ICS 35.040
L 80
备案号:58553—2017

GM

中华人民共和国密码行业标准

GM/T 0048—2016

智能密码钥匙密码检测规范

Cryptography test specification for cryptographic smart token

2016-12-23 发布　　2016-12-23 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：北京握奇智能科技有限公司、飞天诚信科技股份有限公司、北京海泰方圆科技有限公司、北京华大智宝电子系统有限公司、国家密码管理局商用密码检测中心、上海格尔软件股份有限公司、北京创原天地科技有限公司。

本标准主要起草人：汪雪林、李大为、陈国、朱鹏飞、蒋红宇、陈保儒、邓开勇、罗鹏、林春、雷银花、韩琳。

智能密码钥匙密码检测规范

1 范围

本标准规定了智能密码钥匙密码检测环境、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 32915 信息安全技术 二元序列随机性检测方法

GM/T 0006 密码应用标识规范

GM/T 0017—2012 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 0028 密码模块安全技术要求

GM/T 0039 密码模块安全检测要求

3 术语和定义

以下术语和定义适用于本文件。

3.1

智能密码钥匙 cryptographic smart token

实现密码运算、密钥管理功能，提供密码服务的终端密码设备。

3.2

命令 command

向智能密码钥匙发出的一条信息，该信息启动一个操作或请求一个应答。

3.3

响应 response

智能密码钥匙处理完成收到的命令报文后，返回给应用接口的报文。

3.4

消息鉴别码 message authentication code

又称消息认证码，是消息鉴别算法的输出。

3.5

管理员 PIN administrator PIN

管理员的口令，为 ASCII 字符串。

3.6

用户 PIN user PIN

用户的口令，为 ASCII 字符串。