ICS 35.040
L 80
备案号:64815—2018

GM

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)

2018-08-20 发布　　2018-08-20 实施

国家密码管理局　　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　符号和缩略语 …… 2
5　RCC 产品分类 …… 2
5.1　RCC 发起方产品 …… 2
5.2　RCC 响应方产品 …… 2
6　检测要求 …… 2
6.1　一般要求 …… 2
6.2　密码算法 …… 3
6.3　密码服务 …… 3
6.4　数据加解密性能 …… 3
6.5　传输距离 …… 4
6.6　命令交互 …… 4
6.7　RCC 产品 UID …… 4
附录 A（资料性附录）　RCC 测试系统及环境要求 …… 5
附录 B（资料性附录）　RCC 产品应用密钥管理与安全保障要求 …… 7

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2.45 GHz 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2.45 GHz 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2.45 GHz 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2.45 GHz 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2.45 GHz 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2.45 GHz 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。