

ICS 35.030
CCS L 80



中华人民共和国密码行业标准

GM/T 0017—2023

代替 GM/T 0017—2012

智能密码钥匙密码应用接口数据格式规范

Smart token cryptography application interface data format specification

2023-12-04 发布

2024-06-01 实施

国家密码管理局 发布

目 次

前言	III
引言	V
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
4.1 符号	2
4.2 缩略语	2
5 结构模型	3
6 APDU 报文结构	4
6.1 概述	4
6.2 命令 APDU	4
6.3 命令体的编码约定	5
6.4 响应 APDU	6
7 命令头、数据字段和响应状态字的编码约定	6
7.1 概述	6
7.2 CLA(类别)字节	7
7.3 INS(指令)字节	7
7.4 参数字节	10
7.5 数据字段字节	10
7.6 状态字节	10
8 APDU 指令	12
8.1 设备管理指令	12
8.2 访问控制指令	17
8.3 应用管理指令	25
8.4 文件管理指令	31
8.5 容器管理指令	39
8.6 密码服务指令	48
8.7 验证调试类指令	101
9 设备接口协议	112
9.1 使用要求	112
9.2 CCID 协议	112
9.3 USB Mass Storage 协议扩展	112

9.4 HID 协议扩展	116
附录 A (规范性) 设备返回码定义	120
附录 B (规范性) 安全报文计算过程	122
附录 C (资料性) 编程范例	124
附录 D (规范性) SM9 APDU 指令	160
附录 E (资料性) SM9 算法编程范例	192
附录 F (规范性) VPN 相关 APDU 指令	210
附录 G (规范性) BLE 接口协议	217
参考文献	221

前　　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分:标准化文件的结构和起草规则》的规定起草。

本文件代替 GM/T 0017—2012《智能密码钥匙密码应用接口数据格式规范》，与 GM/T 0017—2012 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 删除了术语“智能密码钥匙”（见 2012 年版的 3.1）、“设备”（见 2012 年版的 3.2）、“功能”（见 2012 年版的 3.5）和“消息鉴别码”（见 2012 年版的 3.6）；
- b) 更改了术语“应用”的说明（见 3.5,2012 年版的 3.9）；
- c) 增加了缩略语“ASCII”“BLE”“NFC”和“UUID”（见 4.2）；
- d) 更改了缩略语“CBC”“ECB”“MAC”的说明（见 4.2,2012 年版的第 4 章）；
- e) 更改了“结构模型”的图 1（见第 5 章,2012 年版的第 6 章）；
- f) 更改了 APDU 报文结构概述（见 6.1,2012 年版的 7.1）；
- g) 增加了带密钥的杂凑运算（HMAC）相关指令、验证调试类指令、SM9 APDU 指令和 VPN 相关 APDU 指令（见 7.3、8.6.36、8.6.37、8.6.38、8.6.39、8.7、附录 A、附录 B）；
- h) 更改了 ExtRSAPubKeyOperation（外部 RSA 公钥运算）指令的 INS 字节，由‘60’改为‘8A’（见 7.3、8.6.8.3,2012 年版的 8.3、9.6.9.3）；
- i) 更改了标准版本号，将 GetDevInfo（获取设备信息）指令返回的设备信息中的标准当前版本号由“1.0”更改为“2.0”（见 8.1.3.5,2012 年版的 9.1.3.5）；
- j) 更改了 ChangeDevAuthKey（修改设备认证密钥）指令的命令报文 DATA 字段中对密文数据长度的说明（见 8.2.3.3,2012 年版的 9.2.3.3）；
- k) 更改了 ChangePin（修改 PIN）、VerifyPin（校验 PIN）、UnblockPin（解锁 PIN）指令中使用的杂凑算法，由 SHA1 更改为 SM3（见 8.2.5、8.2.6、8.2.7,2012 年版的 9.2.5、9.2.6、9.2.7）；
- l) 更改了 EnumContainer（枚举容器）、DestroySessionKey（销毁会话密钥）指令的命令报文 Le 字段说明（见 8.5.5.3、8.6.40.3,2012 年版的 9.5.5.3、9.6.38.3）；
- m) 更改了 GetContainerInfo（获取容器信息）、ExportPublicKey（导出公钥）、ImportSessionKey（导入加密会话密钥）指令，增加对 SM9 算法的支持（见 8.5.7、8.6.18、8.6.19,2012 年版的 9.5.7、9.6.24、9.6.25）；
- n) 更改了密码服务指令概述（见 8.6.1,2012 年版的 9.6.1）；
- o) 更改了 GenRSAKeyPair（生成 RSA 签名密钥对）、ImportRSAKeyPair（导入 RSA 加密密钥对）指令的“注意事项”（见 8.6.3.2、8.6.4.2,2012 年版的 9.6.3.2、9.6.4.2）；
- p) 更改了 RSASignData（RSA 签名）和 RSAVerify（RSA 验签）指令的命令报文编码，不再支持 SHA1 算法（见 8.6.5.3、8.6.6.3,2012 年版的 9.6.5.3、9.6.6.3）；
- q) 删除了 RSAExportSessionKeyEx（RSA 导出会话密钥）指令（见 2012 年版的 9.6.8）和 ECCExportSessionKeyEx（ECC 导出会话密钥）指令（见 2012 年版的 9.6.15）；
- r) 更改了 GenerateAgreementDataWithECC（SM2 生成密钥协商参数并输出）、GenerateAgreementDataAndKeyWithECC（SM2 产生协商数据并计算会话密钥）和 GenerateKeyWithECC（SM2 计算会话密钥）指令的响应报文数据域，分别增加了发起方 SM2 公钥和响应方 SM2 公钥，会话密钥 ID 的长度统一为 2 字节（见 8.6.15.5、8.6.16.5、8.6.17.5,2012 年版的 9.6.17.5、9.6.18.5、9.6.19.5）；

- s) 更改了 EncryptInit(加密初始化)、DecryptInit(解密初始化)和 MACInit(消息鉴别码运算初始化)指令的命令报文数据域编码,删除“填充方式”字段(见 8.6.20.4、8.6.24.4、8.6.32.4,2012 年版的 9.6.22.4、9.6.26.4、9.6.34.4);
- t) 更改了 DecryptInit(解密初始化)指令的命令报文数据域,增加了“算法标识”字段(见 8.6.24.4, 2012 年版的 9.6.26.4);
- u) 更改了 DigestInit(密码杂凑初始化)指令的命令报文编码,不再支持 SHA1 算法(见 8.6.28.3, 2012 年版的 9.6.30.3);
- v) 更改了设备接口协议概述(见 9.1,2012 年版的 10.1);
- w) 删除了“设备识别机制”(见 2012 年版的 10.2);
- x) 更改了对大容量存储设备的说明(见 9.3.2,见 2012 年版的 10.4.2);
- y) 增加了 SM9 算法编程范例和蓝牙 BLE 接口协议(见附录 F、附录 G)。

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专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位:北京握奇智能科技有限公司、北京江南天安科技有限公司、北京国脉信安科技有限公司、北京海泰方圆科技股份有限公司、中电科网络安全科技股份有限公司、飞天诚信科技股份有限公司、北京天地融科技有限公司、恒宝股份有限公司、北京数字证书认证中心有限公司、北京天威诚信电子商务服务有限公司、北京国富安电子商务安全认证有限公司、北京华大智宝电子系统有限公司、北京大明五洲科技有限公司、中钞信用卡产业发展有限公司、北京华虹集成电路设计有限责任公司、北京旋极信息技术股份有限公司、北京创原天地科技有限公司、中铁信安(北京)信息安全技术有限公司、北京天诚盛业科技有限公司、东方口岸科技有限公司、格尔软件股份有限公司、北京永新视博数字电视技术有限公司、吉大正元信息技术股份有限公司、深圳市文鼎创数据科技有限公司、武汉天喻信息产业股份有限公司。

本文件主要起草人:刘平、李勃、张渊、汪宗斌、袁峰、蒋红宇、罗俊、郑强、王艳平、李少雄、刘波、李庆、邓小四、汪雪林、李国、胡衍分、朱鹏飞、赵李明、冯承勇、张海松、付伟、封维端、陈国。

本文件及其所代替文件的历次版本发布情况为:

——2012 年首次发布为 GM/T 0017—2012;

——本次为第一次修订。

引　　言

本文件的目标是为公钥密码基础设施应用体系框架下的智能密码钥匙设备制定统一的接口数据格式标准。在设备访问层规定统一的接口数据格式,为该类密码设备的开发、使用及检测提供标准依据和指导,有利于提高该类密码设备的产品化、标准化和互操作性水平。

本文件凡涉及密码算法相关内容,按国家有关法规实施。

智能密码钥匙密码应用接口数据格式规范

1 范围

本文件规定了智能密码钥匙密码应用接口与设备之间的数据交换格式,给出了接口相关数据的类型、格式、参数和使用方法的说明。

本文件适用于智能密码钥匙产品的研制、使用和检测。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 16649.3 识别卡 带触点的集成电路卡 第3部分:电信号和传输协议
- GB/T 35276 信息安全技术 SM2 密码算法使用规范
- GB/T 41389 信息安全技术 SM9 密码算法使用规范
- GM/T 0006 密码应用标识规范
- GM/T 0016 智能密码钥匙密码应用接口规范
- GM/T 0022 IPSec VPN 技术规范
- GM/T 0024 SSL VPN 技术规范
- 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

命令 command

应用接口向设备发出的用于启动一个操作或请求一个应答的信息。

3.2

响应 response

设备处理完成收到的命令后,返回给应用接口的信息。

3.3

管理员 PIN administrator PIN

以 ASCII 字符串表示的管理员口令。

3.4

用户 PIN user PIN

以 ASCII 字符串表示的用户个人口令。

3.5

应用 application

具备独立的权限管理包括容器和文件的结构。