W5181 读写器

用户手册

(V1.1)

北京握奇数据系统有限公司

二〇〇九年九月

修订记录

时间	版本	修订内容
2009-12	1.0	初稿
2012-4-26	1.1	更换产品图片，增加接触卡通讯速率，更新配置说明，更新驱动说明，增加 mifare 卡密钥读取及更改说明

目录

一、读写器功能和性能介绍

W5181系列是握奇公司自主研发、生产的一款既支持符合ISO/IEC 7816-1/2/3的接触式智能卡和24CXX系列的存储卡以及SLE44XX系列的逻辑加密卡，也支持符合ISO/IEC 14443 Type A/Type B 的非接触式智能卡和Mifare one系列非接式存储卡的双界面读写器。 其中接触式智能卡有两个卡座，大卡座和小卡座，小卡座是通常用的SIM卡座。

1. W5181读写器主要功能

- 支持符合 ISO/IEC 14443 Type A/Type B 的 智能卡
- 支持非接触 Mifare 存储卡

- 支持 ISO/IEC 7816 系列接触式智能卡
- 支持 24C01、24C16、4428、4442 的存储卡
- 符合 CCID 协议
- 支持全速 USB 通讯，在 WIN7/Vista 下无需安装驱动
- LED 指示灯，指示电源或通讯状态
- 提供通用接口函数库，可支持多种操作系统和语言开发平台
- 读卡器底层可在线升级

2.W5181 读写器主要技术指标

参数	指标
谐振频率	13.56Mhz±25khz
非接触卡读写距离	非接触 CPU 卡　　0－3 cm 非接触 Mifare 卡　　0－4 cm 非接触 Simpass 卡　0－2.5 cm
天线	内置
取电方式	USB 自取电
支持全速 USB 接口	12Mbps
支持 CCID 协议	CCID 协议
接触卡通讯速率	默认 9600bps，支持自动 PPS（9600-224Kbps）
非接卡通讯速率	106k
无驱无软，支持热插拔	即插即用
支持操作系统	Windows 2000/XP/Vista/win 7
工作电流	≤300mA
工作电压	DC 5V

外型尺寸（H×W×D）	18.4*63.6*100（mm）
工作温度	0℃ ～ 50℃
工作湿度	20% ～ 90%
平均无故障时间	5000 小时
API 函数	PC/SC 规范
LED 灯	两个指示灯，指示电源和操作状态

3. 配套软件

- CCID 驱动
- VC++6.0的演示源程序
- TimeCOS 2.9.1 用户工具

4. 符合标准

- 非接触IC卡读卡器技术规范
- ISO/IEC 14443-1/2/3/4
- ISO/IEC 7816-1/2/3
- USB2.0 标准

5. 产品型号

产品型号 硬件配置说明

W5181 读写器，支持接触卡和非接触卡，内置1个小卡座

二、安装说明

1．W5181读写器的连接

将W5181读写器与PC机的USB口相连

2．USB驱动安装

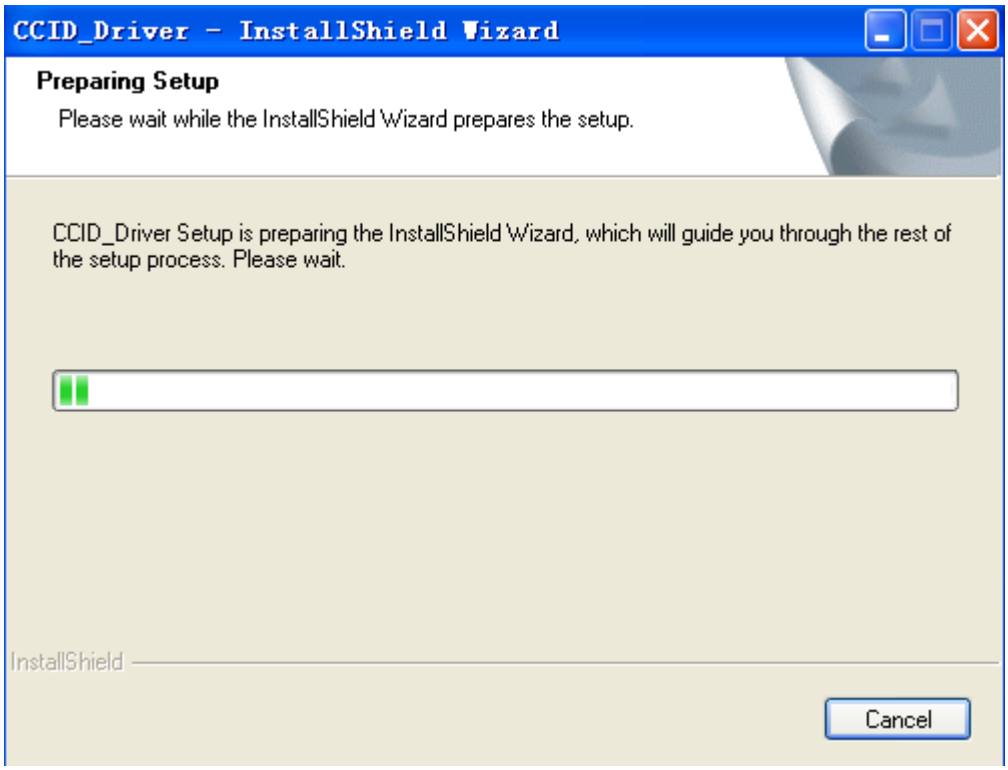
产品驱动及其他资料可通过握奇官网（www.watchdata.com）上获取。

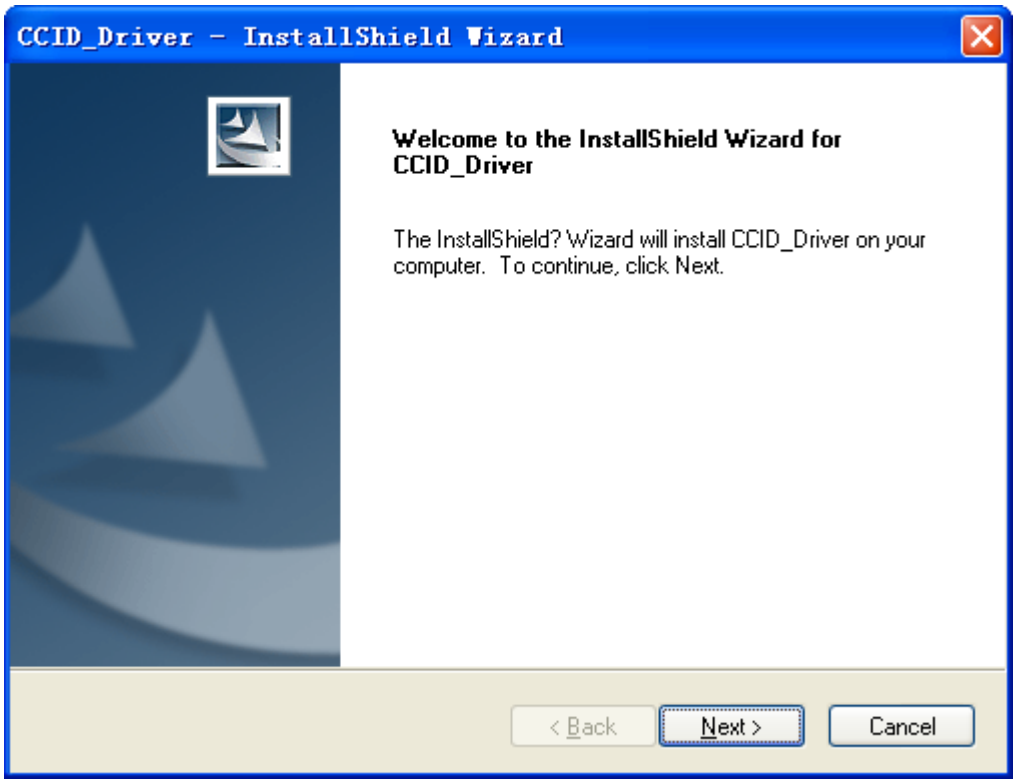
若设备第一次插入电脑后，被识别为USB Smart Card reader，说明该电脑曾经安装过CCID驱动，不用再次安装，可直接使用。

若不能被正常识别，可以通过两种方式进行驱动安装。

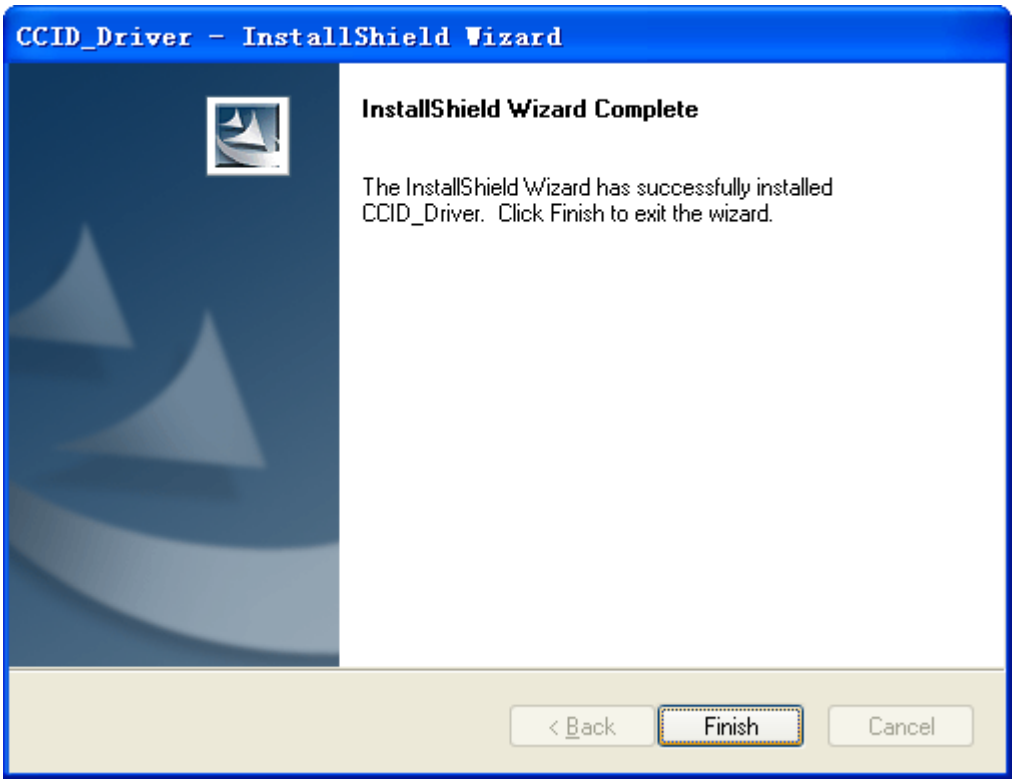
1. 直接通过Setup.exe进行安装，安装过程如下：

第一步：双击“CCID_DRIVER SETUP”文件夹中的setup.exe可执行程序，进行驱动安装界面，如下图：



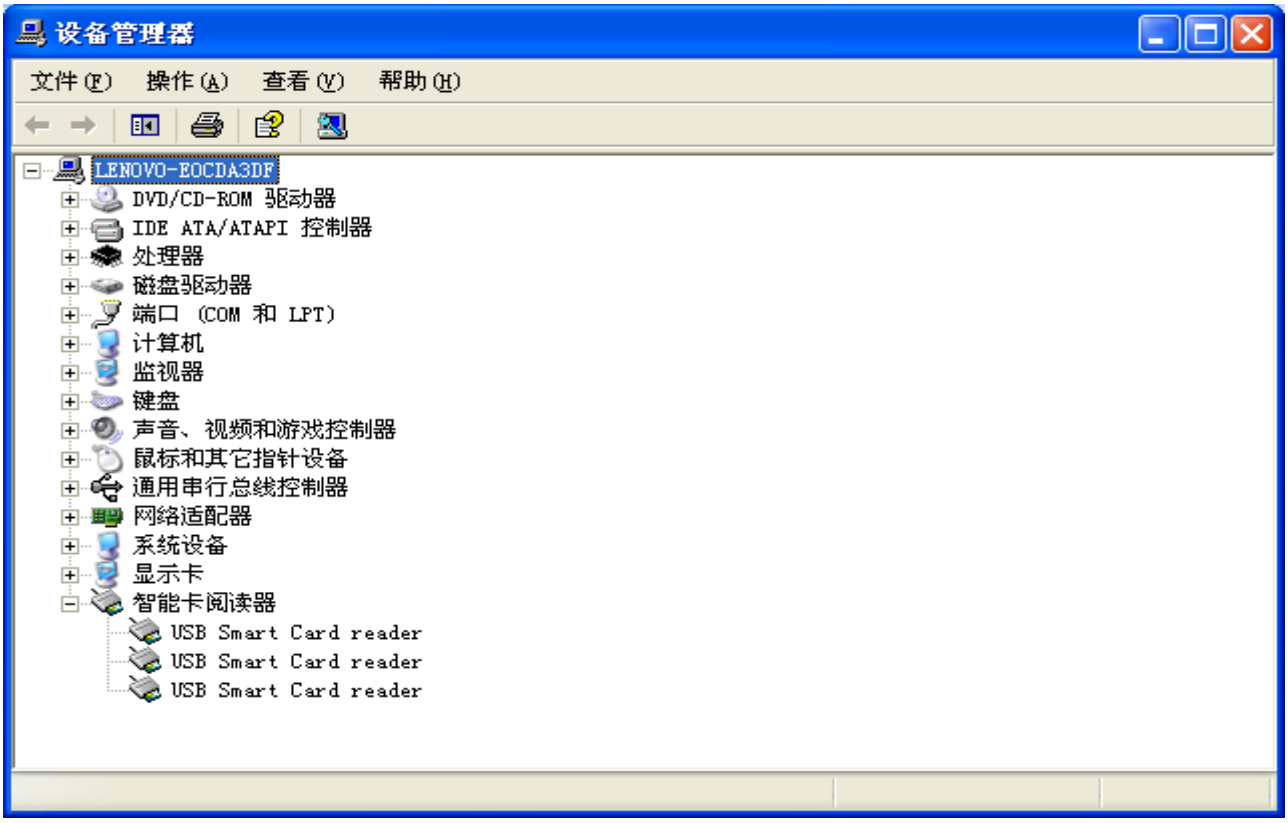


第二步： 弹出“Welcome to the installShield Wizard for CCID Driver”提示后，点击“Next”按钮后，弹出“Finish”按钮，如下图：



第三步：点击“Finish”按钮后，即表示驱动安装完成。

驱动安装成功后，在设备管理器中会在“智能卡阅读器”列表中显示‘USB Smart Card reader’名称，如下图；



2. 通过查找新硬件的方式进行安装，安装过程如下：

以Windows xp 操作系统为例，第一次安装时出现如下界面：

接下来会弹出一个硬件向导, 此处选择”否, 暂时不”, 点击“下一步”。

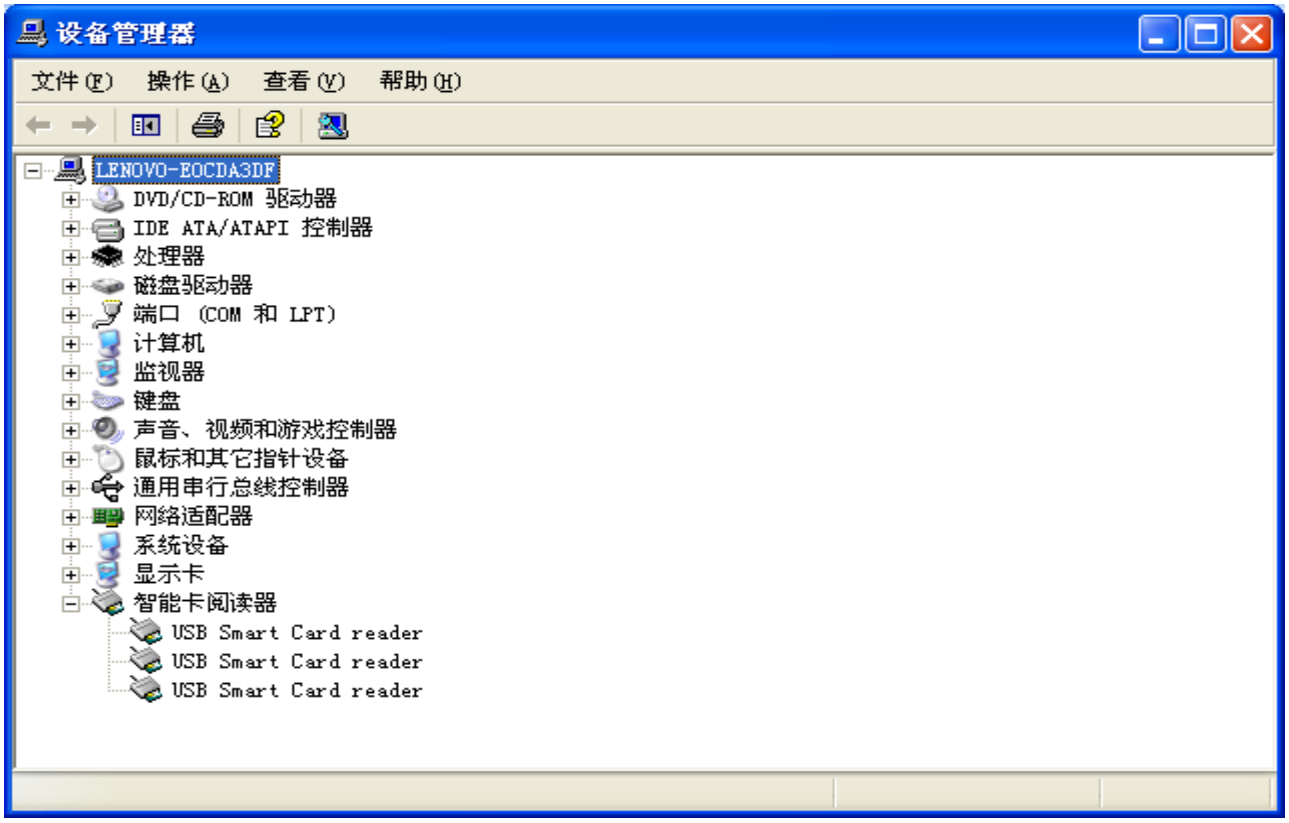
此处选择“从列表或指定位置安装”，然后点击下一步，如下图所示：

选择驱动所在的目录，然后点击“下一步”如下图所示：

然后会将读写器的驱动装到PC机上，完成后会弹出如下窗口：

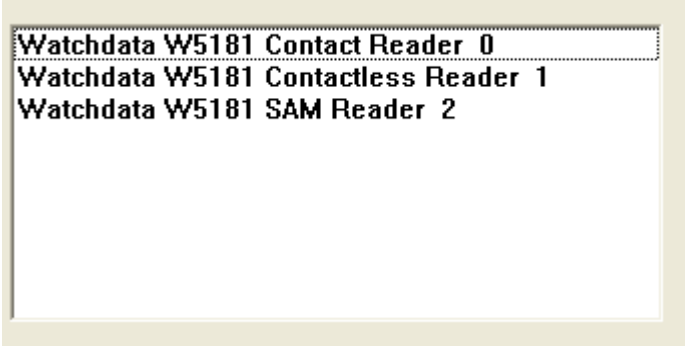
注意：W5181读写器有3个读写器设备，PC机会重复将其它的2个驱动自动完成。但有些系统会要求手动安装，如上所示。

安装成功后，在设备管理器中会显示‘智能卡阅读器’，点其‘+’会显示3个‘USB Smart Card reader’。如下图所示：



3. 读写器设备列表

在WIN XP系统下，调用读写器列表函数会列举出3个读写器设备名称，如下图所示：



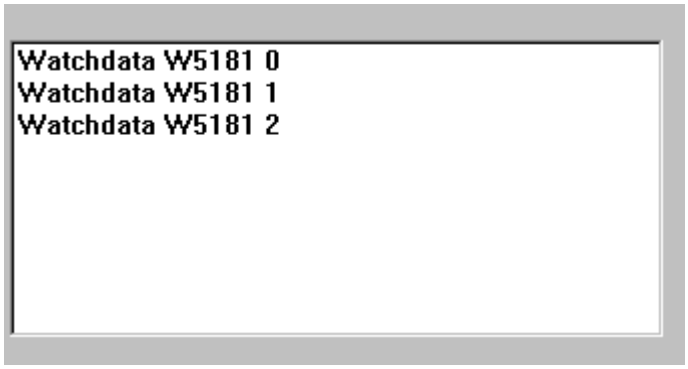
Watchdata W5181 Contact Reader 表示接触卡读写器设备;

Watchdata W5181 Contactless Reader 表示非触卡读写器设备;

Watchdata W5181 SAM Reader 表示SIM卡读写器设备.

注意:在每个读写器设备名称后面,系统会自动加上一个数字0,1,2…….这些数字会根据接入PC系统中的读写器设备数而自动变化,在选择确定某个读写器设备时,最好不包含后面的数字.

在WIN 2000系统下,调用读写器列表函数会列举出3个读写器设备名称,如下图所示:



Watchdata W5181 0 表示SIM卡读写器设备

Watchdata W5181 1 表示非触卡读写器设备;

Watchdata W5181 2 表示接触卡读写器设备

三．对读写器设备特殊命令介绍

1．接触式读写器设备（Watchdata W5181 Contact Reader）

注：在执行以下命令前，需要将接触卡插入接触卡插糟内，使接触式读写器设备有效

以下命令头定义：

CLA ： 命令报文的类别字节（Class Byte of the Command Message）

INS ： 命令的指令字节（Instruction Byte of Command Message）

P1 ： 参数1（Parameter 1）

P2 ： 参数2（Parameter 2）

Lc ： 终端发出的命令数据域的实际长度

Data ： 数据

1.1 接触式读写器特殊指令

特殊命令						
CLA	INS	P1	P2	LC	DATA	功能说明
00	12	00	00	00	无	对接触卡进行热复位
00	17	00	23	01	DATA	控制指令说明 data 数据位含义： b7 b6 b5 b4 b3 b2 b1 b0 b0-b3 保留 b4 控制使能位 1->on 0->off 此位置 0，其它位无效 b5 蜂鸣器 1->on 0->off b6 绿灯 1->on 0->off b7 红灯 1->on 0->off 示例：蜂鸣器响：001700230130
E0	17	34	00	00	无	擦除DFU标志
00	17	34	00	01	01	向DFU标志位写入01
00	17	34	00	01	无	读出DFU标志位，如是01表示标志更新成功，将读写器重新插入PC机的USB口则可进行程序更新

00	19	00	00	00	无	读取读写器固件版本号
00	19	00	01	00	无	读取读写器芯片号，每台读写器的芯片号唯一的

1.2 对24C01/24C16 存储卡命令介绍

CLA	INS	P1	P2	LC	DATA	功能说明
00	12	00	00	00	无	对接触卡进行热复位： 24C01/24C02:3b69+240C010A+5字节0+0x9000 24C16:3b69+240C160A+5字节0+0x9000
00	B0	P1	P2	LEN	无	读取卡上数据 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：00B0002301
00	D6/D0	P1	P2	LEN	DATA	写命令： 指令说明: P1: 高位地址 P2: 低位地址 LEN:写入数据的长度 示例：00D00030021122

1.3 对4428 逻辑加密卡命令介绍

CLA	INS	P1	P2	LC	DATA	功能说明
00	12	00	00	00	无	对接触卡进行热复位： 4428:3b69+92231091+5字节0+ 0x9000
00	B0	P1	P2	LEN	无	读取卡上数据 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：00B0002301
00	20	00	00	LEN	PIN	校验密码： 4428:2Byte 示例：0020000002FFFF
00	24	00	00	LEN	PIN	验证并修改密码命令： 指令说明: LEN:新密码和旧密码的长度和 PIN:旧密码+新密码 示例：0024000004FFFF1122

00	D6/D0	P1	P2	LEN	DATA	向逻辑卡指定起始地址写入LEN字节数据 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：00D000320411223344
80	B0	P1	P2	LEN	无	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) 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：80B0002302
80	D6/D0	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 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：80D00023020133

1.4 对4442 逻辑加密卡命令介绍

CLA	INS	P1	P2	LC	DATA	功能说明
00	12	00	00	00	无	对接触卡进行热复位： 4442:3b69+ A2131091+5字节0+ 0x9000
00	B0	P1	P2	LEN	无	读取卡上数据 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：00B0002301
00	20	00	00	LEN	PIN	校验密码： 4442:3Byte 示例：0020000003FFFFFF
00	24	00	00	LEN	PIN	验证并修改密码命令： 指令说明: LEN:新密码和旧密码的长度和 PIN:旧密码+新密码 示例：0024000006FFFFFF112233
00	D6/D0	00	P2	LEN	DATA	向逻辑卡指定起始地址写入LEN字节数据 指令说明: P1: 高位地址 P2: 低位地址 LEN:数据长度 示例：00D000320411223344

80	B0	00	00	LEN	无	读保护存储器命令 指令说明: 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 示例：80B0000004
00	B0	01	00	04	无	读安全存储区命令 安全存储区共 4bytes 长度 示例：00B0010004
80	D6/D0	00	P2	LEN	DATA	写保护存储器命令 指令说明: 将指定地址的数据写保护 P2 范围：0x00-0x1F 示例：80D0000C02FFFF
00	D6	01	00	04	DATA	写安全存储器: **不建议使用** 对安全存储器进行修改（即修改密码，不校验） 示例：00D601000411223344

返回状态字的说明：

9000：正确

6ff0：通信失败

63CX：X 代表还剩可试次数

6700：长度超出限定值

6982：安全状态不满足

6985：位已写保护，写失败

2. 非接触式读写器设备（Watchdata W5181 Contactless Reader）

特殊命令						
CLA	INS	P1	P2	LC	DATA	功能说明
00	12	00	00	00	无	对接触卡进行复位,返回非接触卡的复位信息

CLA : 命令报文的类别字节（Class Byte of the Command Message）
INS : 命令的指令字节（Instruction Byte of Command Message）
P1 : 参数 1（Parameter 1）
P2 : 参数 2（Parameter 2）
Lc : 终端发出的命令数据域的实际长度
Data : 数据

2.1 对 Mifare one 存储卡命令介绍

注：Mifare one 卡的具体分区介绍，请参考 Mifare one 的详细资料。

CLA	INS	P1	P2	LC	DATA	功能说明
80	11	09	00	00	无	对Mifare卡进行复位
80	11	02	00	08	DATA	命令说明：验证块密码 data 数据说明： Mode:1 Byte 认证方式 Block:1 Byte 块地址 Password: 6 Byte 块密码 例如： 8011 0200 08 0018FFFFFFFFFFFF
80	11	03	00	01	DATA	命令说明：读块数据 data数据说明： Block:1 Byte 块地址 例如： 8011 0300 01 18
80	11	04	00	11	DATA	命令说明：向块写数据 data数据说明： block:1 Byte 块地址 Data:16 Byte 向块内写入的数据 例如： 8011 0400 11 181122334455667788990AABBCCDDEEFF
80	11	05	00	05	DATA	命令说明：钱包初始化 data数据说明： Block: 1Byte 块地址 Money:4 Byte 初始化钱包金额 例如： 8011 0500 05 1810000000
80	11	06	00	05	DATA	命令说明：存款 data数据说明： Block: 1 Byte 块地址 Money: 4 Byte存款金额 例如： 8011 0600 05 1810000000
80	11	07	00	05	DATA	命令说明：扣款 data数据说明： Block: 1 Byte 块地址 Money: 4 Byte 扣款金额 例如： 8011 0700 05 1801000000
80	11	08	00	00	……	去活 Mifare One 卡，使其进入 HALT 状态，无指令数据
80	11	03	00	01	BlockAdr	命令说明：读取所在扇区 A 密钥

						BlockAdr：该扇区密钥所在块地址，每个扇区密钥在最末块存储，如扇区 0 的 A 密钥存储在 03 块 例如： 8011 0300 01 03 读取 0 扇区 A 密钥
80	11	04	00	11	BlockAdr+KAY A+Access Bits+FFFFFFFFFFFF	命令说明：修改所在扇区 A 密钥 BlockAdr：该扇区密钥所在块地址，同上 KAY A+Access Bits+ FFFFFFFFFFFF KAY A:6 bytes 新 KAY A 密钥 Access Bits:状态字(参考 Mifare1 数据手册) 例如： 8011040011 03 111111111111 FF078069ffffffffffff 将 0 扇区 A 密钥修改为 111111111111

3．SIM卡读写器设备(Watchdata W5181 SAM Reader)

打开关闭射频场的命令

打开和关闭射频场命令是通过 SIM 卡读写器设备下发的。

特殊命令						
CLA	INS	P1	P2	LC	DATA	功能说明
80	15	0E	00	01	00	关闭射频场,接触卡复位成功后再打开射频场
80	15	0E	00	01	01	打开射频场,恢复成原始状态
80	15	0E	00	01	02	关闭射频场,非接触读写器设备无效

说明:为了使SIM卡读写器设备在无卡时也能下发命令,在读写器上电时,如果SIM卡糟内无卡,将会上报伪卡信息,使SIM卡读写器设备能够下发命令。

四．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，该通讯协议就是将 APDU 命令在头尾各增加相应的数据，以保证通信数据符合 CCID 协议。

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	Type	1	CCID 指令
	Length	4	Abdata 的长度
	Slot	1	卡槽号
	Bseq	1	结果号
	bBwi	1	块等待时间
	Level Param	2	选择通讯方式
指令	Abdata	1	发送给 CCID 的数据

例 1：CPU 卡取随机数命令

```
6f    05000000    00    f1    00    0000    0084000008
↓        ↓        ↓     ↓     ↓     ↓         ↓
Type Length     Slot Bseq  bBwi Level  Abdata
```

2．从读写器返回信息的格式

信息域	标识	字节长度	含义
通信数据头	Type	1	CCID 指令
	Length	4	Abdata 的长度
	Slot	1	卡槽号
	Bseq	1	结果号
	Bstatus	1	卡槽状态
	bError	1	卡槽错误信息
	BchainParam	1	依据通讯方式返回参数
指令	Abdata	1	从读卡器返回的数据

例：取随机数返回信息如下：

```
80    0a000000 00  1b     00       00       00        c3f5bae6e9487cd99000
↓       ↓      ↓   ↓      ↓        ↓        ↓                  ↓
Type    Len   Slot Bseq Bstatus  bError BchainParam          Abdata
```

3．给读写器上电的命令格式：

信息域	标识	字节长度	含义
通信数据头	Type	1	CCID 指令
	Length	4	长度，默认 00000000h
	Slot	1	卡槽号
	Bseq	1	结果号
	Power Select	1	电压选择
指令	AbRFU	2	保留

例：上电命令

```
62  00000000    00   02     01          0000
↓      ↓        ↓    ↓      ↓           ↓
Type Length    Slot Bseq  Power Select  AbRFU
```

4．上电后从读写器返回信息的格式：

信息域	标识	字节长度	含义
通信数据头	Type	1	CCID 指令
	Length	4	Abdata 的长度
	Slot	1	卡槽号
	Bseq	1	结果号
	Bstatus	1	卡槽状态
	bError	1	卡槽错误信息
	BchainParam	1	依据通讯方式返回参数
指令	Abdata	1	从读卡器返回的数据

例：上电后返回信息如下：

```
80  11000000 00  02     01       00     00   3b6d000057443778878693011edf010a1a
↓      ↓     ↓   ↓      ↓        ↓      ↓                    ↓
Type   Len  Slot Bseq  Bstatus  bError  BchainParam          Abdata
```

5．给读写器下电的命令格式：

信息域	标识	字节长度	含义
通信	Type	1	CCID 指令

数据头	Length	4	长度，默认 00000000h
	Slot	1	卡槽号
	Bseq	1	结果号
指令	AbRFU	2	保留

例：下电命令

63 00000000 00 01 000000

↓ ↓ ↓ ↓ ↓

Type Length Slot Bseq AbRFU

6．下电后从读写器返回信息的格式：

信息域	标识	字节长度	含义
通信数据头	Type	1	CCID 指令
	Length	4	Abdata 的长度
	Slot	1	卡槽号
	Bseq	1	结果号
	Bstatus	1	卡槽状态
	bError	1	卡槽错误信息
	BClockstatus	1	时钟运行状态

例：下电后返回信息如下

81 00000000 00 01 01 00 00

↓ ↓ ↓ ↓ ↓ ↓ ↓

Type Len Slot Bseq Bstatus bError BClockstatus

五．W5181读写器操作函数说明

适应操作系统：

- Windows 2000/XP/2003/Vista 系统

适用的 IC 卡：

- 符合 14443 协议的 CPU 卡(包括 TYPE A 和 TYPE B 和 Mifare 卡)
- ISO7816 协议的 CPU 卡（包括 T=0 和 T=1）

函数动态库名称：

- Winscard.DLL（Windows 自带的 API 函数，以下是主要的几个函数介绍）

1. 与终端建立连接的函数：

```
hContext=hSC;
 lReturn = SCardConnect(hContext,
                        Readers,
                        SCARD_SHARE_SHARED ,
                        SCARD_PROTOCOL_T0|SCARD_PROTOCOL_T1,//SCARD_PROTOCOL_DEFAULT ,
```

```
                    &hCardHandle[index],
                    &dwAP[index] );
```

2. 与终端断开连接的函数：

```
lReturn = SCardDisconnect(hCardHandle[index],
                                    SCARD_UNPOWER_CARD);
```

3. 向终端发送 APDU 指令的函数：

```
lReturn = SCardTransmit(hCardHandle[index],
                        (dwAP[index]==SCARD_PROTOCOL_T0?SCARD_PCI_T0:SCARD_PCI_T1),
                        inBuf,
                        inBufLen,
                        NULL,
                        outBuf,
                        &dwstatusLength );
```

4. 为访问智能卡数据库建立描述表

```
lReturn = SCardEstablishContext(SCARD_SCOPE_SYSTEM,
                                NULL,
                                NULL,
                                &hSC);
```

5. 关闭已经建立的描述表

```
lReturn = SCardReleaseContext(hSC);
```

6. 获取读卡器列表

```
lReturn = SCardListReaders(hSC, NULL,(LPTSTR)&pmszReaders, &cch );
```

7. 分配内存

```
lReturn = SCardGetAttrib(hCardHandle[index],
                         SCARD_ATTR_CHANNEL_ID,
                         (LPBYTE)&pbAttr,
                         &cByte);
```

8. 释放内存

```
lReturn = SCardFreeMemory( hContext, pbAttr );
```

六．注意事项

1） 因为读卡器工作频率为 13.56MHz，所以在读卡器安装现场不得有 13MHz～15MHz 之间强电磁场
2） 为了防止读卡器发射磁场的相互影响，2 台读卡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，因此读卡器周围应尽量避免放置或安装在金属平面上。