FC-533M读卡模块

## 产品功能

本产品为迷你读卡模块，支持卡片种类：IC卡，NFC卡，NFC手机，身份证。

支持输出：WG26、34、66

支持TTL 通讯

支持识别IC卡扇区，验证IC卡扇区密码和特定内容

支持自定义卡号。

## 波特率

19200

## 通讯命令格式

**通讯命令格式软硬件通用格式。**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **标志码** | **读卡器信息** | **软件命令标识** | **控制码** | | **数据码** | | **检验码** | **标志码** |
| **7E** | **机器号** | **信息代码** | **分类** | **命令** | **数据长度** | **数据** | **检验值** | **7E** |
|  | **1Byte** | **2byte** | **1Byte** | **1Byte** | **1Byte** | **可变长度** | **1Byte** |  |

巡更棒信息：

接收此通讯命令的设备信息，指设备机器号,机器号为0表示广播。

软件命令标识信息：

发出此命令的软件命令代码，用于区分此命令是哪个模块发出的，巡更棒不需要处理此数据，只有在返回命令时带上此数据即可。

控制码：

通讯命令的具体含义代码，包含分类，命令二类。

数据码：

当通讯命令包含数据时使用，数据长度指定了此命令中包含数据内容的字节数。

**数据长度的最大值为：120字节。**

检验码：

除标志码和检验码，命令中所有字节都相加然后取尾字节。

## 转译码

由于命令中使用了0x7E作为命令的开始和结束标志，所以7E这个字节就不能出现在命令内容中只能出现在命令头和命令尾。

因此命令中的0x7E和0x7F都必须转换为如下数据后再发送：

0x7E = 0x7F 01

0x7F = 0x7F 02

转译码使用流程是：

1、发送命令：在命令数据生成后，先对命令内容检验和计算，然后再进行0x7E和0x7F的数据检查，发现0x7E或0x7F就进行上面的公式转换，转换后在发送。

2、接受命令：收到数据后应该先按照上面的公式进行数据反转译再进行校验和检验，然后在分析命令和执行具体操作。

## 预定义命令

**预定义返回命令：**

**应答OK包的定义：**

|  |  |  |  |
| --- | --- | --- | --- |
| **控制码** | | **数据码** | |
| **分类** | **命令** | **数据长度** | **数据** |
| **21h** | **01h** | **00h** | **无** |

**后文所有涉及回应，OK应答时，直接使用此定义。**

**应答 校验错 的定义：**

|  |  |  |  |
| --- | --- | --- | --- |
| **控制码** | | **数据码** | |
| **分类** | **命令** | **数据长度** | **数据** |
| **21h** | **03h** | **00h** | **无** |

# 第一类：设备参数

**前言：**

本类中的分类开头一律为0x01；

本类中应答的开头一律为0x31；

一般来讲应答命令中命令，需要和发出的命令一样。

## 一、写入机器号

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0xF1 | 0x01 | 1字节机器号 |

机器号取值：1-255，不可以是0。0是广播码。

**解释：**写入机器号命令不判断命令格式中的巡更棒信息中的机器号。初始化设备不需要清除

应答：OK

## 二、读取机器号

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x01 | 0x00 | 无 |

**解释：**读取机器号命令不判断命令格式中的巡更棒信息中的机器号。

**应答：传送机器号**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x01 | 0x01 | 1字节机器号 |

## 三、获取设备版本号

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x03 | 0x00 | 无 |

获得设备的应用程序版本号。

**应答：传送设备版本号**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x03 | 0x04 | 4字节版本号 |

版本号字节

|  |  |
| --- | --- |
| 版本号 | 修正号 |
| 二字节 | 二字节 |

例如：0x39393232。 Ver 99.22 初始化设备不需要清除

## 四、生产日期

**设置生成日期**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x04 | 0x03 | 年月日（BCD） |

**应答：OK**

**读取生成日期**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x84 | 0x00 | 0 |

**应答：生产日期**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x84 | 0x03 | 年月日（BCD） |

## 五、读卡类型

**设置读卡类型**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x05 | 0x02 | 开关 |

|  |  |
| --- | --- |
| Bit位 | 含义 |
| Bit0 | MF1 IC卡 |
| Bit1 | NFC标签卡 |
| Bit2 | NFC手机 |
| Bit3 | 身份证 |
| Bit4 | CPU IC卡 |
| Bit5 | CPU卡 |
| Bit6 | ID卡 |

读卡类型可一次性支持所有类型卡，也可以选择仅支持其中一种或多种。

**应答：OK**

**读取读卡类型**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x85 | 0x00 | 0 |

**应答：开关**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x85 | 0x02 | 开关 |

## 六、输出格式

**设置输出格式**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x06 | 0x02 | 格式代码 |

**第一字节为输出的数据协议格式**

**第二字节为输出的卡号字节顺序**

**输出协议格式。** WG26、34、66

|  |  |
| --- | --- |
| 值 | 含义 |
| 0 | 禁止输出 |
| 1 | WG26（三字节）+WG34（4字节需短路key1按键） |
| 2 | WG26（三字节）+WG66（八字节需短路key1按键） |

**卡号字节顺序。**

|  |  |
| --- | --- |
| 值 | 含义 |
| 1 | 高位在前，低位在后 |
| 2 | 低位在前，高位在后 |

**应答：OK**

**读取输出格式**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x86 | 0x00 | 0 |

**应答：输出格式**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x86 | 0x01 | 格式代码 |

## 七、IC卡控卡

**设置扇区验证**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x07 | 0x1D | IC卡验证内容 |

**扇区验证参数格式 29字节（0x1D）：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 长度 | 含义 | 值范围 |
| 1 | 1字节 | 开关 | 1 or 0 |
| 2 | 1字节 | 扇区号 | 1-15 |
| 3 | 6字节 | 扇区密码 |  |
| 4 | 1字节 | 密码验证方式 | 1-A密钥  2-B密钥 |
| 5 | 1字节 | 密码计算方式 | 1--直接验证  2--使用动态加密（RC4加密） |
| 6 | 1字节 | 验证扇区内容开关 | 1 or 0 |
| 7 | 1字节 | 扇区内容长度 | 0-16 |
| 8 | 1字节 | 验证数据起始位 | 扇区内的需要验证的数据块起始位  块0 0-15  块1 16-31  块2 32-47 |
| 9 | 16字节 | 验证内容 |  |

**应答：OK**

**读取扇区验证**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x87 | 0x00 | 0 |

**应答：验证参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x87 | 0x1D | IC卡验证内容 |

## 八、IC卡自定义卡号

**设置卡号参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x08 | 0x0C | 卡号参数 |

**IC卡自定义卡号参数格式 12字节（0xC）：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 长度 | 含义 | 值范围 |
| 1 | 1字节 | 开关 | 1 or 0 |
| 2 | 1字节 | 扇区号 | 1-15 |
| 3 | 6字节 | 扇区密码 |  |
| 4 | 1字节 | 密码验证方式 | 1-A密钥  2-B密钥 |
| 5 | 1字节 | 密码计算方式 | 1--直接验证  2--使用动态加密（RC4加密） |
| 6 | 1字节 | 卡号长度 | 2-8 |
| 7 | 1字节 | 卡号数据起始位 | 扇区内的需要验证的数据块起始位  块0 0-15  块1 16-31  块2 32-47 |

**应答：OK**

**读取卡号参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x88 | 0x00 | 0 |

**应答：卡号参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x88 | 0x0C | 卡号参数 |

## 九、读卡时TTL输出卡号

**设置TTL输出参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x09 | 0x05 | 开关 |

1字节开关

1字节波特率；

1字节奇偶校验；

1字节数据位数；

1字节停止位数

波特率取值范围：

|  |  |
| --- | --- |
| 值 | 波特率 |
| 0 | 1200 |
| 1 | 2400 |
| 2 | 4800 |
| 3 | 9600 |
| 4 | 11400 |
| 5 | 19200 |
| 6 | 38400 |
| 7 | 43000 |
| 8 | 56000 |
| 9 | 57600 |
| 10 | 115200 |

奇偶校验取值：

|  |  |  |
| --- | --- | --- |
| 值 | **设置值** | **描述** |
| 0 | N | 无 |
| 1 | E | 偶数 (Even) |
| 2 | O | 奇数 (Odd) |

数据位值直接使用字节数值表示。取值：4-8；

停止位值

|  |  |
| --- | --- |
| 值 | **设置值** |
| 0 | 1 |
| 1 | 1.5 |
| 2 | 2 |

**应答：OK**

**读取TTL输出参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x89 | 0x00 | 0 |

**应答：TTL输出参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x89 | 0x05 | 开关 |

## 十、初始化

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0xFF | 0x00 | 0 |

**应答：OK**

## 十一、控制蜂鸣器

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x0A | 0x01 | 蜂鸣器鸣叫次数 |

**取值范围：1-10**

**应答：OK**

## 十二、控制LED灯

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x0B | 0x01 |  |

**值范围说明：**

**1表示红灯亮**

**2表示绿灯亮**

**应答：OK**

## 十三、经销商代码

经销商代码是制作脱机门禁开门卡时需要使用的，经销商代码和卡号组合后使用国密算法芯片的工作密钥加密后的数据为扇区密码。

### 设置

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x0C | 0x04 | 脱机门禁开门卡用的经销商代码 |

**应答：OK**

### 读取

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x0D | 0x00 | 0 |

**应答：经销商代码**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x0D | 0x04 | 经销商代码 |

## 十四、卡片自动加解密

可以设定将发卡器设定到卡片自动加解密的工作模式下。注意卡片加解密仅适用于兼容MF1 S50的CPU卡，不可对其他种类卡片加解密，检测到其他不符合要求卡片，直接需要蜂鸣器响五声。

### 设置

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x0E | 0x04 | **自动加密参数** |

**应答：OK**

**自动加密参数：**

|  |  |  |  |
| --- | --- | --- | --- |
| 1字节 | 1字节 | 1字节 | 1字节 |
| 功能开关   1. -关闭 2. -开启 | 起始扇区  0-15 | 扇区数量  0-15 | 工作模式   1. -加密 2. -解密 |

### 读取

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x0F | 0x00 | 0 |

**应答：经销商代码**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x0F | 0x04 | **自动加密参数** |

## 十五、IC卡个人姓名、部门存储定义

**设置扇区数据**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x10 | 0x0A | IC卡验证内容 |

**扇区参数 10字节（0x0A）：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 长度 | 含义 | 值范围 |
| 1 | 1字节 | 开关 | 1 or 0 |
| 2 | 1字节 | 扇区号 | 1-15 |
| 3 | 6字节 | 扇区密码 |  |
| 4 | 1字节 | 密码验证方式 | 1-A密钥  2-B密钥 |
| 5 | 1字节 | 密码计算方式 | 1--直接验证 |

**应答：OK**

**扇区中的数据格式定义**

**块0：人员姓名 16B**

**块1：人员编号 10B**

**块2：部门名称 16B**

**编码GB2312**

**读取扇区参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x01 | 0x90 | 0x00 | 0 |

**应答：验证参数**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x31 | 0x90 | 0x0A | 扇区参数 |

# 第二类：IC卡操作

## 一、寻卡

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x02 | 0x00 | 0x00 |  |

**应答：寻卡结果**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x32 | 0x00 | 0x0D | 1字节机器号 |

返回的数据结构：

|  |  |  |  |
| --- | --- | --- | --- |
| 1字节 | 1字节 | 1字节 | 8字节 |
| 寻卡成功或失败 | 卡片类型 | 卡号长度 | 卡号 |
| 0 or 1 |  |  |  |

卡片类型：

|  |  |
| --- | --- |
| 代码 | 含义 |
| 1 | MF1 IC卡 S50 |
| 2 | NFC标签卡 |
| 3 | NFC手机 |
| 4 | 身份证 |
| 5 | CPU IC卡 S50 |
| 6 | CPU卡 |
| 7 | MF1 IC卡 S70 |
| 8 | CPU IC卡 S70 |
| 9 | ID卡 |

## 二、读扇区内容

扇区：

S50卡的取值范围是0-15

S70卡的取值范围是 0-39

块号：

S50卡每个扇区的块号都是0-3，其中块3是密码块

S70卡0-31块扇区的块号是0-3，其中块3是密码块

32-39块扇区的块号是0-15，其中块15是密码块

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x02 | 0x01 | 0x0A | 参数 |

**参数定义**

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 扇区号 |
| 1字节 | 起始数据块 |
| 1字节 | 读取字节数 |
| 1字节 | 密钥验证类型  1--A密钥  2--B密钥 |
| 6字节 | 扇区密码 |

**目前一次读取数据4块数据块内容，即最大每次读取64个字节数据**

**应答：读取结果**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x32 | 0x01 | 0x04+N |  |

结果定义：

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 1--成功  2--密码不正确  3--卡片已离开感应区 |
| 1字节 | 扇区号 |
| 1字节 | 起始数据块 |
| 1字节 | 数据字节数 |
| N字节 | 数据内容 |

## 三、写扇区内容

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x02 | 0x02 | 0x0A+N | 参数 |

**参数定义**

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 扇区号 |
| 1字节 | 起始数据块 |
| 1字节 | 写入块数  一次最大写入4块  取值范围1-4 |
| 1字节 | 密钥验证类型  1--A密钥  2--B密钥 |
| 6字节 | 扇区密码 |
| N字节 | 待写入数据内容 |

**目前一次写入数据4块数据块内容，即最大每次写入64个字节数据**

**注意：每次写入的数据内容必须为16字节的倍数**

**应答：写入结果**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x32 | 0x02 | 0x04 |  |

结果定义：

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 1--成功  2--密码不正确  3--卡片已离开感应区  4--块数据长度不正确 |
| 1字节 | 扇区号 |
| 1字节 | 起始数据块 |
| 1字节 | 写入块数 |

# 第三类：脱机门禁IC卡操作

读写卡的时候注意，只使用动态密码验证，验证不通过就返回密码错误，不使用默认初始密码尝试即0xFFFFFFFFFFFF 这个密码。

意味着卡片在进行读写扇区操作前必须先修改扇区密码。

## 一、读扇区内容

扇区：

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x03 | 0x01 | 0x01 | 扇区号 |

**参数定义**

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 扇区号 |

**要求读取连续的2个扇区，每个扇区读取前3块，返回96个字节。**

**扇区密码使用动态密码，动态密码算法参照《附录3》文件。**

**扇区内容加载后要求对扇区内容进行解密后才返回，扇区内容解密算法参考《附录4》。**

**应答：读取结果**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x33 | 0x01 | 0x01+N |  |

结果定义：

|  |  |  |
| --- | --- | --- |
| 字节序 | 说明 |  |
| 1字节 | 操作状态 | 1--成功  2--扇区密码不正确  3--卡片已离开感应区  4--解密失败  5--卡类型不兼容  6--未检测到卡片  7--国密算法芯片未初始化 |
| 4字节 | 卡号 | 操作状态：1-5时需要携带 |
| 96字节 | 扇区内容 | 操作状态为：1 时需要携带 |

注意：当操作失败时返回的数据长度为1个字节。操作成功时返回1+96字节

注意：读卡时识别卡片型号，仅支持CPU IC卡。需要验证卡片是否为CPU卡。

## 二、写扇区内容

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x03 | 0x02 | 0x01+0x04+0x60 | 参数 |

**参数定义**

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 扇区号 |
| 4字节 | 卡号 |
| 96字节 | 扇区数据块 |

**软件发来的96字节中，其中前48字节为扇区1的数据，需要进行加密后写入扇区1，加密规则参考《附录4》。**

**前48字节的明文计算CRC16，存储在 data[48-49]这个数据区域。**

**后48字节中其中bdata[48-51] 这4个字节是CRC存储区域，前两字节是扇区1明文crc16，后2字节是扇区2后40字节明文的CRC16值。这些值需要硬件更改**

**bdata[52-55]这4字节为明文无需加密。**

**后40字节需要进行加密，加密规则参考《附录4》。**

注意：读卡时识别卡片型号，仅支持CPU IC卡。需要验证卡片是否为CPU卡。

**写卡时需要验证卡片UID是否为指定的UID，否则不能写卡**

**应答：写入结果**

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x33 | 0x02 | 0x01 |  |

结果定义：

|  |  |
| --- | --- |
| 字节序 | 说明 |
| 1字节 | 1--成功  2--扇区密码不正确  3--卡片已离开感应区  4--数据长度不正确  5--卡类型不兼容  6--卡号不匹配  7--未检测到卡片  8--国密算法芯片未初始化 |

# 第四类：读卡消息

此类别的消息为控制板主动发送的，信息代码为固定的：0xFFFF。上位机无需做任何回应。

## 读卡消息

|  |  |  |  |
| --- | --- | --- | --- |
| 控制码 | | 数据码 | |
| 分类 | 命令 | 数据长度 | 数据 |
| 0x19 | 0x01 | 1+1+N | 消息内容 |

消息内容格式：

|  |  |  |
| --- | --- | --- |
| 序号 | 长度 | 含义 |
| 1 | 1字节 | 卡类 |
| 2 | 1字节 | 卡号长度 |
| 3 | 2-8字节 | 卡号 |

卡类代码：

|  |  |
| --- | --- |
| 代码 | 含义 |
| 1 | MF1 IC卡 S50 |
| 2 | NFC标签卡 |
| 3 | NFC手机 |
| 4 | 身份证 |
| 5 | CPU IC卡 S50 |
| 6 | CPU卡 |
| 7 | MF1 IC卡 S70 |
| 8 | CPU IC卡 S70 |
| 9 | ID卡 |
| 10 | 二维码 |

# 第四类 默认值

机器号：无默认值，初始化不能修改

版本号：固件版本号，初始化保持最新的

生成日期：无默认值，初始化不可修改

读卡类型： 默认支持 M1 IC卡，NFC卡，CPU卡，身份证卡

输出格式：默认输出：WG34（四字节）,字节序：高位在前低位在后

IC卡控卡：无默认值，初始化不可修改。

IC卡自定义卡号：无默认值，初始化不可修改

读卡TTL输出卡号：默认值：开启，输出波特率：19200,n,8,1

# 附录1 IC卡动态密码算法

动态密码的算法思路是：

1. 首先根据扇区密码（6字节）和卡号（4字节）混淆生成一个newkey（10字节）
2. 然后再把newkey进行混淆生成一个6字节的newdata。
3. 使用rc4加密，密钥就是newkey，明文就是newdata，真正的扇区密码就是加密后的密文。
4. RC4加密运算时采用的卡号是物理卡号，并且是固定的4字节 “低位在前，高位在后”格式下输出的卡号作为加密基准。

源代码如下：

/\*将卡号和密钥混淆后使用RC4加密

返回值：

1 -- 表示加密完成

-1 -- 表示key 长度不足6字节

-2 -- 表示 cardcode 长度不足4字节

-3 -- 表示 result\_len 长度不足6字节

\*/

RC4\_API long WINAPI Create\_Section\_Password(BYTE \*key, long key\_len, BYTE \*cardcode, long cardcode\_len, BYTE \*SectionPWD, long SectionPWD\_len)

{

if (key\_len < 6)

{

return -1;

}

if (cardcode\_len < 4)

{

return -2;

}

if (SectionPWD\_len < 6)

{

return -3;

}

BYTE newKey[10];

BYTE newData[6];

newKey[6] = key[0];

newKey[4] = key[1];

newKey[8] = key[2];

newKey[5] = key[3];

newKey[2] = key[4];

newKey[0] = key[5];

newKey[1] = cardcode[0];

newKey[7] = cardcode[1];

newKey[3] = cardcode[2];

newKey[9] = cardcode[3];

newData[0] = newKey[1];

newData[1] = newKey[9];

newData[2] = newKey[5];

newData[3] = newKey[6];

newData[4] = newKey[7];

newData[5] = newKey[3];

RC4\_Encrypt(newKey, 10, newData, 6, SectionPWD, 6);

return 1;

}

# 附录2 IC设置卡

系统支持一个设置卡功能，卡片起始扇区为1扇区，密钥为：FC0261006535

数据表：

|  |  |  |
| --- | --- | --- |
| 序号 | 字节 | 描述 |
| 1 | 2 | 读卡类型 |
| 2 | 2 | 输出格式 |
| 3 | 0x1D | IC卡控卡参数 |
| 4 | 0xC | IC卡自定义卡号 |
| 5 | 0x3 | TTL输出参数  1字节开关  1字节波特率；  1字节奇偶校验； |

总共48个字节

使用的扇区为扇区 1。密钥为：FC0261006535

第2扇区

|  |  |  |
| --- | --- | --- |
| 序号 | 字节 | 描述 |
| 1 | 10 | 个人信息扇区参数 |

总共10个字节

使用的扇区为扇区 2。密钥为：FC0261006535

# 附录3 脱机开门卡扇区和扇区密码计算规则

1. IC卡开门卡使用2个扇区，第一个扇区存储开门权限相关信息，第二个扇区存储待导入的挂失卡、黑名单卡。（详情请参考《附录5 IC开门卡结构》）
2. IC卡开门卡使用的2个扇区是连贯的，第一个扇区后紧接着就是第二个扇区
3. 将卡号（4字节）+ 经销商代码（4字节）作为明码传递给国密算法芯片
4. 使用国密算法芯片中存储的【工作密钥】进行加密（SM7算法）
5. 获取国密算法芯片中返回的密文前6字节作为卡片的扇区密码

# 附录4 脱机开门卡扇区数据加解密规则

1. C卡第一扇区数据为全加密数据
2. IC卡第二扇区数据的前8字节为明文，后40字节为加密数据
3. 加解密的密钥计算规则：
   1. 取卡号UID的4个字节（例如：0x01020304），存放到数组 keyA
   2. 取扇区密码（上一个过程中计算出的密码8字节，不是截取后的6字节） ，存放到数组KeyB
   3. 取经销商代码4字节，存放到数组KeyC
   4. KeyA(4字节) + Keyb(8字节) + KeyC(4字节) = KeyD(16字节)
   5. KeyD 使用国密算法中的[工作密钥] 加密后的密文即是加解密中的密钥
4. 加解密算法采用国密算法芯片中的SM7，密钥采用上一步计算出的密文，IV采用0x8372F0B6067DBC0C
5. 达到一卡一密，防止篡改卡内数据或从其他卡中复制数据。

# 附录5 脱机开门卡结构

## 扇区1 开门权限

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 内容 | 数据长度 |  |
| 1 | 开门密码 | 4字节 | 0-3 |
| 2 | 进出标识；0----进，1----出，其它---进出 | 1字节 | 4 |
| 3 | 截止日期；BCD码，年月日 | 3字节 | 5,6,7 |
| 4 | 开门时段；1-64 | 1字节 | 8 |
| 5 | 有效开门次数；0-65535；0--无效；65535--无限制 | 2字节 | 9,10 |
| 6 | 各权限卡类型  Bit0、bit1 表示权限1  Bit2、bit3 表示权限2  Bit4、bit5 表示权限3 | 1字节 | 11 |
| 7 | 权限1（3字节区域地址+9字节门地址表） | 12字节 |  |
| 8 | 权限2（3字节区域地址+9字节门地址表） | 12字节 |  |
| 9 | 权限3（3字节区域地址+9字节门地址表） | 12字节 |  |

权限格式：

|  |  |  |
| --- | --- | --- |
| 1 | 1级标识码，卡类型为2、3、4级权限时有效 | 1字节 |
| 2 | 2级标识码，卡类型为3、4级权限时有效 | 1字节 |
| 3 | 3级标识码，卡类型为4级权限时有效 | 1字节 |
| 4 | **地址数据表**  **此表中的数据根据不同权限级别对应的标识码是不同的。**  每个bit表示一个地址，一共可以表示72个地址。  地址位顺序从高至低依次表示1-72个地址。  第一个字节最高位表示地址1.最后一个字节最低位表示地址72。 | 9字节 |

byte[] tmp = {181, 26, 126, 8, 63, 75, 86, 13, 200};

地址 二进制

01 -- 08 : 10110101

09 -- 16 : 00011010

17 -- 24 : 01111110

25 -- 32 : 00001000

33 -- 40 : 00111111

41 -- 48 : 01001011

49 -- 56 : 01010110

57 -- 64 : 00001101

65 -- 72 : 11001000

卡类型2bit。值含义：0--4级权限 1--3级权限，2--2级权限，3--1级权限

**4级权限**:

表示需要验证4个字段：1级标识码，2级标识码，3级标识码，地址数据(4级标识码)

刷卡开门时，控制器需要验证1、2、3级标识码是否和机器匹配，匹配后再验证地址数据中对应4级标识码的bit位是否为1。

**3级权限**：

需要验证3个字段：1级标识码，2级标识码，地址数据(3级标识码）

刷卡开门时，控制器需要验证1、2级标识码是否和机器匹配，匹配后再验证地址数据中对应3级标识码的bit位是否为1。（3级权限时地址表里使用的是3级标识码。） 此类型权限不验证4级标识码

**2级权限**：

需要验证2个字段：1级标识码，地址数据(2级标识码）

刷卡开门时，控制器需要验证1级标识码是否和机器匹配，匹配后再验证地址数据中对应2级标识码的bit位是否为1。（2级权限时地址表里使用的是2级标识码。） 此类型权限不验证3、4级标识码

**1级权限**：

需要验证1个字段：地址数据(1级标识码)

刷卡开门时，控制器只验证地址数据中对应1级标识码的bit位是否为1。（1级权限时地址表里使用的是1级标识码。） 此类型权限不验证2、3、4级标识码

## 扇区2 附加数据区

**格式定义：**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 内容 | 数据长度 |  |
| 1 | 权限扇区明文CRC16值 | 2字节 |  |
| 2 | 附加扇区后40字节明文CRC16值 | 2字节 |  |
| 3 | 扇区中卡片字节长度，取值（4或8） | 1字节 |  |
| 4 | 扇区中存储的卡片数量（0-8） | 1字节 |  |
| 5 | 起始日期，压缩格式，年月日，年到2127年  日5b、月4b、年7b | 2字节 |  |
| 6 | 待导入到门禁机中卡片数据  当卡片字节数为4时，每个卡占用5字节，最多能存储8张卡片数据，格式如下：  卡号4字节 + 1字节操作类型  当卡片字节数为8时，每个卡占用9字节，最多能存储4张卡片数据，格式如下：  卡号8字节 + 1字节操作类型  **操作类型：**1--挂失卡；2--黑名单卡；3--删除卡；其他--表示无效。  注意：此区域数据是加密数据，需要解密后使用 | 40字节 |  |