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。

3.6

容器　container

密码设备中用于保存密钥所划分的唯一性存储空间。

3.7

设备认证　device authentication

智能密码钥匙对应用程序的认证。

3.8

设备认证密钥　device authentication key

用于设备认证的密钥。

3.9

设备标签　device label

设备的别名。

注：由用户进行设定并存储于设备内部。

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

(B_1)	表示字节(B_1)的值
$B_1 \parallel B_2$	表示字节 B_1(最高有效字节)和 B_2(最低有效字节)的并置
$(B_1 \parallel B_2)$	表示字节 B_1 和 B_2 并置的值
Lc	APDU 命令的报文数据域长度
Le	APDU 命令的期望返回数据长度
P1	APDU 命令头中的参数 1
P2	APDU 命令头中的参数 2
SW1	APDU 命令的返回状态码 1
SW2	APDU 命令的返回状态码 2
XX	表示 1 个字节 16 进制数
XXXX	表示 2 个字节 16 进制数
XX…XX	表示若干个字节 16 进制数

4.2　缩略语

下列缩略语适用于本文件。

APDU	应用协议数据单元(Application Protocol Data Unit)
API	应用编程接口(Application Programming Interface)
ASCII	美国信息交换标准码(American Standard Code for Information Interchange)
BLE	低功耗蓝牙(Bluetooth Low Energy)
CBC	密文分组链接(Cipher Block Chaining)
CCID	集成电路卡接口设备(Integreted Circuits Card Interface Device)
CLA	APDU 的类型字节(Class Type)
COS	卡操作系统(Card Operating System)
ECB	电码本(Electronic Codebook)
HID	人机接口设备(Human Interface Device)

ICC	集成电路卡(Integrated Circuit Card)
INS	APDU 的命令字节(Instruction Byte of Command Message)
MAC	消息鉴别码(Message Authentication Code)
NFC	近场通信(Near Field Communication)
PIN	个人识别码(Personal Identification Number)
PKCS	公钥密码使用标准(the Public-Key Cryptography Standard)
PKCS #1	公钥密码使用标准系列规范中的第 1 部分(The Public—Key Cryptography Standard Part 1)
PKI	公钥基础设施(Public Key Infrastructure)
RFU	保留给未来使用(Reserved for future use)
UMS	大容量存储设备(USB Mass Storage)
USB	通用串行总线(Universal Serials BUS)
UUID	通用唯一识别码(Universally Unique Identifier)

5 结构模型

智能密码钥匙密码应用接口数据格式位于智能密码钥匙应用程序与设备之间,见图 1。

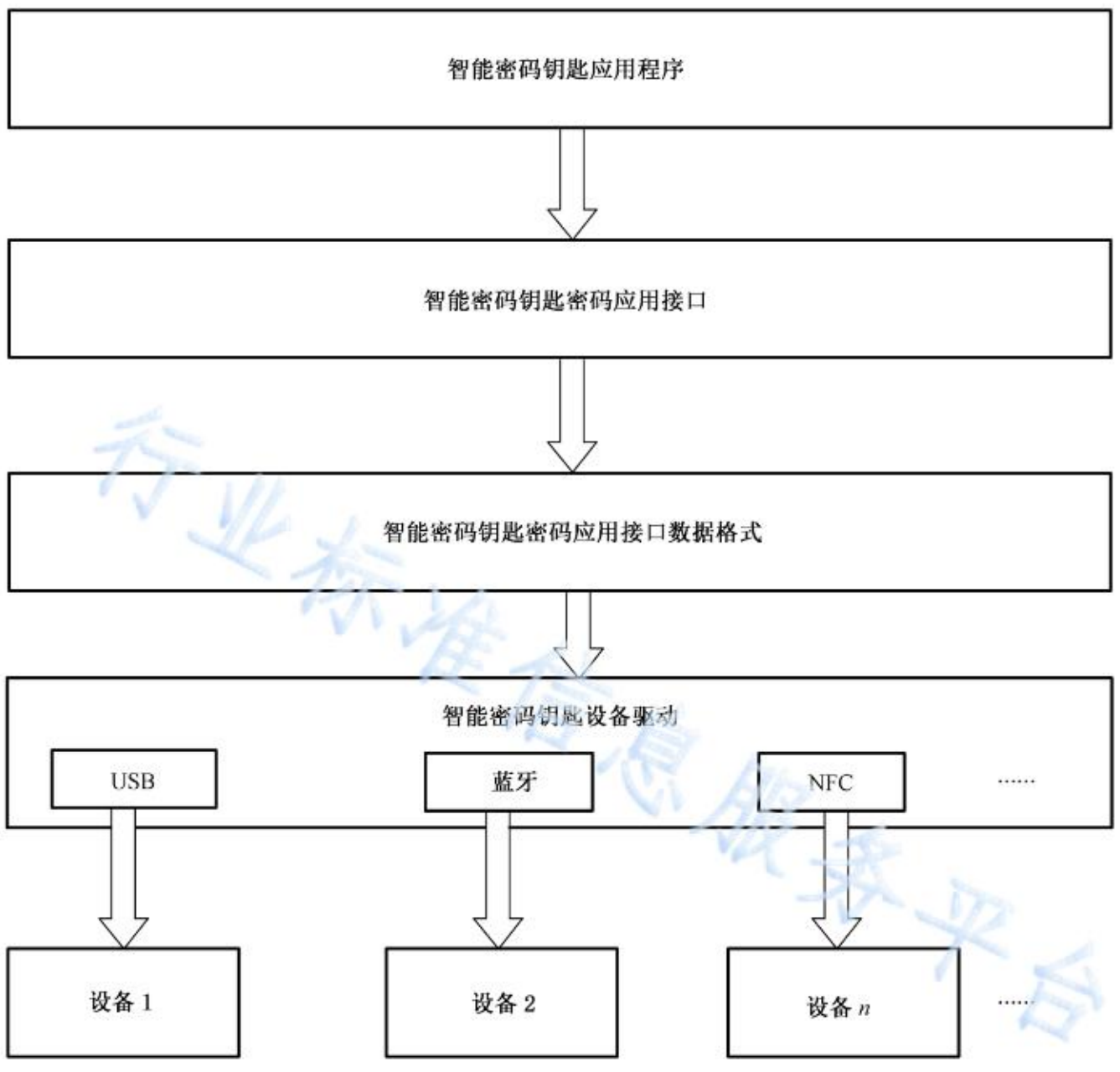

图 1 数据格式规范在应用层次关系中的位置

6 APDU 报文结构

6.1 概述

智能密码钥匙密码应用接口与设备之间的数据交换以 APDU 的形式进行编码。

应用协议由发送命令、接收实体处理命令以及返回响应组成。因此，特定的响应对应于特定的命令，称作为命令响应对。

命令报文和响应报文统称为 APDU，命令报文从接口设备发送到密码钥匙，响应报文由密码钥匙返回到接口设备。

在命令响应对中，命令报文和响应报文都可包含有数据，共有 4 种组合，见表 1。

表 1 命令响应对内的数据

情况	命令数据	期望响应的数据
1	无数据	无数据
2	无数据	有数据
3	有数据	无数据
4	有数据	有数据

6.2 命令 APDU

命令 APDU 结构见图 2，本条所定义的命令 APDU 由下列内容组成：

——必备的 4 字节命令头(CLA　INS　P1　P2)；

——有条件的可变长度主体。

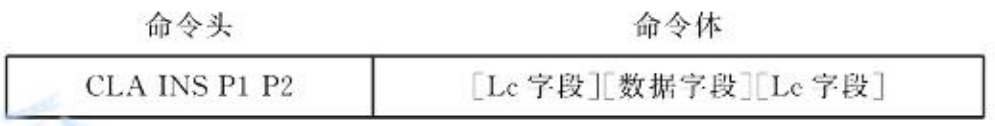

图 2 命令 APDU 结构

在命令 APDU 的数据字段中出现的字节数用 Lc 来表示。

在响应 APDU 的数据字段中期望的字节最大数用 Le(期望数据的长度)来表示。当 Le 字段只包含 0 时，则要求有效数据字节的最大数。

按照表 1 中的 4 种情况，对应的命令 APDU 的 4 种结构见图 3。

图 3 命令 APDU 的 4 种结构

在情况 1 中，长度 Lc 为 0，因此 Lc 字段和数据字段都为空。长度 Le 也为 0，因此 Le 字段为空。从而，命令体为空。

在情况 2 中，长度 Lc 为 0，因此 Lc 字段和数据字段都为空。长度 Le 不为 0，因此 Le 字段存在。从而，命令体由 Le 字段组成。

在情况 3 中，长度 Lc 不为 0，因此 Lc 字段存在，并且数据字段由 Lc 后续字节组成。长度 Le 为 0，因此 Le 字段为空。从而命令体由 Lc 字段后紧跟着数据字段组成。

在情况 4 中，长度 Lc 不为 0，因此 Lc 字段存在，并且数据字段由 Lc 后续字节组成。长度 Le 也不为 0，因此 Le 字段也存在。从而命令体由 Lc 字段后紧跟着数据字段和 Le 字段组成。

6.3 命令体的编码约定

在情况 1 中，命令 APDU 的命令体为空。这种命令 APDU 未带长度字段。

在情况 2、3 和 4 中，命令 APDU 的命令体由 $B_1 \sim B_L$ 所表示的 L 字节组成，见图 4。这种命令体运载了 1 个或 2 个长度字段；B1 是第 1 个长度字段的一部分。

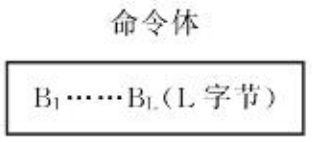

图 4 不为空的命令体

本文件要求 Lc 字段和 Le 字段应为扩充方式编码（B_1 的值为‘00’，并且每个长度值都按 2 个其他字节进行编码）。

按照表 1 和图 3 中的 4 种情况及可能的 Lc、Le 扩展，命令 APDU 的编码见表 2。

表 2 命令 APDU 的编码

条件			情况
L＝0；	—	—	1
L＝3；	$(B_1)=0$；	—	2
L＝3＋$(B_2 \parallel B_3)$；	$(B_1)=0$；	$(B_2 \parallel B_3)\neq 0$	3
L＝5＋$(B_2 \parallel B_3)$；	$(B_1)=0$；	$(B_2 \parallel B_3)\neq 0$	4

任何其他命令 APDU 为无效的。

对以上 4 种情况说明如下。

情况 1：L＝0，主体为空。

——没有字节用于值为 0 的 Lc。

——没有数据字节存在。

——没有字节用于值为 0 的 Le。

情况 2：L＝3，并且$(B_1)=0$。

——没有字节用于值为 0 的 Lc 。

——没有数据字节存在。

——Le 字段由 3 个字节组成，其中 $B_1=0$，B_2 和 B_3 为 Le 的实际值，B_2 为高位字节。若 Le 为 0，则期望返回数据的 65 536 字节。

情况 3：L＝3＋$(B_2 \parallel B_3)$，$(B_1)=0$，并且$(B_2 \parallel B_3)\neq 0$。

——Lc 字段由前 3 个字节组成，其中，B_2 和 B_3 为 Lc 的实际值（1～65 535），B_2 为高位字节。

——$B_1 \sim B_L$ 是数据字段中的 Lc 字节。