ICS 35.040
L 80
备案号：

中华人民共和国密码行业标准

GM/T 0064- 2018

限域通信(RCC)密码检测要求

Cryptography test requirements for range controlled communication (RCC)

（报批稿）

××××-××-××发布　　××××-××-××实施

国家密码管理局　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

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这些专利的责任。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位： 国家密码管理局商用密码检测中心、国民技术股份有限公司、武汉天喻信息产业股份有限公司、天地融科技股份有限公司、深圳长城开发科技股份有限公司。

本标准主要起草人：周国良、杨贤伟、罗鹏、李美祥、李大为、莫凡、郭懿嵩、牟宁波、查道友、李国友、雷银花、崔永娜。

限域通信(RCC)密码检测要求

1 范围

本标准针对采用密码技术的限域通信（RCC）产品，规定了密码和安全方面的检测内容及要求，RCC产品的其他功能检测按照其相应的产品检验规范进行。

本标准适用于限域通信（RCC）产品的密码检测。

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 32907-2016 信息安全技术 SM4分组密码算法

GB/T 32915-2016 信息安全技术 二元序列随机性检测规范

GB/T 33736-2017 手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口技术要求

GB/T 33737-2017 手机支付 基于2.45GHz RCC（限域通信）技术的智能卡测试方法

GB/T 33738-2017 手机支付 基于2.45GHz RCC（限域通信）技术的智能卡技术要求

GB/T 33740-2017 手机支付 基于2.45GHz RCC（限域通信）技术的非接触射频接口测试方法

GB/T 33741-2017 手机支付 基于2.45GHz RCC（限域通信）技术的非接触式读写器终端技术要求

GB/T 34096-2017 手机支付 基于2.45GHz RCC（限域通信）技术的非接触式读写器终端测试方法

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 所界定的以及下列术语和定义适用于本文件。

3.1

限域通信 range controlled communication

通信距离范围可控的近距离无线通信技术。

3.2

发起方 initiator

限域通信系统中控制通信的一方。

3.3

响应方 target

限域通信系统中对发起方命令请求做出响应的一方。

3.4

被测设备 device under test

被测试的对象，为响应方产品或者发起方产品。

3.5

测试指令 test command

测试专用的特殊消息命令。

3.6

静默 mute

被测设备在接收到测试指令后不做任何响应。

4 符号和缩略语

下列缩略语适用于本文件。

APDU	应用协议数据单元（application protocol data unit）
API	应用程序编程接口（application programming interface）
POS	销售点终端（point of sale）
RCC	限域通信（range controlled communication）
SD	安全数据存储卡（secure digital memory card）
SIM	用户识别模块（subscriber identity module）
UID	惟一标识符（unique identifier）

5 RCC 产品分类

5.1 RCC 发起方产品

RCC发起方产品是指支持RCC通讯协议且在RCC通讯会话中作为发起一方的产品，包括RCC读写器模块、支持RCC的POS终端设备等。RCC发起方产品功能实现遵循GB/T 33741-2017要求，RCC发起方产品功能测试遵循GB/T 34096-2017要求，测试系统与环境参见本标准附录A。RCC发起方产品若为上层应用提供密码服务时，其应用密钥管理和安全保障要求参见附录B。

5.2 RCC 响应方产品

RCC响应方产品是指支持RCC通讯协议且在RCC通讯会话中作为响应一方的产品，包括RCC-SIM、RCC-SD卡等智能卡。RCC响应方产品功能实现遵循GB/T 33738-2017要求，RCC响应方产品功能测试遵循GB/T 33737-2017要求，测试系统与环境参见本标准附录A。RCC响应方产品若为上层应用提供密码服务时，其应用密钥管理和安全保障要求参见附录B。

6 检测要求

6.1 一般要求

本标准主要检测RCC产品中实现的随机数、RCC通讯链路数据加密算法、RCC产品密码服务、以及产品密码运算性能等。

RCC产品应采用国家密码管理主管部门认可的密码算法，密码算法实现应合规正确有效。

RCC产品应明确声明所支持的应用密码功能，产品各项密码功能应合规正确有效。

RCC产品密码部分应具备自检功能。

6.2 密码算法

6.2.1 随机数检测

6.2.1.1 检测要求

依据GB/T 32915-2016进行检测。

6.2.1.2 判定准则

随机数通过GB/T 32915-2016中规定的所有项目的检测。

6.2.2 通讯链路加密算法实现正确性

6.2.2.1 检测要求

对RCC产品所提供的链路加密算法正确性进行检测。

RCC产品应使用SM4密码算法ECB工作模式或CBC工作模式，数据加解密结果应正确有效。

6.2.2.2 判定准则

RCC产品能够按照GB/T 32907-2016的规定，正确实现SM4密码算法功能。

6.3 密码服务

6.3.1 信道传输机密性

6.3.1.1 检测要求

RCC产品能够根据需要，为射频信道链路层传输的APDU数据提供透明的传输机密性保护。

RCC产品采用SM4密码算法对射频信道链路层传输的APDU数据包进行加密保护，其传输机密性保护应正确有效。

6.3.1.2 判定准则

射频信道传输的APDU数据在链路层传输过程中能够根据需要采用SM4密码算法进行机密性保护。

6.3.2 数据加解密服务

6.3.2.1 检测要求

RCC产品如果利用自身硬件密码资源为上层应用提供了数据加解密服务等其他的密码服务功能，则应为上层应用提供相应的API接口。

6.3.2.2 判定准则

通过API接口调用RCC产品提供的RCC数据加解密服务功能，得到的运算结果应正确有效。

6.4 数据加解密性能

6.4.1 检测要求

测试 RCC 产品在链路层对传输的 APDU 数据报文进行加解密的速度。

6.4.2 判定准则

RCC 产品链路加解密性能应能满足 RCC 应用对数据传输效率的要求。

6.5 传输距离

6.5.1 检测要求

RCC产品采用磁信道传输敏感信息,其磁信道数据信号的传输距离应严格控制在安全的距离范围内。

6.5.2 判定准则

RCC产品的刷卡距离范围不大于10cm。

6.6 命令交互

6.6.1 有效命令测试

6.6.1.1 检测要求

采用GB/T 33740-2017附录A中定义的测试指令进行有效命令测试。测试指令使用GB/T 33736-2017中定义的有效请求/响应命令，验证RCC产品的命令交互过程是否正确有效。

6.6.1.2 判定准则

通过测试指令向被测设备发送GB/T 33736-2017中定义的有效请求/响应命令，被测设备应能够按照GB/T 33736-2017的协议要求做出正确操作和响应。

6.6.2 非法或无效命令测试

6.6.2.1 检测要求

采用GB/T 33740-2017附录A中定义的测试指令进行非法或无效命令测试。测试指令使用非法命令（即GB/T 33736-2017中未定义的请求/响应命令）或者无效命令（即部分字段内容值与GB/T 33736-2017定义不符的请求/响应命令），检验RCC产品的命令交互过程是否正确有效。

6.6.2.2 判定准则

通过测试指令向被测设备发送非法或者无效的请求/响应命令，RCC产品应能够报错或保持静默。

6.7 RCC 产品 UID

6.7.1 检测要求

验证RCC产品标识的惟一性。

6.7.2 判定准则

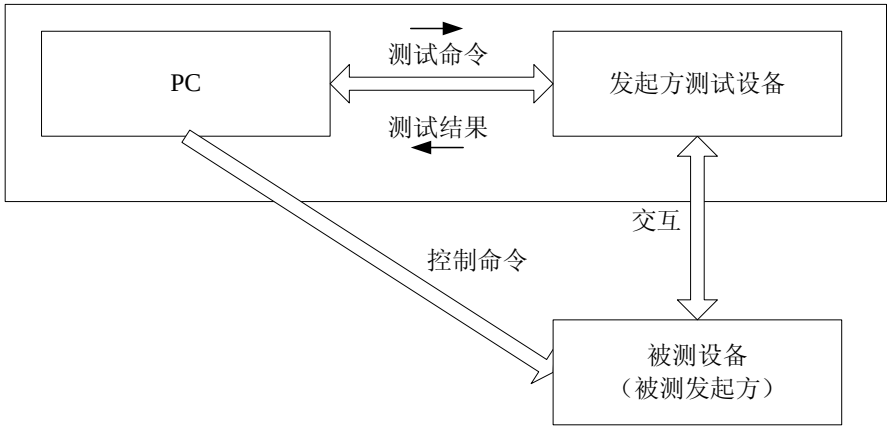
RCC产品具有标识，且提供的标识具有惟一性。

附 录 A
（资料性附录）
RCC 测试系统及环境要求

A.1 测试系统要求

A.1.1 RCC发起方产品测试系统

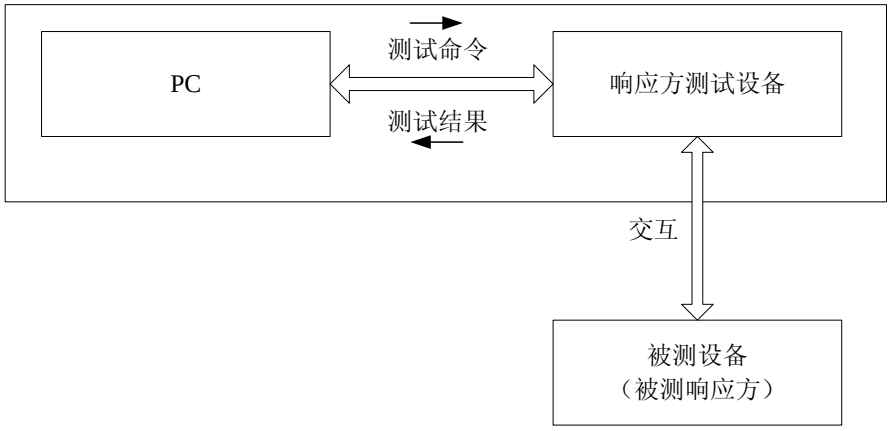
RCC发起方产品测试系统结构如图A.1 所示。测试系统包括：发起方测试设备、PC机等，其中发起方测试设备用于模拟响应方与被测设备（被测发起方）进行交互、PC机用于运行RCC测试工具软件。



图A.1 RCC 发起方设备测试系统示意图

A.1.2 RCC响应方产品测试系统

RCC响应方产品测试系统如图A.2 所示。测试系统包括：响应方测试设备、PC机等，其中响应方测试设备用于模拟发起方与被测设备（被测响应方）进行交互、PC机用于运行RCC测试工具软件。



图A.2 RCC 响应方设备测试系统示意图

A.2 测试环境要求

在没有特殊规定的情况下，测试环境温度为24℃±3℃（73℉±5℉）、相对湿度为40%至60%之间。

附 录 B
（资料性附录）
RCC 产品应用密钥管理与安全保障要求

B.1 RCC产品应用密钥管理

B.1.1 应用密钥生成

RCC产品使用的应用密钥数据可由安全芯片产生的真随机数生成或外部导入。

B.1.2 应用密钥存储

RCC产品如果需要存储应用密钥，则应能够正确、有效地将应用密钥存储在安全芯片内的安全区域，应用密钥不能被攻击者读出，满足相关应用标准对密钥存储的要求。

B.1.3 应用密钥使用

RCC产品应能够根据密钥的类型和使用场合等情况正确、有效地使用安全芯片内的应用密钥,满足相关应用标准对密钥使用的要求。

B.1.4 应用密钥更新

RCC产品如果具备应用密钥更新功能，则应能够正确、有效地更新安全芯片内的应用密钥。

B.1.5 应用密钥导入

RCC产品如果具备应用密钥导入功能，则应能够正确、有效地将应用密钥导入安全芯片内。

B.1.6 应用密钥清除

RCC产品应能够根据应用需要正确、有效地清除存储在安全芯片内的应用密钥。

B.2 RCC产品安全保障

B.2.1 文档管理

RCC产品设计开发文档齐全，保存完好，文档管理要求如下：

a)RCC产品的开发流程、配置管理、交付运行、算法功能开发和工具技术等各类文档齐全；

b)在生命周期的各个阶段须具有追踪记录文档；

c)RCC产品的开发流程的各个阶段需明确界定；

d)对RCC产品开发过程中各阶段完成的任务及相应的输出须具有明确要求。

B.2.2 开发环境安全

RCC产品开发环境须具有相应的规章制度及安全配置。

B.2.3 隐式通道声明

RCC产品开发者须提供产品涉及密码的部分不存在隐式通道的声明文件。

B.2.4 人员

RCC产品生命周期的各个阶段所涉及的工作人员须具有明确的职能划分。

B.2.5 源文件

RCC产品源文件须安全保管，并具有相应的访问控制措施。