ICS 35.040
L 80
备案号:44628—2014

GM

中华人民共和国密码行业标准

GM/T 0027—2014

智能密码钥匙技术规范

Technique requirements for smart token

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前　言

本标准依据 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。

本标准主要起草单位：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。

本标准主要起草人：汪雪林、朱鹏飞、蒋红宇、广忠海、陈国、陈保儒、于华章、罗鹏、谭武征。

智能密码钥匙技术规范

1 范围

本标准规定了智能密码钥匙的功能要求、硬件要求、软件要求、性能要求、安全要求、环境适应性要求和可靠性要求等有关内容。

本标准适用于智能密码钥匙的研制、开发、测试和使用，也可用于指导智能密码钥匙的检测。

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 4208—2008 外壳保护等级(IP 代码)

GB/T 17964 信息安全技术 分组密码算法的工作模式

GM/T 0002 SM4 分组密码算法

GM/T 0003 SM2 椭圆曲线公钥密码算法

GM/T 0004 SM3 密码杂凑算法

GM/T 0005 随机性检测规范

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0016 智能密码钥匙密码应用接口规范

GM/T 0017 智能密码钥匙密码应用接口数据格式规范

3 术语和定义

下列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，一般使用 USB 接口形态。

3.2

口令 password

用于鉴别身份或验证访问授权的字符串。

3.3

设备认证 device authentication

智能密码钥匙对应用程序的认证。

3.4

设备认证密钥 device authentication key

管理终端认证智能密码钥匙的密钥。

3.5

对称密码算法 symmetric cryptographic algorithm

加密和解密使用相同密钥的密码算法。