Utap/Uyee产品COS应用接口手册

（版本：6.0.5.2）

中国金融认证中心

2022年07月6日

版权声明：本文档的版权属于中国金融认证中心，任何人或组织未经许可，

不得擅自修改、拷贝或以其它方式使用本文档中的内容

文档修订记录

本文档会随时保持更新，请与中国金融认证中心索要最新版本

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **内容** | **日期** | **编写** | **审核** |
| 6.0.0.1 | 完成初稿 | 2018/11/12 | 赵波 |  |
| 6.0.0.2 | 修改个别指令报文格式 | 2019/3/27 | 姜晓新 |  |
| 6.0.0.3 | 修改“导入SM2密钥对”和“导入加密会话密钥”接口 | 2019/11/5 | 赵波 |  |
| 6.0.1.0 | 增加导入用户密钥对接口，仅用于定制版本需求 | 2020/10/10 | 姜晓新 |  |
| 6.0.2.0 | 增加对称算法运算接口；整理文档格式 | 2021/3/16 | 姜晓新 |  |
| 6.0.3.0 | 确认累积修订记录，文档整理 | 2021/10/29 | 姜晓新 |  |
| 6.0.3.1 | 增加密钥协商接口 | 2021/11/4 | 王旭 |  |
| 6.0.4.1 | 增加3.3.39至3.3.45接口 | 2022/02/22 | 王旭 |  |
| 6.0.5.1 | Utap v6.1.6.1（含）以后版本支持外部运算和密钥协商接口 | 2022/7/6 | 王旭 |  |
| 6.0.5.2 | 修改3.3.47, 3.3.49, 3.3.52部分字段长度 | 2022/10/10 | 王旭 |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：对该文件内容增加、删除或修改须填写此修订记录，详细记载变更信息，以保证其可追溯性。

目 录

[1 关于本手册 1](#_Toc96509651)

[2 主要功能实现机制 1](#_Toc96509652)

[2.1 设备管理 1](#_Toc96509653)

[2.1.1 生命周期阶段划分 1](#_Toc96509654)

[2.1.2 生产阶段 2](#_Toc96509655)

[2.2 文件管理 7](#_Toc96509656)

[2.3 应用管理 9](#_Toc96509657)

[2.4 容器管理 12](#_Toc96509658)

[2.4.1 容器文件 12](#_Toc96509659)

[2.4.2 容器管理 14](#_Toc96509660)

[2.5 身份鉴别 14](#_Toc96509661)

[2.6 权限控制 15](#_Toc96509662)

[2.6.1 权限状态 15](#_Toc96509663)

[2.6.2 指令集合 16](#_Toc96509664)

[2.6.3 CAPDU指令与权限控制 20](#_Toc96509665)

[2.6.4 RAPDU权限状态管理 21](#_Toc96509666)

[2.7 密码运算 22](#_Toc96509667)

[2.8 传输协议 23](#_Toc96509668)

[2.9 按键控制 23](#_Toc96509669)

[3 APDU指令 23](#_Toc96509670)

[3.1 指令结构 23](#_Toc96509671)

[3.2 指令列表 25](#_Toc96509672)

[3.3 指令描述 28](#_Toc96509673)

[3.3.1 设置设备标签（0x02） 28](#_Toc96509674)

[3.3.2 设置设备序列号（0x03） 29](#_Toc96509675)

[3.3.3 获取设备信息（0x04） 30](#_Toc96509676)

[3.3.4 初始化设备认证密钥（0x05） 31](#_Toc96509677)

[3.3.5 导入设备认证信息（0x06） 33](#_Toc96509678)

[3.3.6 导出设备认证信息（0x07） 34](#_Toc96509679)

[3.3.7 擦除COS（0x08） 35](#_Toc96509680)

[3.3.8 清空MF（0x09） 36](#_Toc96509681)

[3.3.9 协商传输会话密钥（0x0A） 37](#_Toc96509682)

[3.3.10 设备认证（0x10） 38](#_Toc96509683)

[3.3.11 获取PIN信息（0x14） 39](#_Toc96509684)

[3.3.12 修改PIN（0x16） 40](#_Toc96509685)

[3.3.13 校验PIN（0x18） 42](#_Toc96509686)

[3.3.14 解锁PIN（0x1A） 44](#_Toc96509687)

[3.3.15 清除应用安全状态（0x1C） 46](#_Toc96509688)

[3.3.16 创建数据文件（0x30） 47](#_Toc96509689)

[3.3.17 删除数据文件（0x32） 48](#_Toc96509690)

[3.3.18 获取文件信息（0x36） 49](#_Toc96509691)

[3.3.19 读数据文件（0x38） 50](#_Toc96509692)

[3.3.20 写数据文件（0x3A） 51](#_Toc96509693)

[3.3.21 初始化文件系统（0x3E） 52](#_Toc96509694)

[3.3.22 创建应用（0x20） 53](#_Toc96509695)

[3.3.23 获取应用配置信息（0x2A） 54](#_Toc96509696)

[3.3.24 恢复应用初始化状态（0x2B） 55](#_Toc96509697)

[3.3.25 创建容器（0x40） 57](#_Toc96509698)

[3.3.26 枚举容器（0x46） 58](#_Toc96509699)

[3.3.27 删除容器（0x48） 59](#_Toc96509700)

[3.3.28 获取容器信息（0x4A） 60](#_Toc96509701)

[3.3.29 导入数字证书（0x4C） 61](#_Toc96509702)

[3.3.30 导出数字证书（0x4E） 62](#_Toc96509703)

[3.3.31 生成随机数（0x50） 63](#_Toc96509704)

[3.3.32 生成RSA密钥对（0x54） 64](#_Toc96509705)

[3.3.33 导入RSA密钥对（0x56） 65](#_Toc96509706)

[3.3.34 RSA私钥运算（0x57） 67](#_Toc96509707)

[3.3.35 生成SM2密钥对（0x70） 69](#_Toc96509708)

[3.3.36 导入SM2密钥对（0x72） 70](#_Toc96509709)

[3.3.37 SM2私钥签名（0x73） 72](#_Toc96509710)

[3.3.38 SM2私钥解密（0x75） 73](#_Toc96509711)

[3.3.39 SM2生成并导出会话密钥（0x78）\* 74](#_Toc96509712)

[3.3.40 SM2外来公钥加密（0x7A）\* 75](#_Toc96509714)

[3.3.41 SM2外来私钥解密（0x7C）\* 76](#_Toc96509715)

[3.3.42 SM2外来私钥签名（0x7E）\* 77](#_Toc96509716)

[3.3.43 SM2生成密钥协商参数（0x82） 78](#_Toc96509717)

[3.3.44 SM2产生协商数据并计算会话密钥（0x84） 80](#_Toc96509718)

[3.3.45 SM2计算会话密钥（0x86） 82](#_Toc96509719)

[3.3.46 导出公钥（0x88） 84](#_Toc96509720)

[3.3.47 导入加密会话密钥（0xA0） 85](#_Toc96509721)

[3.3.48 导入会话密钥（0xA2） 87](#_Toc96509722)

[3.3.49 加密初始化（0xA4） 88](#_Toc96509723)

[3.3.50 多组数据加密（0xA8） 89](#_Toc96509724)

[3.3.51 结束加密（0xAA） 90](#_Toc96509725)

[3.3.52 解密初始化（0xAC） 91](#_Toc96509726)

[3.3.53 多组数据解密（0xB0） 92](#_Toc96509727)

[3.3.54 结束解密（0xB2） 93](#_Toc96509728)

[3.3.55 销毁会话密钥（0xC4） 94](#_Toc96509729)

[3.3.56 读外部Flash芯片信息（0xE0） 95](#_Toc96509730)

[3.3.57 擦外部FLASH（0xE1） 96](#_Toc96509731)

[3.3.58 写外部FLASH（0xE2） 97](#_Toc96509732)

[3.3.59 读外部FLASH（0xE3） 98](#_Toc96509733)

[3.3.60 按键测试（0xE4） 99](#_Toc96509734)

[3.3.61 密码算法测试（0xE8） 100](#_Toc96509735)

[3.3.62 写外部FLASH用户区（0xE9） 101](#_Toc96509736)

[3.3.63 读外部FLASH用户区（0xEA） 102](#_Toc96509737)

[3.3.64 导入密钥加密密钥（0xEB） 103](#_Toc96509738)

[3.3.65 导出密钥加密密钥（0xEC） 104](#_Toc96509739)

[4 状态码表 105](#_Toc96509740)

# 关于本手册

本手册主要内容：

（1）Utap/Uyee COS设备管理、文件管理、应用管理、容器管理、访问控制、密码运算和通信协议等主要功能的实现机制；

（2）APDU命令与响应格式。

# 主要功能实现机制

## 设备管理

### 生命周期阶段划分

表格2‑1 Utap的生命周期定义

|  |  |  |
| --- | --- | --- |
| 阶段 | 状态（状态码） | 内容 |
| 开发测试 | 开发 | 产品设计开发 |
| 测试 | 功能、性能测试 |
| 生产 | 0xFFFF | 芯片初始状态 |
| 0x0001 | 写SN完成标志位 |
| 0x0002 | 写Label完成标志位 |
| 0x0004 | 设备密钥初始化完成标志位 |
| 0x0008 | 生产密钥初始化完成标志位 |
| 0x0010 | 管理密钥初始化完成标志位 |
| 0x0020 | 文件系统初始化完成标志位 |
| 0x0040 | 应用创建完成标志位，创建应用是生产过程的最后一步，完成后生命周期进入使用阶段。 |
| 使用 | 0x007F | 提供用户使用 |
| 废止 | 废止 | 无法在应用系统中继续使用 |

### 生产阶段

#### 生产状态标志位

生产阶段主要完成：下载COS、写入ISO镜像文件、设置设备序列号、设置设备标签、初始化设备密钥、初始化文件系统、创建应用等操作。

生命周期初始状态为0xFFFF，按照标志位的方式记录生产过程的每一步操作。创建应用是生产阶段的最后一步操作，必须在其它操作执行完成后才可执行（控制状态字为0x003F）。完成应用创建，通过第一次质检后（Utap产品按键功能检测，Uyee产品算法功能检测）COS将生命周期状态置为应用（0x007F）状态。

在应用配置文件中写入应用参数。应用参数的数据结构在GM/T 0017-2012中定义的数据结构基础上进行扩展，将原Utap中配置文件中的数据结构包括在内。

Utap默认应用ID为0x0000。配置参数采用加密方式一次写入到配置文件中。如果生产环境安全可控，出厂初始化和应用初始化可连续进行。如果生产环境不可控，在工厂只进行设置SN（含）以前的出厂初始化操作。

完成应用初始化后，COS将生命周期状态置为使用阶段（0x007F）。

#### 内部存储区

（1）CODE，256KB，存储COS代码。

（2）COS\_DATA，16KB，用于存储COS内部数据，包括：SN、Label、设备密钥对（DevKeyPair）、设备认证密钥（DevAuthKey）、设备生产密钥对对设备密钥对公钥HASH的签名结果、设备生产密钥对公钥、设备管理密钥对公钥。

（3）FILE\_SYSTEM，160KB，用于存储文件系统，文件系统包括：文件系统结构（两套FAT和FDT互为备份）、120KB文件系统数据、文件操作数据备份区（用于实现文件内容写操作时的掉电保护）。

#### 设备信息描述

设备信息描述数据结构采用GM/T 0017-2012中定义的数据结构。COS内部维护设备信息描述数据结构，除Label字段和SerialNumber字段外，其它字段的值在COS版本发布时为确定值。

表格2‑2 设备信息描述

|  |  |  |
| --- | --- | --- |
| 设备信息描述数据结构定义 | | |
| typedef struct Struct\_version{  BYTE major;  BYTE minor;  }VERSION;  typedef struct Struct\_cosDEVINFO{  StruVersion StructVersion;  StruVersion SpecificationVersion;  UINT8 Manufacturer[64];  UINT8 Issuer[64];  UINT8 Label[32];  UINT8 SerialNumber[32];  StruVersion HWVersion; //BigEndian  StruVersion FirmwareVersion; //BigEndian  UINT32 AlgSymCap; //BigEndian  UINT32 AlgAsymCap; //BigEndian  UINT32 AlgHashCap; //BigEndian  UINT32 DevAuthAlgId; //BigEndian  UINT32 TotalSpace; //BigEndian  UINT32 FreeSpace; //BigEndian  UINT16 MaxApduDataLen; //BigEndian  UINT16 UserAuthMethod; //BigEndian  UINT16 DeviceType;//BigEndian  UINT8 MaxContainerNum;  UINT8 MaxCertNum;  UINT16 MaxFileNum; //BigEndian  UINT16 LifeStatus; //LittleEndian  UINT8 CosHeader[8];  UINT8 UartCtrlFlag;  UINT8 ChipType;  UINT8 DefaultPINChangeRule;  UINT8 Reserved[41];} | | |
| 序号 | 数据项 | 意义 |
| 1 | StructVersion | 版本号 |
| 2 | SpecificationVersion | 版本号 |
| 3 | Manufacturer | 设备厂商信息 |
| 4 | Issuer | 发行厂商信息 |
| 5 | Label | 设备标签 |
| 6 | SerialNumber | 序列号（KeyID） |
| 7 | HWVersion | 设备硬件版本 |
| 8 | FirmwareVersion | 设备固件版本 |
| 9 | AlgSymCap | 分组密码算法标识 |
| 10 | AlgAsymCap | 非对称密码算法标识 |
| 11 | AlgHashCap | 密码杂凑算法标识 |
| 12 | DevAuthAlgId | 设备认证分组密码算法标识 |
| 13 | TotalSpace | 设备总空间大小 |
| 14 | FreeSpace | 用户可用空间大小 |
| 15 | MaxApduDataLen | 这边支持的APDU命令数据域最大长度 |
| 16 | UserAuthMethod | 用户认证方式 |
| 17 | DeviceType | 设备类型 |
| 18 | MaxContainerNum | 应用支持的最大容器数量 |
| 19 | MaxCertNum | 应用支持的最大证书数量 |
| 20 | MaxFileNum | 应用支持的最大文件数 |
| 21 | LifeStatus | 当前生命周期状态 |
| 22 | CosHeader | 产品名称 |
| 23 | UartCtrlFlag | Ulan（AS569+Q）BLE下载状态 |
| 24 | ChipType | 芯片型号 |
| 25 | DefaultPINChangeRule | Ucan默认PIN修改策略 |
| 26 | Reserved | 保留字节 |

以下数据项需要特别说明：

（1）Label项，在出厂初始化时通过APDU指令设置Label项的默认值。

（2）SerialNumber项，在出厂初始化时通过APDU指令设置，意义等同于KeyID。

（3）DevAuthAlgId项在原有意义的基础上扩展为设备认证、通信加密过程使用的分组密码算法标识。如果设置为SM4算法，通信加密过程使用SM2算法协商消息密钥；如果设置为TDES，通信加密过程使用RSA1024算法协商消息密钥。

（4）HWVersion和FirmwareVersion，major表示公司4位版本号中的前两位，minor表示公司4位版本号中的后两位。

（5）ChipType指示芯片类型，’H’为华大IS32U512A芯片，’S’为晟元AS569芯片。

#### 生产Key和管理Key

在生产Utap前，需要制作生产Key和管理Key（根据客户需求选择使用）。通过行政管理机制保证生产Key和管理Key安全可控。

生产Key内部保存2对设备生产密钥对（RSA1024和SM2密钥对各一对），2对设备管理密钥对（RSA1024和SM2密钥对各一对）。生产Key可通过密钥导入与导出接口复制生产或制作管理Key。生产初始化工具根据Utap设备信息描述中的DevAuthAlgId项，选择使用相应算法的设备生产密钥对Utap设备密钥对（DevKeyPair）公钥的HASH（RSA密钥对，使用SHA1对数据进行HASH；SM2密钥对，使用SM3对数据进行HASH）结果进行签名，将签名结果、对应的设备生产密钥对公钥，以及对应算法的设备管理密钥对公钥保存到Utap设备。在出厂初始化完成后，使用阶段前，可使用生产Key通过挑战应答方式对Utap执行擦除COS和清空MF。

管理Key内部保存设备管理密钥对。管理Key为选配产品，用户可选择使用管理Key实现用户PIN本地/远程解锁功能。客户只能选择管理Key和管理员PIN中的一种方式对Utap进行管理。管理员通过PIN码对管理Key进行操作。

## 文件管理

COS采用树型文件结构对文件进行管理，在文件系统初始化时，创建如图2‑1所示的文件结构。虚线部分为图章数据文件，由PKCS11库随时创建。

COS内部通过文件属性进行访问控制，文件属性定义见图2‑1：



图2‑1 Utap初始文件结构

表格2‑3 文件属性

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 类型 | 名称 | 备注 | |
| 1 | UINT16 | wFileId | 文件ID，0x3F00为MF专有ID。 | |
| 2 | UINT16 | wFileLen | 文件长度，单位为字节，创建的文件长度不得超过24KB，不得超过剩余空间 | |
| 3 | UINT8 | bFileType | 文件类型，MF/DF文件：0x10；EF文件：0x20 | |
| 4 | UINT8 | bFDTIndex | 文件属性在FDT表中的序号（内部使用） | |
| 5 | UINT8 | bSecTrans | APDU数据加密传输控制，0xB4，密文传输；其它值，明文传输 | |
| 6 | UINT8 | bRFU | 预留 | |
| 7 | UINT8 | bReadControl | 读权限控制字段 | 自由权限：0x00  外部认证：0x01  管理员权限：0x10  用户权限：0x11  配置权限：0x20  禁止权限：0xFF |
| 8 | UINT8 | bWriteControl | 写权限控制字段 |
| 9 | UINT8 | bDelControl | 删除权限控制字段 |
| 10 | UINT8 | bUseControl | 使用权限控制字段 |
| 11 | UINT8 | bFleClass | EF文件种类，应用配置文件，0x01；容器文件，0x11；数据文件，0x21 | |
| 12 | UINT8 | baRFU[3] | 预留 | |

## 应用管理

应用参数的数据结构在GM/T 0017-2012中定义的数据结构基础上进行扩展。支持创建应用和获取应用配置信息功能。

（1）创建应用，仅在生产阶段进行应用初始化时可用。创建应用的过程就是在应用配置文件中写入应用参数。

（2）获取应用配置信息，返回除用户敏感信息外的其它配置信息，主要用于检验应用配置信息的正确性。

应用配置文件ID为0x0000，采用单应用方式，应用配置文件在MF文件夹内。

表格2‑4 应用信息数据结构

|  |  |  |
| --- | --- | --- |
| 应用信息描述数据结构定义 | | |
| typedef struct StruAppInfoPin  {  UINT8 PinType;  UINT8 ModifiedFlag;  UINT8 IniRetryCount;  UINT8 CurrRetryCount;  UINT8 IniPin[32];  UINT8 ModifiedPin[32];  }  typedef struct StruAppInfoSys  {  UINT8 PIDh;  UINT8 PIDl;  UINT8 ButtonTimeout;  UINT8 HashButtonContr;  UINT8 InsButtonContr;  UINT8 WorkPettern;  UINT8 SecKeepTime;  UINT8 ContainerPolicy;  UINT8 UnlockMode;  UINT8 bRFU[7];  UINT8 APDUBitMap[16];  UINT8 Descriptor[8];  }  typedef struct StruAppInfo  {  UINT8 AppName[32];  StruAPPInfoPIN AdminPin;  StruAPPInfoPIN UserPin;  StruAppInfoSys AppSysConfig;  } | | |
| 序号 | 数据项 | 意义 |
| 1 | PinType | PIN类型 |
| 2 | ModifiedFlag | PIN修改标识 |
| 3 | IniRetryCount | 初始重试次数 |
| 4 | CurrRetryCount | 当前重试次数 |
| 5 | IniPin | 初始PIN |
| 6 | ModifiedPin | 修改PIN |
| 7 | PIDh | USB接口PID高字节 |
| 8 | PIDl | USB接口PID低字节 |
| 13 | ButtonTimeout | 按键延时 |
| 14 | HashButtonCtrl | HASH按键控制位，0不需，1需要，默认SHA256需要按键，其他不要需要按键:0x04。  Bit 0:MD5；  Bit 1:SHA1；  Bit 2:SHA256；  Bit 3:SHA512；  Bit 4:SHAMD5；  Bit 5:SHA384; |
| 15 | InsButtonCtrl | 指令按键控制位，0不需，1需要，默认都要需要按键:0xFF。  Bit 0:验证PIN；  Bit 1:修改PIN；  Bit 2:初始化；  Bit 3:SM2签名； |
| 14 | WorkPettern | 工作模式 |
| 15 | SecKeepTime | 安全状态保持超时时间 |
| 16 | ContainerPolicyBitMap | 容器管理策略位图 |
| 17 | UnlockMode | 解锁模式 |
| 17 | bRFU | 预留 |
| 18 | APDUBitMap | 指令使能控制位图 |
| 19 | Descriptor | 描述信息 |

## 容器管理

参考GM/T 0017-2012中定义的容器逻辑结构和容器管理功能接口实现容器管理。

### 容器文件

Utap基于容器文件对容器进行管理，单个应用支持5个容器文件，在应用初始化初始化文件系统时统一创建。文件ID为：0xC000，0xC010，0xC020，0xC030，0xC040。

容器文件内部主要包括三个组成部分，容器信息、密钥对和数字证书。

相关数据结构参考GM/T 0017-2012中定义的容器逻辑结构和C10/C100产品中定义的容器数据结构。

表格2‑5 容器信息数据结构

|  |  |  |
| --- | --- | --- |
| 容器信息数据结构定义 | | |
| #define CONTAINER\_TYPE\_NAMED (0x00)  #define CONTAINER\_TYPE\_RSA (0x01)  #define CONTAINER\_TYPE\_SM2 (0x02)  #define CONTAINER\_TYPE\_EMPTY (0xFF)  #define CONTAINER\_NAME\_MAXLEN (40)  typedef struct  {  UINT8 Type;  UINT8 Status;  UINT8 FileIDh;  UINT8 FileIDl;  UINT8 ExKeyType;  UINT8 ExCertFlag;  UINT8 SignKeyType;  UINT8 SignCertFlag;  UINT8 StepFlag;  UINT8 NameLen;  } ContainerHeadInfo,\*PContainerHeadInfo;  typedef struct  {  ContainerHeadInfo ContainerHead;  UINT8 Name[CONTAINER\_NAME\_MAXLEN];  } Container\_Info,\*PContainer\_Info; | | |
| 序号 | 数据项 | 意义 |
| 1 | Type | 容器类型 |
| 2 | Status | 容器状态，后4位有效 |
| 3 | FileIDh | 容器文件ID高字节 |
| 4 | FileIDl | 容器文件ID低字节 |
| 5 | ExKeyType | 加密密钥对类型 |
| 6 | ExCertFlag | 是否存在加密证书标识 |
| 7 | SignKeyType | 签名密钥对类型 |
| 8 | SignCertFlag | 是否存在签名证书标识 |
| 9 | StepFlag | 容器内部步骤标识 |
| 10 | NameLen | 容器名称长度 |
| 11 | Name | 容器名称 |

### 容器管理

提供创建容器、删除容器、枚举容器、获取容器信息、导入数字证书和导出数字证书。

## 身份鉴别

身份鉴别包括：设备认证、用户PIN码验证、管理员PIN码验证。

鉴别方式与Ulan5相同。在PIN码验证成功后，COS内部保存用户角色和授权码，并将授权码返回给应用，应用使用授权码可完成需要用户/管理员权限的一次指令或一个完整过程的多次指令。

PIN码验证、修改和解锁过程均通过挑战应答机制完成，挑战和应答过程全部采用加密通信方式完成。以下以PIN码验证过程对挑战应答过程进行描述：

（1）应用向Utap获取挑战码，挑战码包括16字节随机数R1和RSA1024临时密钥对公钥（n，e）。

（2）应用计算用户输入PIN的MD5得到M1。使用M1与R1拼接再进行MD5得到M2，对M2使用临时密钥对公钥进行加密，得到应答码C1并将其发送给Utap。

（3）Utap使用临时密钥对私钥对C1进行解密得到M2，对内部加密存储的PIN数据进行解密，采用与应用相同的步骤进行计算，将计算结果与M2进行比较，判定PIN码验证是否通过。若验证通过，则返回授权码。

根据应用信息数据结构中的PIN属性，可配置PIN最大可重试次数（默认8次，国测要求不超过10次），当重试次数还有3次时，强制用户通过确认按键启动PIN验证操作。

可使用管理员PIN或管理Key对用户PIN进行解锁或重置。当使用管理Key时，需要在应答码后附加管理key对应答码的签名结果。

## 权限控制

采用角色、授权码（仅用于用户角色）和权限状态的形式体现当前用户权限。

采用用户权限与指令集合相关联的综合控制策略，解决在数字证书下载、数字签名等需要多步操作的过程中，操作过程的完整性与用户权限控制问题。

### 权限状态

（1）无权限，设备上电状态。

（2）设备权限，完成设备认证（即，外部认证），执行清除应用安全状态时不清除设备权限。

（3）用户权限，通过用户PIN验证时的权限状态。

（4）用户密码应用权限，需要进行多步操作的密码应用，如XML报文签名等，在多步操作过程中为用户保持的权限状态。

（5）用户证书下载权限，需要进行多指令操作的数字证书下载过程中，为用户保持的权限状态。

### 指令集合

表格2‑6 指令集合

|  |  |
| --- | --- |
| 集合名称 | 指令 |
| 生产阶段指令集合 | APDU\_INS\_DEV\_SET\_LABEL  APDU\_INS\_DEV\_SET\_SN  APDU\_INS\_DEV\_GET\_INFO  APDU\_INS\_DEV\_KEY\_INI  APDU\_INS\_DEV\_IMPORT\_AUTH\_KEY  APDU\_INS\_DEV\_EXPORT\_AUTH\_KEY  APDU\_INS\_DEV\_ERASE\_COS  APDU\_INS\_DEV\_FORMAT\_MF  APDU\_INS\_DEV\_IMPORT\_SESSION\_KEY  APDU\_INS\_DEV\_AUTH  APDU\_INS\_PIN\_GET\_INFO  APDU\_INS\_PIN\_VERIFY  APDU\_INS\_FILE\_GET\_INFO  APDU\_INS\_FILE\_READ  APDU\_INS\_FILE\_WRITE  APDU\_INS\_FILE\_INI  APDU\_INS\_APP\_CREATE  APDU\_INS\_CRYPTO\_GET\_RANDOM  APDU\_INS\_APPEND\_FLASH\_GET\_INFO  APDU\_INS\_APPEND\_FLASH\_ERASE  APDU\_INS\_APPEND\_FLASH\_WRITE  APDU\_INS\_APPEND\_FLASH\_READ  APDU\_INS\_APPEND\_TEST\_BUTTON  APDU\_INS\_APPEND\_TEST\_ALG |
| 用户阶段指令集合 | APDU\_INS\_DEV\_SET\_LABEL  APDU\_INS\_DEV\_GET\_INFO  APDU\_INS\_DEV\_EXPORT\_AUTH\_KEY  APDU\_INS\_DEV\_ERASE\_COS  APDU\_INS\_DEV\_IMPORT\_SESSION\_KEY  APDU\_INS\_DEV\_AUTH  APDU\_INS\_PIN\_GET\_INFO  APDU\_INS\_PIN\_CHANGE  APDU\_INS\_PIN\_VERIFY  APDU\_INS\_PIN\_UNLOCK  APDU\_INS\_PIN\_CLEAR\_SECURE\_STATUS  APDU\_INS\_FILE\_CREATE  APDU\_INS\_FILE\_DELETE  APDU\_INS\_FILE\_GET\_INFO  APDU\_INS\_FILE\_READ  APDU\_INS\_FILE\_WRITE  APDU\_INS\_APP\_GET\_CONFIG  APDU\_INS\_APP\_INI  APDU\_INS\_CTNR\_CREATE  APDU\_INS\_CTNR\_ENUM  APDU\_INS\_CTNR\_DELETE  APDU\_INS\_CTNR\_GET\_INFO  APDU\_INS\_CTNR\_IMPORT\_CERT  APDU\_INS\_CTNR\_EXPORT\_CERT  APDU\_INS\_CRYPTO\_GET\_RANDOM  APDU\_INS\_CRYPTO\_GEN\_RSA\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_RSA\_KEY  APDU\_INS\_CRYPTO\_RSA\_PRI\_KEY\_OP  APDU\_INS\_CRYPTO\_GEN\_SM2\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_SM2\_KEY  APDU\_INS\_CRYPTO\_SM2\_SIGN  APDU\_INS\_CRYPTO\_SM2\_DECRYPT  APDU\_INS\_CRYPTO\_EXPORT\_PUB\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_EN\_KEY  APDU\_INS\_APPEND\_FLASH\_GET\_INFO  APDU\_INS\_APPEND\_FLASH\_READ  APDU\_INS\_SM2\_GEN\_AGREE\_DATA  APDU\_INS\_SM2\_GEN\_AGREE\_DATA\_AND\_KEY  APDU\_INS\_SM2\_GENERATE\_KEY |
| 用户权限指令集合 | APDU\_INS\_CTNR\_CREATE  APDU\_INS\_CTNR\_DELETE  APDU\_INS\_CTNR\_IMPORT\_CERT  APDU\_INS\_CRYPTO\_GEN\_RSA\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_RSA\_KEY  APDU\_INS\_CRYPTO\_RSA\_PRI\_KEY\_OP  APDU\_INS\_CRYPTO\_GEN\_SM2\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_SM2\_KEY  APDU\_INS\_CRYPTO\_SM2\_SIGN  APDU\_INS\_CRYPTO\_SM2\_DECRYPT  APDU\_INS\_CRYPTO\_IMPORT\_EN\_KEY  APDU\_INS\_SM2\_GEN\_AGREE\_DATA  APDU\_INS\_SM2\_GEN\_AGREE\_DATA\_AND\_KEY  APDU\_INS\_SM2\_GENERATE\_KEY |
| 用户权限证书下载指令集合 | APDU\_INS\_CTNR\_CREATE  APDU\_INS\_CTNR\_DELETE  APDU\_INS\_CTNR\_IMPORT\_CERT  APDU\_INS\_CRYPTO\_GEN\_RSA\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_RSA\_KEY  APDU\_INS\_CRYPTO\_RSA\_PRI\_KEY\_OP  APDU\_INS\_CRYPTO\_GEN\_SM2\_KEY  APDU\_INS\_CRYPTO\_IMPORT\_SM2\_KEY  APDU\_INS\_CRYPTO\_SM2\_SIGN  APDU\_INS\_CRYPTO\_IMPORT\_EN\_KEY |
| 用户权限密码运算指令集合 | APDU\_INS\_CRYPTO\_RSA\_PRI\_KEY\_OP  APDU\_INS\_CRYPTO\_SM2\_SIGN  APDU\_INS\_CRYPTO\_SM2\_DECRYPT |
| 设备认证权限指令集合 | APDU\_INS\_DEV\_SET\_LABEL  APDU\_INS\_FILE\_CREATE  APDU\_INS\_FILE\_DELETE  APDU\_INS\_FILE\_GET\_INFO  APDU\_INS\_FILE\_READ  APDU\_INS\_FILE\_WRITE |
| 设置权限状态指令集合 | APDU\_INS\_DEV\_AUTH  APDU\_INS\_PIN\_CHANGE  APDU\_INS\_PIN\_VERIFY  APDU\_INS\_PIN\_UNLOCK  APDU\_INS\_PIN\_CLEAR\_SECURE\_STATUS |

### CAPDU指令与权限控制



图2‑2 CAPDU指令与权限控制流程示意图

### RAPDU权限状态管理



图2‑3 RAPDU权限状态管理流程示意图

## 密码运算

表格2‑7 密码算法标识

|  |  |  |
| --- | --- | --- |
| 序号 | 密码算法 | 标识 |
| 1 | ALG\_RSA1024 | 0x01 |
| 2 | ALG\_DES | 0x02 |
| 3 | ALG\_DES\_112 | 0x03 |
| 4 | ALG\_DES3 | 0x04 |
| 5 | ALG\_RSA2048 | 0x07 |
| 6 | ALG\_RC4 | 0x08 |
| 7 | ALG\_MD5 | 0x0a |
| 8 | ALG\_SHA1 | 0x0b |
| 9 | ALG\_SHA256 | 0x0c |
| 10 | ALG\_SHA512 | 0x0d |
| 11 | ALG\_SHAMD5 | 0x0e |
| 12 | ALG\_SHA384 | 0x0f |
| 13 | ALG\_SM1 | 0x10 |
| 14 | ALG\_SM2 | 0x11 |
| 15 | ALG\_SM3 | 0x12 |
| 16 | ALG\_SM4 | 0x13 |
|  | 分组算法运算模式 |  |
| 1 | ALG\_MODE\_ECB | 0x01 |
| 2 | ALG\_MODE\_CBC | 0x02 |
| 3 | ALG\_MODE\_OFB | 0x04 |
| 4 | ALG\_MODE\_CFB | 0x08 |

## 传输协议

支持RSA1024+3DES和SM2+SM4两种方式，上层应用依据设备信息描述中DevAuthAlgId字段的值进行选择。一般情况，标准版本和定制化版本使用SM2+SM4方式，有特殊要求的测试场合使用RSA1024+3DES方式。

## 按键控制

本节内容仅涉及Utap产品。



图2‑4 按键流程

# APDU指令

## 指令结构

APDU指令和响应结构见表格3‑1、表格3‑2和表格3‑3，指令和响应数据包最大长度为350字节，要求Lc和Le不得大于320。

关于大小端字节序的说明：

指令和响应数据默认都是大端字节序，除非特殊说明。APDU指令中Lc和Le为两字节，均为大端字节序。对于包含文件ID、应用ID、容器ID、证书ID字段的指令，这些ID（2字节）都是大端字节序。

表格3‑1 APDU指令结构

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 指令头 | | | | | | | | 数据 |
| Byte | Byte | Byte | Byte | Byte | Byte | Byte | Byte | n Byte（n=Lc） |
| CLA | INS | P1 | P2 | Lc | | Le | | DATA |
| 说明：  CLA表示APDU类型，明文传输时，CLA为0xB0，密文传输时，CLA为0xB4。  INS表示APDU指令码。  P1和P2分别表示APDU指令中的参数1和参数2.  Lc表示数据域长度，大端序。  Le表示期望返回数据域长度，大端序。 | | | | | | | | |

表格3‑2 APDU响应结构

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 状态字 | | | | 数据 |
| Byte | Byte | Byte | Byte | n Byte（n=Len） |
| SW1 | SW2 | Len | | DATA |
| 说明：  SW1和SW2分别表示APDU响应状态码1和状态码2。  Len表示响应数据域长度，大端序。 | | | | |

密文传输时，需要对指令和响应结构中的数据部分进行扩展和填充，然后再进行数据加密。

表格3‑3 加密通信数据域结构

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Byte | Byte | Byte | Byte | n Byte（n=Len） | PKCS5 |
| Identification | | NetDataLen | | NetData | Padding |
| 说明：  Identification，加密通信过程由应用层发起，初始值首字节为消息密钥首字节，COS返回时填充随机数，下一条加密指令时，应用层需要使用上一条指令COS返回的随机数进行填充。  NetDataLen表示NetData数据长度，大端序。  Padding为PKCS5格式填充。 | | | | | |

## 指令列表

本指令列表仅包括标准产品指令，民生银行C100配套Utap、高性能密码卡配套Utap等项目特殊定制产品指令见相关设计文档。

表格3‑4 指令列表

| 序号 | CLA | INS | 指令名称 | 生命周期 | 章节 |
| --- | --- | --- | --- | --- | --- |
|  | 0xB0 | 0x02 | 设置设备标签 | 生产/使用 | 3.3.1 |
|  | 0xB0 | 0x03 | 设置设备序列号 | 生产 | 3.3.2 |
|  | 0xB0 | 0x04 | 获取设备信息 | 生产/使用 | 3.3.3 |
|  | 0xB0 | 0x05 | 初始化设备认证密钥 | 生产 | 3.3.4 |
|  | 0xB0 | 0x06 | 导入设备认证信息 | 生产 | 3.3.5 |
|  | 0xB0 | 0x07 | 导出设备认证信息 | 生产/使用 | 3.3.6 |
|  | 0xB0 | 0x08 | 擦除COS | 生产/使用 | 3.3.7 |
|  | 0xB0 | 0x09 | 清空MF | 生产 | 3.3.8 |
|  | 0xB0 | 0x0A | 协商传输会话密钥 | 生产/使用 | 3.3.9 |
|  | 0xB0 | 0x10 | 设备认证 | 生产/使用 | 3.3.10 |
|  | 0xB4 | 0x14 | 获取PIN信息 | 生产/使用 | 3.3.11 |
|  | 0xB4 | 0x16 | 修改PIN | 使用 | 3.3.12 |
|  | 0xB4 | 0x18 | 校验PIN | 生产/使用 | 3.3.13 |
|  | 0xB4 | 0x1A | 解锁PIN | 使用 | 3.3.14 |
|  | 0xB0 | 0x1C | 清除应用安全状态 | 使用 | 3.3.15 |
|  | 0xB0 | 0x30 | 创建数据文件 | 使用 | 3.3.16 |
|  | 0xB0 | 0x32 | 删除数据文件 | 使用 | 3.3.17 |
|  | 0xB0 | 0x36 | 获取数据文件信息 | 生产/使用 | 3.3.18 |
|  | 0xB0 | 0x38 | 读数据文件 | 生产/使用 | 3.3.19 |
|  | 0xB0 | 0x3A | 写数据文件 | 生产/使用 | 3.3.20 |
|  | 0xB0 | 0x3E | 初始化文件系统 | 生产 | 3.3.21 |
|  | 0xB4 | 0x20 | 创建应用 | 生产 | 3.3.22 |
|  | 0xB0 | 0x2A | 获取应用配置信息 | 使用 | 3.3.23 |
|  | 0xB4 | 0x2B | 恢复应用初始化状态 | 使用 | 3.3.24 |
|  | 0xB4 | 0x40 | 创建容器 | 使用 | 3.3.25 |
|  | 0xB0 | 0x46 | 枚举容器 | 使用 | 3.3.26 |
|  | 0xB4 | 0x48 | 删除容器 | 使用 | 3.3.27 |
|  | 0xB0 | 0x4A | 获取容器信息 | 使用 | 3.3.28 |
|  | 0xB4 | 0x4C | 导入数字证书 | 使用 | 3.3.29 |
|  | 0xB0 | 0x4E | 导出数字证书 | 使用 | 3.3.30 |
|  | 0xB0 | 0x50 | 生成随机数 | 生产/使用 | 3.3.31 |
|  | 0xB4 | 0x54 | 生成RSA密钥对 | 使用 | 3.3.32 |
|  | 0xB4 | 0x56 | 导入RSA密钥对 | 使用 | 3.3.33 |
|  | 0xB4 | 0x57 | RSA私钥运算 | 使用 | 3.3.34 |
|  | 0xB4 | 0x70 | 生成SM2密钥对 | 使用 | 3.3.35 |
|  | 0xB4 | 0x72 | 导入SM2密钥对 | 使用 | 3.3.36 |
|  | 0xB4 | 0x73 | SM2私钥签名 | 使用 | 3.3.37 |
|  | 0xB4 | 0x75 | SM2私钥解密 | 使用 | 3.3.38 |
|  | 0xB0 | 0x78 | SM2生成并导出会话密钥 | 使用 | 3.3.39 |
|  | 0xB0 | 0x7A | SM2外来公钥加密 | 使用 | 3.3.47 |
|  | 0xB4 | 0x7C | SM2外来私钥解密 | 使用 | 3.3.48 |
|  | 0xB4 | 0x7E | SM2外来私钥签名 | 使用 | 3.3.49 |
|  | 0xB0 | 0x82 | SM2生成密钥协商参数 | 使用 | 3.3.50 |
|  | 0xB0 | 0x84 | SM2产生协商数据并计算会话密钥 | 使用 | 3.3.51 |
|  | 0xB0 | 0x86 | SM2计算会话密钥 | 使用 | 3.3.52 |
|  | 0xB0 | 0x88 | 导出公钥 | 使用 | 3.3.53 |
|  | 0xB4 | 0xA0 | 导入加密会话密钥 | 使用 | 3.3.54 |
|  | 0xB4 | 0xA2 | 导入会话密钥 | 使用 | 3.3.55 |
|  | 0xB0 | 0xA4 | 加密初始化 | 使用 | 3.3.56 |
|  | 0xB0 | 0xA8 | 多组数据加密 | 使用 | 3.3.57 |
|  | 0xB0 | 0xAA | 结束加密 | 使用 | 3.3.58 |
|  | 0xB0 | 0xAC | 解密初始化 | 使用 | 3.3.59 |
|  | 0xB0 | 0xB0 | 多组数据解密 | 使用 | 3.3.60 |
|  | 0xB0 | 0xB2 | 结束解密 | 使用 | 3.3.61 |
|  | 0xB0 | 0xC4 | 销毁会话密钥 | 使用 | 3.3.62 |
|  | 0xB0 | 0xE0 | 读外部Flash芯片信息 | 生产/使用 | 3.3.63 |
|  | 0xB0 | 0xE1 | 擦外部FLASH | 生产 | 3.3.64 |
|  | 0xB0 | 0xE2 | 写外部FLASH | 生产 | 3.3.65 |
|  | 0xB0 | 0xE3 | 读外部FLASH | 生产/使用 | 3.3.59 |
|  | 0xB0 | 0xE4 | 按键测试 | 生产 | 3.3.60 |
|  | 0xB0 | 0xE8 | 密码算法测试 | 生产 | 3.3.61 |
|  | 0xB0 | 0xE9 | 写外部FLASH用户区 | 使用 | 3.3.62 |
|  | 0xB0 | 0xEA | 读外部FLASH用户区 | 使用 | 3.3.63 |
|  | 0xB0 | 0xEB | 导入密钥加密密钥 | 使用 | 3.3.64 |
|  | 0xB0 | 0xEC | 导出密钥加密密钥 | 使用 | 3.3.65 |

## 指令描述

### 设置设备标签（0x02）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑5 设置设备标签

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x02 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0001 <= Lc <= 0x0020 | |
| Le | 0x0000 | |
| Data | 标签数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | NULL | |
| 说明 | 标签有效数据长度应小于等于32字节。  6.0.0版本要求Lc = 0x0020，不足32字节时，末尾部分用0x00填充。 | | |

### 设置设备序列号（0x03）

（1）定义与范围

该指令为生产阶段生命周期指令。

（2）指令与响应报文

表格3‑6 设置设备序列号

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x03 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0001 <= Lc <= 0x0010 | |
| Le | 0x0000 | |
| Data | 序列号数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000。 | |
| Data | NULL | |
| 说明 | （1）Utap v6.1.3.1（含）和Uyee v7.0.5.1（含）以前的版本，设备序列号为数字和字母的任意组合，以后的版本为所有可见字符的ASCII码；  （2）Utap v6.0.2.1（含）和Uyee v7.0.0.1（含）以前版本要求Lc = 0x0010支持变长SN，以后版本支持变长SN。 | | |

### 获取设备信息（0x04）

（1）定义与范围

通过输入不同参数，可获取完整的设备信息描述数据结构，或单独获取设备标签、设备序列号和安全芯片序列号。

（2）指令与响应报文

表格3‑7 获取设备信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x04 | |
| P1 | 0x00：获取完整的设备信息描述  0x01：获取设备标签  0x02：获取设备序列号  0x03：获取安全芯片序列号 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | P1=0x00时，Le=0x0120  P1=0x01时，Le=0x0020  P1=0x02时，Le=0x0010  P1=0x03时，Le=0x0010 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 期望返回的设备信息 | |
| 说明 | （1）P1=0时，设备信息主要包括设备标签、设备序列号、版本号、设备算法类型、当前生命周期状态以及所支持的容器和文件最大数量等等。  （2）详细请参考2.1.2.3设备信息结构体定义，只有生命周期状态(LifeStatus)为小端序，其它UINT16、UINT32类型变量均为大端序。 | | |

### 初始化设备认证密钥（0x05）

（1）定义与范围

该指令为生产阶段生命周期指令。

（2）指令与响应报文

表格3‑8 初始化设备认证密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x05 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0010 | |
| Le | 0x0084或0x0040 | |
| Data | 设备认证密钥 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 设备密钥对公钥 | |
| 说明 | （1）设备密钥对的类型由设备描述信息DevAuthAlgId确定。DevAuthAlgId为3DES算法时，设备密钥对使用RSA1024算法，Le值为0x0084；DevAuthAlgId为SM4算法时，设备密钥对使用SM2算法，Le值为0x0040。一般情况下都是用SM4算法；Le的值即为设备密钥对的公钥长度。  （2）RSA算法公钥格式为：Modulus（RSA模长/8字节）||PublicExponent（4字节，固定为0x00010001）；其中n为小端字节序，e为大端字节序。  （3）SM2算法公钥格式为XCoordinate（32字节）||YCoordinate（32字节）。  （4）此指令完成写入设备认证密钥和生成设备密钥对的功能，并且输出设备密钥对的公钥。 | | |

### 导入设备认证信息（0x06）

（1）定义与范围

该指令为生产阶段生命周期指令。

（2）指令与响应报文

表格3‑9 导入设备认证信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x06 | |
| P1 | 0x00：导入设备生产密钥对公钥和签名结果  0x01：导入设备管理密钥对公钥 | |
| P2 | 0x00 | |
| Lc | P1=0x00时，0x0104或0x0080  P1=0x01时，0x0084或0x0040 | |
| Le | 0x0000 | |
| Data | 设备认证信息 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | （1）导入生产密钥对和管理密钥对时，算法类型由Utap的设备描述信息DevAuthAlgId确定。DevAuthAlgId为3DES算法时，生产和管理密钥对使用RSA1024算法；DevAuthAlgId为SM4算法时，生产和管理密钥对使用SM2算法。一般情况都使用SM4算法；Lc的值与算法类型有关。  （2）P1=0x00时数据格式为：公钥|签名结果。 | | |

### 导出设备认证信息（0x07）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑10 导出设备认证信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x07 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | 0x0104或0x0080 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0104或0x0080 | |
| Data | 设备密钥对公钥和设备生产密钥对签名结果 | |
| 说明 | （1）Le的值由设备描述信息DevAuthAlgId确定，3DES算法时，使用RSA1024算法；SM4算法时，使用SM2算法；  （2）数据格式为：设备密钥对公钥|设备生产密钥对签名结果。 | | |

### 擦除COS（0x08）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑11 擦除COS

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x08 | |
| P1 | 0x00：获取挑战码  0x01：输入应答码 | |
| P2 | 0x00 | |
| Lc | P1=0x00时，0x0000  P1=0x01时，0x0080或0x0040 | |
| Le | P1=0x00时，0x0010  P1=0x01时，0x0000 | |
| Data | P1=0x00时，Null  P1=0x01时，应答码 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
|  | 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 挑战码或Null | |
| 说明 | （1）应答码为生产Key内对应的设备生产密钥对对（生产KEY的应用名称||挑战码）HASH值的签名结果；  （2）Utap内部没有导入设备认证信息时，任意应答码有效。 | | |

### 清空MF（0x09）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑12 清空MF

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x09 | |
| P1 | 0x00：获取挑战码  0x01：输入应答码 | |
| P2 | 0x00 | |
| Lc | P1=0x00时，0x0000  P1=0x01时，0x0080或0x0040 | |
| Le | P1=0x00时，0x0010  P1=0x01时，0x0000 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
|  | 其它值 | 见状态码表 |
| Len | 0x00 | |
| Data | 挑战码或Null | |
| 说明 | （1）应答码为生产Key内对应的设备生产密钥对对（生产KEY的应用名称||挑战码）HASH值的签名结果。  （2）Utap内部没有导入设备认证信息时，任意应答码有效。 | | |

### 协商传输会话密钥（0x0A）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑13 协商传输会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x0A | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0080或0x0081 | |
| Le | 0x0000 | |
| Data | 加密的会话密钥 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0 | |
| Data | Null | |
| 说明 | （1）会话密钥由中间件产生，使用设备认证密钥CBC模式加密，再使用设备密钥对公钥进行加密；  （2）RSA算法Lc为0x0080；SM2算法，32字节（16字节消息密钥的加密结果）+97。 | | |

### 设备认证（0x10）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑14 设备认证

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x10 | |
| P1 | 0x00：获取设备认证挑战码  0x01：输入设备认证应答码 | |
| P2 | 0x00 | |
| Lc | P1=0x00时，0x0000  P1=0x01时，0x0018或0x0020 | |
| Le | P1=0x00时，0x0010  P1=0x01时，0x0000 | |
| Data | P1=0x00时，Null  P1=0x01时，应答码 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x00 | |
| Data | 挑战码或Null | |
| 说明 | （1）第一步，中间件从Utap获取认证挑战码；  （2）第二步，中间件使用设备认证密钥对挑战码进行加密(PKCS5填充/3DES CBC或PKCS5填充/SM4 CBC)生成应答码，发送给Utap进行认证。 | | |

### 获取PIN信息（0x14）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑15 获取PIN信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0/B4 | |
| INS | 0x14 | |
| P1 | 0x00 | |
| P2 | PIN类型（0x00为管理员PIN，0x01为用户PIN） | |
| Lc | 0x0002 | |
| Le | 0x0004 | |
| Data | 应用ID（0x0000） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 长度由Len决定。 | |
| 说明 | （1）最大重试次数（1字节）||当前剩余重试次数（1字节）||出厂默认PIN码状态||当前设备认证状态；  （2）出厂默认PIN码状态为0x01表示建立应用后，PIN码还没有修改过。0x00表示PIN码已修改。 | | |

### 修改PIN（0x16）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑16 修改PIN

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x16 | |
| P1 | 0x00：获取挑战码  0x01：输入应答码 | |
| P2 | P1=0x00时，P2=0x00表示管理员PIN，P2=0x01表示用户PIN P1=0x01时，P2=0x00 | |
| Lc | P1=0x00时，0x0002  P1=0x01时，0x0082 | |
| Le | P1=0x00时，0x0094  P1=0x01时，0x0000 | |
| Data | P1=0x00时，应用ID（2字节）  P1=0x01时，应用ID（2字节）||应答码（使用临时密钥对对处理后的新旧PIN的加密数据） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | P1=0x00时，挑战码；P1=0x01，Null | |
| 说明 | （1）挑战码为临时生成的随机数R1（16字节）和临时RSA1024公钥（132字节）；  （2）应用对pin旧值（6～32字节）进行MD5摘要，得到16字节摘要结果M1，对M1||R1进行MD5，得到16字节的摘要结果M2。对PIN新值（6～32字节）进行MD5摘要，得到16字节摘要结果M3；  （3）应用对M2||M3进行P1填充，使用临时密钥对公钥进行加密，得到应答码。 | | |

### 校验PIN（0x18）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑17 校验PIN

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x18 | |
| P1 | 0x00：获取挑战码  0x01：输入应答码 | |
| P2 | P1=0x00时，P2=0x00表示管理员PIN，P2=0x01表示用户PIN P1=0x01时，P2=0x00 | |
| Lc | P1=0x00时，0x0002  P1=0x01时，0x0082 | |
| Le | P1=0x00时，0x0094  P1=0x01时，0x0010 | |
| Data | P1=0x00时，应用ID（2字节）  P1=0x01时，应用ID（2字节）||应答码（使用临时密钥对对处理后的PIN的加密数据） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | P1=0x00时，挑战码；P1=0x01，当验证成功时反馈16字节授权码，否则为Null。 | |
| 说明 | （1）挑战码为临时生成的随机数R1（16字节）和临时RSA1024公钥（132字节）；  （2）应用对PIN值（6～32字节）进行MD5摘要，得到16字节摘要结果M1，对M1||R1进行MD5，得到16字节的摘要结果M2；  （3）应用对M2进行P1填充，使用临时密钥对公钥进行加密，得到应答码。 | | |

### 解锁PIN（0x1A）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑18 解锁PIN

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x1A | |
| P1 | 0x00：获取挑战码  0x01：输入应答码 | |
| P2 | P1=0x00时，P2=0x00  P1=0x01时，P2=0x00表示使用管理员PIN解锁；P2=0x01表示使用管理Key解锁 | |
| Lc | P1=0x00时，0x0002  P1=0x01，P2=0x00即管理员PIN解锁时，0x0082  P1=0x01，P2=0x01即管理KEY解锁时，0x0042（SM2算法）/0x0082（RSA算法） | |
| Le | P1=0x00时，0x0094  P1=0x01时，0x0000 | |
| Data | P1=0x00时，应用ID（2字节）  P1=0x01时，P2=0x00时，应用ID（2字节）||应答码（128字节）  P1=0x01时，P2=0x01时，应用ID（2字节）||解锁码（0x40或者0x80字节，管理Key的签名结果） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | P1=0x00时，挑战码；P1=0x01，Null | |
| 说明 | （1）挑战码为临时生成的随机数R1（16字节）和临时RSA1024公钥（132字节）；当使用管理Key解锁方式时，这里输出的公钥值为无效值，后续不使用。  （2）管理员PIN解锁方式：应用对管理员PIN值（6～32字节）进行MD5摘要，得到16字节摘要结果M1，对M1||R1进行MD5，得到16字节的摘要结果M2。应用对M2进行P1填充，使用临时密钥对公钥进行加密，得到应答码；  （3）管理Key解锁方式： i)上层应用在挑战码（R1）前加上SN，作为解锁时使用的挑战码。 ii)生成解锁码流程中，上层应用收到挑战码后，将（SN+ R1）发送给管理KEY，管理Key对(appName+SN+R1)计算哈希（SHA1或SM3）后进行签名，将签名结果发送给上层应用。签名结果就是解锁码。  （4）Utap根据所采用不同的解锁方式，进行不同的处理过程。  （5）本指令执行成功后，用户PIN码恢复到默认值。 | | |

### 清除应用安全状态（0x1C）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑19 清楚应用安全状态

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x1C | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0002 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节，值为0x0000） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 仅清除应用安全状态，保持当前设备认证状态。 | | |

### 创建数据文件（0x30）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑20 创建数据文件

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x30 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0006 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||文件ID（2字节，大端）||文件长度（2字节，大端） | |
| 响应 | SW1SW2 | 0x9000 | 执行成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | （1）创建文件的File ID不能等于0x3F00；EF文件长度不能等于0；在相同目录内，不可有相同ID的同类型文件；  （2）使用阶段只能创建数据文件，单个文件最大长度为24KB，文件其它属性在COS内部赋值，FileType=0x20，FDTIndex=0，FileClass=0x21（二进制数据文件），权限都为0x00。 | | |

### 删除数据文件（0x32）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑21 删除数据文件

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x32 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0004 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||File ID（2字节，大端） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| data | Null | |
| 说明 | 只允许删除数据文件。 | | |

### 获取文件信息（0x36）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑22 获取文件信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x36 | |
| P1 | 0x00：获取文件长度信息  0x01：获取数据文件HASH值 | |
| P2 | 0x00 | |
| Lc | 0x0004 | |
| Le | P1=0x00时，0x0002  P1=0x01时，0x0014 | |
| Data | 应用ID（2字节）||File ID（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 执行成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| data | 期望得到的数据文件信息 | |
| 说明 | 获取文件长度信息对文件系统中所有文件有效；获取数据文件SHA1值仅对数据文件有效。 | | |

### 读数据文件（0x38）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑23 读取数据文件

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x38 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0006 | |
| Le | 最大值为0x0100 | |
| Data | 应用ID（2字节）||文件ID（2字节，大端）||偏移（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 长度由Len决定 | |
| 说明 | 指令仅对数据文件有效 | | |

### 写数据文件（0x3A）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑24 写数据文件

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x3A | |
| P1 | 写状态：  0xA1：FIRST\_UPDATE  0xB1：FIRST\_FINAL  0xA0：UPDATE  0xB0：FINAL | |
| P2 | 0x00 | |
| Lc | 0x0XXX | |
| Le | 0x0000 | |
| Data | 应用ID（2字节，大端）||文件ID（2字节，大端）||偏移（2字节）||待写入数据的长度（2字节，值不能为0）||待写入数据（最长256字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 指令仅对数据文件有效。 | | |

### 初始化文件系统（0x3E）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑25 初始化文件系统

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x3E | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | 0x0000 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 根据图2‑1创建文件（不含图中虚线部分的图章数据文件），指令只在生产初始化阶段执行。 | | |

### 创建应用（0x20）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑26 创建应用

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x20 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x00D2 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||应用信息结构体（208字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 当前版本支持MF下的单应用，应用ID=0x0000。应用初始化阶段指令。 | | |

### 获取应用配置信息（0x2A）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑27 获取应用配置信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x2A | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0002 | |
| Le | 0x0048 | |
| Data | 应用ID（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 返回的数据结构：AppName（32字节）|| AppSysConfig（40字节） | | |

### 恢复应用初始化状态（0x2B）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑28 恢复应用初始化状态

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x2B | |
| P1 | 0x00：获取挑战码  0x01：输入应答码 | |
| P2 | P1=0x00时，P2=0x00  P1=0x01时，P2=0x00表示使用管理员PIN恢复；P2=0x01表示使用管理Key恢复 | |
| Lc | P1=0x00时，0x0002  P1=0x01，P2=0x00时，0x0082  P1=0x01，P2=0x01时，0x0042/0x0082 | |
| Le | P1=0x00时，0x0094  P1=0x01时，0x0000 | |
| Data | P1=0x00时，应用ID（2字节）  P1=0x01时，P2=0x00时，应用ID（2字节）||应答码（128字节）  P1=0x01时，P2=0x01时，应用ID（2字节）||解锁码（0x40或者0x80字节，管理Key的签名结果） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | P1=0x00时，挑战码；P1=0x01，Null | |
| 说明 | （1）挑战码为临时生成的随机数（16字节）和临时RSA1024公钥（132字节）；当使用管理Key解锁方式时，这里输出的公钥值为无效值，后续不使用。  （2）管理员PIN恢复方式：应用对管理员PIN值（6～32字节）进行MD5摘要，得到16字节摘要结果M1，对M1||R1进行MD5，得到16字节的摘要结果M2。应用对M2进行P1填充，使用临时密钥对公钥进行加密，得到应答码；；  （3）管理Key恢复方式： i)上层应用在挑战码（R1）前加上SN，作为恢复初始状态时使用的挑战码。 ii)生成恢复初始状态码流程中，上层应用收到挑战码后，将（SN+ R1）发送给管理KEY，管理Key对(appName+SN+R1)计算哈希（SHA1或SM3）后进行签名，将签名结果发送给上层应用。签名结果就是恢复初始状态码。  （4）Utap根据所采用不同的恢复方式，进行不同的处理过程，与解锁PIN过程类似。  （5）本指令执行成功后，指定应用恢复到初始状态。 | | |

### 创建容器（0x40）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑29 创建容器

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x40 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 发送的数据长度，大于18，小于等于58。 | |
| Le | 0x0000 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器名称（最长40字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 创建容器时，默认配置为首先删除仅有容器名称的空容器。可在应用初始化阶段对此配置进行修改。 | | |

### 枚举容器（0x46）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑30 枚举容器

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x46 | |
| P1 | 0x00：可用容器  0x01：全部容器（不包括空容器和只有容器名称的容器） | |
| P2 | 0x00：枚举容器名  0x01：枚举容器信息数据结构  0x02：枚举容器头部主要信息 | |
| Lc | 0x0002 | |
| Le | 不大于0x140 | |
| Data | 应用ID（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为实际的数据长度；其它情况时，值为0x0000。 | |
| Data | 容器名称列表或容器信息结构体列表 | |
| 说明 | （1）最多5个容器；  （2）容器名称列表：name string + '\0' +… + name string + '\0\0'；  （3）全部容器信息数据结构50字节，最多250（0xFA）字节；  （4）容器头部主要信息包括数据结构前10个字节。 | | |

### 删除容器（0x48）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑31 删除容器

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x48 | |
| P1 | 0x00 | |
| P2 | 0x00：使用容器索引  0x01：使用容器名称 | |
| Lc | 发送的数据长度 | |
| Le | 0x0000 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器索引（1字节）||容器名称（最长40字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 成功执行后，将清空容器文件的全部内容。 | | |

### 获取容器信息（0x4A）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑32 获取容器信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x4A | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 容器名称的字节数 | |
| Le | 0x0008 | |
| Data | 容器名称（最长40字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 容器基本信息 | |
| 说明 | （1）容器信息为容器信息数据结构的前8个字节，包括容器文件ID（大端），密钥对类型、密钥对状态、容器状态等。  （2）中间件需要保存容器文件ID，用于在目标容器中生成/导入密钥对，并使用目标容器的密钥对进行签名等操作。 | | |

### 导入数字证书（0x4C）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑33 导入数字证书

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x4C | |
| P1 | 写状态：  0xA1：FIRST\_UPDATE  0xB1：FIRST\_FINAL  0xA0：UPDATE  0xB0：FINAL | |
| P2 | 0x00 | |
| Lc | 发送的数据长度 | |
| Le | 0x0000 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||偏移（2字节）||待写入数据的长度（2字节）||待写入数据（最长256字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0 | |
| Data | Null | |
| 说明 | 容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）。  容器密钥/证书ID为大端序。 | | |

### 导出数字证书（0x4E）

（1）定义与范围

支持数字证书文件HASH计算功能。

（2）指令与响应报文

表格3‑34 导出数字证书

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x4E | |
| P1 | 0x00：获取数字证书内容  0x01：获取数字证书的HASH值 | |
| P2 | 0x00 | |
| Lc | 0x0006 | |
| Le | P1=0x00时：期望读出的数据长度（最大值为0x0100）  P1=0x01时：0x0014 | |
| Data | 应用ID（2字节）||容器密钥/证书ID（2字节）||偏移（2字节，P1=0x01值为0x0000） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0 | |
| Data | 数字证书内容或HASH值 | |
| 说明 | （1）使用SHA1算法对数字证书内容进行HASH  （2）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）。  容器密钥/证书ID为大端序。 | | |

### 生成随机数（0x50）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑35 生成随机数

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x50 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x00 | |
| Le | 0x0008至0x0080 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 随机数据，长度由Len决定。 | |
| 说明 |  | | |

### 生成RSA密钥对（0x54）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑36 生成RSA密钥对

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x54 | |
| P1 | 0x01：RSA1024；0x07：RSA2048 | |
| P2 | 0x00 | |
| Lc | 0x0018 | |
| Le | 0x0000 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||公钥指数（大端顺序，4字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）。  容器密钥/证书ID为大端序。 | | |

### 导入RSA密钥对（0x56）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑37 导入RSA密钥对

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x56 | |
| P1 | 0x00：分块输入加密的RSA密钥对  0x01：使用导入的会话密钥解密RSA密钥对并保存到指定容器中 | |
| P2 | P1=0x00时：偏移序号（0x00，0x01，0x02），RSA1024两包，RSA2048为三包  P1=0x01时：0x00表示明文；0x01表示密文 | |
| Lc | P1=0x00时：0x0114  P1=0x01时：0x0015 | |
| Le | 0x0000 | |
| Data | P1=0x00时：授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||分块的RSA密钥对数据  P1=0x01时：授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||密钥类型（1字节，0x01表示RSA1024，0x07表示RSA2048） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | （1）加密方式为3DES ECB，加密方式导入密钥对前，需通过导入加密会话密钥指令成功导入对称密钥；  （2）加密的RSA密钥对数据，RSA1024至少发送384字节，RSA2048至少发送640字节；  （3）RSA1024密钥对是明文时，需要按照n||d||e的顺序传送；  （4）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）  （5）容器密钥/证书ID为大端序。 | | |

### RSA私钥运算（0x57）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑38 RSA私钥运算

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x57 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0094/0x0114 | |
| Le | 0x0080/0x0100 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||PKCS1填充数据（RSA1024时长度为0x80，RSA2048时长度为0x100） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 期望得到的运算结果 | |
| 说明 | （1）检查输入数据填充格式为PKCS1签名数据填充格式时，HASH算法支持SHA1、MD5、SHA1MD5、SHA256、SHA384和SHA512。根据配置文件决定签名是否需要按键；  （2）检查输入数据填充格式不符合签名数据格式时，暂时判定为解密操作，私钥运算完成后检查是否符合PKCS1解密数据填充格式；  （3）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）。容器密钥/证书ID为大端序。  （4）注意：UYEE v7.1.3.1（含）之后版本，支持PSS格式填充。 | | |

### 生成SM2密钥对（0x70）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑39 生成SM2密钥对

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x70 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0014 | |
| Le | 0x0000 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）。容器密钥/证书ID为大端序。 | | |

### 导入SM2密钥对（0x72）

（1）定义与范围

使用临时密钥对解密，将得到的SM2密钥对保存到密钥容器中。

（2）指令与响应报文

表格3‑40 导入SM2密钥对

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x72 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | CA数据格式导入：0x00D5  SFK数据格式导入：0x00FC | |
| Le | 0x0000 | |
| Data | CA数据格式导入：授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||加密的SM2密钥对(193字节)  SKF数据信封数据格式导入：授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||SKF接口中ImportECCKeyPair命令报文数据由偏移4开始。 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 容器密钥/证书ID为大端序。  CA数据格式导入：  （1）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）；  （2）加密数据格式兼容：0x04||C1||C2||C3和0x04||C1||C3||C2；  （3）SM2密钥对格式：X（32字节）||Y（32字节）||d（32字节）；  （4）当容器密钥/证书ID无效时，会选取同容器另外一对密钥进行解密操作（当前为ExchgKey/ExchgCert改为SignKey/SignCert，当前为SignKey/SignCert改为ExchgKey/ExchgCert）；  SKF数据信封数据格式时：  （1）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）；  （2）数字信封格式参见SKF接口中ImportECCKeyPair命令报文数据由偏移4开始；  （3）当容器密钥/证书ID无效时，会选取同容器另外一对密钥进行解密操作（当前为ExchgKey/ExchgCert改为SignKey/SignCert，当前为SignKey/SignCert改为ExchgKey/ExchgCert）。 | | |

### SM2私钥签名（0x73）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑41 私钥签名

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x73 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0034 | |
| Le | 0x0040 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||哈希值（32字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 长度由Len决定 | |
| 说明 | 容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）。容器密钥/证书ID为大端序。 | | |

### SM2私钥解密（0x75）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑42 SM2私钥解密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x75 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 不大于0x00F5 | |
| Le | 解密结果长度不大于0x0080 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||加密数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 长度由Len决定。 | |
| 说明 | （1）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）；容器密钥/证书ID为大端序。  （2）加密数据格式兼容：0x04||C1||C2||C3和0x04||C1||C3||C2；  （3）支持最大128字节加密，因此加密数据长度不大于1+128+96=225字节。 | | |

### SM2生成并导出会话密钥（0x78）

（1）定义与范围

在设备的指定容器中生成会话密钥并用外部公钥加密导出。

（2）指令与响应报文

表格3‑43 生成并导出会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x78 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0048 | |
| Le | 0x007A | |
| Data | 应用ID（2字节）||外部公钥的密钥位长度（4字节，bitLen）||外部公钥X（bitLen/8字节）||外部公钥Y（bitLen/8字节）|| AlgType(算法1字节)||算法模式（1字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 密文C1的位长度（4字节，bitLen）||密文C1的X（bitLen/8字节）||密文C1的Y（bitLen/8字节）||密文C3（32字节）||密文C2数据长度（4字节）||密文C2数据||会话密钥ID（2字节） | |
| 说明 | （1）应用ID为大端序。  （2）算法AlgType，SM1:0x10，SM4:0x13；算法模式，ECB：0x01，CBC：0x02。  （3）仅限于Utap v6.1.6.1（含）和UYEE v7.1.1.1（含）以后版本支持此接口。 | | |

### SM2外来公钥加密（0x7A）

（1）定义与范围

使用外部传入的SM2公钥对输入数据做加密运算并输出结果。

（2）指令与响应报文

表格3‑44 SM2外来公钥加密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x7A | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 大于0x0048，不大于0x00C8 | |
| Le | 不大于0x00E0 | |
| Data | 外部公钥的密钥位长度（4字节，bitLen）||外部公钥X（bitLen/8字节）||外部公钥Y（bitLen/8字节）||待加密的数据长度（4字节，dataLen）||待加密数据（dataLen字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 密钥位长度（4字节，bitLen）||密文C1的X（bitLen/8字节）||密文C1的Y（bitLen/8字节）||密文C3（32字节）||密文C2数据长度（4字节）||密文C2数据 | |
| 说明 | （1）任何时候都可以执行此命令。  （2）待加密原文长度最大为128字节，因此加密数据长度最大为128+96=224字节。  （3）仅限于Utap v6.1.6.1（含）和UYEE v7.1.1.1（含）以后版本支持此接口。 | | |

### SM2外来私钥解密（0x7C）

（1）定义与范围

使用外部传入的SM2私钥对输入数据做解密运算并输出结果。

（2）指令与响应报文

表格3‑45 SM2外来私钥解密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x7C | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 大于0x0088，不大于0x0108 | |
| Le | 不大于0x0084 | |
| Data | 密钥位长度（4字节，bitLen）||外部私钥（bitLen/8字节）||密文C1的X（bitLen/8字节）||密文C1的Y（bitLen/8字节）||密文C3（32字节）||密文C2数据长度（4字节）||密文C2数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 解密后的明文数据长度（4字节）||明文数据 | |
| 说明 | （1）任何时候都可以执行此命令。  （2）支持原文长度最大为128字节，因此密文数据长度最大为128+96=224字节。  （3）仅限于Utap v6.1.6.1（含）和UYEE v7.1.1.1（含）以后版本支持此接口。 | | |

### SM2外来私钥签名（0x7E）

（1）定义与范围

使用外部传入的SM2私钥对输入数据做签名运算并输出结果。

（2）指令与响应报文

表格3‑46 外来私钥签名

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 代码 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0x7E | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0048 | |
| Le | 0x0040 | |
| Data | 密钥位长度（4字节，bitLen）||外部私钥（bitLen/8字节）||待签名数据长度（4字节）||待签名数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 签名结果R||S | |
| 说明 | （1）任何时候都可以执行此命令。  （2）输入的待签名数据为待签原始数据经过预处理的杂凑值。  （3）仅限于Utap v6.1.6.1（含）和UYEE v7.1.1.1（含）以后版本支持此接口。 | | |

### SM2生成密钥协商参数（0x82）

（1）定义与范围

使用SM2密钥协商算法，为计算会话密钥而产生协商参数，返回临时SM2密钥对的公钥和协商句柄。

为协商会话密钥，协商的发起方应首先执行此指令。

（2）指令与响应报文

表格3‑47 SM2生成密钥协商参数

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x82 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 不大于0x2A | |
| Le | 0x0048（SM2密钥位长是256） | |
| Data | 应用ID（2字节）||容器ID（2字节）||会话密钥算法标识（2字节）||发起方ID长度（4字节）||发起方的ID（设定长度不大于0x20） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 发起方临时密钥位长度（4字节，bitLen）||发起方临时密钥公钥X（bitLen/8字节）||发起方临时密钥公钥Y（bitLen/8字节）||密钥协商句柄（4字节） | |
| 说明 | （1）为协商会话密钥，协商的发起方应首先执行此指令。  （2）指令和响应中的多字节字段均为大端字节序。  （3）发起方ID和响应方ID，设定其长度不大于0x20。Lc和Le的值设定了密钥位长是256。  （4）其中，会话密钥算法标识：算法AlgType(1字节，SM1:0x10，SM4:0x13)||算法模式（1字节，ECB：0x01，CBC：0x02）。  （5）本指令仅Utap v6.1.6.1（含）和Uyee v7.0.6.1（含）以后版本支持。 | | |

### SM2产生协商数据并计算会话密钥（0x84）

（1）定义与范围

使用SM2密钥协商算法，产生协商参数并计算会话密钥，输出临时SM2密钥对公钥，并返回产生的密钥句柄。

本指令由协商的响应方执行。

（2）指令与响应报文

表格3‑48 SM2产生协商数据并计算会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x84 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 不大于0x00D6 | |
| Le | 0x0048 | |
| Data | 详细数据格式见下面说明 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 响应方临时密钥对的密钥位长度(4,bitLen)|| 响应方临时密钥公钥X(bitLen/8)||响应方临时密钥公钥Y(bitLen/8)||会话密钥ID（4） | |
| 说明 | （1）本指令由协商的响应方执行。  （2）指令和响应中的多字节字段均为大端字节序。  （3）指令报文数据格式如下，小括号中的数字是字节长度，英文是含义或字节长度：  应用ID(2)||密钥ID(2)||会话密钥算法标识(2)|| 发起方密钥对的密钥位长度(4,bitLen)||发起方密钥公钥X (bitLen/8)|| 发起方密钥公钥Y (bitLen/8)|| 发起方临时密钥对的密钥位长度(4,bitLenTmp)||发起方临时密钥公钥X (bitLenTmp/8)|| 发起方临时密钥公钥Y (bitLenTmp/8)||发起方ID长度 (4,sIDLen)||发起方ID (sIDLen)||响应方ID长度 (4，rIDLen)||响应方ID (rIDLen)  （4）发起方ID和响应方ID，设定其长度不大于0x20。Lc和Le的值设定了密钥位长是256。  （5）密钥ID=容器文件ID +密钥标识（0x01表示ExchgKey，0x02表示SignKey），大端字节序。  （6）会话密钥算法标识：算法AlgType(1字节，SM1:0x10，SM4:0x13)||算法模式（1字节，ECB：0x01，CBC：0x02）。  （7）本指令仅Utap v6.1.6.1（含）和Uyee v7.0.6.1（含）以后版本支持。 | | |

### SM2计算会话密钥（0x86）

（1）定义与范围

使用SM2密钥协商算法，使用自身协商句柄和响应方的协商参数计算会话密钥，同时返回会话密钥句柄。

协商的发起方获得响应方的协商参数后调用本函数，计算会话密钥。

（2）指令与响应报文

表格3‑49 SM2计算会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x86 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 不大于0x00B4 | |
| Le | 0x0004 | |
| Data | 详细数据格式见下面说明 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 会话密钥ID | |
| 说明 | （1）协商的发起方获得响应方的协商参数后调用本函数，计算会话密钥。  （2）指令和响应中的多字节字段均为大端字节序。  （3）指令报文数据格式如下，小括号中的数字是字节长度，英文是含义或字节长度：  应用ID(2)||密钥ID(2)||发起方的密钥协商句柄(4)||响应方密钥对的密钥位长度(4,bitLen)|| 响应方密钥公钥X (bitLen/8)|| 响应方密钥公钥Y (bitLen/8)|| 响应方临时密钥对的密钥位长度(4,bitLenTmp)|| 响应方临时密钥公钥X (bitLenTmp/8)|| 响应方临时密钥公钥Y (bitLenTmp/8)||响应方ID长度 (4，rIDLen)||响应方ID (rIDLen)  （4）发起方ID和响应方ID，设定其长度不大于0x20。Lc和Le的值设定了密钥位长是256。  （5）密钥ID=容器文件ID +密钥标识（0x01表示ExchgKey，0x02表示SignKey），大端字节序。  （6）本指令仅Utap v6.1.6.1（含）和Uyee v7.0.6.1（含）以后版本支持。 | | |

### 导出公钥（0x88）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑50 导出公钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0x88 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0004 | |
| Le | 0x0040/0x0084/0x0104 | |
| Data | 应用ID（2字节）|容器密钥/证书ID（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 公钥数据长度 | |
| Data | 公钥数据 | |
| 说明 | （1）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）；容器密钥/证书ID为大端序。  （2）RSA算法公钥格式为：Modulus（RSA模长/8字节）||PublicExponent（4字节，一般为0x00010001）；  （3）SM2算法公钥格式为X（32字节）||Y（32字节）。 | | |

### 导入加密会话密钥（0xA0）

（1）定义与范围

支持RSA和SM2算法导入加密会话密钥，用于实现RSA加密密钥对导入功能，以及对称算法加解密密钥加密导入。

（2）指令与响应报文

表格3‑51 导入加密会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0xA0 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0094/0x0114/大于0x61小于等于0x81 | |
| Le | 0x0000 | |
| Data | 授权码（16字节）||应用ID（2字节）||容器密钥/证书ID（2字节）||RSA公钥加密的对称密钥数据（128字节或256字节）或者SM2公钥加密的对称密钥数据（大于0x61小于等于0x81字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | （1）在导入加密的RSA密钥对前调用，或者进行数据加解密前调用；  （2）容器密钥/证书ID=容器文件ID +密钥/证书标识（0x01表示ExchgKey/ExchgCert，0x02表示SignKey/SignCert）；容器密钥/证书ID为大端序。  （3）支持SKF接口导入；  （4）当容器密钥/证书ID无效时，会选取同容器另外一对密钥进行解密操作（当前为ExchgKey/ExchgCert改为SignKey/SignCert，当前为SignKey/SignCert改为ExchgKey/ExchgCert）；  （5）SM2加密数据格式兼容：0x04||C1||C2||C3和0x04||C1||C3||C2；  （6）使用SM2算法加密导入会话密钥时，仅支持不大于32字节SM1/SM4算法密钥，加密后的数据长度不大于1+32+96=129字节。 | | |

### 导入会话密钥（0xA2）

（1）定义与范围

明文方式导入会话密钥，明文导入的会话密钥仅支持导入16字节密钥数据，支持的密码算法为SM1（ECB和CBC模式）、SM4（ECB和CBC模式）。

（2）指令与响应报文

表格3‑52 导入会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB4 | |
| INS | 0xA2 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0018 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||容器密钥/证书ID（2字节）||会话密钥数据（20字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | （1）会话密钥数据格式： AlgType(算法1字节)||算法模式（1字节）||SymKeyLen（会话密钥长度，2字节）||SymKey（会话密钥明文，16字节）。  （2）算法AlgType，SM1:0x10，SM4:0x13；算法模式，ECB：0x01，CBC：0x02。  （3）容器密钥/证书ID为大端序。 | | |

### 加密初始化（0xA4）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑53 加密初始化

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xA4 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 不大于0x0032 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节）||密钥参数（28字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 数据格式： AlgType(算法1字节)||算法模式（1字节）||IVLen（起始向量的实际长度，2字节）||IV（起始向量，不大于32字节）||PaddingType（填充方式，4字节）||FeedBitLen（反馈值的位长度，4字节）。  算法AlgType，SM1:0x10，SM4:0x13；算法模式，ECB：0x01，CBC：0x02。  容器密钥/证书ID为大端序。 | | |

### 多组数据加密（0xA8）

（1）定义与范围

待加密数据长度必须为分组长度的整数倍，设备不对分组数据进行补位填充操作。

（2）指令与响应报文

表格3‑54 多组数据加密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xA8 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 发送的数据长度 | |
| Le | 加密结果长度不大于0x0080 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节）||待加密的明文分组数据（每次发送最大长度128字节，最小为1个分组长度） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 长度由Len决定。 | |
| 说明 | 容器密钥 ID为大端序。 | | |

### 结束加密（0xAA）

（1）定义与范围

待加密数据长度必须为分组长度的整数倍，设备不对分组数据进行补位填充操作。

（2）指令与响应报文

表格3‑55 结束加密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xAA | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 发送的数据长度 | |
| Le | 加密结果长度不大于0x0080 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节）||最后一段待加密的明文分组数据（发送最大长度128字节），或者无数据。 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 长度由Len决定。 | |
| 说明 | 容器密钥ID为大端序。 | | |

### 解密初始化（0xAC）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑56 解密初始化

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xAC | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 不大于0x0032 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节）||密钥参数（28字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | （1）数据格式： AlgType(算法1字节)||算法模式（1字节）||IVLen（起始向量的实际长度，2字节）||IV（起始向量，不大于32字节）||PaddingType（填充方式，4字节）||FeedBitLen（反馈值的位长度，4字节）。  （2）算法AlgType，SM1:0x10，SM4:0x13；算法模式，ECB：0x01，CBC：0x02。  （3）容器密钥ID为大端序。 | | |

### 多组数据解密（0xB0）

（1）定义与范围

待解密数据长度必须为分组长度的整数倍，设备不对补位填充的分组数据进行去填充操作。

（2）指令与响应报文

表格3‑57 多组数据解密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xB0 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 发送的数据长度 | |
| Le | 解密结果长度不大于0x0080 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节）||待解密的明文分组数据（每次发送最大长度128字节，最小为1个分组长度） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 长度由Len决定。 | |
| 说明 | 容器密钥ID为大端序。 | | |

### 结束解密（0xB2）

（1）定义与范围

待解密数据长度必须为分组长度的整数倍，设备不对补位填充的分组数据进行去填充操作。

（2）指令与响应报文

表格3‑58 结束解密

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xB2 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 发送的数据长度 | |
| Le | 解密结果长度不大于0x0080 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节）||最后一段待解密的明文分组数据（发送最大长度128字节），或者无数据。 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0。 | |
| Data | 长度由Len决定。 | |
| 说明 | 容器密钥ID为大端序。 | | |

### 销毁会话密钥（0xC4）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑59 销毁会话密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xC4 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0004 | |
| Le | 0x0000 | |
| Data | 应用ID（2字节）||容器密钥ID（2字节） | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 | 容器密钥ID为大端序。 | | |

### 读外部Flash芯片信息（0xE0）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑60 读外部FLASH芯片信息

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE0 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | 0x0006 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0 | |
| Data | 长度由Len决定 | |
| 说明 | 数据格式：厂商ID（1字节）||存储类型（1字节）||容量（4字节）。 | | |

### 擦外部FLASH（0xE1）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑61 擦外部FLASH

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE1 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | 0x0000 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x00 | |
| Data | Null | |
| 说明 |  | | |

### 写外部FLASH（0xE2）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑62 写外部FLASH

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE2 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0104 | |
| Le | 0x0000 | |
| Data | 起始地址和数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x00 | |
| Data | Null | |
| 说明 | 发送的数据格式：起始地址（4）字节|数据。 | | |

### 读外部FLASH（0xE3）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑63 读外部FLASH

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE3 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0004 | |
| Le | 0x0100 | |
| Data | 起始地址 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 长度由Len决定 | |
| 说明 |  | | |

### 按键测试（0xE4）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑64 按键测试

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE4 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | 0x0001 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
|  |  |
| Len | 0x0001 | |
| Data | 按键标识 | |
| 说明 | 按键标识：0x03：确认键。按键测试接口仅对Utap产品有效。 | | |

### 密码算法测试（0xE8）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑65 密码算法测试

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE8 | |
| P1 | 0x01：RSA1024  0x07：RSA2048  0x11：SM2 | |
| P2 | 0x00 | |
| Lc | 0x0000 | |
| Le | 0x0000 | |
| Data | Null | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x0000 | |
| Data | Null | |
| 说明 |  | | |

### 写外部FLASH用户区（0xE9）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑66 写外部FLASH

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xE9 | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x0104 | |
| Le | 0x0000 | |
| Data | 起始地址和数据 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x00 | |
| Data | Null | |
| 说明 | 发送的数据格式：起始地址（4）字节|数据。  起始地址必须为256的整数倍；  起始地址+数据长度不得超过512K； | | |

### 读外部FLASH用户区（0xEA）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑67 写外部FLASH

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xEA | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x04 | |
| Le | 不大于0x800 | |
| Data | 起始地址 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 0x00 | |
| Data | Null | |
| 说明 | 发送的数据格式：起始地址（4）字节。  起始地址必须为256的整数倍；  起始地址+数据长度不得超过512K；  单次读取最大2K； | | |

### 导入密钥加密密钥（0xEB）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑68 导入密钥加密密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xEB | |
| P1 | 0x00:获取公钥  0x01:导入密钥加密密钥 | |
| P2 | 0x00 | |
| Lc | P1=0x00：0x10  P1=0x01：0x81 | |
| Le | P1=0x00：0x40  P1=0x01：0x00 | |
| Data | P1=0x00：授权码（16字节）  P1=0x01：授权码（16字节）+ 加密后的密钥加密密钥 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | P1=0x00：密钥共享密钥的公钥  P1=0x01：NULL | |
| 说明 | （1）加密后的密钥加密密钥：0x04||C1||C2||C3和0x04||C1||C3||C2；  （2）公钥格式为X（32字节）||Y（32字节）；  （3）该指令用于加密卡备份密钥。 | | |

### 导出密钥加密密钥（0xEC）

（1）定义与范围

无。

（2）指令与响应报文

表格3‑69 导入密钥加密密钥

|  |  |  |  |
| --- | --- | --- | --- |
| 类型 | 名称 | 赋值与描述 | |
| 指令 | CLA | 0xB0 | |
| INS | 0xEC | |
| P1 | 0x00 | |
| P2 | 0x00 | |
| Lc | 0x50 | |
| Le | 0x71 | |
| Data | 授权码（16字节）+ 接受方公钥 | |
| 响应 | SW1SW2 | 0x9000 | 成功 |
| 其它值 | 见状态码表 |
| Len | 成功时，值为Le；其它情况时，值为0x0000 | |
| Data | 加密后的密钥加密密钥 | |
| 说明 | （1）加密后的密钥加密密钥：0x04||C1||C2||C3和0x04||C1||C3||C2；  （2）公钥格式为X（32字节）||Y（32字节）；  （3）该指令用于加密卡备份密钥。 | | |

# 状态码表

表格4‑1 状态码表

| 序号 | 状态码 | 状态码定义 | 状态码说明 | |
| --- | --- | --- | --- | --- |
|  | 0x9000 | APDU\_EXEC\_SUCCESS | 成功 | |
|  | 0x63CX | R\_CMDX | PIN码验证失败  （X为剩余可尝试次数） | |
|  | 0x6700 | R\_LENERR | Lc/Le数据长度错误 | |
|  | 0x6A86 | R\_PARAMERR | P1或P2参数错误 | |
|  | 0x6981 | R\_NOCONTROL\_DEV | 设备认证权限不满足 | |
|  | 0x6982 | R\_NOCONTROL\_USER | 应用安全状态不满足 | |
|  | 0x6983 | R\_PINLOCK | PIN码锁定 | |
|  | 0x6D00 | R\_INSERR | 非法的INS | |
|  | 0x6900 | R\_CLADISMATCH | 非法的CLA | |
|  | 0xF101 | R\_FILE\_ID\_ERR | 文件ID错误 | |
|  | 0xF102 | R\_FILE\_ID\_UNEXISTED | 文件ID不存在 | |
|  | 0xF103 | R\_FILE\_ID\_EXISTED | 文件ID已存在 | |
|  | 0xF104 | R\_FILE\_SIZE\_ERR | 文件长度错误 | |
|  | 0xF105 | R\_FILE\_DATA\_SPACE\_ERR | 文件系统数据存储空间不足 | |
|  | 0xF106 | R\_FILE\_NUMBER\_SPACE\_ERR | 文件数量已经达到最大值，无法创建文件 | |
|  | 0xF107 | R\_FILE\_TYPE\_ERR | 文件属性类型非法 | |
|  | 0xF108 | R\_FILE\_CLASS\_ERR | 文件类型非法  （只有二进制文件可读写删除、计算哈希值） | |
|  | 0xF109 | R\_FILE\_CONTROL\_ERR | （未使用） | |
|  | 0xF10A | R\_FILE\_ADDRESS\_ERR | 文件系统内部地址错误 | |
|  | 0xF10B | R\_FILE\_STRUCTURL\_ERR | 文件系统内部结构错误 | |
|  | 0xF10C | R\_FILE\_NOT\_EMPTY | 待释放文件空间非空 | |
|  | 0xF10D | R\_FILE\_BAD\_BLOCK | 文件系统存储空间有坏块 | |
|  | 0xF10E | R\_FILE\_PARAM\_ERR | 文件操作参数错误 | |
|  | 0xF110 | R\_FILE\_APP\_NAME\_EMPTY | 应用名称不存在 | |
|  | 0xF201 | R\_CONTAINER\_EXISTED | 容器已存在 | |
|  | 0xF202 | R\_CONTAINER\_UNEXISTED | 容器不存在 | |
|  | 0xF203 | R\_CONTAINER\_EMPTY | （未使用） | |
|  | 0xF204 | R\_CONTAINER\_NO\_EMPTY | 无可用的容器 | |
|  | 0xF205 | R\_CONTAINER\_FINISH | 容器状态已完整 | |
|  | 0xF206 | R\_CONTAINER\_UNFINISH | 容器状态非完整 | |
|  | 0xF207 | R\_CONTAINER\_CERT\_EXISTED | 证书已存在 | |
|  | 0xF208 | R\_CONTAINER\_CERT\_UNEXISTED | 证书不存在 | |
|  | 0xF209 | R\_CONTAINER\_KEY\_EXISTED | （未使用） | |
|  | 0xF20A | R\_CONTAINER\_KEY\_UNEXISTED | 密钥不存在 | |
|  | 0xF20B | R\_CONTAINER\_ID\_ERR | 容器ID错误 | |
|  | 0xF20C | R\_CONTAINER\_PARAM\_ERR | 容器操作参数错误 | |
|  | 0xF20D | R\_CONTAINER\_TYPE\_ERR | 容器类型错误 | |
|  | 0xF20E | R\_CONTAINER\_INDEX\_ERR | 容器索引错误 | |
|  | 0xF20F | R\_CONTAINER\_CERT\_STRU\_ERR | 数字证书各式错误 | |
|  | 0xF210 | R\_CONTAINER\_STRU\_ERR | 容器结构错误 | |
|  | 0xF301 | R\_DEV\_XF\_WRITE\_ERROR | 写外部FLASH错误 | |
|  | 0xF302 | R\_DEV\_XF\_READ\_ERROR | 读外部FLASH错误 | |
|  | 0xF303 | R\_DEV\_XF\_ERASE\_ERROR | 擦除外部FLASH错误 | |
|  | 0xF304 | R\_DEV\_XF\_NOT\_EXIST | 外部FLASH不存在 | |
|  | 0xF305 | R\_DEV\_XF\_ADDR\_ERROR | 外部FLASH地址错误 | |
|  | 0xF311 | R\_DEV\_SF\_WRITE\_ERROR | 写内部FLASH错误 | |
|  | 0xF312 | R\_DEV\_SF\_READ\_ERROR | 读内部FLASH错误 | |
|  | 0xF321 | R\_DEV\_BUTTON\_WAIT | 按键等待 | |
|  | 0xF323 | R\_DEV\_BUTTON\_TIMEOUT | 按键超时 | |
|  | 0xF324 | R\_DEV\_BUTTON\_ILLEGAL | 按键异常 | |
|  | 0xF325 | R\_DEV\_BUTTON\_FIRST\_ENTER | 第一次按键确认 | |
|  | 0xF331 | R\_DEV\_SN\_FORMAT\_WRONG | 设备序列号非法  （必须为字母或数字） | |
|  | 0xF332 | R\_DEV\_SN\_NOT\_EXIST | 设备序列号不存在 | |
|  | 0xF335 | R\_DEV\_LABEL\_NOT\_EXIST | 设备标签不存在 | |
|  | 0xF336 | R\_DEV\_EXAUTH\_KEY\_NOT\_EXIST | 外部认证密钥不存在 | |
|  | 0xF341 | R\_DEV\_CHANNEL\_CONFLICT | 通信通道冲突  （MSD或HID） | |
|  | 0xF371 | R\_DEV\_CFG\_INFO\_ALG\_ERROR | 算法配置错误 | |
|  | 0xF401 | R\_PIN\_DATA\_NOT\_EXIST | PIN数据不存在 | |
|  | 0xF402 | R\_PIN\_RAND\_CHALLENGE | 挑战码错误 | |
|  | 0xF403 | R\_PIN\_AUTHCODE\_WRONG | 授权码错误 | |
|  | 0xF404 | R\_PIN\_AUTHCODE\_INVLD | 授权码不存在 | |
|  | 0xF501 | R\_CRYPTO\_XML\_FORMAT\_ERR | XML报文格式错误 | |
|  | 0xF502 | R\_CRYPTO\_XML\_SHOWTOOLONG | 屏幕显示数据太长 | |
|  | 0xF503 | R\_CRYPTO\_XML\_WATMSG | XML报文解析未完成，继续等待数据 | |
|  | 0xF511 | R\_CRYPTO\_KEY\_FORMATDATA\_ERR | 密钥解析错误 | |
|  | 0xF512 | R\_CTYPTO\_KEY\_TYPE\_ERR | 密钥类型错误 | |
|  | 0xF513 | R\_CTYPTO\_KEY\_HASH\_ERR | 密钥哈希错误 | |
|  | 0xF514 | R\_CTYPTO\_KEY\_USESTATUS\_ERR | 密钥状态错误 | |
|  | 0xF515 | R\_CTYPTO\_KEY\_ID\_ERR | 密钥ID错误 | |
|  | 0xF516 | R\_CTYPTO\_KEY\_GENINCARD\_ERR | 密钥属性错误（必须内部生成的密钥才允许报文签名） | |
|  | 0xF517 | R\_CTYPTO\_KEY\_DATA\_TYPE\_ERR | 密钥数据类型错误 | |
|  | 0xF521 | R\_CTYPTO\_OPT\_HASHTYPE\_ERR | 哈希类型错误 | |
|  | 0xF522 | R\_CTYPTO\_OPT\_DATA\_ERR | 运算数据错误 | |
|  | 0xF523 | R\_CTYPTO\_OPT\_PADDINGHASH\_ERR | 填充哈希类型错误 | |
|  | 0xF524 | R\_CTYPTO\_OPT\_RESULT\_ERR | 运算结果错误 | |
|  | 0xF525 | R\_CTYPTO\_OPT\_PADDINGDATA\_ERR | 运算结果的填充错误 | |
|  | 0xF526 | R\_CTYPTO\_OPT\_PADDINGRAND\_ERR | 密文随机数填充错误 | |
|  | 0xF527 | R\_CTYPTO\_OPT\_VERIFY\_ERR | 挑战码验签错误 | |
|  | 0xF531 | R\_CTYPTO\_ALG\_NOT\_SUPPORT | 算法不支持 | |
|  | 0xF534 | R\_CTYPTO\_ALG\_BITS\_ERR | 算法模长错误 | |
|  | 0xF535 | R\_CTYPTO\_ALG\_LEN\_ERR | 密钥长度错误 | |
|  | 0xF541 | R\_CTYPTO\_AGREE\_USERID\_LEN\_ERR | 密钥协商用户ID长度错误 | |
|  | 0xF53 | R\_CTYPTO\_AGREE\_HANDLE\_ERR | 密钥协商句柄错误 | |
|  | 0xF53 | R\_CTYPTO\_KEY\_BITLEN\_ERR | 外部密钥位长错误 | |
|  | 0xF601 | R\_OTHER\_APDUBODY\_DATA\_ERR | 步骤控制数据检查错误 | |
|  | 0xF602 | R\_OTHER\_STEPCONTRCODE\_SETP\_ERR | 步骤错误 | |
|  | 0xF603 | R\_OTHER\_CHALLENGE\_STEP\_ERR | 挑战步骤错误 | |
|  | 0xF604 | R\_OTHER\_LIFE\_STATUS\_ERR | 生命周期状态错误 | |
|  | 0xF605 | R\_OTHER\_LIFE\_STATUS\_BIT\_ERR | 生命周期设置数据错误 | |
|  | 0xFAXY | R\_ALG\_BASE\_ERR | 算法错误  （XY为算法内部错误码） | |
|  | 0xFA11 | DESNull | 输入为空 | DES算法 |
|  | 0xFA12 | DESLengthError | 长度错误 |
|  | 0xFA13 | DESLengthZero | 输入长度为0 |
|  | 0xFA14 | DESStateError | 时钟状态异常，或未初始化 |
|  | 0xFA15 | DESSeedError | 随机数种子错误 |
|  | 0xFA16 | DESCloseError | 时钟关闭异常 |
|  | 0xFA17 | DESAttacked | 算法被攻击 |
|  | 0xFA21 | TDESNull | 输入为空 | TDES算法 |
|  | 0xFA22 | TDESLengthError | 长度错误 |
|  | 0xFA23 | TDESLengthZero | 输入长度为0 |
|  | 0xFA24 | TDESStateError | 状态异常，或函数调用顺序错误 |
|  | 0xFA25 | TDESSeedError | 随机数种子错误 |
|  | 0xFA26 | TDESKeyLenError | 密钥长度选择错误 |
|  | 0xFA27 | TDESCloseError | 时钟关闭异常 |
|  | 0xFA28 | TDESAttacked | 算法被攻击 |
|  | 0xFA31 | SM4Null | 输入为空 | SM4算法 |
|  | 0xFA32 | SM4LengthError | 长度错误 |
|  | 0xFA33 | SM4LengthZero | 输入长度为0 |
|  | 0xFA34 | SM4StateError | 时钟状态异常，或未初始化 |
|  | 0xFA35 | SM4SeedError | 随机数种子错误 |
|  | 0xFA36 | SM4CloseError | 时钟关闭异常 |
|  | 0xFA37 | SM4Attacked | 算法被攻击 |
|  | 0xFA41 | ModInvNotExsited | 模逆不存在 | RSA算法 |
|  | 0xFA42 | FillEArgError | 填充E值算法错误 |
|  | 0xFA43 | RSANBitlenError | N值长度错误 |
|  | 0xFA44 | RSAEBitlenError | E值长度错误 |
|  | 0xFA45 | RSANEvenError | N值偶数错误 |
|  | 0xFA46 | AHECModExpCalError | AHEC模计算错误 |
|  | 0xFA47 | SafeModExpError | 安全模式指数错误 |
|  | 0xFA48 | SafeCRTModExpError | CRT安全模式指数错误 |
|  | 0xFA49 | RSACloseError | 时钟关闭异常 |
|  | 0xFA4A | RSAWordlenError | 字长度错误 |
|  | 0xFA4B | PrimeTestError | 测试异常 |
|  | 0xFA4C | RNGGenerateError | 生成密钥错误 |
|  | 0xFA51 | SM2BufferNull | 空指针 | SM2算法 |
|  | 0xFA52 | SM2LengthError | 输入长度错误 |
|  | 0xFA53 | PubKeyNot04 | 公钥不以04开头 |
|  | 0xFA54 | PubKeyError | 公钥错误 |
|  | 0xFA55 | PriKeyError | 私钥错误 |
|  | 0xFA56 | SM2NotInCurve | 点不在曲线上 |
|  | 0xFA57 | SM2RandomTooLong | 随机数K过大 |
|  | 0xFA58 | SM2ZeroALL | 全0 |
|  | 0xFA59 | SM2DecryVerifyFailed | 解密校验失败 |
|  | 0xFA5A | SM2SignFailed | 签名失败 |
|  | 0xFA5B | SM2VerifyFailed | 验签失败 |
|  | 0xFA5C | SM2ECCPError | 点乘运算错误 |
|  | 0xFA5D | SM2KError | 安全版点乘运算中k被篡改 |
|  | 0xFA5E | SM2NOMODINV | 模逆不存在 |
|  | 0xFA5F | SM2SetCipherError | 密文格式错误 |
|  | 0xFA61 | LENERR | SAC RAM长度错误 | 随机数 |
|  | 0xFA62 | POKERERR | Poker测试出错 |
|  | 0xFA63 | ADDRNULL | 地址为0 |
|  | 0xFA64 | RNGMODERR | 模式错误 |
|  | 0xFAA1 | R\_ALG\_ADPT\_DES\_NOT\_INIT | DES算法未初始化 | 适配层自定义算法错误 |
|  | 0xFAA2 | R\_ALG\_ADPT\_DES\_MODE\_ERR | DES算法模式错误 |
|  | 0xFAA3 | R\_ALG\_ADPT\_RSA\_SET\_BIT\_ERR | RSA算法设置比特错误 |
|  | 0xFAA4 | R\_ALG\_ADPT\_RSA\_E\_ERR | RSA算法E值错误 |
|  | 0xFAA5 | R\_ALG\_ADPT\_RSA\_BIT\_LEN\_ERR | RSA算法公私钥比特错误 |
|  | 0xFAA6 | R\_ALG\_ADPT\_SM2\_ROLE\_ERR | SM2算法角色错误 |
|  | 0xFAA7 | R\_ALG\_ADPT\_RAND\_LEN\_ERR | 随机数长度错误 |
|  | 0xFAA8 | R\_ALG\_ADPT\_RAND\_BUF\_ERR | 随机数分配内存为空 |
|  | 0xFAB1 | R\_ALG\_RSA\_DECRYPT\_ERR | RSA算法解密失败 | 应用层算法错误 |
|  | 0xFAB2 | R\_ALG\_RSA\_VERIFY\_ERR | RSA算法验签失败 |