/T 0101-2020

码上扫一扫 正版服务到