**锦弘霖智能POS AP与SP通讯协议规范**

|  |  |  |  |
| --- | --- | --- | --- |
| 项目编号 |  | | |
| 文件状态 | [√]草稿 [] 正式发布 | | |
| 当前版本 | V1.2 | | |
| 拟 制 |  | 日期 |  |
| 审 核 |  | 日期 |  |
| 批 准 |  | 日期 |  |

公司:

地址:

电话:

传真:

# 版本历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 作者 | 参与者 | 发布日期 | 备注 |
| V1.0 | 邓经清 |  | 2022/08/10 | 1. 初始版本 |
| V1.1 | 邓经清 |  | 2022/08/10 | 1. 增加单独寻卡指令； 2. 增加发送寻卡结果报文； |
| V1.2 | 邓经清 |  | 2022/09/01 | 1. 删除接口：获取当前 KSN； 2. 删除接口：KSN 自增 1； |
| V1.2 | 邓经清 |  | 2022/09/08 | 1. 增加文件下载章节； 2. TP增加：设置触控有效区域； |
| V1.3 | 邓经清 |  | 2022/09/19 | 1. 单独寻卡报文超时时间单位改为ms，占4个字节 2. 打印机6C指令增加包序号；第0包为结束； |
| V1.3 | 邓经清 |  | 2022/09/29 | 1. 修改0x3F设置触控参数，增加上报的超时时间； 2. 增加0x2F，使能下位机进入BOOT； |
| V1.3 | 邓经清 |  | 2022/10/19 | 1. 删除解触发指令0x85； 2. 增加安全功能；（写SN、解自毁、重置BOOT...） |
| V1.4 | 邓经清 |  | 2022年11月15日 | 1. 单独寻卡模块，证通使用统一一个命令字处理； |
| V1.4 | 邓经清 |  | 2022年12月26日 | 1. 0x46指令，删除参数：手输卡号的最小长度、手输卡号的最大长度 2. 0x47指令，增加参数：按键键值； |
| V1.4 | 邓经清 |  | 2023年01月05日 | 1. 增加算法模块 |
| V1.4 | 邓经清 |  | 2023年02月02日 | 1.增加通讯数据加密协议； |
| V1.4 | 邓经清 |  | 2023年02月13日 | 1.增加复位下位机指令； |
| V1.4 | 邓经清 |  | 2023年02月22日 | 1.增加设置终端序列号（命令字:0x28） |
| V1.4 | 邓经清 |  | 2023年03月16日 | 1. 增加获取键盘随机数（命令字:0x7E） 2. 增加设置按键坐标（命令字:0x7F） |
| V1.4 | 邓经清 |  | 2023年03月29日 | 1. 增加解触发指令（命令字:0x86） |
| V1.4 | 邓经清 |  | 2023年05月09日 | 修改开启触发指令（命令字:0x85），增加配置防抖参数； |
| V1.4 | 邓经清 |  | 2023年5月30日 | 增加获取芯片序列号（命令字:0x29） |
| V1.4 | 邓经清 |  | 2023年6月14日 | 增加结束寻卡（命令字:0x48） |
| V1.4 | 邓经清 |  | 2023年7月28日 | 增加使能下位机立即进入休眠模式（命令字:0x2A） |
| V1.4 | 邓经清 | 张家柱 | 2023年9月21日 | 增加下位机系统关机（命令字:0x26） |
| V1.4 | 邓经清 | 张家柱 | 2023年10月30日 | 增加Mifare卡认证（命令字：0x54）  增加Mifare卡操作（命令字：0x55） |
| V1.4 | 邓经清 | 张家柱 | 2023年12月11日 | 扫码模块命令字调整（0x90 → 0x5A, 0x91 → 0x5B, 0x92 → 0x5C） |
| V1.4 | 邓经清 | 张家柱 | 2023年12月30日 | 0x30：增加参数配置是否主动上报按键值；  0x3A：增加参数配置是否主动上报坐标值； |
| V1.4 | 邓经清 | 张家柱 | 2023年03月01日 | 0x85：增加配置参数复位检查开关； |
| V1.4 | 邓经清 | 张家柱 | 2023年03月08日 | 0x84：增加返回参数复位检查开关； |
| V1.4 | 邓经清 | 张家柱 | 2023年07月30日 | 0x84：增加返回参数自毁开启标志； |

# 引言

## 背景

此协议适用于：上位机与安全芯片间通讯；

## 术语、定义和缩略语

略

## 规范性引用文件

略

## 编写目的

略

# 通信协议

## 协议描述

通信协议定义了安全芯片与上位机之间信息交换的规则。无论硬件上采用UART 、SPI还是USB 接口型式，都采用同一套通讯协议和报文集。

安全芯片与上位机之间进行数据通讯采用“命令－应答”的方式，其中上位机作为主动方，安全芯片为被动方，由上位机发送命令，安全芯片应答**(除非以下报文有特殊说明，上位机均为主动方)**。

## 协议说明

**请求应答报文数据遵循以下格式: （明文）**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 起始位 | B | 1 | 固定为0x02 |
| 命令字 | B | 1 | 报文类型 |
| 指示位 | B | 1 | 0x2F, 请求报文  0x3F, 通知报文  0x4F, 响应报文 |
| 长度 | B | 2 | 数据域长度，十六进制 ，高位在前，低位在后。比如： 0x01 0x10 表示长度为 272 个 Byte |
| 数据域 | B | N |  |
| 结束位 | B | 1 | 固定为0x03 |
| 校验码 | B | 1 | 从命令字到数据域的异或和校验 |

**请求应答报文数据遵循以下格式: （密文）**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 起始位 | B | 1 | 固定为0x02 |
| 命令字 | B | 1 | 报文类型 |
| 指示位 | B | 1 | 0x2F, 请求报文  0x3F, 通知报文  0x4F, 响应报文 |
| 加密后的数据长度 | B | 2 | 数据域长度，十六进制 ，高位在前，低位在后。比如： 0x01 0x10 表示长度为 272 个 Byte  （16倍数） |
| 长度+数据域密文 | B | N | 1. 将实际数据长度2字节和数据域明文作为整体，末尾补0x00，补齐16倍数长度； 2. AES加密； |
| 结束位 | B | 1 | 固定为0x03 |
| 校验码 | B | 1 | 从命令字到长度+数据域密文的异或和校验 |

**注：在以下报文定义时，只定义命令字和数据域明文**

## 符号定义

|  |  |
| --- | --- |
| 字符 | 描述 |
| A | 字母向左靠，右部多余部分填空格。 |
| AN | 字母和/或数字，左靠，右部多余部分填空格。 |
| S | 特殊符号。 |
| ANS | 字母、数字和/或特殊符号，左靠，右部多余部分填空格。 |
| AS | 字母和/或特殊符号，左靠，右部多余部分填空格。 |
| b | 二进制位(bit) 。 |
| B | 二进制字节(Byte) 。 |
| YY | 年。 |
| MM | 月。 |
| DD | 日。 |
| hh | 时。 |
| mm | 分。 |
| ss | 秒。 |
| N | 变长。 |
| LVAR | 可变长度域,1字节长度(B)+数据。 |
| LLVAR | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

# 系统模块

## 设置通讯方式 （命令字:0x11）

**功能说明:**

设置通讯方式

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 设置通讯模式 | B | 1 | 0x00 不需要检测通讯模块  0x01 GPRS,4G 等  0x02 WIFI  0x04 蓝牙 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 获取网络制式（命令字:0x12）

**功能说明:**

获取网络制式

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 网络制式 | B | 1 | //无线网络制式  0x00 4G  0x01 2G |

## 读取系统版本信息 （命令字:0x17）

**功能说明:**

获取系统版本信息.

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 版本类型 | B | 1 | 0x00 //硬件(内部版本号) # 上位机为准（整机版本）  0x01 //Boot 版本号 # 下位机的BOOT  0x02 //内核版本号 # 上位机的内核版本（基础包）  0x03 //系统版本号 # 下位机的MNT  0x04 //底层库版本 # 外接设备版本（如：520K键盘）  0x05 //SDK 版本号 # 上位机的MNT |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 版本号 | LVAR | N | 1字节长度+数据 （最大32字节） |

## 获取硬件序列号（命令字:0x18）

**功能说明:**

获取硬件序列号.

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 硬件序列号 | LVAR | N | 1字节长度+数据 （最大32字节） |

## 获取设备型号（命令字:0x19）

**功能说明:**

获取设备型号.

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 设备型号 | LVAR | N | 1字节长度+数据 （最大16字节） |

## 获取客户自定义序列号 （命令字:0x1A）

**功能说明:**

获取客户自定义序列号.

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 客户自定义序列号 | LVAR | N | 1字节长度+数据 （最大32字节） |

## 设置时钟（命令字:0x1B）

**功能说明:**

设置时钟

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 日期、时间参数 | B | 6 | 格 式 为YYMMDDhhmmss,BCD码,共6个字节  长 ( 有 效 时 间 范 围 :2000-1-1 ~  2099-12-31) |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 获取时钟 （命令字:0x1C）

**功能说明:**

获取时钟

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 日期、时间 | B | 6 | 格 式 为YYMMDDhhmmss,BCD码,共6个字节  长 ( 有 效 时 间 范 围 :2000-1-1 ~  2099-12-31) |

## 蜂鸣（命令字:0x20）

**功能说明:**

蜂鸣器按固定频率发声

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 蜂鸣类型 | B | 1 | 0x00:正常鸣叫 (1声)  0x01:异常鸣叫 (3声) |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 蜂鸣器按指定的频率发声（命令字:0x21）

**功能说明:**

蜂鸣器按指定的频率发声,非阻塞

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 设定的频率 | B | 4 |  |
| 持续发声时间,单位:ms | B | 4 |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 点亮 LED 指示灯（命令字:0x22）

**功能说明:**

点亮 LED 指示灯

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 指示灯 ID | B | 4 | 指示灯 ID,按位控制  0x01 蓝灯  0x02 黄灯  0x04 绿灯  0x08 红灯  0x0F 所有灯 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 熄灭 LED 指示灯（命令字:0x23）

**功能说明:**

熄灭 LED 指示灯

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 指示灯 ID | B | 4 | 指示灯 ID,按位控制  0x01 蓝灯  0x02 黄灯  0x04 绿灯  0x08 红灯  0x0F 所有灯 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## LED 指示灯闪烁（命令字:0x24）

**功能说明:**

LED 指示灯闪烁,非阻塞

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 指示灯 ID | B | 4 | 指示灯 ID,按位控制  0x01 蓝灯  0x02 黄灯  0x04 绿灯  0x08 红灯  0x0F 所有灯 |
| 闪烁的周期 | B | 4 | 每 Frequence 毫秒闪烁一次， 单位： ms |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 系统复位（命令字:0x25）

**功能说明:**

系统复位

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 系统关机（命令字:0x26）

**功能说明:**

系统关机，下位机接收到此命令，执行软复位操作；

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## ~~设置无操作进入低功耗的超时时间（命令字:0x27）【已弃用】~~

**~~功能说明:~~**

~~设置系统无操作时进入低功耗时间~~

**~~请求报文数据域：~~**

|  |  |  |  |
| --- | --- | --- | --- |
| ~~名称~~ | ~~类型~~ | ~~长度~~ | **~~描述~~** |
| ~~休眠超时时间参数~~ | ~~B~~ | ~~4~~ | ~~Bit0~23 系统进入低功耗的超时时间,~~  ~~单位:ms,=0 表示不会进入低功能;~~  ~~Bit24~31 进入低功耗的关机时间~~  ~~单位:分钟,=0 不关机;~~ |

**~~应答报文数据域：~~**

|  |  |  |  |
| --- | --- | --- | --- |
| ~~名称~~ | ~~类型~~ | ~~长度~~ | **~~描述~~** |
| ~~应答码~~ | ~~B~~ | ~~4~~ | ~~0 成功(只有在0成功时，才有后续报文)~~  ~~其他 参考附录通用错误定义~~ |

## 设置终端序列号（命令字:0x28）

**功能说明:**

设置终端序列号（SN和客户SN）

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 终端序列号数据(SN) | LVAR | N | 1字节长度+数据 （最大32字节） |
| 客户自定义序列号数据(CSN) | LVAR | N | 1字节长度+数据 （最大32字节） |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 获取芯片序列号（命令字:0x29）

**功能说明:**

获取芯片序列号（CPU ID）

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 芯片序列号数据(CPU ID) | LVAR | N | 1字节长度+数据 （最大32字节） |

## 使能下位机立即进入休眠模式（命令字:0x2A）

**功能说明:**

使能下位机立即进入休眠模式

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 唤醒方式 | B | 4 | BIT0 // 按任意键时退出低功耗状态  BIT1 // 上位机IO唤醒  BIT2 // IC卡唤醒  BIT3 // 磁条卡唤醒  BIT4 // 非接卡唤醒  BIT5 // 触摸屏唤醒  ... |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 唤醒方式 | B | 4 | BIT0 // 按任意键时退出低功耗状态  BIT1 // 上位机IO唤醒  BIT2 // IC卡唤醒  BIT3 // 磁条卡唤醒  BIT4 // 非接卡唤醒  BIT5 // 触摸屏唤醒  ... |

## 下位机进入BOOT或查询状态（命令字:0x2F）

**功能说明:**

使能下位机停留BOOT，或查询状态；

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 类型 | B | 1 | =0x00 查询下位机的状态  =0x01 使能下位机进入BOOT模式 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 查询结果  （注：只有当类型=0时，才有此字段） | B | 1 | BIT7;(0为BOOT模式，1为MNT模式)  BIT2 ~ BIT6:(预留)  BIT1:(1为无固件)  BIT0:(1为未加密) |

# 键盘模块

## 打开键盘 （命令字:0x30）

**功能说明:**

打开键盘设备

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 禁用键盘主动上报开关 | B | 1 | I90: 无此字段，默认主动上报；其它机型默认不主动上报；  = 1，不主动上报；  = 0，主动上报； |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 关闭键盘 （命令字:0x31）

**功能说明:**

关闭键盘设备

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 读取按键值 （命令字:0x32）

**功能说明:**

读取按键值

注：政通客户：做成主动上报键值；

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 按键值,见下面按键键值定义  0x30 按键0  0x31 按键1  0x32 按键2  0x33 按键3  0x34 按键4  0x35 按键5  0x36 按键6  0x37 按键7  0x38 按键8  0x39 按键9  0x07 字母  0x08 退格  0x0D 确认  0x12 向左  0x13 向右  0x14 菜单  0x15 功能  0x19 打印向上走纸  0x1B 取消  0x26 向上  0x28 向下  0x2A '\*'键  0x2E 清除  0xFF 无效按键  0x00 超时无按键  其他 无效按键 |

## 清除按键缓存 （命令字:0x33）

**功能说明:**

清除按键缓存

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 设置打开关闭按键音 （命令字:0x34）

**功能说明:**

设置打开关闭按键音

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 按键音控制状态 | B | 1 | 0x00 //键盘按键音关闭  0x01 //键盘按键音打开(默认) |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 设置按键背光 （命令字:0x35）

**功能说明:**

设置按键背光

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 按键背光控制状态 | B | 1 | 0x00 //键盘背光关闭(默认)  0x01 //键盘背光打开 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 读取按键状态 （命令字:0x36）

**功能说明:**

读取按键状态，可以读取按键的键值及状态；（按下、弹起、长按）

注：此协议仅适用于喇叭外接键盘

1. 键盘外设主动上报（指示位为0x3F）状态（按下、弹起、长按），空闲时不上报；
2. 当键盘上报键值为 0xFE 发起握手请求，表示键盘请求握手，上位机响应(指示位为0x4F)成功；

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 按键值,见下面按键键值定义  0x30 按键0  0x31 按键1  0x32 按键2  0x33 按键3  0x34 按键4  0x35 按键5  0x36 按键6  0x37 按键7  0x38 按键8  0x39 按键9  0x07 字母  0x08 退格  0x0D 确认  0x12 向左  0x13 向右  0x14 菜单  0x15 功能  0x19 打印向上走纸  0x1B 取消  0x26 向上  0x28 向下  0x2A '\*'键  0x81 '.'键  0x2E 清除  0xFE 发起握手请求  0xFF 无效按键  0x00 超时无按键  其他 无效按键 |
| 按键状态 | B | 1 | ~~0x01 按下状态（已取消此状态）~~  0x02 弹起状态（压下不超过1S后弹起，短按值）  0x03 长按状态（压下超过1S）  注：0x03长按状态，不会上报0x02弹起包； |

# TP模块

## 打开 TP（命令字:0x3A）

**功能说明:**

打开 TP

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 禁用坐标主动上报开关 | B | 1 | I90: 无此字段，默认主动上报；其它机型默认不主动上报；  = 1，不主动上报；  = 0，主动上报； |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 关闭 TP（命令字:0x3B）

**功能说明:**

关闭 TP

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

## 检查是否支持 TP（命令字:0x3C）

**功能说明:**

检查 TP 是否支持

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0x00 支持  其他 不支持 |

## 获取触控坐标值（命令字:0x3E）

**功能说明:**

获取触控坐标值， 屏幕左上角为起点坐标(0,0)

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| X坐标 | B | 4 |  |
| Y坐标 | B | 4 |  |

## 设置触控参数（命令字:0x3F）

**功能说明:**

设置触控有效区域， 屏幕左上角为起点坐标(0,0)。和上报坐标信息最小时间间隔；

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 有效X起始坐标 | B | 4 | 默认值为0 |
| 有效Y起始坐标 | B | 4 | 默认值为0 |
| 有效X结束坐标 | B | 4 | 默认值为319 |
| 有效Y结束坐标 | B | 4 | 默认值为239 |
| 上报坐标时间最小间隔（ms） | B | 4 | 默认值为20ms |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

# 磁条卡

## 打开磁条卡设备（命令字:0x40）

**功能说明:**

打开磁条卡设备

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1101 失败  -1102 参数错误  -1103 未刷卡  其他 参考附录通用错误定义 |

## 关闭磁条卡设备（命令字:0x41）

**功能说明:**

关闭磁条卡设备

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1101 失败  -1102 参数错误  -1103 未刷卡  其他 参考附录通用错误定义 |

## 检查是否有刷磁条卡（命令字:0x42）

**功能说明:**

检查是否有刷磁条卡

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1101 失败  -1102 参数错误  -1103 未刷卡  其他 参考附录通用错误定义 |

## 读磁条卡数据（命令字:0x43）

**功能说明:**

检查是否有刷磁条卡

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1101 失败  -1102 参数错误  -1103 未刷卡  其他 参考附录通用错误定义 |
| Track1 | LVAR | N | 1字节长度+数据  读取到的 1 磁道数据  [不带起始符和结束符] |
| Track2 | LVAR | N | 1字节长度+数据  读取到的 2 磁道数据  [不带起始符和结束符] |
| Track3 | LVAR | N | 1字节长度+数据  读取到的 3 磁道数据  [不带起始符和结束符] |

## 清除磁卡数据缓冲（命令字:0x44）

**功能说明:**

清除磁卡缓冲区数据

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1101 失败  -1102 参数错误  -1103 未刷卡  其他 参考附录通用错误定义 |

## 格式化磁道信息（命令字:0x45）

**功能说明:**

格式化磁道信息

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| Track1 | LVAR | N | 1字节长度+数据  读取到的 1 磁道数据  [不带起始符和结束符] |
| Track2 | LVAR | N | 1字节长度+数据  读取到的 2 磁道数据  [不带起始符和结束符] |
| Track3 | LVAR | N | 1字节长度+数据  读取到的 3 磁道数据  [不带起始符和结束符] |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1101 失败  -1102 参数错误  -1103 未刷卡  其他 参考附录通用错误定义 |
| 卡号 | LVAR | N | 1字节长度+数据 (最大20字节) |
| 有效期 | LVAR | N | 1字节长度+数据 (最大4字节) |
| 持卡人姓名 | LVAR | N | 1字节长度+数据 (最大32字节) |
| 服务代码 | LVAR | N | 1字节长度+数据 (最大3字节) |

# IC卡模块

## 打开 IC 卡模块（命令字:0x4A）

**功能说明:**

打开 IC 卡模块,对模块进行初始化

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 卡类型 | B | 1 | 0x00 CPU 卡  0x01 At24cxx  0x02 MEMORY 卡 |
| 卡座号 | B | 1 | 0x00 标准大卡IC卡座  0x01 SAM 1  0x02 SAM 2  0x03 SAM 3  0x04 SAM 4 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1201 失败  -1202 参数错误  -1203 卡不在座子上  -1204 卡未上电  -1205 超时错误,或无响应(L1 TIME OUT ERROR)  -1206 协议错误（L1 PROTOCOL ERROR）  -1207 传输错误,任何其他错误其他 参考附录通用错误定义 |

## 关闭 IC 卡模块（命令字:0x4B）

**功能说明:**

关闭 IC 卡模块。如模块下电则下电,然后关闭

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 卡类型 | B | 1 | 0x00 CPU 卡  0x01 At24cxx  0x02 MEMORY 卡 |
| 卡座号 | B | 1 | 0x00 标准大卡IC卡座  0x01 SAM 1  0x02 SAM 2  0x03 SAM 3  0x04 SAM 4 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1201 失败  -1202 参数错误  -1203 卡不在座子上  -1204 卡未上电  -1205 超时错误,或无响应(L1 TIME OUT ERROR)  -1206 协议错误（L1 PROTOCOL ERROR）  -1207 传输错误,任何其他错误其他 参考附录通用错误定义 |

## 检查 ICC 状态（命令字:0x4C）

**功能说明:**

检查 ICC 状态，模块上电成功之后才有效。

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 卡类型 | B | 1 | 0x00 CPU 卡  0x01 At24cxx  0x02 MEMORY 卡 |
| 卡座号 | B | 1 | 0x00 标准大卡IC卡座  0x01 SAM 1  0x02 SAM 2  0x03 SAM 3  0x04 SAM 4 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)卡在座子上  -1201 失败  -1202 参数错误  -1203 卡不在座子上  -1204 卡未上电  -1205 超时错误,或无响应(L1 TIME OUT ERROR)  -1206 协议错误（L1 PROTOCOL ERROR）  -1207 传输错误,任何其他错误其他 参考附录通用错误定义 |

## IC 卡上电复位（命令字:0x4D）

**功能说明:**

打开 ICC 模块,对模块上电复位。

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 卡类型 | B | 1 | 0x00 CPU 卡  0x01 At24cxx  0x02 MEMORY 卡 |
| 卡座号 | B | 1 | 0x00 标准大卡IC卡座  0x01 SAM 1  0x02 SAM 2  0x03 SAM 3  0x04 SAM 4 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)卡在座子上  -1201 失败  -1202 参数错误  -1203 卡不在座子上  -1204 卡未上电  -1205 超时错误,或无响应(L1 TIME OUT ERROR)  -1206 协议错误（L1 PROTOCOL ERROR）  -1207 传输错误,任何其他错误其他 参考附录通用错误定义 |
| 复位数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## IC 卡模块下电 （命令字:0x4E）

**功能说明:**

对IC 卡模块下电

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 卡类型 | B | 1 | 0x00 CPU 卡  0x01 At24cxx  0x02 MEMORY 卡 |
| 卡座号 | B | 1 | 0x00 标准大卡IC卡座  0x01 SAM 1  0x02 SAM 2  0x03 SAM 3  0x04 SAM 4 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1201 失败  -1202 参数错误  -1203 卡不在座子上  -1204 卡未上电  -1205 超时错误,或无响应(L1 TIME OUT ERROR)  -1206 协议错误（L1 PROTOCOL ERROR）  -1207 传输错误,任何其他错误其他 参考附录通用错误定义 |

## IC 卡发送 APDU 命令 （命令字:0x4F）

**功能说明:**

IC 卡发送 APDU 命令.

APDU 发送数据格式：

CLA+INS+P1+p2+Lc+DATA+ Le（有期望返回数据 le 存在 反之不存在 Le）

返回数据：

DADA+SWA+SWB

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 卡座号 | B | 1 | 0x00 标准大卡IC卡座  0x01 SAM 1  0x02 SAM 2  0x03 SAM 3  0x04 SAM 4 |
| 发送的卡片数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1201 失败  -1202 参数错误  -1203 卡不在座子上  -1204 卡未上电  -1205 超时错误,或无响应(L1 TIME OUT ERROR)  -1206 协议错误（L1 PROTOCOL ERROR）  -1207 传输错误,任何其他错误其他 参考附录通用错误定义 |
| 卡片返回数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

# 非接卡模块

## 打开非接模块（命令字:0x50）

**功能说明:**

打开非接模块,并上电

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1301 失败  -1302 参数错误  -1303 未搜寻到卡片  -1304 感应区内卡片过多（多卡冲突）  -1305 超时错误(L1 TIME OUT ERROR)  -1306 协议错误（L1 PROTOCOL ERROR)  -1307 传输错误,任何其他错误  其他 参考附录通用错误定义 |

## 关闭非接模块（命令字:0x51）

**功能说明:**

对非接模块下电,并关闭

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1301 失败  -1302 参数错误  -1303 未搜寻到卡片  -1304 感应区内卡片过多（多卡冲突）  -1305 超时错误(L1 TIME OUT ERROR)  -1306 协议错误（L1 PROTOCOL ERROR)  -1307 传输错误,任何其他错误  其他 参考附录通用错误定义 |

## 寻卡激活（命令字:0x52）

**功能说明:**

寻卡激活

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 非接卡类型 | B | 1 | 0x01 Type A卡, 13.56M  0x02 Type B卡, 13.56M  0x04 M1卡, 13.56M  0x08 Type C卡  支持多种,按位表示,用或"|"的方式 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1301 失败  -1302 参数错误  -1303 未搜寻到卡片  -1304 感应区内卡片过多（多卡冲突）  -1305 超时错误(L1 TIME OUT ERROR)  -1306 协议错误（L1 PROTOCOL ERROR)  -1307 传输错误,任何其他错误  其他 参考附录通用错误定义 |
| 读到的非接卡类型 | B | 1 | ‘A’ —搜寻到 A 型卡  ‘B’ —搜寻到 B 型卡  ‘M’ —搜寻到 M1 卡  ‘F’ —搜寻到 Felica 卡 |
| 序列号 | LVAR | N | 可变长度域,1字节长度+数据。  对 于 A,B 型 卡 最 少 分 配 10 字  节；对于 FELICA 卡,最少分配 16 字节的  idm,8bytes IDm + 8bytes PMm. |
| CID | LVAR | N | 可变长度域,1字节长度+数据。  指向存取卡片逻辑通道号的缓冲区，该通道号由驱动内部分配和指定， 取值范围为 0~14。  按照 ISO14443 的规定， 感应区内最多可以有 15 张卡片供轮流操作。目前的搜寻模式下， 仅允许感应区内存在一张卡， 故 CID[0]总是返回为0x00, 且后续对应用传入的有效的CID 值(0~14)均按默认的 0x00 处理.若不想输出通道号，可置 CID 为NULL |
| 错误代码、 卡片响应信息等内容的缓冲区 | LVAR | N | 可变长度域,1字节长度+数据。  存取详细错误代码、 卡片响应信息等内容  Other[0] ： 后续字节的长度  Other[1-2] 返回详细的错误代码(低字节在前)； 卡搜寻的过程较为复杂，用此返回值来进行异常错误的准确定位  Other[3…] 对于 A 型卡， 返回： ATQA[2] +SAK1 + [SAK2] + [SAK3]+ ATS\_Len +  ATS; 其中, ATQA 2 字节, SAK 1 字节, 根据卡片序列号的长短, 可能存在 SAK2, SAK3 信息, 均为一个字节. ATS\_Len 为 1 个字节. ATS 的长度由 ATS\_Len 指定.  对 于 B 型 卡 ， 返 回 卡 片 的 ATQB（Answer To Request B） 信息， 其长度为 12 字节对于 M1 卡， 返回： ATQA[2] + SAK1有关 ATS、 ATQB、 ATQA 的详细信息请查阅 ISO14443-3、 ISO14443-4 的相关部分。  Other[…299] 尾部的内容为保留字节， 用于未来扩展； 目前全输出 0x00若需要输出该信息， Other 指向的缓冲区大小至少应为 300 字节。若不想输出该信息， 可置 Other 为NULL。 |

## 发送 APDU 命令（命令字:0x53）

**功能说明:**

发送 APDU 命令

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 发送的数据 | LLVAR | N | 可变长度域,2字节长度+数据。 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1301 失败  -1302 参数错误  -1303 未搜寻到卡片  -1304 感应区内卡片过多（多卡冲突）  -1305 超时错误(L1 TIME OUT ERROR)  -1306 协议错误（L1 PROTOCOL ERROR)  -1307 传输错误,任何其他错误  其他 参考附录通用错误定义 |
| 接收的数据 | LLVAR | N | 可变长度域,2字节长度+数据。 |

## Mifare卡认证（命令字:0x54）

**功能说明:**

Mifare卡认证

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 块号 | B | 1 | 块编号 |
| 密钥类型 | B | 1 | ‘A'或‘B’ |
| 卡片序列号（UID） | LVAR | N | 可变长度域,1字节长度+数据；  卡片序列号（UID），通过寻卡函数获得（有效长度4bytes） |
| 认证密钥 | LVAR | N | 可变长度域,1字节长度+数据；  认证密钥（6字节的密钥信息） |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1301 失败  -1302 参数错误  -1303 未搜寻到卡片  -1304 感应区内卡片过多（多卡冲突）  -1305 超时错误(L1 TIME OUT ERROR)  -1306 协议错误（L1 PROTOCOL ERROR)  -1307 传输错误,任何其他错误  其他 参考附录通用错误定义 |

## Mifare卡操作（命令字:0x55）

**功能说明:**

Mifare卡操作

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 操作指令 | B | 1 | l ‘r’ 或 ‘R’：读操作  l ‘w’ 或‘W’：写操作  l ‘+’：加操作  l ‘-’：减操作  ‘>’：传输或备份 |
| 要访问的块号 | B | 1 | 要访问的块编号 |
| 目标块号 | B | 1 | 在运算结果中写入的块号（读取或写入块时，ucDesBlockNo是NULL） |
| 数据 | LVAR | N | 可变长度域,1字节长度+数据；  l对于写操作：为输入块数据（大小为6个字节）；  l对于“+”或“-”操作：为输入块数据（大小为4字节）  l对于传输操作，此数据段没有实际意义； |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1301 失败  -1302 参数错误  -1303 未搜寻到卡片  -1304 感应区内卡片过多（多卡冲突）  -1305 超时错误(L1 TIME OUT ERROR)  -1306 协议错误（L1 PROTOCOL ERROR)  -1307 传输错误,任何其他错误  其他 参考附录通用错误定义 |
| 数据 | LVAR | N | 可变长度域,1字节长度+数据；  l对于读取操作，pucVal输出块数据；（大小为6个字节； |

# 单独寻卡模块

## 单独寻卡报文（命令字:0x46）

**功能说明:**

只寻卡、判断是否刷磁条卡，插入 IC 卡，寻非接卡等。

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 寻卡方式 | B | 1 | Bit 0: 1 SWIPE\_CARD\_HAND//手输  Bit 1: 1 SWIPE\_CARD\_MAG //刷卡  Bit 2: 1 SWIPE\_CARD\_ICC //IC卡  Bit 3: 1 SWIPE\_CARD\_RF //RF  按位组合使用 |
| 寻卡超时时间 | B | 4 | 单位:ms |

**应答报文数据域：（注：证通响应报文，参考：发送寻卡结果报文（命令字:0x47））**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  其他错误  注：收到请求数据解析成功后立即响应 |

## 发送寻卡结果报文（命令字:0x47）

**功能说明:**

本报文由安全芯片发起（**指示位 = 0x3F**），上位机响应，发送寻到的卡类型；

注：证通此命令字用**0x46**（**指示位 = 0x4F**）响应；

**通知报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  -120 取消退出  -121 超时退出  其他错误 |
| 寻到卡类型 | B | 1 | Bit 0: 1 SWIPE\_CARD\_HAND//手输  Bit 1: 1 SWIPE\_CARD\_MAG //刷卡  Bit 2: 1 SWIPE\_CARD\_ICC //IC卡  Bit 3: 1 SWIPE\_CARD\_RF //RF |
| 按键键值 | B | 1 | 注：   1. 只有当寻卡类型为手输（SWIPE\_CARD\_HAND）时，才有此字段； 2. 键值范围（除开机键、取消键外的任意按键）； |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  -120 取消退出  -121 超时退出  其他错误 |

## 结束寻卡（命令字:0x48）

**功能说明:**

刷卡流程内，上位机下发指令此指令，下位机关闭磁条卡、IC卡、非接卡模块，并响应报文；

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  其他错误 |

# 扫码模块

## 打开扫码（命令字:0x5A）

**功能说明:**

打开扫码

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  其他 参考附录通用错误定义 |

## 关闭扫码（命令字:0x5B）

**功能说明:**

关闭扫码

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  其他 参考附录通用错误定义 |

## 读取扫码数据（命令字:0x5C）

**功能说明:**

读取扫码数据

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 超时时间 | B | 4 | 单位:ms |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 解码后的数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

# 打印机模块

## 检查是否支持打印机 （命令字:0x61）

**功能说明:**

检查打印机是否支持

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 支持  其他 不支持 |

## 打开打印机 （命令字:0x62）

**功能说明:**

初始化打印机,对打印机上电

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1401 失败， 或内存不足  -1402 参数错误  -1403 打印机缺纸  -1404 温度过高  -1405 打印机设备故障  其他 参考附录通用错误定义 |

## 关闭打印机 （命令字:0x63）

**功能说明:**

关闭打印机

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1401 失败， 或内存不足  -1402 参数错误  -1403 打印机缺纸  -1404 温度过高  -1405 打印机设备故障  其他 参考附录通用错误定义 |

## 查询打印机状态 （命令字:0x64）

**功能说明:**

查询打印机状态

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1401 失败， 或内存不足  -1402 参数错误  -1403 打印机缺纸  -1404 温度过高  -1405 打印机设备故障  其他 参考附录通用错误定义 |

## 设置打印灰度 （命令字:0x65）

**功能说明:**

设置打印灰度

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 打印灰度等级 | B | 1 |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1401 失败， 或内存不足  -1402 参数错误  -1403 打印机缺纸  -1404 温度过高  -1405 打印机设备故障  其他 参考附录通用错误定义 |

## 走纸 （命令字:0x6B）

**功能说明:**

走纸

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 像素点 | B | 4 | 走纸的像素点 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1401 失败， 或内存不足  -1402 参数错误  -1403 打印机缺纸  -1404 温度过高  -1405 打印机设备故障  其他 参考附录通用错误定义 |

## 打印位图数据（命令字:0x6C）

**功能说明:**

打印位图数据

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 数据包序号 | B | 1 | 1~255循环，表示为数据包下发过程；  = 0 表示最后一包，此时下位机执行打印数据 |
| 打印位图点阵数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |
| 打印位图点阵数据的宽度 | B | 4 |  |
| 打印位图点阵数据的高度 | B | 4 |  |
| 打印属性 | B | 1 | 0x01 左对齐  0x02 右对齐  0x04 居中 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1401 失败， 或内存不足  -1402 参数错误  -1403 打印机缺纸  -1404 温度过高  -1405 打印机设备故障  其他 参考附录通用错误定义 |

# 密码键盘模块

## 打开密码键盘（命令字:0x70）

**功能说明:**

打开密码键盘

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |

## 关闭密码键盘（命令字:0x71）

**功能说明:**

关闭密码键盘功能

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |

## 获取随机数（命令字:0x72）

**功能说明:**

获取随机数

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 需要获取的随机数长度 | B | 4 |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 随机数数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## 更新主密钥（命令字:0x73）

**功能说明:**

更新主密钥

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 主密钥索引 | B | 4 | 主密钥索引[0...],默认索引的最后三组为传输主密钥索引 |
| 主密钥数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：主密钥长度,无校验时为 8,16,24,有校  验则需在无校验的基础上加 1~7字  节校验 |
| 解(加)密主密钥索引 | B | 4 | 解(加)密主密钥索引,当以明文方式  写入时此参数无效 |
| 写入模式 | B | 1 | Bit 0,1:  =0x00 SDK\_PED\_DECRYPT 为主钥  解密后写入  =0x01 SDK\_PED\_ENCRYPT 为主钥  加密后写入  =0x02 SDK\_PED\_PLAINTEXT 直接  写入(明文)  Bit6,7  =0x00 SDK\_PED\_DES DES/3DES  =0x80 SDK\_PED\_SM4 SM4  =0x40 SDK\_PED\_AES  =0xC0 SDK\_PED\_XOR  ... |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |

## 更新工作密钥（命令字:0x74）

**功能说明:**

更新工作密钥

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 主密钥索引 | B | 4 |  |
| Pin 密钥密文 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：Pin 密钥密文长度(无此密钥长度为  0),无校验时为 8,16,24,有校验验则需  在无校验的基础上加 1~7 字节校验 |
| Mac 密钥密文 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：Mac 密钥密文长度(无此密钥长度为  0),无校验时为 8,16,24 ,有校验验则需  在无校验的基础上加 1~7 字节校验。 |
| TDK 密钥密文 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：TDK 密钥密文长度(无此密钥长度为  0),无校验时为 8,16,24 ,有校验验则需  在无校验的基础上加 1~7 字节校验。 |
| 写入模式 | B | 1 | 模式  Bit 0,1:  =0x00 SDK\_PED\_DECRYPT 为主钥  解密后写入  =0x01 SDK\_PED\_ENCRYPT 为主钥  加密后写入  =0x02 SDK\_PED\_PLAINTEXT 直接  写入(明文)  Bit6,7  =0x00 SDK\_PED\_DES DES/3DES  =0x80 SDK\_PED\_SM4 SM4  =0x40 SDK\_PED\_AES |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |

## 加解密数据（命令字:0x75）

**功能说明:**

按指定的工作密钥进行加解密数据

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 主密钥索引 | B | 4 |  |
| 工作密钥类型 | B | 1 | 0x01 磁道密钥  0x02 MAC密钥  0x03 主密钥 |
| 初始向量 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：初始向量(一般为 8 字节 0x00),8byte  当加解密模式为 AES,SM4 时,初始向  量(一般为 16 字节 0x00),16byte  ECB 模块下此参数无效 |
| 待加密数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：待加密数据长度(所有 DES 算法 8 字  节整倍数,SM4/AES 为 16 字节整倍  数) |
| 算法模式 | B | 1 | 0x00 ECB  0x01 CBC  0x02 CFB  0x03 OFB |
| 模式 | B | 1 | Bit 0,1:  =0x00 SDK\_PED\_DECRYPT 解密  =0x01 SDK\_PED\_ENCRYPT 加密  Bit2,3,4,5  =0x00 使用工作秘钥的长度  =0x04 SDK\_PED\_KEY\_LEN8 8 字节  秘钥  =0x08 SDK\_PED\_KEY\_LEN16 16 字  节秘钥  =0x10 SDK\_PED\_KEY\_LEN24 24 字  节秘钥  =0x20 SDK\_PED\_KEY\_LEN32 32 字  节秘钥  Bit6,7  =0x00 SDK\_PED\_DES DES/3DES  =0x80 SDK\_PED\_SM4 SM4  =0x40 SDK\_PED\_AES |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 加密后的数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## 加密磁道数据（命令字:0x76）

**功能说明:**

加密磁道数据

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 主密钥索引 | B | 4 |  |
| 磁道加密方式 | B | 1 | Bit 0~3  0x00 TD\_CUP 银联算法  ...  Bit6,7  0x00 DES/3DES  0x80 SM4  0x40 AES |
| 待加密的磁道数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 加密后的磁道数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## 计算 MAC（命令字:0x77）

**功能说明:**

计算 MAC

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 主密钥索引 | B | 4 |  |
| 待计算数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |
| MAC 算法模式 | B | 1 | Bit 0~3: MAC 算法模式  0x00 X9\_9 算法(使用 DES 3DES 密钥)  0x01 XOR(使用 DES 3DES 密钥)  0x02 X9\_19 EMV 算法(使用 3DES密钥)  0x03 ECB 银联算法(使用 DES/3DES 密钥)  0x04 ECB 银联算法(只使用 DES密钥)  0x05 ECB 银联算法(使用 DES/3DES 密钥,最后不转成 ASC)  ...  Bit6,7  =0x00 DES/3DES  =0x80 SM4  =0x40 AES |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 计算后的 MAC 值 | B | 8 |  |

## 输入联机 PIN（命令字:0x78）

**功能说明:**

输入联机 PIN

补充说明：

|  |  |  |
| --- | --- | --- |
| **AP** |  | **SE** |
| 1 | → 发送请求：输入联机 PIN |  |
| 2 | ← 上报按键：0-9数字键，上报键值‘ \*’ |  |
| 3 | ← 上报结果 |  |

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 主密钥索引 | B | 4 |  |
| 支持 PIN 的长度 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  支持 PIN 的长度,长度不支持 1,2,3  如 ：  “0,4,5,6,7,8,9,10,11,12”,能输入 4~12位之间的任意长度 PIN,支持 bypass；  “0,6”,只支持输入 6 位长度 PIN,支持  bypass；  “0,4,6”,只支持输入 4 或 6 位长度 PIN,  支持 bypass； |
| 显示\*号的行号 | B | 4 | 显示\*号的行号 |
| 显示\*号的列号 | B | 4 | 显示\*号的列号,单位:像素点 |
| 卡号 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |
| 加密方式 | B | 1 | Bit 0~4:  0x00 X98  0x04 HLB  ...  Bit6,7  0x00 DES/3DES  0x80 SM4  0x40 AES |
| 等待输入时间 | B | 4 | 等待输入时间, 单位:ms |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 密文 PIN | B | 8 |  |

## ~~输入脱机密文 PIN（命令字:0x79） 【暂不支持】~~

**功能说明:**

输入脱机密文 PIN；

补充说明：

|  |  |  |
| --- | --- | --- |
| **AP** |  | **SE** |
| 1 | → 发送请求：输入脱机密文 PIN |  |
| 2 | ← 上报按键：0-9数字键，上报键值‘ \*’ |  |
| 3 | ← 上报结果 |  |

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 支持 PIN 的长度 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  支持 PIN 的长度,长度不支持 1,2,3  如 ：  “0,4,5,6,7,8,9,10,11,12”,能输入 4~12位之间的任意长度 PIN,支持 bypass；  “0,6”,只支持输入 6 位长度 PIN,支持  bypass；  “0,4,6”,只支持输入 4 或 6 位长度 PIN,  支持 bypass； |
| 显示\*号的行号 | B | 4 | 显示\*号的行号 |
| 显示\*号的列号 | B | 4 | 显示\*号的列号,单位:像素点 |
| 超时时间 | B | 4 | 超时时间,单位:ms |
| IC 卡随机数 | B | 8 |  |
| 公钥 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| PIN 校验响应的 APDU | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## ~~输入脱机明文 PIN（命令字:0x7A） 【暂不支持】~~

**功能说明:**

输入脱机明文 PIN

补充说明：

|  |  |  |
| --- | --- | --- |
| **AP** |  | **SE** |
| 1 | → 发送请求：输入脱机密文 PIN |  |
| 2 | ← 上报按键：0-9数字键，上报键值‘ \*’ |  |
| 3 | ← 上报结果 |  |

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 支持 PIN 的长度 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  支持 PIN 的长度,长度不支持 1,2,3  如 ：  “0,4,5,6,7,8,9,10,11,12”,能输入 4~12位之间的任意长度 PIN,支持 bypass；  “0,6”,只支持输入 6 位长度 PIN,支持  bypass；  “0,4,6”,只支持输入 4 或 6 位长度 PIN,  支持 bypass； |
| 显示\*号的行号 | B | 4 | 显示\*号的行号 |
| 显示\*号的列号 | B | 4 | 显示\*号的列号,单位:像素点 |
| 超时时间 | B | 4 | 超时时间,单位:ms |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| PIN 校验响应的 APDU | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## 生成 RSA 密钥对输出公钥(N+E) （命令字:0x7B）

**功能说明:**

RSA 密钥组生成 - 并输出 RSA 模数(N)

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 期望生成 RSA 密钥长度 | B | 4 | 期望生成 RSA 密钥长度(单位:bit) |
| 公钥指数 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 公钥模 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## 使用已生成 RSA 私钥加密(N+D) （命令字:0x7C）

**功能说明:**

RSA 钥加密或解密 (N+D)

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 输入数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  (最大加密数据长度受 Rsa密钥长度限制) |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 输出数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## 硬件序列号加密（命令字:0x7D）

**功能说明:**

硬件序列号加密

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 待加密数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：当 模式 = 0x00 时,加密数据为:硬  件序列号(6 位厂商编号+2 位终端类型+最大 42 位自定义序列号） +加密随机因子(银行卡交易采用 2 域卡号后 6 位),使用 ASC 码  当 模式 = 0x01 时 ,为待加密数据(长度为 16 字节整倍数) |
| 模式 | B | 1 | 0x00 按银联 21 号文标准对硬件序列  号加密  0x01 直接对加密数据进行 SM4 算法  加密 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1503 持卡人直接按确认（无密码）  -1504 用户取消输入PIN  -1505 超时退出  -1506 输入 PIN 一小时不能超过 120 次  -1507 密钥值重复  -1508 无效密钥索引  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1520 密码键盘初始化失败  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 加密后数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  加密后数据,当对硬件序列号加密时  为 MAC(长度为 8byte） |

## 获取键盘随机数（命令字:0x7E） （仅限智能pos用）

**功能说明:**

获取键盘随机数；

|  |  |  |
| --- | --- | --- |
| 1 | 4 | 9 |
| 3 | 0 | 8 |
| 6 | 7 | 5 |
| ← | 2 | 取消 |
|  | 确认 |  |

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1521 获取随机数失败  -1522 终端已自毁  其他 参考附录通用错误定义 |
| 键盘随机数 | B | 13 | 随机排序后的键值列表（0x30, 0x39, 0x32, 0x36, 0x33, 0x34, 0x37, 0x38, 0x31, 0x35） |

## 设置按键坐标（命令字:0x7F） （仅限智能pos用）

**功能说明:**

设置触摸屏按键坐标；

坐标排序根据指令0x7F收到的键盘随机数排序下发；

例：0x30, 0x39, 0x32, 0x36, 0x33, 0x34, 0x37, 0x38, 0x31, 0x35，退格、确认、取消

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 按键随机数索引[0] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[1] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[2] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[3] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[4] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[5] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[6] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[7] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[8] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 按键随机数索引[9] | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 退格键坐标 | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 确认键坐标 | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |
| 取消键坐标 | B | 8 | 起始X：（2 bytes）  起始Y：（2 bytes）  结束X：（2 bytes）  结束Y：（2 bytes） |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  -1501 其它错误  -1502 参数错误  -1522 终端已自毁  其他 参考附录通用错误定义 |

## 查看触发状态（命令字:0x84）

**功能说明:**

查看触发状态

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 无 |  |  |  |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功，未触发  **其它：**  Bit 0-15 位: 从低到高每一位对应一路触发, 0 表示未触发, 1 表示已触发  其中：  Bit0-7: 对应触点断路触发, 比如00000101 表示第 0、2 路已触发  Bit 8: 温度已触发  Bit 9: 电压已触发  Bit 10: 频率已触发  Bit 15: 有其它触发  Bit 16-31 位: 保留 |
| 复位检查开关 | B | 1 | 0 关闭  1 开启 |
| 自毁开启标志 | B | 1 | 0 关闭 （关闭时，复位检查开关无效）  1 开启 |

## 开启触发（命令字:0x85）

**功能说明:**

开启触发

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 防抖时间 | B | 4 | 触发防抖时间（单位ms）   1. 最大支持设置防抖时间为2000ms； 2. 无此参数，默认防抖时间为0ms； |
| 复位检查开关 | B | 1 | 0 关闭  1 开启  注：无此字段，默认开启 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  **其它：**  Bit 0-15 位: 从低到高每一位对应一路触发, 0 表示未触发, 1 表示已触发  其中：  Bit0-7: 对应触点断路触发, 比如00000101 表示第 0、2 路已触发  Bit 8: 温度已触发  Bit 9: 电压已触发  Bit 10: 频率已触发  Bit 15: 有其它触发  Bit 16-31 位: 保留 |

## 解触发（命令字:0x86）（证通专用）

**功能说明:**

解锁触发状态

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 模式 | B | 1 | BIT 0 - 1: 解锁模式  = 0x00，解锁后，关闭触发；  = 0x01，解锁后，开启触发；  BIT7：恢复密钥使能  = 0x00，不恢复密钥；  = 0x80，恢复密钥；  其它位保留 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功，未触发  **其它：**  Bit 0-15 位: 从低到高每一位对应一路触发, 0 表示未触发, 1 表示已触发  其中：  Bit0-7: 对应触点断路触发, 比如00000101 表示第 0、2 路已触发  Bit 8: 温度已触发  Bit 9: 电压已触发  Bit 10: 频率已触发  Bit 15: 有其它触发  Bit 16-31 位: 保留 |

## 密钥检查（命令字:0x87）（证通专用）

**功能说明:**

密钥检查

注意：此处只检查密钥数据是否存在，自毁不会限制。上层APP自行结合0x84指令使用！！！

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 需要检测密钥的类型 | B | 1 | 0x00 // PIN密钥  0x01 // TD密钥  0x02 // MAC密钥  0x03 // 主密钥  0x05 // 双向认证密钥1  0x06 // 双向认证密钥2 |
| 需要检测密钥的索引 | B | 4 | 0 - 99 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  -1502 参数错误  -1509 未设置密钥  -1510 主密钥校验错  -1511 PIN密钥校验错  -1512 TD密钥校验错  -1513 MAC密钥校验错  -1523 密钥触发禁用 |
| KCV值 | LVAR | N | 可变长度域,1字节长度(B 高位在前，低位在后)+数据。  KCV值 |

# 算法模块

## SM3哈希算法（命令字:0x95）

**功能说明:**

SM3哈希算法

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 待计算数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  其他 参考附录通用错误定义 |
| 结果 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  说明：结果为32个字节的摘要信息,十六进制数（HEX）表示 |

## DES加解密算法（命令字:0x96）

**功能说明:**

DES加解密算法

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 算法模式 | B | 1 | #define SDK\_MATH\_MODE\_ECB (0x00)  #define SDK\_MATH\_MODE\_CBC (0x01)  #define SDK\_MATH\_MODE\_CFB (0x02)  #define SDK\_MATH\_MODE\_OFB (0x03) |
| 加解密模式 | B | 1 | #define SDK\_MATH\_DECRYPT (0x00)  #define SDK\_MATH\_ENCRYPT (0x01) |
| 初始向量 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：初始向量(一般为8字节0x00),8byte.  ECB模式下此参数无效,传入为长度为0； |
| 待计算数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：待计算数据长度,8byte的整数倍 |
| 密钥 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：密钥(8,16,24byte),根据密钥长度来做DES,3DES,三重DES加解密 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功  其他 参考附录通用错误定义 |
| 结果数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## AES加解密算法（命令字:0x97）

**功能说明:**

AES加解密算法

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 算法模式 | B | 1 | #define SDK\_MATH\_MODE\_ECB (0x00)  #define SDK\_MATH\_MODE\_CBC (0x01)  #define SDK\_MATH\_MODE\_CFB (0x02)  #define SDK\_MATH\_MODE\_OFB (0x03) |
| 加解密模式 | B | 1 | #define SDK\_MATH\_DECRYPT (0x00)  #define SDK\_MATH\_ENCRYPT (0x01) |
| 初始向量 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：初始向量(一般为16字节0x00),16byte.  ECB模式下此参数无效,传入为长度为0； |
| 待计算数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：待计算数据长度,16byte的整数倍 |
| 密钥 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：密钥长度(16,24,32byte) |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 结果数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## SM4加解密算法（命令字:0x98）

**功能说明:**

SM4加解密算法

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 算法模式 | B | 1 | #define SDK\_MATH\_MODE\_ECB (0x00)  #define SDK\_MATH\_MODE\_CBC (0x01)  #define SDK\_MATH\_MODE\_CFB (0x02)  #define SDK\_MATH\_MODE\_OFB (0x03) |
| 加解密模式 | B | 1 | #define SDK\_MATH\_DECRYPT (0x00)  #define SDK\_MATH\_ENCRYPT (0x01) |
| 密钥 | B | 16 | 密钥 |
| 初始向量 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：初始向量(一般为16字节0x00),16byte.  ECB模式下此参数无效,传入为长度为0； |
| 待计算数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：待计算数据长度,16byte的整数倍 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 结果数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## SM2加解密（命令字:0x99）

**功能说明:**

SM2加解密

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 加解密模式 | B | 1 | #define SDK\_MATH\_DECRYPT (0x00)  #define SDK\_MATH\_ENCRYPT (0x01) |
| 待计算数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |
| 密钥 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：加密用公钥（64 byte）/解密用私钥（32 byte） |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 结果数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。 |

## SM2签名算法（命令字:0x9A）

**功能说明:**

SM2签名算法

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 公钥 | B | 64 |  |
| 私钥 | B | 32 |  |
| UID | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：   1. UID的默认长度为16个字节。 默认值为0x31、0x32、0x33、0x34、0x35，0x36、0x37、0x38、0x31、0x32、0x33、0x34、0x35，0x36、0x37、0x38； 2. UID支持最大长度512Bytes |
| 待签名的数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：待签名数据最大长度2048Bytes |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |
| 验签值 | B | 64 |  |

## SM2验签算法（命令字:0x9B）

**功能说明:**

SM2验签算法

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 验签值 | B | 64 |  |
| 公钥 | B | 64 |  |
| UID | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：   1. UID的默认长度为16个字节。 默认值为0x31、0x32、0x33、0x34、0x35，0x36、0x37、0x38、0x31、0x32、0x33、0x34、0x35，0x36、0x37、0x38；   UID支持最大长度512Bytes |
| 要验签的数据 | LLVAR | N | 可变长度域,2字节长度(B 高位在前，低位在后)+数据。  注：待验签的数据最大长度2048Bytes |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0 成功(只有在0成功时，才有后续报文)  其他 参考附录通用错误定义 |

# 文件下载

## 启动下载 (命令字：0xAA)

**功能说明:**

文件下载请求；

**请求报文：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 下载的文件类型 | B | 1 | 0x01:参数（带wifi， 扫码，电签参数）  0x02:字库  0xA0:应用  0xA1:HAL MNT  0xA2:固件  0xA4:资源  0xA5:修改字库  0xA6:增加字库  0xA7:扫码库  ... |
| 压缩格式 | B | 1 | 0x00 不压缩  0x01 单包压缩  0x02 文件压缩 |
| 参数是否可重新更新 | B | 1 | 0x00 不可重置  0x01 可重置  YC3121以后机器修改为：  0x00 不可重置  0x02 表示可重置 |
| 保留 | B | 1 | 0x00 |
| 文件字节 | B | 4 |  |
| 文件内容CRC32 | B | 4 | 高位在前 |
| 文件名 | B | N | LVAR 1字节长度+文件名长度 |

**应答报文：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 应答码 | B | 4 | 0x00 成功(只有在0x00时，才有后继报文)  其他 SDK返回错误码 |
| 单包长度 | B | 2 |  |
| 起始偏移 | B | 4 | 用于断点续传，无或0x00000000为从头开始 |

## 文件下载 (命令字：0xAB)

**功能说明:**

文件下载；

**请求报文：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 包序号 | B | 1 | 1~255循环，当为0时为最后一包 |
| 文件数据偏移量 | B | 4 | 高位在前 |
| 文件数据 | B | N | LLVAR 2字节长度+文件数据 |

**应答报文：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 应答码 | B | 4 | 0x00 成功(只有在0x00时，才有后继报文)  其他 SDK返回错误码 |

# 安全功能

### 内部认证(命令字：0xA0)

**功能说明:**

内部认证

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 随机数R1 |  |  | 工具下发明文随机数 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0x00 成功(只有在0x00时，才有后继报文)  其他 SDK返回错误码 |
| 加密随机数R1(Key1) | B | 8 | 用Key1加密随机数R1 |
| 随机数R2 | B | 8 | POS发送明文随机数R2 |

### 外部认证后硬件序列号下载(命令字：0xA1)

**功能说明:**

硬件序列号及秘钥下载

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 加密随机数R2(Key2) | B | 8 | 工具收到加密随机数R1(Key1)后解密对比，通过才发送本指令  工具用Key2加密随机数R2得到加密随机数R2(Key2) |
| 自毁重置标志 | B | 1 | 0x01 重置  0x00 不重置 |
| SN号重置标志 | B | 1 | 0x01 重置  0x00 不重置 |
| 日期时间 | BCD | 7 | 格式： YYYYMMDDhhmmss |
| 硬件序列号 | B | N | LVAR 1字节长度+硬件序列号(ASC) |
| 硬件序列号密钥 | B | N | LVAR 1字节长度+传输密钥索引(1byte)+硬件序列号密钥加密值(16byte)+校验(4byte) |
| 主密钥 | B | N | LVAR 1字节长度+传输密钥索引(1byte)+主密钥加密值(8或16或24byte)+校验(4byte) |
| 客户自定义序列号 | B | N | LVAR 1字节长度+客户自定义序列号(ASC) |
| 机构私钥 | B | N | LVAR 2字节长度+机构私钥（ASC,PEM格式私钥，只取Base64编码部分) |
| 附加密钥 | B | N | LLVAR 2字节附加密钥数据总长 + 1字节附加密钥组数 + 附加密钥。  （附加密钥格式与“主密钥”相同，即：1字节长度+1字节传输密钥索引+附加密钥密文+4字节校验） |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0x00 成功(只有在0x00时，才有后继报文)  其他 SDK返回错误码  终端收到加密随机数R2Key2)后解密与R2对比，通过才执行下面操作 |
| 硬件信息 | B | N | LLVAR 2字节长度+终端信息列表(TLV结构：Tag(1byte)+L(1byte长度)+V(数据))  // 终端信息TAG  #define INFO\_MERCHANT\_NAME (0xA0) // 平台名称  #define INFO\_MNT\_VER (0xA1) // mnt版本  #define INFO\_HARDWARE\_VER (0xA2) // 硬件版本号(参数文件控制)  #define INFO\_BOOT\_VER (0xA3) // BOOT版本号  #define INFO\_APP\_VER (0xA4) // 应用版本  #define INFO\_SN (0xA5) // SN  #define INFO\_DATE (0xA6) // 出厂日期  #define INFO\_GSM\_VER (0xA7) // GPRS模块版本  #define INFO\_SDK\_VER (0xA8) // SDK VER  #define INFO\_IMEI (0xA9) // IMEI  #define INFO\_ICCID (0xAA) // ICCID  #define INFO\_IMSI (0xAB) // IMSI  #define INFO\_TERM\_TYPE (0xAC) // 终端类型  #define INFO\_OPTION (0xAD) // 硬件选配信息(TP/SCAN/WIFI)  #define INFO\_EFLASH (0xAE) // 外部FLAHS型号  #define INFO\_CSN (0xAF) // 客户CSN号  #define INFO\_LCD (0xB0)  // LCD类型  #define INFO\_RES (0xB1)  // 资源名称 |

### 外部认证后解锁(命令字：0xA7)

**功能说明:**

解锁

**请求报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 加密随机数R2(Key2) | B | 8 | 工具收到加密随机数R1(Key1)后解密对比，通过才发送本指令  工具用Key2加密随机数R2得到加密随机数R2(Key2) |
| 自毁重置标志 | B | 1 | 0x01 解锁  0x00 锁定 |

**应答报文数据域：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | **描述** |
| 应答码 | B | 4 | 0x00 成功  其他 SDK返回错误码  终端收到加密随机数R2Key2)后解密与R2对比，通过才执行下面操作 |

### 外部认证后加密芯片ID (命令字：0xA8)

**功能说明:**

加密芯片ID

**请求报文：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | | 类型 | 长度 | | 描述 |
| 加密随机数R2(Key2) | B | | | 8 | 工具收到加密随机数R1(Key1)后解密对比，通过才发送本指令  终端收到加密随机数R2Key2)后解密与R2对比，通过才执行下面操作 |

**应答报文：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 应答码 | B | 4 | 0x00 成功;  0x01 下发校验值,校验错误;  0x02 加密结果,写入存储操作失败;  0x03 加密结果,写入后校验失败; |

### 外部认证后重置Boot(命令字：0xA9)

**功能说明:**

校验后恢复成原厂Boot模式

**请求报文：**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | | 类型 | 长度 | | 描述 |
| 加密随机数R2(Key2) | B | | | 8 | 工具收到加密随机数R1(Key1)后解密对比，通过才发送本指令  终端收到加密随机数R2Key2)后解密与R2对比，通过才执行下面操作 |

**应答报文：**

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 长度 | 描述 |
| 应答码 | B | 4 | 0x00 成功;  0x01 下发校验值,校验错误; |

# 附录

## 通用错误定义