**FM17550读卡模块**

**操作说明书**

重庆智之屋科技发展

有限公司

变更记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本号** | **修改点说明** | **变更日期** | **变更人** | **审批人** |
| V0 | 创建 | 2018-01-25 | 刘健 |  |
|  | 增加设置串口波特率功能 | 2018-01-29 | 刘健 |  |
|  | keyA密码验证失败、读/写失败返回相应的状态字节 | 2018-05-18 | 刘健 |  |
|  | 0x30—重启设备，进入bootloader模式  0x31-- bootloader模式下，接收到升级数据  0x32-- bootloader模式下，接收到升级数据长度、校验和等信息 | 2018-07-20 | 刘健 |  |
|  | 修改6.1描述。转载秘钥时，由一次只装载一个秘钥（keyA或keyB）修改为keyA、keyB同时装载 | 2018-11-12 | 刘健 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**修改点说明的内容有如下几种：创建、修改（+修改说明）、删除（+删除说明）**

目录

[1 概述 4](#_Toc520450441)

[1.1 目的 4](#_Toc520450442)

[1.2 适用范围 4](#_Toc520450443)

[2 缩写和术语 4](#_Toc520450444)

[3系统功能 4](#_Toc520450445)

[4系统框图 5](#_Toc520450446)

[5传输协议格式 5](#_Toc520450447)

[5.1 数据传输协议 5](#_Toc520450448)

[5.1.1 串口协议 5](#_Toc520450449)

[5.1.2 控制字符定义 5](#_Toc520450450)

[5.2 协议描述 6](#_Toc520450451)

[5.2.1 协议通信帧描述 6](#_Toc520450452)

[5.2.2 上位机发送命令至模块 通信必须先由上位机发送命令和数据给模块， 模块执行命令完毕后，再将执行命令后的状态和响应数据发回给上位机。上位机发送格式如表 5 所示。 7](#_Toc520450453)

[5.2.3 从机返回数据至上位机 7](#_Toc520450454)

[5.2.4 上位机命令值列表 8](#_Toc520450455)

[5.2.5 模块返回状态值列表 8](#_Toc520450456)

[6功能验证 9](#_Toc520450457)

[6.1 装载密钥 9](#_Toc520450458)

[6.2 激活卡片并获取卡号 10](#_Toc520450459)

[6.3 写块区数据 12](#_Toc520450460)

[6.4 读块区数据 13](#_Toc520450461)

[6.5 自动寻卡 14](#_Toc520450462)

[6.6 设置串口波特率 16](#_Toc520450463)

[6.7 在线升级（iap） 16](#_Toc520450464)

[6.7.1 重启读卡器，进入bootloader 16](#_Toc520450465)

[6.7.2 bootloader模式下，发送升级数据 17](#_Toc520450466)

[6.7.2 bootloader模式下，发送累加校验和等信息 17](#_Toc520450467)

[7参考文件 18](#_Toc520450468)

[8附录 18](#_Toc520450469)

# 1 概述

## 1.1 目的

文档编写目的是为了阐述FM17550读卡模块系统的操作。

## 1.2 适用范围

本说明书的预期读者为系统设计人员、系统测试人员。

# 2 缩写和术语

|  |  |
| --- | --- |
| **名称** | **中文解释** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 3系统功能

◇支持以下A、B卡功能模式

A卡：密钥重置、获取卡号、读/写块区数据、自动寻卡；

B卡：自动寻卡

各功能模式可通过上位机下发指令进行切换。

◇与上位机串口通讯反馈时间少于500ms。

◇接上位机接口支持： UART、USB

◇串口通信波特率9600bit/s

# 4系统框图



注：连接PC机时使用模块MICRO USB接口，MICRO USB接口供电；连接STM32时使用STM8串口，需单独供电。

# 5传输协议格式

## 5.1 数据传输协议

### 5.1.1 串口协议

串行接口通信过程中一帧的数据格式采用 1 个起始位，8 个数据位、无奇偶  
校验位、1 个停止位。

### 5.1.2 控制字符定义

下表列出了FM17550读卡模块与上位机串行通信过程中用到的控制字符定义。

|  |  |  |
| --- | --- | --- |
| **描述** | **定义** | **值** |
| 开始符 | STX | 0x20 |
| 终止符 | ETX | 0x03 |
| 无应答 | NAK | 0x15 |

表1 控制字符定义

## 5.2 协议描述

### 5.2.1 协议通信帧描述

数据通信以一帧为单位进行，格式如下：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **起始符 STX** | **命令/状态 CMD/Status** | **数据长度 Length** | **数据 DATA** | **校验和 BCC** | **帧结束符 ETX** |
| 1byte | 1byte | 1byte | N bytes | 1byte | 1byte |

表 2 数据通信帧结构

数据帧中各字段说明如表 3 所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **字段** | **长度** | **说明** | **补充** |
| STX | 1 | STX=0x20，数据帧的起始符，每一帧数据都是以 STX 开始 |  |
| SEQNR | 1 | 该数据帧包序号，从 0 到 255 循环。可以用来作为通信间的错误检查，从机（模块）接收到上位机发来的信息，在应答信息中发出一个同样的 SEQ信息，上位机可以通过此信息检查是否发生的“包丢失”的错误。第一个包的 SEQ 可为任意值。 | 该 字 段 上位机 发 送 和接 收 的 应该相同（在线升级固定写为0xFF） |
| Cmd/status | 1 | 上位机——从机：命令 Command 从机——上位机：状态 Status |  |
| length | 1 | 该帧所带数据信息长度若模块返回状态不为 0（OK），则 Length=0。 |  |
| DATA | Length | 数据信息,长度等于 Length |  |
| BCC | 1 | 校验和。从包号（SEQNR）开始到数据（DATA）的最后一字节异或取反。 |  |
| ETC | 1 | ETX=0x03，是一个帧的结束标志 |  |

表 3 数据帧各字段说明

为了下文的描述，把 SEQ+CMD/Status+LEN+DATA+BCC 同称为数据块 DATA Block。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **DATA BLOCK** | **包号**  **SEQNR** | **命令/状态 CMD/Status** | **数据长度 Length** | **数据 DATA** | **校验和 BCC** |
| 1byte | 1byte | 1byte | N bytes | 1byte | 1byte |

表 4 数据块 DATA BLOCK

数据帧接收规则：  
 一帧的结束一定是 ETX，但接收到 0x03 则不一定是帧结束；  
 帧长必须不小于 6 字节，最大不能超过 62 字节，且帧长必须等于数据长度加 6；  
 BCC 计算必须正确。  
 上位机发送数据必须符合以上规则，否则从机不会执行任何命令，也不会有任何错误响应。同样上位机接收从机的数据也必须符合以上规则，如果不符合，上位机必须丢弃这帧数据。

### 5.2.2 上位机发送命令至模块 通信必须先由上位机发送命令和数据给模块， 模块执行命令完毕后，再将执行命令后的状态和响应数据发回给上位机。上位机发送格式如表 5 所示。

|  |  |  |  |
| --- | --- | --- | --- |
| **上位机** | **数据传送方向** | **模块** | **说明** |
| STX+DATA BLOCK+ETX | → |  | 一次将一帧数据全部发送完。 |

表 5 上位机发送给模块遵循的格式

用户在给FM17550读卡模块发送命令时，连续的发送 STX (0x20)+数据块+0x03(结束符)。通过判断模块返回数据的正确性来判断模块是否正确执行了本条命令。

5.2.3 从机返回数据至上位机  
 FM17550读卡模块在接收到上位机发送的数据后，根据数据块的内容执行相应命令，并将执行命令后的状态或者数据（以下将状态和数据都统称为数据）返回给上位机。模块发送格式如表 6 所示：

|  |  |  |
| --- | --- | --- |
| **模块** | **数据传送方向** | **上位机** |
| STX + DATA BLOCK+ETX | → |  |

表 6 模块发送格式

### 5.2.4 上位机命令值列表

|  |  |
| --- | --- |
| **命令值** | **功能描述** |
| 0x20 | 改变存贮在模块内密匙区中的密钥 |
| 0x21 | 发命令获取卡号并激活卡片 |
| 0x22 | 从卡中指定块中读出一个16字节的块 |
| 0x23 | 向卡中指定块写入一16字节的数据块 |
| ~~0x24~~ | ~~读取指定扇区中0-2块共48字节数据~~ |
| 0x25 | 设置进入检测卡片模式，掉电保存 |
| ~~0x26~~ | ~~设置进入自动读卡模式，掉电保存~~ |
| ~~0x27~~ | ~~将卡置于挂起模式~~ |
| ~~0x28~~ | ~~关闭模块~~ |
| ~~0x29~~ | ~~关闭天线输出数ms，使卡复位~~ |
| ~~0x2a~~ | ~~配置模块的天线驱动模式~~ |
| ~~0x2b~~ | ~~读取模块信息~~ |
| ~~0x2c~~ | ~~将控制位置为高电平~~ |
| ~~0x2d~~ | ~~将控制位置为低电平~~ |
| ~~0x2e~~ | ~~输出驱动蜂鸣器信号，能控制动作时间 间隙时间和重复次数~~ |
| 0x2f | 设置串口波特率 |
| 0x30 | 进入bootloader模式 |
| 0x31 | bootloader模式下接收到升级数据 |
| 0x32 | bootloader模式下接收到升级数据长度、校验和等信息 |

表 7 上位机命令值列表

### 5.2.5 模块返回状态值列表

|  |  |  |
| --- | --- | --- |
| **名称** | **状态值（Status）** | **描述** |
| OK, COMM\_OK | 0 | 函数调用成功 |
| COMM\_ERR | 0xff | 串行通信错误 |
| **READ\_ERR** | 0x12 | *调用 Read 函数出错* |
| **WRITE\_ERR** | 0x0f | *调用 Write 函数出错* |
| **KEY\_ERR** | 0x09 | *证实密码错* |
| **COMM\_ILLEGAL** | 0xFE | *非法指令* |
|  |  |  |

表 8 模块返回状态值列表

# 6功能验证

## 6.1 装载密钥

主机→FM17550读卡模块 （命令模式） ：  
SEQNR： 0 （可自定义）  
COMMAND： 0x20  
LENGTH： 6

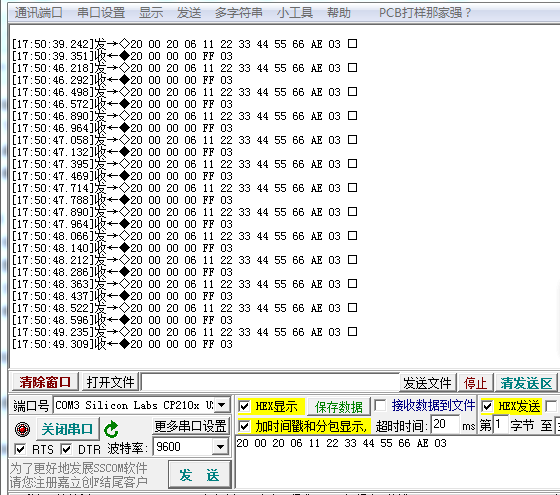
KeyA：DATA[0] ~ DATA[5]  
KeyB：DATA[6] ~ DATA[11]  
例如：往密匙区装载密匙： 0x11 0x22 0x33 0x44 0x55 0x66 的数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x20 | 0x0B | 0x11 0x22 0x33 0x44 0x55 0x66  0xxx … | 0xxx | 0x03 |

FM17550读卡模块→主机（响应模式） ：  
SEQNR： 0  
STATUS： OK，COMM\_ERR 中的某一个  
LENGTH： 0  
DATA[0]： 无  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x00 | none | 0xFF | 0x03 |

通过上位机PC端串口实测如下：



## 6.2 激活卡片并获取卡号

|  |  |  |  |
| --- | --- | --- | --- |
| **卡类型** | **类型值** | **卡类型** | **类型值** |
| Mifare1 S50 | 0x0004 | SHC1101 | 0x0004 |
| Mifare1 S70 | 0x0002 | SHC1102 | 0x3300 |
| Mifare Light | 0x0010 | 11RF32 | 0x0004 |
| Mifare UltraLight | 0x0044 |  |  |

表 9 常用卡片类型值

|  |  |  |  |
| --- | --- | --- | --- |
| **卡类型** | **最后一级选择应答的应答值** | **卡类型** | **最后一级选择应答的应答值** |
| Mifare1 S50 | 0x08 | Mifare0 UltraLight | 0x04 |
| Mifare1 S70 | 0x18 | SHC1101 | 0x22 |
| Mifare1 Light | 0x01 | 11RF32 | 0x08 |

表 10 常用卡的最后一级选择应答的应答值

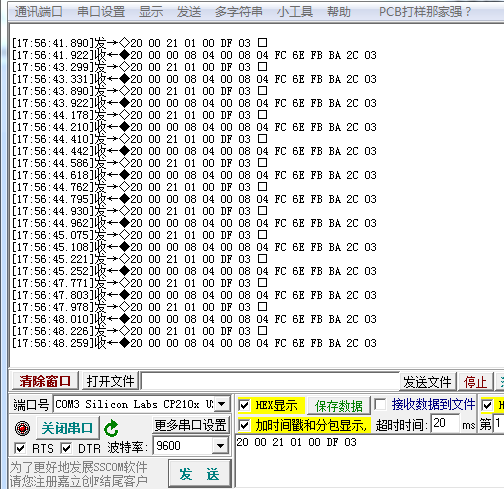
主机→FM17550读卡模块 （命令模式） ：  
SEQNR： 0 （可自定义）COMMAND： 0x21  
LENGTH： 1  
DATA[0]： 0x00--请求天线范围内 全部卡片  
例如： 激活卡的数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x21 | 0x01 | 0x00 | 0xxx | 0x03 |

FM17550读卡模块→主机（响应模式） ：  
SEQNR： 0  
STATUS： OK，COMM\_ERR 中的某一个  
LENGTH： 4 字节+序列号的长度， Mifare1 S50、 S70、 Light 卡： 8 字节，  
Mifare0 UltraLight 和 Mifare3 Desfire 卡： 11 字节  
DATA[0..1]： 请求应答， 2 个字节的卡片类型值，表9  
DATA[2]： 最后一级选择应答的应答值，表10  
DATA[3]：返回卡号的长度， 4 或 7   
DATA[4..（4+ 卡号长度 -1）]：返回卡号  
例如： 一张序列号为 0x007e0a42 的 Mifare1 S50 卡返回的数据

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x08 | 0x04 0x00 0x08 0x04 0x42 0x0A 0x7E 0x00 | 0xXX | 0x03 |

通过上位机PC端串口实测如下：



## 6.3 写块区数据

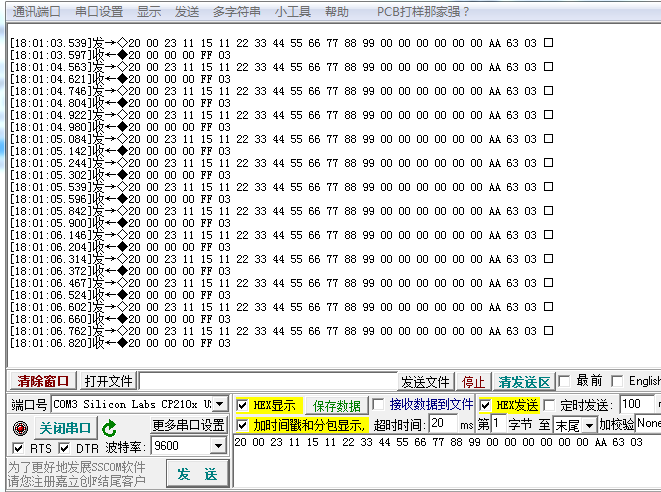
主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0 （可自定义）  
COMMAND： 0x23  
LENGTH： 17  
DATA[0]： Block  
DATA[1]： 所要写的第一个字节  
：  
DATA[16]： 所要写的最后一个字节  
例如：往块 2 写入数据的数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x23 | 0x11 | 0x02 16 字节数据 | 0xXX | 0x03 |

FM17550读卡模块→主机（响应模式） ：  
SEQNR： 0  
STATUS： OK ， COMM\_ERR ，**WRITE\_ERR，KEY\_ERR, READ\_ERR**中的某一个  
LENGTH： 0  
DATA[0]： 无  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x00 | none | 0xFF | 0x03 |

通过上位机PC端串口实测如下：



## 6.4 读块区数据

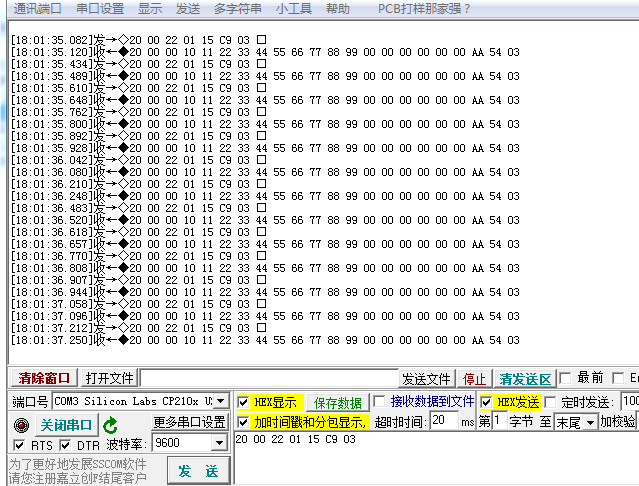
主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0 （可自定义）  
COMMAND： 0x22  
LENGTH： 1  
DATA[0]： Block  
例如：读取块 2 的数据的数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x22 | 0x01 | 0x02 | 0xxx | 0x03 |

FM17550读卡模块→主机（响应模式） ：  
SEQNR： 0  
STATUS： OK ， COMM\_ERR, **WRITE\_ERR，KEY\_ERR, READ\_ERR** 中的某一个  
LENGTH： 16  
DATA[0]： 所访问块的第一个字节  
：  
DATA[15]： 所访问块的最后一个字节  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x10 | 16 字节数据 | 0xXX | 0x03 |

通过上位机PC端串口实测如下：



## 6.5 自动寻卡

主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0 （可自定义）  
COMMAND： 0x25  
LENGTH： 1  
DATA[0]：  
例如：检测卡片是否靠近的数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x25 | 0x01 | 0x00 | 0xxx | 0x03 |

FM17550读卡模块→主机（对命令的应答） ：  
SEQNR： 0  
STATUS： OK， COMM\_ERR 中的某一个  
LENGTH： 0  
DATA[0]： 无  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x00 | none | 0xFF | 0x03 |

在主动检测卡片模式下，如果有卡靠近模块，模块回主动读取卡号并回发。回发格式如  
下：  
FM17550读卡模块→主机（有卡靠近后的应答） ：  
SEQNR： 0  
STATUS： OK，COMM\_ERR 中的某一个  
LENGTH： 4 字节+序列号的长度， Mifare1 S50、 S70、 Light 卡： 8 字节，  
Mifare0 UltraLight 和 Mifare3 Desfire 卡： 11 字节  
DATA[0..1]： 请求应答， 2 个字节的卡片类型， 其意义见表 9。  
DATA[2]： 最后一级选择应答的应答,其意义见表 10DATA[3]：返回卡号的长度， 4 或 7  
DATA[4..（4+ 卡号长度-1）]：返回卡号， 4 字节或 7 字节  
例如： 一张序列号为 0x007e0a42 的 Mifare1 S50 卡靠近返回的数据

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x08 | 0x04 0x00 0x08 0x04 0x42 0x0A 0x7E 0x00 | 0xXX | 0x03 |

通过上位机PC端串口实测如下：



## 6.6 设置串口波特率

主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0 （可自定义）  
COMMAND： 0x2f  
LENGTH： 0x04  
DATA[0~3]：串口波特率数据，高字节在前低字节在后  
例如：命令数据帧（以115200bit/为例）

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x2f | 0x04 | 0x00 0x01 0xc2 0x00 | 0x17 | 0x03 |

FM17550读卡模块→主机（对命令的应答:新的波特率下应答） ：  
SEQNR： 0  
STATUS： OK， COMM\_ERR 中的某一个  
LENGTH： 0  
DATA[0]： 无  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x00 | 0x00 | 0x00 | none | 0xFF | 0x03 |

## 6.7 在线升级（iap）

### 6.7.1 重启读卡器，进入bootloader

主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0x0 （可自定义）  
COMMAND： 0x30  
LENGTH： 0x01  
DATA[0]： 0x0  
例如：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0x0 | 0x30 | 0x01 | 0x00 | 0xCE | 0x03 |

FM17550读卡模块→主机（无应答）

### 6.7.2 bootloader模式下，发送升级数据

主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0xff （可自定义）  
COMMAND： 0x31  
LENGTH： 0x40  
DATA[0~63]：   
例如：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0xff | 0x31 | 0x40 | 0x00 … | 0xxx | 0x03 |

FM17550读卡模块→主机 ：  
SEQNR： 0xff  
STATUS： OK， COMM\_ERR 中的某一个  
LENGTH： 0  
DATA[0]： 无  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0xff | 0x00/0xff | 0x00 | none | 0xxx | 0x03 |

### 6.7.2 bootloader模式下，发送累加校验和等信息

主机→FM17550读卡模块 命令模式） ：  
SEQNR： 0xff （可自定义）  
COMMAND： 0x32  
LENGTH： 0x08  
DATA[0~3]： 升级包数据总长度

DATA[4~7]： 升级包数据累加校验和  
例如：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **CMD** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0xff | 0x32 | 0x08 | 0x00 … | 0xxx | 0x03 |

FM17550读卡模块→主机 ：  
SEQNR： 0xff  
STATUS： OK， COMM\_ERR 中的某一个  
LENGTH： 0  
DATA[0]： 无  
例如：数据帧

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STX** | **SEQNR** | **Status** | **Length** | **DATA** | **BCC** | **ETX** |
| 0x20 | 0xff | 0x00/0xff | 0x00 | none | 0xxx | 0x03 |

# 7参考文件

|  |  |
| --- | --- |
| **序号** | **文件名称** |
| 1 | 基于FM17550读卡模块需求\_接口说明 |
| 2 | FM17550\_um.pdf |
| 3 | mifare卡读写模块UART接口TX522B应用指南（新版协议）\_V2.0.pdf |

# 8附录