ICS 35.040
L 80
备案号:38315—2013

GM

中华人民共和国密码行业标准

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

2012-11-22 发布　　2012-11-22 实施

国家密码管理局　　发 布

目　　次

前言 …… Ⅴ
引言 …… Ⅵ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　记号 …… 3
6　结构模型 …… 3
7　APDU 报文结构 …… 4
7.1　概述 …… 4
7.2　命令 APDU …… 5
7.3　命令体的编码约定 …… 5
7.4　响应 APDU …… 6
8　命令头、数据字段和响应状态字的编码约定 …… 7
8.1　概述 …… 7
8.2　CLA(类别)字节 …… 7
8.3　INS(指令)字节 …… 7
8.4　参数字节 …… 9
8.5　数据字段字节 …… 10
8.6　状态字节 …… 10
9　APDU 指令 …… 11
9.1　设备管理指令 …… 11
9.1.1　概述 …… 11
9.1.2　SetLabel(设置设备标签) …… 12
9.1.3　GetDevInfo(获取设备信息) …… 13
9.2　访问控制指令 …… 16
9.2.1　概述 …… 16
9.2.2　DevAuth (设备认证) …… 16
9.2.3　ChangeDevAuthKey(修改设备认证密钥) …… 17
9.2.4　GetPinInfo (获取 PIN 信息) …… 18
9.2.5　ChangePin (修改 PIN) …… 19
9.2.6　VerifyPin (校验 PIN) …… 21
9.2.7　UnblockPin (解锁 PIN) …… 22
9.2.8　ClearSecureState (清除应用安全状态) …… 23
9.3　应用管理指令 …… 24
9.3.1　概述 …… 24

9.3.2 CreateApplication（创建应用） …… 24
9.3.3 EnumApplication（枚举应用）…… 25
9.3.4 DeleteApplication（删除应用）…… 26
9.3.5 OpenApplication（打开应用） …… 27
9.3.6 CloseApplication（关闭应用） …… 29
9.4 文件管理指令…… 29
9.4.1 概述…… 29
9.4.2 CreateFile(创建文件） …… 30
9.4.3 DeleteFile(删除文件） …… 31
9.4.4 EnumFiles(枚举文件） …… 32
9.4.5 GetFileInfo(获取文件信息）…… 33
9.4.6 ReadFile（读文件） …… 34
9.4.7 WriteFile（写文件） …… 35
9.5 容器管理指令…… 37
9.5.1 概述…… 37
9.5.2 CreateContainer(创建容器）…… 37
9.5.3 OpenContainer(打开容器） …… 38
9.5.4 CloseContainer(关闭容器） …… 39
9.5.5 EnumContainer（枚举容器） …… 40
9.5.6 DeleteContainer（删除容器） …… 41
9.5.7 GetContainerInfo(获取容器信息） …… 42
9.5.8 ImportCertificate(导入数字证书） …… 43
9.5.9 ExportCertificate(导出数字证书） …… 44
9.6 密码服务指令…… 45
9.6.1 概述…… 45
9.6.2 GenRandom（生成随机数）…… 45
9.6.3 GenRSAKeyPair（生成 RSA 签名密钥对） …… 46
9.6.4 ImportRSAKeyPair（导入 RSA 加密密钥对） …… 48
9.6.5 RSASignData（RSA 签名） …… 49
9.6.6 RSAVerify(RSA 验签） …… 50
9.6.7 RSAExportSessionKey（RSA 生成并导出会话密钥） …… 52
9.6.8 RSAExportSessionKeyEx（RSA 导出会话密钥）…… 53
9.6.9 ExtRSAPubKeyOperation(RSA 外来公钥运算）…… 55
9.6.10 GenECCKeyPair(生成 ECC 签名密钥对） …… 56
9.6.11 ImportECCKeyPair(导入 ECC 加密密钥对） …… 57
9.6.12 ECCSignData(ECC 签名） …… 60
9.6.13 ECCVerify(ECC 验签） …… 61
9.6.14 ECCExportSessionKey(ECC 生成并导出会话密钥） …… 63
9.6.15 ECCExportSessionKeyEx(ECC 导出会话密钥）…… 65
9.6.16 ExtECCEncrypt(ECC 外来公钥加密）…… 66
9.6.17 GenerateAgreementDataWithECC(ECC 生成密钥协商参数并输出） …… 68
9.6.18 GenerateAgreementDataAndKeyWithECC(ECC 产生协商数据并计算会话密钥）…… 69
9.6.19 GenerateKeyWithECC(ECC 计算会话密钥） …… 71

9.6.20 ExportPublicKey(导出公钥) …… 73
9.6.21 ImportSessionKey(导入加密会话密钥) …… 74
9.6.22 EncryptInit(加密初始化) …… 76
9.6.23 Encrypt(单组数据加密) …… 77
9.6.24 EncryptUpdate(多组数据加密) …… 78
9.6.25 EncryptFinal(结束加密) …… 79
9.6.26 DecryptInit(解密初始化) …… 81
9.6.27 Decrypt(单组数据解密) …… 82
9.6.28 DecryptUpdate(多组数据解密) …… 83
9.6.29 DecryptFinal(结束解密) …… 84
9.6.30 DigestInit(密码杂凑初始化) …… 85
9.6.31 Digest(单组数据密码杂凑) …… 87
9.6.32 DigestUpdate(多组数据密码杂凑) …… 88
9.6.33 DigestFinal(结束密码杂凑) …… 89
9.6.34 MacInit(消息鉴别码运算初始化) …… 90
9.6.35 Mac(单组数据消息鉴别码运算) …… 91
9.6.36 MacUpdate(多组数据消息鉴别码运算) …… 92
9.6.37 MacFinal(结束消息鉴别码运算) …… 93
9.6.38 DestroySessionKey(销毁会话密钥) …… 94
10 设备协议 …… 95
10.1 概述 …… 95
10.2 设备识别机制 …… 96
10.3 CCID 协议 …… 96
10.4 USB Mass Storage 协议扩展 …… 96
10.4.1 术语 …… 96
10.4.2 大容量存储设备(USB Mass Storage) …… 96
10.4.3 APDU 命令响应对 …… 97
10.4.4 错误代码类型 …… 99
10.5 HID 协议扩展 …… 99
10.5.1 术语 …… 99
10.5.2 HID 协议简介 …… 100
10.5.3 数据包格式 …… 100
附录 A(规范性附录) 设备返回码定义和说明 …… 104
附录 B(规范性附录) 安全报文计算说明 …… 106
附录 C(资料性附录) 编程范例 …… 108
C.1 设备认证 …… 108
C.2 修改设备认证密钥 …… 110
C.3 设置设备标签 …… 111
C.4 添加应用 …… 112
C.5 删除应用 …… 114
C.6 修改 PIN …… 115
C.7 校验 PIN …… 118

C.8 PIN 解锁 …… 122
C.9 创建密钥容器 …… 125
C.10 删除密钥容器 …… 128
C.11 ECC 证书制作流程 …… 131
C.12 使用 SM2 密钥对进行数字签名 …… 137
C.13 使用 SM2 进行数字签名验证 …… 139
C.14 使用 SM2 密钥对交换会话密钥 …… 141

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。

本标准的附录 A、附录 B 为规范性附录，附录 C 为资料性附录。

本标准由国家密码管理局提出并归口。

本标准主要起草单位：北京江南天安科技有限公司、北京握奇智能科技有限公司、北京飞天诚信科技有限公司、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。

本标准参与制定单位：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，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、格尔世纪智能卡科技有限公司，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。

本标准主要起草人：刘平、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。

引　言

国家密码管理局发布的GM/T 0016《智能密码钥匙密码应用接口规范》,在应用层为国内智能密码钥匙的使用提供了统一的技术标准和接口规范,取得了良好的效果。为了更好地解决此接口规范与不同设备提供商的产品兼容性问题,在设备访问层提供统一的接口数据格式,编制《智能密码钥匙密码应用接口数据格式规范》很有必要。本标准在GM/T 0016《智能密码钥匙密码应用接口规范》的基础上进一步规定了这类产品的数据访问接口,从数据类型、数据格式、参数描述和定义、安全性要求等方面进行了具体描述,可用于指导相关产品的研制、使用和检测。

本标准涉及的密码算法按照国家密码管理部门的要求使用。

智能密码钥匙
密码应用接口数据格式规范

1 范围

本标准规定了基于PKI密码体系的智能密码钥匙应用接口数据格式，给出了接口相关数据的类型、格式、参数的定义和描述、安全性要求。

本标准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。

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—2012 智能密码钥匙密码应用接口规范

ISO 7816-4 识别卡——带触点的集成电路卡 第4部分：组织、安全和交换命令

PKCS #1—RSA 实验室，RSA加密标准，v2.1，2002.7

Specification for Integrated Circuit(s) Cards Interface Devices，Revision 1.1，2005

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 smart token

能完成密码功能和安全存储的终端密码产品，一般采用USB接口。

3.2

设备 device

本标准中将智能密码钥匙统称为设备。

3.3

命令 command

应用接口向设备发出的一条信息，该信息启动一个操作或请求一个应答。

3.4

响应 response

设备处理完成收到的命令报文后，返回给应用接口的报文。

3.5

功能 function

由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。