ICS 35.040
L 80
备案号：64814—2018

GM

中华人民共和国密码行业标准

GM/T 0063—2018

智能密码钥匙密码应用接口检测规范

Cryptography application interface test specification for cryptographic smart token

2018-08-20 发布　　2018-08-20 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：深圳市文鼎创数据科技有限公司、国家密码管理局商用密码检测中心、北京握奇智能科技有限公司、天地融科技股份有限公司、飞天诚信科技股份有限公司。

本标准主要起草人：刘伟丰、周国良、吴玲玲、伍友良、董静、李大为、罗鹏、汪雪林、张渊、李勃、牟宁波、李成伟、朱鹏飞、莫凡。

智能密码钥匙密码应用接口检测规范

1 范围

本标准规定了智能密码钥匙密码应用接口检测环境、检测内容和检测方法。

本标准适用于智能密码钥匙密码应用接口检测，也可用于指导智能密码钥匙的研制和使用。

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 25064 信息安全技术 公钥基础设施电子签名格式规范

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 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规范

GB/T 32918—2016 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 33560 信息安全技术 密码应用标识规范

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 35291 信息安全技术 智能密码钥匙应用接口规范

GM/T 0014 数字证书认证系统密码协议规范

GM/T 0015 基于 SM2 密码算法的数字证书格式规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

GM/T 0027 智能密码钥匙技术规范

GM/T 0031 安全电子签章密码应用技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

容器 container

密码设备中用于保存密钥和证书所划分的唯一性存储空间。

3.2

应用 application

包括容器和文件的一种结构，具备独立的权限管理。

3.3

设备 device

智能密码钥匙的统称。

3.4

设备认证 device authentication

应用程序对智能密码钥匙的认证。