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。

3.6

公钥密码算法/非对称密码算法　puclic-key cryptographic algorithm/asymmetric cryptographic algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开,另一个密钥(私钥)必须保密,且由公钥求解私钥是计算不可行的。

3.7

密码杂凑算法　cryptographic hash algorithm

又称杂凑算法、密码散列算法或哈希算法。该算法将一个任意长的比特串映射到一个固定长的比特串,且满足下列三个特性:

a)　为一个给定的输出找出能映射到该输出的一个输入是计算上困难的;

b)　为一个给定的输入找出能映射到同一个输出的另一个输入是计算上困难的;

c)　要发现不同的输入映射到同一输出是计算上困难的。

3.8

消息鉴别码　message authentication code;MAC

又称消息认证码,是消息鉴别算法的输出。

3.9

公钥　public key

非对称密码算法中可以公开的密钥。

3.10

私钥　private key

非对称密码算法中只能由拥有者使用的不公开的密钥。

3.11

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.12

解密　decipherment/decryption

加密过程对应的逆过程。

3.13

数字签名　digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果,该结果只能用签名者的公钥进行验证,用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.14

签名验证　signature verification

验证者使用签名者的公钥对数字签名进行验证的过程。

3.15

用户密钥/用户密钥对　user key / user key pair

存储在智能密码钥匙内部的用于应用密码运算的对称密钥/非对称密钥对,非对称密钥对包含签名密钥对和加密密钥对。

3.16

会话密钥　session key

在一次会话中使用的数据加密密钥。

3.17

SM2 算法　SM2 algorithm

一种椭圆曲线公钥密码算法，其密钥长度为 256 比特。

3.18

SM3 算法　SM3 algorithm

一种杂凑算法，其输出为 256 比特。

3.19

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.20

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。

3.21

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。

3.22

Dock 接口　Dock interface

苹果公司为 iPod、iPhone、iPad 等设备设计的 30 针专用接口，用于数据传输。

3.23

Lightning 接口　Lightning interface

苹果公司为 iPod、iPhone、iPad 等设备设计的 8 针专用接口，用于数据传输。

3.24

音码接口　audio interface

采用耳机和麦克进行数据传输的接口。

3.25

SD 接口　secure digital interface

采用 SD 卡进行数据传输的接口。

4　缩略语

下列缩略语适用于本文件。

API：应用程序接口，简称应用接口(Application Program Interface)

CBC：(分组密码的)密码分组链接(工作模式)(Cipher Block Chaining)

ECB：(分组密码的)电子密码本(工作模式)(Electronic Code Book)

MAC：消息鉴别码(Message Authentication Code)

5　功能要求

5.1　初始化

智能密码钥匙的初始化包括：

- 出厂初始化：出厂时需对设备认证密钥进行初始化。
- 应用初始化：在应用提供商对设备进行发行时需对设备认证密钥进行修改，并建立相应的应用(需设置的参数包含管理员口令、用户口令、应用中容器个数、应用中密钥对最大个数、应用需

要支持的最大证书个数、应用可创建的最大容器个数等)。

5.2 密码运算功能要求

5.2.1 分组密码算法

智能密码钥匙必须支持 SM4 分组密码算法,其实现应符合 GM/T 0002 的要求。

分组密码算法的工作模式至少应包括电子密码本(ECB)和密码分组链接(CBC)两种模式,应符合 GB/T 17964 的要求。

分组密钥算法的标识应符合 GM/T 0006 的要求。

5.2.2 公钥密码算法

智能密码钥匙必须支持 SM2 公钥密码算法,其实现应符合 GM/T 0003 的要求。

公钥密钥算法的标识应符合 GM/T 0006 的要求。

智能密码钥匙对 SM2 公钥密码算法的使用必须符合 GM/T 0009 的要求。

5.2.3 密码杂凑算法

智能密码钥匙必须支持 SM3 密码杂凑算法,其实现应符合 GM/T 0004 的要求。

杂凑算法的标识应符合 GM/T 0006 的要求。

5.2.4 消息鉴别码

智能密码钥匙对消息鉴别码的处理应符合 GM/T 0017 的要求。

5.3 密钥管理

5.3.1 密钥结构

智能密码钥匙必须至少支持三种密钥:设备认证密钥、用户密钥、会话密钥。

设备认证密钥用于终端管理程序与设备之间的相互认证,以获得终端对设备上的应用进行管理的权限。用户密钥指用于签名和签名验证、加密和解密的非对称密钥对。会话密钥指临时从外部密文导入或内部临时生成的对称密钥,使用完毕或设备掉电后即消失。

5.3.2 密钥管理功能

智能密码钥匙应具有对用户密钥和会话密钥的产生、存储、使用、导入、导出、协商等功能。智能密码钥匙各种密钥的使用和访问权限应符合 GM/T 0016 和 GM/T 0017 的要求。

5.3.3 密钥存储

智能密码钥匙的密钥空间必须能够至少保存 2 对 RSA 密钥对、2 对 SM2 密钥对和 2 个对称密钥(包含 1 个设备认证密钥和 1 个会话密钥的空间)。

智能密码钥匙中密钥必须安全存储。所有私钥都不可导出,对称密钥不可以明文导出。

5.3.4 随机数生成

智能密码钥匙应具备随机数生成功能。智能密码钥匙生成的随机数需符合 GM/T 0005,其随机数应由多路硬件噪声源产生。在使用随机数前能对生成的随机数进行偏“0”、偏“1”、“0、1”平衡等常规检测,能通过检测接口对智能密码钥匙所生成的随机数进行样本采集。这里的偏“0”、偏“1”、“0、1”平衡等常规检测是指检测随机数二元序列中 0、1 的个数是否相近,检测随机数是否具有较好的 0、1 平衡性。

5.4 设备管理

智能密码钥匙应具有设备管理功能，如设备认证密钥的更新，应用的删除、创建等。设备管理功能应符合 GM/T 0017 的要求。

5.5 设备自检

设备自检功能主要包括固件完整性、密码算法正确性、随机数发生器、算法协处理器、存储密钥和数据的完整性检查等。可以是设备上电时自检，也可通过为上层应用提供相应功能服务时进行对应的自检功能。

在检查不通过时应返回错误状态码或物理的报警指示并停止工作。

5.6 其他功能

其他功能如应用管理、容器管理、文件管理、访问控制、密码服务，需符合 GM/T 0017 的要求。

6 硬件要求

6.1 接口

智能密码钥匙的硬件接口至少支持但不限于下列接口中的一个：USB、SD、Dock、Lightning、Bluetooth、NFC、音码、WiFi、ISO 7816、ISO 14443 或其他接口。

6.2 芯片

智能密码钥匙的核心芯片需经过国家密码管理部门的审批。

6.3 线路传输

智能密码钥匙在 USB 接口的线路传输协议应符合 GM/T 0017 的要求。

7 软件要求

智能密码钥匙支持的 APDU 命令应符合 GM/T 0017 的要求。如果有扩展指令必须以文档形式明确说明。

8 性能要求

8.1 RSA 算法

通过 GM/T 0017 定义的接口进行 RSA 密钥对生成、数字签名、签名验证、加解密运算。RSA 算法的性能应不低于附录 A 的指标要求。

8.2 SM2 算法

通过 GM/T 0017 定义的接口进行 SM2 密钥对生成、数字签名、签名验证、加解密运算。SM2 算法的性能应不低于附录 A 的指标要求。

8.3 SM3 算法

通过 GM/T 0017 定义的接口进行 SM3 杂凑运算。SM3 算法的性能应不低于附录 A 的指标要求。

8.4 SM4 算法

通过 GM/T 0017 定义的接口进行 SM4 加解密运算。SM4 算法的性能应不低于附录 A 的指标要求。

9 安全要求

9.1 密码算法

智能密码钥匙应至少具备公钥密码算法、分组密码算法和杂凑算法。各类密码算法的配置和使用应按照国家密码管理部门的相关规定实施。各类密码算法的使用应保证在其使用有效期内。

9.2 密钥管理

智能密码钥匙在密钥管理方面，应满足以下要求：

a) 设备发行时，必须对设备认证密钥进行修改。

b) 应保证口令和对称密钥的存储和使用安全：
   - 口令长度应不小于 6 个字符，使用错误口令登录的次数限制应不超过 10 次；
   - 采用安全的方式存储和访问口令，存储在智能密码钥匙内部的口令不能以任何形式输出；
   - 在管理终端和智能密码钥匙之间传输的所有口令和密钥均应加密传输，并保证在传输过程中能够防范重放攻击。

c) 应保证私钥在生成、存储和使用阶段的安全：
   - 签名私钥应在智能密码钥匙内部生成，且不能以任何形式输出；
   - 加密私钥必须以密文方式导入，且不能导出；
   - 应保证私钥的唯一性，不得固化密钥对和用于生成密钥对的素数；
   - 私钥的存储和访问应采用安全的方式，使用过程中不能以任何形式泄露私钥；
   - 智能密码钥匙每次执行签名等敏感操作前均应经过客户身份鉴别，每次执行签名等敏感操作后均应立即清除相应身份鉴别权限。

d) 智能密码钥匙内部存储的密钥应具备防止解剖、探测和非法读取有效的密钥保护机制。

e) 智能密码钥匙应具备抵抗以下各种攻击的能力，包括但不限于：
   - 能量分析攻击，包括简单能量分析和差分能量分析；
   - 电磁分析攻击，包括简单电磁分析和差分电磁分析；
   - 时间分析攻击；
   - 错误注入攻击。

f) 在外部环境发生变化时，智能密码钥匙不应泄露敏感信息或影响安全功能。外部环境的变化包含但不限于：
   - 高低温；
   - 高低电压；
   - 强光干扰；
   - 电磁干扰；
   - 紫外线干扰；
   - 静电干扰；
   - 电压毛刺干扰。

g) 智能密码钥匙内部存储的密钥应具备防止非法使用的权限控制机制。

9.3 多应用安全

智能密码钥匙应支持多应用创建，多应用之间应相互独立，应采用安全机制防止跨应用的非法访问。

9.4 线路传输安全

在设备发行阶段，要求管理终端与智能密码钥匙之间的敏感数据以密文方式传输。

在使用阶段，对客户端程序与智能密码钥匙之间的数据传输方式不做要求。

9.5 设备软件安全防护

智能密码钥匙的固件接口需符合 GM/T 0017，应用接口需符合 GM/T 0016。

应设计安全机制保证智能密码钥匙软件的安全，防范被恶意攻击、篡改、替换或反向工程分析。

10 环境适应性要求

10.1 气候环境适应性

气候环境适应性应符合表 1 的规定。

表 1 气候环境适应性

气候条件		参数
温度	工作	0 ℃～40 ℃
	贮存运输	—20 ℃～55 ℃
相对湿度	工作	20%～85%(40 ℃)
	贮存运输	20%～93%(40 ℃)

10.2 机械环境适应性

机械环境适应性应符合表 2 的规定。

表 2 机械环境适应性

机械条件		参数
静电	接触放电	±4 kV
	空气放电	±8 kV
跌落		1 m
振动		频率范围：10 Hz～150 Hz 振动幅值：3.5 mm 持续时间：30 min
防尘防水		遵守 GB/T 4208—2008 中 IP44 的要求

11 可靠性要求

11.1 平均无故障工作时间

智能密码钥匙的平均无故障工作时间 MTBF 由其中的各个部件的可靠性决定。

智能密码钥匙的平均无故障工作时间 MTBF 应大于 1000 h。

11.2 文件写入次数

在通过 GM/T 0017 定义的文件访问接口对二进制文件进行写入操作时，最低写入次数应不低于 5 万次。

11.3 掉电保护

智能密码钥匙需支持密钥生成、密码运算、文件读写、口令验证和修改等操作过程中的掉电保护功能。

附 录 A
（规范性附录）
算法性能要求

A.1 RSA 算法性能要求(2048 bits)

RSA 算法性能要求(2048 bits)见表 A.1。

表 A.1 RSA 算法性能要求

接口形态	密钥对平均生成时间/s	数字签名时间/ms	签名验证时间/ms	公钥加密/Kbit/s	私钥解密/Kbit/s
USB	＜15	＜500	＜500	＞4	＞4
SD	＜15	＜700	＜700	＞4	＞4
Dock/Lightning	＜15	＜1 000	＜1 000	＞2	＞2
Bluetooth	＜15	＜1 000	＜1 000	＞2	＞2
NFC	＜15	＜1 000	＜1 000	＞2	＞2
音码	＜20	＜4 000	＜3 000	＞0.3	＞0.3

A.2 SM2 算法性能要求

SM2 算法性能要求见表 A.2。

表 A.2 SM2 算法性能要求

接口形态	密钥对平均生成时间/s	数字签名时间/ms	签名验证时间/ms	公钥加密/Kbit/s	私钥解密/Kbit/s
USB	＜5	＜500	＜500	＞4	＞4
SD	＜5	＜500	＜500	＞4	＞4
Dock/Lightning	＜5	＜1 000	＜1 000	＞2	＞2
Bluetooth	＜5	＜1 000	＜1 000	＞2	＞2
NFC	＜5	＜1 000	＜1 000	＞2	＞2
音码	＜7	＜3 000	＜4 000	＞0.3	＞0.3

A.3 SM3 算法性能要求

SM3 算法性能要求见表 A.3。

表 A.3　SM3 算法性能要求

接口形态	杂凑/Kbit/s
USB	＞ 5
SD	＞ 5
Dock/Lightning	＞ 2
Bluetooth	＞ 2
NFC	＞ 2
音码	＞ 0.3

A.4　SM4 算法性能要求

SM4 算法性能要求见表 A.4。

表 A.4　SM4 算法性能要求

接口形态	加密/Kbit/s	解密/Kbit/s
USB	＞ 5	＞ 5
SD	＞ 5	＞ 5
Dock/Lightning	＞ 2	＞ 2
Bluetooth	＞ 2	＞ 2
NFC	＞ 2	＞ 2
音码	＞ 0.5	＞ 0.5

参 考 文 献

[1] GB/T 2423.1—2008 电工电子产品环境试验 第2部分:试验方法 试验A:低温.

[2] GB/T 2423.2—2008 电工电子产品环境试验 第2部分:试验方法 试验B:高温.

[3] GB/T 2423.8—1995 电工电子产品环境试验 第2部分:试验方法 试验Ed:自由跌落.

[4] GB/T 2423.3—2006 电工电子产品环境试验 第2部分:试验方法 试验Cab:恒定湿热试验.

[5] GB/T 2423.10—2008 电工电子产品环境试验 第2部分:试验方法 试验Fc:振动(正弦).

[6] GB/T 17626.2—2006 电磁兼容 试验和测量技术 静电放电抗扰度试验.

[7] JR/T 0068—2012 网上银行系统信息安全通用规范.

中华人民共和国密码
行业标准
智能密码钥匙技术规范
GM/T 0027—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.25 字数 24 千字
2014年4月第一版 2014年4月第一次印刷
*
书号:155066·2-27019

GM/T 0027-2014