扫码读写器用户手册
(V1.0)

北京握奇

二○一八年八月

目录

一 扫码读写器功能和性能介绍

扫码读写器支持 ISO14443 TypeA/TypeB 的非接触 CPU 卡、Mifare one 卡、读取二代身份证以及具有 2/3 磁道的磁条卡功能，外置密码键盘，内置最大支持 4 个符合 ISO7816-3 SIM 尺寸的 SAM 卡，以及标准卡尺寸的接触卡座（接触卡支持接触 CPU 卡/逻辑加密卡 4442/4428），支持条形码，二维码的读取，USB 通讯接口，并且支持无驱无软，操作简单，功能齐全，外观精美，性能稳定，质量可靠，适用于各种 IC 卡的应用系统。

1. 主要功能

- 支持符合 ISO14443 TypeA/TypeB 的非接触卡
- 支持 Mifare one 卡
- 支持读取二代身份证
- 支持标准卡尺寸接触卡（支持多速率通讯）
- 内置最多可支持 4 个 SIM 卡尺寸的 SAM 卡座，支持符合 ISO7816 的 CPU 卡（支持多速率）
- 支持具有 2、3 磁道的磁条卡（选配）
- 支持条形码，二维码的读取
- 支持全速 USB 通讯，速率 12Mbps
- 内置蜂鸣器，用户可以控制
- 3 个指示灯（蓝/红/绿）

2. 符合标准

- 〈非接触 IC 卡读写器技术规范〉
- 〈ISO14443-1/2/3/4〉
- 〈ISO7816-1/2/3/4〉
- 〈GA467 居民身份证验证安全控制模块接口技术规范〉
- 〈ISO7810 磁条卡部分规范〉
- 〈EIA-232-E 串口通讯标准〉
- 〈USB2.0 标准〉

二 主要技术指标

参数	指标
接触卡通讯速率（CPU 卡）（标准尺寸卡座）	9600/19200/38400/57600/115200/230000 /460000bps
接触卡工作电压（标准尺寸卡座）	3V、5V
支持的卡类型（标准尺寸卡座）	7816 标准 CPU IC 卡（T=0,T=1），SLE4428 ，SLE4442，AT88SC1604， AT88SC1608 等系列存储卡
SAM 卡座的接触卡通讯速率	9600
SAM 卡座(SAM1-SAM4)接触卡工作电压	3V
SAM 卡座支持的卡类型	7816 标准的 CPU 卡（T=0，T=1）
非接触卡支持的卡类型	IS014443 TypeA/TypeB 的非接触卡 Mifare one（S50，S70， Ultralight 等卡）
磁条卡	支持 2、3 轨的磁条卡读功能（选配）
二代证	支持 ISO14443B 的中华人民共和国二代身份证卡片
读卡距离	0～3CM
密码键盘接口	可外接密码键盘（选配）
扫码（选配） （注：性能可能会受到条形码质量和环境条件的影响）	补光灯：白光
	精度：一维条码≥10mil；二维码≥15mil
	识读速度：<3 次/s
	支持条码类型： Code11, Code39/Code93,ITF-6, ITF-4，Code 128， Industrial 2of5, Standard 2of5, Matrix 2of5, MSI Plessy, GS1 Databar, Code11,QR Code, PDF 417
	工作模式：（1）命令读取，（2）虚拟键盘自动上送
	读取距离：0-9 cm
指示灯	3 个 LED 指示灯（蓝/红/绿），指示通讯，电源，接触卡卡状态
USB 线	线长 1.5 米
工作电压	DC5V±0.5V
工作温度	0℃ ~50℃
操作系统	Win XP/ Win Vista/ Windows 7/ Windows 2008/ Win 8/ Windows 10/中标麒麟/Ubutu
USB 通讯	USB2.0 全速 12Mbps
谐振频率	13.56MHz±7kHz
平均无故障时间	5000 小时
驱动	无驱

三 读写器通讯协议

本通讯协议指的是 IC 卡读写器与上位机之间数据传输的格式，用户也可以按照此格式，通过不同的系统与 IC 卡读写器进行通讯连接。总体来说，该通讯协议就是在 ISO7816 协议的 APDU 指令基础上，在头尾各增加相应的数据，以保证通信数据的完整和正确性。

特别说明：本手册里与命令相关的的数字默认为十六进制。

1.发送到读写器的命令格式：

信息域	标识	字节长度	含义
通信数据头	NAD	1	0x12：大卡用户卡座 0x15：非接触卡 0x16：小 SAM 卡座 0x17：小 SAM 卡座 0x18：小 SAM 卡座 0x19：小 SAM 卡座 0x1A：磁条卡 0x1B：二代证模块 0x1C：扫码 0x00：读写器自定义指令
	PCB	1	USB 口：HID 协议中定义的包编号 串口：LEN 的高位字节
	LEN	1	数据长度，包括 CLA INS P1 P2 Lc DATA
APDU 指令	CLA	1	指令类型
	INS	1	指令码
	P1	1	指令参数 1
	P2	1	指令参数 2
	Lc	1	输入数据长度或期望返回数据长度
	DATA	0-FF	输入数据
校验字节	XOR	1	XOR 校验值（从 NAD 开始的所有数据做异或计算的结果） USB 模式下不存在

例 1：CPU 卡选择主文件（3F00）命令

12 00 07 00 A4 00 00 02 3F 00 8C

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

NAD PCB LEN CLA INS P1 P2 Lc (D A T A) XOR（串口存在，USB 口不存在）

例 2：CPU 卡复位命令

12 00 05 00 12 00 00 00 05

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

NAD PCB LEN CLA INS P1 P2 Lc XOR（串口存在，USB 口不存在）

2.从读写器返回信息的格式

标识	字节长度	含义
NAD	1	发送命令 NAD 的半字节互换 例如发送 NAD=12，返回 NAD=21
PCB	1	默认为 00
LEN	1	数据长度，包括 DATA SW1 SW2
DATA	0-FF	返回数据
SW1	1	状态字节 1
SW2	1	状态字节 2
XOR	1	XOR 校验值（从 NAD 开始的所有数据做异或计算的结果） USB 模式下不存在

例 1 返回信息如下：

21 00 02 61 XX XOR

↓ ↓ ↓ ↓ ↓ ↓

NAD PCB LEN SW1 SW2 XOR（USB 时不存在）

例 2 返回信息如下

21 00 13 3B6D0000574446224A864341301F131C12 90 00 7F

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

NAD PCB LEN (←-————————D A T A－—-————→) SW1 SW2 XOR（串口存在，USB 口不存在）

其中 90 00 是读写器自动补上状态字节 SW1 SW2

四 动态库的说明

适应操作系统：

Windows XP/7/8/10

1、读写器及 CPU 卡读写接口函数

此部分是针对 CPU 卡的操作函数，推荐的函数调用顺序

CT_open　　打开设备获得设备句柄
ICC_set_NAD　　设置卡座 NAD，默认值为 00
ICC_reset　　对 IC 卡复位
…
ICC_tsi_api　　对 IC 卡读写器进行操作
...
CT_close　　关闭打开设备的连接

1）打开 IC 卡终端端口

HANDLE WINAPI CT_open(
char *name,
unsigned int param1,
unsigned char param2
);
参数：
（A）串口读写器
name：读写器与 PC 相连的端口，可取 COM1 COM2 COM3 COM4 等
param1：波特率，可取 9600、19200、38400、57600 或 115200
param2：奇偶校验，仅仅支持"N"无校验
（B）USB 读写器
name:　　可取"hid1","hid2","hidN"等,1<=N<=9
序号分配原则，有以下情况:
i) 系统上所有 N 个设备均处于断开状态，则调用"hid1","hid2",...,"hidN"依次打开设备，跟插入顺序无关。
ii) 系统上存在 N 个已建立连接的设备，插上一新设备并打开此设备，则需从"hid1"～"hid(N+1)"依次调用。

param1:　未使用,设为 0
param2:　未使用,设为 0　　返回值：
INVALID_HANDLE_VALUE(-1)表示打开端口失败；
其他值(大于 0)为打开的端口句柄，用于卡操作函数的 fd

示例：

```
//以下的程序为以 9600 波特率，无校验方式打开与 COM1 口连接的串口读写器
HANDLE fDev;                    //定义句柄，用于保存端口句柄
char devName[5];                //用于保存端口名称
strcpy(devName, "COM1");        //获得端口名称
fDev = CT_open(devName ,9600, 'N');  //以相应的格式打开端口，并得到端口句柄
if(fDev == INVALID_HANDLE_VALUE)        //判断端口是否正确打开
{
   MessageBox("Open Device Error!");
   return;
}
```

2）关闭与 IC 卡读写器相连的端口（必须用 CT_open 打开的端口）

```
int WINAPI CT_close(
    HANDLE fd
    );
```

参数：

fd ： 为函数 CT_open 所返回的句柄

返回值：

-1：失败 0：成功

示例：

```
//以下示例为关闭以 CT_open()函数打开的读写器
int ret;        //定义 int 变量用于保存关闭函数返回值
ret = CT_close( fDev );         //关闭端口，并获得结果
if(ret == -1)       //判断端口是否正确关闭
{
   MessageBox("Close Deivce Error");
}
```

3）对设备当前激活插槽中的 IC 卡进行复位

```
unsigned WINAPI ICC_reset(
    HANDLE fd,
    unsigned char *lenr,
    unsigned char *resp
    );
```

参数：

fd ： 已打开的端口描述符

lenr ： 为对 IC 卡复位所返回的复位数据的长度

resp ： 复位的数据结果

返回值：

0x9000 成功

0x6200 无卡

0x6201 协议不认识

0x6FF0 卡通讯失败或其它未知的错误

0xFFFF 通迅失败

说明：

此函数受 ICC_set_NAD 函数影响，对读写器可设置为 12 与 15、16、17、18、19

示例：

```
//以下示例，为对 CPU 卡片进行复位
unsigned int sw;          //定义变量分别用于保存返回状态值
unsigned int lenr, resp[256];  //定义变量分别用于保存返回数据长度及数据
ICC_set_NAD(fDev,0x12);  //设置NAD为0x12
sw = ICC_reset(fDev, &lenr, resp);          //执行复位指令
if(sw != 0x9000)          //判断是否执行成功
{
    …  //操作失败后，用户的处理
}
```

4）从外设向 CPU 卡或读写器发送 APDU 命令并接收应答

comm的结构：CLA INS P1 P2 Lc DATA [Le] 其中DATA长度为Lc字节

resp 的结构：DATA 其中 DATA 长度为 Le 字节

```
unsigned WINAPI ICC_tsi_api(
    HANDLE fd,
    unsigned char len,
    unsigned char *comm,
    unsigned char *lenr,
    unsigned char *resp
    );
```

参数：

fd ： 已打开的端口描述符

len ： 命令 comm 的长度

comm ： 发向卡上的命令

lenr ： 从卡上接收到的数据长度

resp ： 从卡上接收到的数据

返回值：

0xFFFF 通迅失败（发送命令或接收返回的数据失败）

0x6FF0 卡通讯失败或其它未知的错误

其它为从卡上返回的状态 SW1 SW2

说明：

该函数适用于所有 CPU 卡操作，一次最多可读 255 个字节，写 255 个字节，并且切换串口波特率的指令只可以在此函数中实现

示例：

```
//以下示例为发送取版本号指令并显示
unsigned char lens;            //定义发送的数据长度变量
unsigned char lenr;            //定义保存返回数据长度变量
unsigned char comm[300];  //定义发送指令数组
unsigned char resp[300];          //定义接收数据数组
unsigned int sw;               //定义变量用于保存返回状态值
char tmpbuf[300];              //定义变量用于保存转化为字符型值的返回值
CString strDisplay;            //定义变量用于显示
ICC_set_NAD(fDev,0x12);      //设置NAD为0x12
memcpy(comm,"\x00\x19\x00\x00\x00",5);            //设置十六进制的指令
lens=5;                    //设置指令长度为5
sw=ICC_tsi_api(fDev,lens,comm,&lenr,resp);            //发送指令并取得返回值
if(sw!=0x9000)          //对指令执行是否成功进行判断
{
   MessageBox("Get Reader Firmware Version Error!");
}else
{
   BinToCHex((unsigned char *)tmpbuf,resp,lenr);        //将返回值转换为字符以供
显示
   tmpbuf[lenr*2]=0;
   strDisplay=CString(tmpbuf);
   MessageBox("Firmware Version is "+strDisplay);
}
```

5）从外设向 T=0 的 CPU 卡发送 APDU 命令并接收应答

```
unsigned WINAPI ICC_tsi_apiT0(
    HANDLE fd,
    unsigned int len,
    unsigned char *comm,
    unsigned int *lenr,
    unsigned char *resp
    );
```

参数：

fd ： 已打开的端口描述符

len ： 命令 comm 的长度

comm ： 发向卡上的命令

lenr ： 从卡上接收到的数据长度

resp ： 从卡上接收到的数据

返回值：

0xFFFF 通迅失败（发送命令或接收返回的数据失败）

0x6FF0 卡通讯失败或其它未知的错误

其它为从卡上返回的状态 SW1 SW2

说明：

该函数只适用于在读写器读写 T=0 的支持 256 字节读写的 CPU 卡，

使用该函数一次可读多达 256 字节（len=0），写多达 255 个字节的数据

示例：

同上，写入数据和返回值可达 255 字节

6）设置 CPU 卡读写地址 NAD

```
void WINAPI ICC_set_NAD(
    HANDLE fd,
    unsigned char nad
    );
```

参数：

fd ： 已打开的端口描述符

nad ： 读写地址

返回值：

无

说明：

该函数适用于读写器，系统缺省值为 00

00 对主卡操作

12 对读写器或主卡操作

13 选择读写器的 ESAM 卡操作

……

示例：

```
ICC_set_NAD(fDev,0x12);      //设置NAD为0x12
```

7）检查读写器的主卡座否插入 IC 卡

```
unsigned WINAPI ICC_present(
    HANDLE fd
    );
```

参数：

fd ： 已打开的端口描述符

返回值：

0x9000 已插入 IC 卡

0x6200 没有插入卡或卡没插到位

示例：

```
//此例程为检查卡片是否存在
unsigned int sw;          //定义返回状态变量
sw = ICC_present(fDev);   //检查是否插入卡操作
if(sw != 0x9000)          //判断是否执行成功
{
    …  //操作失败后，用户的处理
```

}

8）写 CPU 卡的二进制文件

unsigned WINAPI ICC_write_file(
HANDLE fd,
unsigned int offset,
unsigned int len,
unsigned char *data
);

参数：

fd ： 已打开的端口描述符
offset ： 二进制文件的偏移量
len ： 要写入卡上的数据长度
data ： 要写入卡上的数据

返回值：

0xFFFF 通迅失败（发送命令或接收返回的数据失败）
0x6FF0 卡通讯失败或其它未知的错误
其它为从卡上返回的状态 SW1 SW2

说明：

该函数适用于所有 CPU 卡操作，用户必须先选择要操作的二进制文件

示例：

```
//此示例为向 CPU 卡的二进制文件写入 3 个数据，请先对 CPU 卡片复位后，选择相应二进制文件
unsigned int offset = 0;          //定义写入数据地址的偏移量变量，并赋初值
unsigned int len;                 //定义写入数据长度的变量
unsigned char data[3]={0, 1, 2};  //定义写入数据变量，并赋初值
len = 3;                  //写入数据的长度为 3 字节
sw = ICC_write_file(fDev, offset, len, data);    //写入二进制文件 3 字节数据操作
if(sw != 0x9000)          //判断是否执行成功
{
    …  //操作失败后，用户的处理
}
```

9）读 CPU 卡的二进制文件

unsigned WINAPI ICC_read_file(
HANDLE fd,
unsigned int offset,
unsigned int len,
unsigned char *data
);

参数：

fd ： 已打开的端口描述符
offset ： 二进制文件的偏移量
len ： 要读卡上的数据长度
data ： 要读卡上的数据

返回值：

0xFFFF 通迅失败（发送命令或接收返回的数据失败）
0x6FF0 卡通讯失败或其它未知的错误
其它为从卡上返回的状态 SW1 SW2

说明：

该函数适用于所有 CPU 卡操作，用户必须先选择要操作的二进制文件

示例：

//此示例为向 CPU 卡的二进制文件读取 3 个数据，请先对 CPU 卡片复位后，选择相应二进制文件

```
unsigned int offset = 0;          //定义读取数据地址的偏移量变量，并赋初值
unsigned int len;                 //定义读取数据长度的变量
unsigned char data[256];//定义读取数据变量
len = 3;                  //读取数据的长度为 3 字节
sw = ICC_read_file (fDev, offset, len, data);     //读取二进制文件 3 字节数据操作
if(sw != 0x9000)          //判断是否执行成功
{
    …  //操作失败后，用户的处理
}
```

五 读写器自定义指令

读写器指令表							
NAD	CLA	INS	P1	P2	Lc	Data	功能说明
00	00	19	00	00	00		取读写器版本号
00	B0	16	RATE	01	00		修改读写器与 PC 间的串口通讯速率： 00:9600bps 01:19200bps 02:38400 bps 03:57600 bps 04:115200 bps 其它无效
	B0	F2	P1	P2	00		蜂鸣器鸣叫，P1 P2 鸣叫时间参数，约 0.1 秒数（P1 为高位，P2 为低位）
	B0	17	00	23	01	data	LED 灯控制。Data: bit6 绿灯控制位：1 on 0 off bit4 控制有效位：1 on 0 off bit3 蓝灯控制位：1 on 0 off
	00	19	01	01	Le		读设备序列号，Le 的长度小于 20
12	00	12	P1	00	00		接触卡 P1 指令通讯速率复位,固定可选值: 11: 9600bps 12: 19200bps 13: 38400bps 94: 57600bps 95: 115200bps 上述设置后，掉电失效
12	B0	16	P1	00	00		接触卡 P1 指令通讯速率复位,固定可选值: 11: 9600bps 12: 19200bps 13: 38400bps 94: 57600bps 95: 115200bps 上述设置后，掉电仍然有效

15	B0	06	00	00	04	DATA	延时等待指令： 1、非接读卡器等待卡片返回时间（FWI），单位us.最大等待时间小于 15S(F00000). 2、Data = 00 00 00 00.取消等待时间，按照复位时与卡片协商等待时间。 3、发复位指令（B0/00 12 00 00 00）设置失效。 4、读卡器上电设置失效。 例：B0 06 00 00 04 00 00 03 E8,等待 1ms(W2690要再加 260us)，卡片无数据返回将退出数据接收并返回 6FF0.
	B0	12	P1	P2	00		复位并 PPS 成要求速率，P1:PCD→PICC、P2:PICC→PCD、P1=P2；00:106Kbps；01:212K；02:424K；03:848K；04:1.7M(仅高速卡支持)
	B0	12	00	00	01	01	仅复位 TYPE A 卡
	B0	12	00	00	01	02	仅复位 TYPE B 卡
	B0	15	0E	00	01	00	关场
	80	11	P1	P2	Lc	data	Mifare One 卡参见<非接触卡的指令使用说明>

1. 读写器通用指令返回状态 SW1SW2 的含义

0x 9000：操作成功

0x 6FF0：卡通讯失败或其它未知的错误

0x 6D00：不识别的读写器命令

0x 6200/6201：指定操作的卡不存在

0x 70/75XX：非接触卡复位失败

0x 76XX：通讯失败

FFFF(-1)：PC 与读写器通讯失败

六 加密卡操作指令

读写器指令表							
NAD	CLA	INS	P1	P2	Lc	Data	功能说明
12	00	12	00	00	00		SLE4428 类别字节 92231091（h） SLE4442 类别字节 A2131091（h） AT88SC1608 卡复位信息 2CAA88A0（h） T24C01（或 AT24C02）类别字节 240C010A (h) AT24C16 类别字节 240C160A (h)
	00	B0	P1	P2	LEN		读逻辑卡相应起始地址开始的 LEN 字节数据； 注：SLE4442，只使用 P2，P1 置为 0；SLE4428，需使用 P1 和 P2。 P1(高位地址) P2（低位地址） LEN（数据长度） 注：当 LEN=0 时，为读 256 字节命令
	00	20	00	00	LEN	PIN	校验密码；注：SLE4442 的密码为 3bytes；SLE4428 的密码为 2bytes；
	00	D6	P1	P2	LEN	Data	向逻辑卡指定起始地址写入 LEN 字节数据； 注：SLE4442，只使用 P2，P1 置为 0；最大 256 字节，包括 0～31 保护存储区中未保护的字节，32～255 核对密码成功后的应用数据区。 SLE4428 需使用 P1 和 P2。
	00	24	00	00	LEN		修改密码
	SLE4428 专用命令						
	80	B0	P1	P2	LEN		带保护位读出逻辑卡指定起始地址的 LEN/2 字节数； 因保护位单独占 1byte,发指令时，LEN 为实际需要长度的 2 倍。 保护位说明： 0x80:该地址未写保护，可写入 0x00:该地址已写保护，不可再写入
	80	D6	P1	P2	LEN	Data	向逻辑卡指定起始地址写入 LEN 字节数据，并写保护位
	20	D6	P1	P2	LEN	Data	向逻辑卡指定起始地址写入 LEN 字节数据，并写保护位
	SLE4442 专用命令						

80	B0	00	00	LEN		读保护存储器命令； LEN 小于 4 时，返回长度为 LEN 长度数据，当 LEN 大于等于 4 时，返回 4bytes 保护存储器数据。因保护存储区共 4bytes
00	B0	01	00	04		读安全存储器命令
80	D6	00	P2	LEN	Data	写保护数据区并修改保护存储器中相应位命令；将指定地址的数据写保护； 若写入的数据和原有数据不同，则写保护失败 P2 范围：0x00-0x1F
00	D6	01	00	04	Data	写安全存储器 对安全存储器进行修改（即修改密码，不校验）

读写器指令返回状态 SW1SW2 的含义：

0x9000：正确

0x6FF0：通信错误

0x6700：长度超出限定值

0x6982：安全状态不满足

0x6985：位已写保护，写失败

0x6A80：写保护数据与相应地址数据不同，写失败

0x63CX：X 代表还剩可试次数

七 读写器非接触卡指令

1. 读写器可以自动识别 TypeA 和 TypeB 非接触卡片，以及标准的 Mifare One 卡片。
2. 标准非接触的 CPU 卡使用流程：
   a) 设置 nad 为 0x15
   b) 发送 cpu 卡的命令: CLA INS P1 P2 LC DATA
3. Mifare One 卡片的操作

命令说明表：

CLA	INS	P1	P2	LC	COMMAND	命令描述
80	11	09	00	00	----------	按 mifare 1 复位卡片
80	11	02	00	08	密钥类型（1 字节，60：keyA；61：keyB）+待认证的块号（1 字节）+密钥值（6 字节）	利用指令中给定的密钥进行认证
80	11	03	00	01	经过认证的块号（1 字节）	读 mifare 卡
80	11	04	00	11	经过认证的块号（1 字节）+数据字节（16 字节）	写 mifare 卡
80	11	05	00	05	经过认证的块号（1 字节）+金额数（4 字节）	将 Mifare 1 卡的块初始化为其规定的钱包形式。 注：4 字节的金额数为低位在前，高位在后。
80	11	06	00	05	经过认证的块号（1 字节）+金额数（4 字节）	向 mifare 1 卡的钱包块内添加金额 注：4 字节的金额数为低位在前，高位在后。
80	11	07	00	05	经过认证的块号（1 字节）+金额数（4 字节）	在 Mifare 1 卡的钱包块中扣除给定的金额 注：4 字节的金额数为低位在前，高位在后。

注意：对 Mifare One 卡进行块读写等操作时，只要换块操作，就要在块操作之前对该块进行复位操作（即发送 8011090000），然后再验证块密码，以及读写等操作。

读写器指令返回状态 SW1SW2 的含义：

0x 9000：正确

0x 6982：没有经过认证

0x 6983/6984：认证失败

0x 6FF0：初始化失败

0x 6FF3：写数据错误

0x 6FF5：超时

0x 6FF8：返回数据长度错误

八 磁条卡指令

读写器指令表							
NAD	CLA	INS	P1	P2	Lc	Data	功能说明
1A	80	17	03	P2	00		设置虚拟键盘都需上传哪几个磁道的信息给 PC 机. 默认为二磁道，磁道号信息存储在 flash 中，该设置变更后，掉电后状态不会被改变。 P2： 2. 二磁道 3. 三磁道 6. 二三磁道
	80	17	03	00	01		读取目前设置的磁道号，磁道号说明: 2. 二磁道 3. 三磁道 6. 二三磁道
	00	19	06	P2	00		磁条卡通道转换,P2： 0，模拟键盘通道 1， 普通卡通道（受控模式）
	00	19	20	P2	00		等待刷卡，P2:刷卡等待时间，表示多少秒内刷卡，最长 3min 钟。超时后返回模拟键盘通道。
	00	B0	P1	00	00		在卡通道模式下，读磁条卡相应磁道信息。P1: 00 代表 2、3 磁道， 02 代表第二磁道， 03 代表第三磁道
	00	19	21	00	00		清除刷卡信息，读取完刷卡信息后，必须清刷卡信息，信息清除后，卡通道变为模拟键盘通道。

读写器指令返回状态 SW1SW2 的含义：

0x9000：操作成功

0x6FF0：设置错误或其它未知的错误

0x6902：刷卡超时

0x6D00：不支持命令

0x6985：通道错误

九 密码键盘(型号 YD-511DS-A,外置可选)指令

读写器指令表							
NAD	CLA	INS	P1	P2	Lc	Data	功能说明
00	00	F8	00	01	03	2580	设置串口通信速率为 9600bps。P1:校验标志，00 无校验；02 偶校验；03 奇校验；P2:停止位；P3:指令长度
	00	F9	00	00	03	1B4330(/31)	清屏显示，最后一字节为 30 时为清第一行显示，为 31 时为清第二行
	00	F9	08	P2	03	001B49	“请输入密码”声音提示。P2:等待时间<180S；密码长度取决于键盘本身能输入的长度
	00	F9	08	P2	03	001B45	“请重新输入密码”声音提示。P2:等待时间；密码长度取决于键盘本身能输入的长度
	00/B0	F9	08	P2	01	1byte	说明： P2:最长 180S Data： 0x81，请再输入一次密码 0x82,您好，请输入密码 0x84，请输入原密码 0x85,请输入新密码
	00/B0	F9	00	00	01	83/86	0x83，回主页面 welcome 0x86，语音提示密码修改成功，延时 2s 后回主页面 Welcome

读写器指令返回状态 SW1SW2 的含义：

0x9000：操作成功

0x6F00：设置失败

0x6902：按键超时

0x6d00：不支持命令

十 读二代身份证指令

	读写器指令表							
NAD	Preamble	Len1	Len2	CMD	Para	Data	CHK	功能说明
1B	aa aa aa 96 69	00	03	12	FF	-----	xx	读 SAM_V 管理信息，返回 16 字节编号
		00	04	61	FF	Data	xx	设置SAM_V与射频模块一帧通信数据的最大字节数，Data 范围为 0x18~0xff,建议不超过 0x80
		00	03	20	01	-----	xx	寻找证/卡命令
		00	03	20	02	-----	xx	读取证/卡命令
		00	03	30	01	-----	xx	读固定信息，SAM_V 读取并验证证/卡固定信息，验证正确返回固定信息

读写器指令返回状态 SW1SW2 SW3 的含义：

SW1,SW2 表示证/卡返回的状态字节数；SW3 表示 SAM_V 操作状态。详见下面的 SAM_V 应答码

CHK:检验和，1 字节

0x9000：操作成功

0x6d00：不支持命令

数据输入/输出帧格式说明：

输入：Preamble Len1 Len2 CMD Para Data CHK

输出：Preamble Len1 Len2 SW1 SW2 SW3 Data CHK

SAM_V 应答码

SAM_V 应答码				
SW1	SW2	SW3	Data	功能说明
00	00	90	和具体命令有关，可能为空	操作成功
00	00	9F	证/卡芯片管理号	寻找证/卡成功
00	00	10	-----	接收业务终端数据的校验和错
00	00	11	-----	接收业务终端数据的长度错
00	00	21	-----	接收业务终端的命令错误
00	00	23	-----	越权操作
00	00	24	-----	无法识别的错误
xx	xx	31	-----	证/卡认证 SAM_V 失败
xx	xx	32	-----	SAM_V 认证证/卡失败
00	00	33	-----	信息验证错误

xx	xx	40	-----	无法识别的卡类型
xx	xx	41	-----	读证/卡操作失败
xx	xx	47	-----	取随机数失败
00	00	60	-----	SAM_V 自检失败
00	00	66	-----	SAM_V 未经授权，无法使用
00	00	80	-----	寻找证/卡失败
xx	xx	81	-----	选取证/卡失败
00	00	91	-----	证/卡中此项无内容

十一 扫码

读写器指令表							
NAD	CLA	INS	P1	P2	Lc	Data	功能说明
1C	00/B0	B0	00	P2	00		启动扫码模块在规定的超时时间内扫码
	B0	17	00	23	01	XX	设置扫码模块补光灯模式 XX: 00：闪烁模式 02：无照明模式 03：读码时常亮模式
	80	17	03	XX	00		修改上电默认扫码信息上传方式 XX ： 00 自动上传 01 命令方式
	80	17	03	00	01		获取当前存储的上电默认上送方式 扫码模式+9000 扫码模式： 00：自动上传 01：命令方式获取

读写器指令返回状态 SW1SW2 的含义：

9000：成功

6d00：不支持此指令

6902：超时

6ff0：错误

十二 注意事项

1）因为读写器工作频率为13.56MHz，所以在读写器安装现场不得有13MHz～15MHz之间强电磁场。
2）为了防止读写器发射磁场的相互影响，2台读写器的安装距离应大于10CM。
3）金属平面对电磁波有反射和屏蔽作用，因此读写器应尽量避免放置或安装在金属平面上。

十三 声明

此产品为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。