恺乐 KLM900 系列模块指令示例（部分）

备注：模块出厂默认波特率 115200bps，数据位 8 位，停止位 1 位，无奇偶校验。波特率可通过软件进行修改。

以下协议说明通用 KLM900,KLM926,KLM930,KLM400 模块

用户在拿到 KLM900 系列模块后，如果是连接单片机 MCU，Arduino，PLC 等嵌入式集成开发应用，则需根据通讯协议文档里面的指令进行收发数据。通讯协议里面对整个模块做了全面的协议说明，而在实际使用里面，并不需要全部用到，用户只需要根据自己的使用选择即可，无需全部看。本文档我们根据用户应用最多的基本指令做示列，如需其它指令用户可参考协议文档查看。

模块连接上后，可通过发送以下固定指令来判断模块是否正常通信：

发送： BB 00 B7 00 00 B7 7E //获取模块功率

正常返回：BB 01 B7 00 02 07 D0 91 7E //模块正常返回 表示连接正常

实际使用里面用户一般用的最多的功能是：

1 模块功率设置：

功能说明：功率越大，信号越强，一般无需调整，只有需要降低读距的时候调整。

功率设置：KLM900 功率最高 20,最低 12.5，间隔 1.5，出厂默认 20

KLM926 功率最高 26,最低 18.5，间隔 1.5，出厂默认 26

指令帧：发送 BB 00 B6 00 02 07 D0 8F 7E

(表示最大设置，也是默认设置，发射功率 KLM900 为 20dbm,KLM926 为 26dbm)

BB 00 B6 00 02 07 3A F9 7E

(表示发射功率 KLM900 为 18.5dbm,KLM926 为 24.5dbm)

BB 00 B6 00 02 06 A4 62 7E

(表示发射功率 KLM900 为 17dbm,KLM926 为 23dbm)

BB 00 B6 00 02 06 0E CC 7E

(表示发射功率 KLM900 为 15.5dbm,KLM926 为 21.5dbm)

BB 00 B6 00 02 05 78 35 7E

(表示发射功率 KLM 900 为 14dbm,KLM926 为 20dbm)

BB 00 B6 00 02 04 E2 9E 7E

(表示发射功率 KLM900 为 12.5dbm,KLM926 为 18.5dbm)

正常返回：BB 01 B6 00 01 00 B8 7E //设置成功

错误返回：BB*****7E，错误返回请查看通讯协议文档错误代码 CODE

2 读卡号 EPC：

功能说明：用于单个识别或者批量识别卡号（EPC）使用，此功能有两个执行命令，一个是单次轮询：发送此命令后，模块只执行一次，执行一次后就结束，另一个是多次轮询：这个指令适合多标签识别（批量识别），此命令帧里面有一个次数的帧数据，模块执行这个命令的时候，会根据这个次数进行，到达这个次数后，执行结束。次数可最高 65535（HEX：FFFF）次，次数用户根据需要选择即可，在多次轮询执行的过程中，如果需要中断结束，则需要发送停止多次轮询指令。

单次轮询：发送 BB 00 22 00 00 22 7E

正常返回报文示列 1（24 位长度的卡号）：

BB 02 22 00 11 DC 30 00 E2 80 68 94 00 00 50 24 58 95 B5 EB D5 F9 6E 7E

帧头　　长度　　RSSI　　PC　　卡号（EPC）　　CRC　　校验　　停止位

长度：第 4-5 两个字节，0011（hex 格式），表示后面 17 个字节长度（RSSI+PC+EPC+CRC）

卡号 EPC 数据为：E2 80 68 94 00 00 50 24 58 95 B5 EB

正常返回报文示列 2（8 位长度的卡号）：

BB　02 22　00 09　CF　10 00　03 26 92 01　　2A 79　6B　7E

帧头　　长度　　RSSI　　PC　　卡号（EPC）　　CRC　　校验　　停止位

卡号 EPC 数据为：03269201

异常报文：BB 01 FF 00 01 15 16 7E　（表示没有读到卡，无卡）

返回其它报文请查看通讯协议文档错误代码 CODE

多次轮询：发送 BB 00 27 00 03 22 FF FF 4A 7E　（FF FF 表示发送次数 65535，4A 校验位）

或 BB 00 27 00 03 22 00 64 B0 7E　（00 64 表示发送次数 100 次，B0 校验位）

次数为变量，根据需要自己设置（格式 hex）

校验位为从第二个字节 00 到最后一个指令参数（倒数第三个） 累加和，并只取累加和最低一个字节(LSB)。

返回报文示列：

BB 02 22 00 11 C9 34 00 10 77 54 75 46 33 40 38 46 05 14 50 66 A9 31 7E　//有读到卡号

BB 02 22 00 11 C9 34 00 10 77 54 75 46 33 40 38 46 05 14 50 66 A9 31 7E　//有读到卡号

BB 02 22 00 11 C9 34 00 10 77 54 75 46 33 40 38 46 05 14 50 66 A9 31 7E　//有读到卡号

BB 02 22 00 09 CF 10 00 03 26 92 01 2A 79 6B 7E　//有读到卡号

BB 02 22 00 11 C2 30 00 E2 80 68 94 00 00 50 24 58 95 B5 EB D5 F9 54 7E //有读到卡号

BB 02 22 00 09 CF 10 00 03 26 92 01 2A 79 6B 7E //有读到卡号

BB 01 FF 00 01 15 16 7E //未读到卡

BB 02 22 00 09 CB 10 00 03 26 83 48 C3 D6 95 7E //有读到卡号

……

返回的报文里面以上面格式出现，如果你使用的电子标签的卡号都是一样的长度比如上面第一条，卡号为 10 77 54 75 46 33 40 38 46 05 14 50（24 位长度卡号），那么读到标签数据后收到的每一段正常的报文长度都是固定的 24byte，模块在读卡的时候不一定每一次发送的命令都会有卡号，这个是正常的，所以在里面会有未读到卡的返回帧 BB 01 FF 00 01 15 16 7E。我们可以以这个规律作为筛选条件，只要不是 24 位长度卡号的报文就直接丢弃即可（前提必须是卡号长度都是一样的）

如果你的应用不限制标签的长度，在遇到卡号长度不同的标签的时候，收到的报文帧长度就是不一样的，如上面的 BB 02 22 00 09 CF 10 00 03 26 92 01 2A 79 6B 7E，这个就是模块读到了一个标签卡号长度只有 8 位的数据，这个也是正常的，我们只要按照通讯协议里面 通知帧定义解析即可（和单次轮询返回帧解析一样）。

返回其它报文请查看通讯协议文档错误代码 CODE

停止多次轮询：发送 BB 00 28 00 00 28 7E

（需要中断多次轮询的时候发送，发送后多次轮询结束执行）

正常返回 BB 01 28 00 01 00 2A 7E

返回其它报文请查看通讯协议文档错误代码 CODE

3　Select 操作（写数据，读其它区数据）

此命令用于对电子标签的数据区进行读写操作，在多标签的情况下，可以根据 Select 参数只对特定标签进行轮询和读写等操作。电子标签一般有四个数据区区（EPC 区，USER 区,TID 区，密码区），对标签的数据区操作，需要根据自己的实际应用来，如果你只是读标签卡号，用上面的轮询指令即可无需看后面内容，如果你是要写 EPC 卡号、读写 USER 区（注：很多芯片没有 USER 区，在操作这个区的时候需先了解自己操作的芯片标签是

否有这个区)、加密 这些操作则需要了解 select。

在对指定标签进行数据区读写操作前，我们要先设置 Select 参数指定，指定后，就可以在多个标签里面只对这个标签进行操作。

比如我们对一张标签的卡号为 03 26 92 01 46 33 40 38 46 05 14 50 进行操作（提前通过单次或者多次轮询已经获取到了标签的卡号)：

Select 设定发送：

BB 00 0C 00 13 01 00 00 00 20 60 00 03 26 92 01 46 33 40 38 46 05 14 50 FC 7E

返回：BB 01 0C 00 01 00 0E 7E //设置成功

返回其它报文请查看通讯协议文档错误代码 CODE

读操作：

BB 00 39 00 09 00 00 00 00 03 00 00 00 06 4B 7E 读 USER 区

长度 密码 USER 区 开始地址 写入长度（字）校验 停止位

读到数据返回：BB 01 0C 00 01 00 0E 7E //select 设置成功

BB 01 39 00 1B 0E 34 00 03 26 92 01 46 33 40 38 46 05 14 50 00 00 00 00 00 00 00 00 00 00 00 F3 7E//读到数据

长度 PC EPC 卡号 USER 数据 校验 停止位

0E：PC+EPC 的长度，上面 14 转成 16 进制就是 0E

错误返回：（错误返回会返回两条指令帧，一个是 select set 的回复帧，第二个就是读操作的回复帧）

BB 01 0C 00 01 00 0E 7E //select 设置成功

BB 01 FF 00 01 09 0A 7E // 第三个字节 FF，第六个字节（error code）是 09：没有找到标签

// 第三个字节 FF，第六个字节（error code）是 16：访问密码不正确

// 第三个字节 FF，第六个字节（error code）是 A3：超出芯片容量范围

//第三个字节 FF， 第六个字节（error code）是其它数据，可参考文档错误代码或者就直接定义错误

BB 00 39 00 09 00 00 00 00 02 00 00 00 06 4A 7E 读 TID 区

长度 密码 TID 区 开始地址 长度（字） 校验 停止位

读到数据返回：BB 01 0C 00 01 00 0E 7E //select 设置成功

BB 01 39 00 1B 0E 34 00 03 26 92 01 46 33 40 38 46 05 14 50 E2 80 F3 37 20 00 F0 00 01 26 5F 80 95 7E//读到数据

EPC 卡号 TID 数据 校验 停止位

错误返回：参考上面读 USER 区错误返回

BB 00 39 00 09 00 00 00 00 00 00 02 00 02 46 7E 读密码区

长度 密码 密码区 开始地址 长度（字） 校验 停止位

读到数据返回：BB 01 0C 00 01 00 0E 7E //select 设置成功

BB 01 39 00 13 0E 34 00 03 26 92 01 46 33 40 38 46 05 14 50 00 00 00 00 EB 7E //读到数据

EPC 卡号 密码数据 校验 停止位

错误返回：参考上面读 USER 区错误返回

注意：长度（字）:1 个字=4 位 16 进制数据。出厂默认密码 8 个 0。EPC 区 01，密码区 00，TID 区 02，user 区 03

写操作(TID 区数据不可写)

重写 EPC 号为 1111 2222 3333 4444 5555 6666 的发送指令:

BB 00 49 00 15 00 00 00 00 01 00 02 00 06 11 11 22 22 33 33 44 44 55 55 66 66 31 7E

长度　　8 位密码　EPC 区　起始地址　长度　　写入的 EPC 数据　　校验

写入数据正确返回：BB 01 0C 00 01 00 0E 7E　　//select 设置成功

BB 01 49　00 10　0E　30 00　03 26 92 01 46 33 40 38 46 05 14 50　　00　　F4　　7E

长度　　PC　　修改前的标签卡号 EPC　　执行成功　　停止位　　校验位

错误返回：（错误返回会返回两条指令帧，一个是 select set 的回复帧，第二个就是读操作的回复帧）

BB 01 0C 00 01 00 0E 7E　//select 设置成功

BB 01 FF 00 01 10 11 7E　// 第三个字节 FF，第六个字节是 10（error code）:表示没有找到标签

// 第三个字节 FF，第六个字节是 16（error code）:表示没有访问密码不正确

// 第三个字节 FF，第六个字节是 B3（error code）:表示超出芯片容量范围

// 第三个字节 FF，第六个字节（error code）是其它数据，可参考文档错误代码或者就直接定义错误

写 USER 区数据为 1111 2222 3333 4444 5555 6666 的发送指令:

BB 00 49 00 15 00 00 00 00　03　00 00　00 06 11 11 22 22 33 33 44 44 55 55 66 66 31 7E

长度　　8 位密码　　USER 区　起始地址　长度　　写入的 user 数据　　校验

写入数据正确返回：　BB 01 0C 00 01 00 0E 7E　//select 设置成功

BB 01 49　00 10　　0E　30 00　30 08 33 B2 DD D9 01 40 00 00 00 00　　00　　AC　　7E

长度　　PC　　标签卡号 EPC　　执行成功　　停止位　　校验位

错误返回：参考上面错误返回

4　设置 射频频率 操作

发送：BB 00 07 00 01 01 09 7E ；设置国标 2 （频率 920~925MHz）；//常用

BB 00 07 00 01 02 0A 7E ；设置美标 （频率 902~928MHz）；//常用

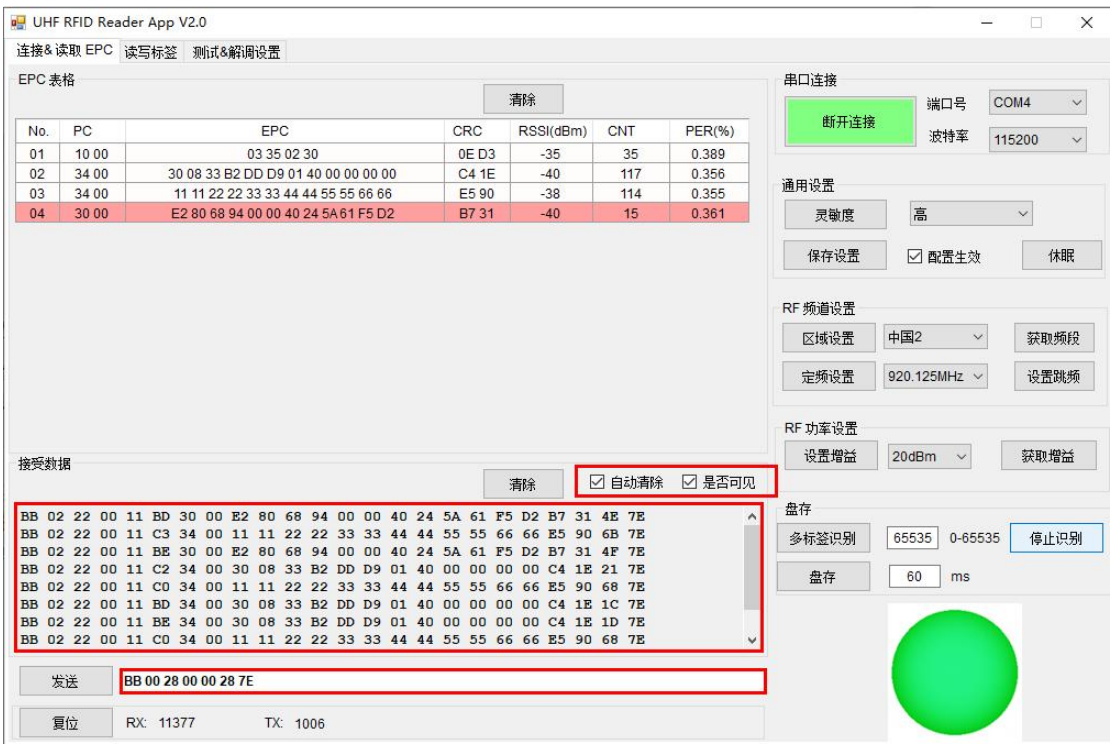
BB 00 07 00 01 03 0B 7E ；设置欧标 （频率 865~868MHz）； //欧洲地区使用

BB 00 07 00 01 04 0C 7E ；设置国标 1 （频率 840~845MHz）；//几乎用不到

接收：　BB 01 07 00 01 00 09 7E//设置成功

注意：模块的频率一般和天线的频率要搭配，比如使用欧标频率的话，天线也必须要这个频率，如果天线不是这个频率，就无法获得正常的效果。

以上为 KLM900 系列模块最常规使用的功能指令，其它指令请您参看通信协议文档进行查看，您也可以把 DEMO 软件打开，连接上后，打开软件上监控，然后操作软件上任何按钮，就可以获取到当前操作的详细指令帧，这样可以更快的方便您的使用。使用中有任何问题您也可以联系我们咨询，感谢您的阅读。



指令对照表

```
enum cmd_code {
        CMD_HELLO                       = 0x01,
        CMD_HEART_BEAT  = 0x02,
        CMD_GET_MODULE_INFO     = 0x03,
```

```
CMD_SINGLE_ID           = 0x22,
CMD_MULTI_ID            = 0x27,
CMD_STOP_MULTI          = 0x28,
CMD_READ_DATA           = 0x39,
CMD_WRITE_DATA          = 0x49,
CMD_LOCK_UNLOCK         = 0x82,
CMD_KILL                        = 0x65,
CMD_SET_REGION  = 0x07,
CMD_INSERT_FHSS_CHANNEL = 0xA9,
CMD_GET_RF_CHANNEL = 0xbb,
CMD_SET_RF_CHANNEL = 0xAB,
CMD_SET_CHN2_CHANNEL= 0xAF,
CMD_SET_US_CHANNEL                      = 0xAC,     //      For     RFCONN
Conference
CMD_OPEN_PA                     = 0xAE,             // For RFCONN Conference
CMD_SET_FHSS      = 0xAD,
CMD_SET_POWER   = 0xB6,
CMD_GET_POWER   = 0xB7,
CMD_GET_SELECT_PARA     = 0x0B,
CMD_SET_SELECT_PARA = 0x0C,
CMD_GET_QUERY_PARA= 0x0D,
CMD_SET_QUERY_PARA = 0x0E,
CMD_SET_CW                      = 0xB0,
CMD_SET_BLF             = 0xBF,
CMD_FAIL                        = 0xFF,
CMD_SUCCESS             = 0x00,
CMD_SET_SFR             = 0xFE,
CMD_READ_SFR            = 0xFD,
CMD_INIT_SFR            = 0xEC,
CMD_CAL_MX              = 0xEA,
```

```
    CMD_CAL_LPF                 = 0xED,
    CMD_READ_MEM                = 0xFB,
    CMD_SET_INV_MODE  =   0x12,
    CMD_SET_UART_BAUDRATE     = 0x11,

    CMD_SCAN_JAMMER  =   0xF2,
    CMD_SCAN_RSSI     =   0xF3,
    CMD_AUTO_ADJUST_CH
    =                           0xF4,

    CMD_SET_MODEM_PARA  =   0xF0,
    CMD_READ_MODEM_PARA =   0xF1,
    CMD_SET_ENV_MODE  =   0xF5,
    CMD_TEST_RESET  =   0x55,

    CMD_POWERDOWN_MODE
    =                           0x17,
    CMD_SET_SLEEP_TIME
    =                          0x1D,
    CMD_IO_CONTROL  =   0x1A,
    CMD_RESTART       =   0x19,
    CMD_LOAD_NV_CONFIG
    =                           0x0A,
    CMD_SAVE_NV_CONFIG
    =                           0x09,
    CMD_ENABLE_FW_ISP_UPDATE = 0x1F,

    CMD_SET_READ_ADDR      = 0x14
};
```