



# HUADA读卡器串口通信协议

## 广东华大互联网股份有限公司

地址： 深圳市龙岗区天安数码城4栋A座16楼

网址： [www.hd-os.com](http://www.hd-os.com)

## 目录

1 串口通信协议简介 .....	5
1.1 本章概述 .....	5
1.2 Host->Client协议解析 .....	5
1.3 Client->Host协议解析 .....	6
2 卡片指令集 .....	7
2.1 接触CPU冷复位 .....	7
2.2 接触CPU热复位 .....	8
2.3 接触CPU下电 .....	9
2.4 接触CPUAPDU .....	10
2.5 获取卡座状态 .....	11
2.6 4428卡上电 .....	12
2.7 4428卡下电 .....	13
2.8 4428卡认证 .....	14
2.9 4428卡读数据 .....	15
2.10 4428卡写数据 .....	16
2.11 4428卡读保护区 .....	17
2.12 4428卡写保护区 .....	18
2.13 4428卡修改密钥 .....	19
2.14 4428卡密钥剩余认证次数 .....	20
2.15 4442卡上电 .....	21
2.16 4442卡下电 .....	22
2.17 4442卡认证 .....	23
2.18 4442卡读数据 .....	24
2.19 4442卡写数据 .....	25
2.20 4442卡读保护区 .....	26
2.21 4442卡写保护区 .....	27

2.22 4442卡修改密钥 .....	28
2.23 4442卡密钥剩余认证次数 .....	29
2.24 磁条卡读取 .....	30
2.25 超时取消 .....	31
2.26 Type A .....	32
2.28 ISO14443 Protocol .....	34
2.29 M1认证 .....	34
2.30 M1读操作 .....	35
2.31 M1写操作 .....	36
2.32 M1增值 .....	36
2.33 M1减值 .....	37
2.34 M1装载密钥 .....	38



# 1 串口通信协议简介

## 1.1 本章概述

读卡器为Host，键盘为Client。

双方通过USART口通信，115200bps

、1位起始位、8位数据位、1位停止位、无奇偶校验。

**数据域**长度不超过1024字节。

下述将对协议作基本介绍，分别是：

- Host->Client协议解析
- Client->Host协议解析

## 1.2 Host->Client协议解析

协议包含起始帧、长度域、信息类型域、数据域、校验字节、结束帧等信息,如表1-1所示。

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
2	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度),如长度1500, 则为DC 05
6	bMessageType	1	00-FF	信息类型域
7	abData	ByteArray		数据域(长度为0则不存在)
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表1-1Host->Client协议解析

## 1.3 Client->Host协议解析

协议包含起始帧、长度域、状态域、数据域、校验字节、结束帧等信息,如表1-2所示。

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
2	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度),如长度1500, 则为DC 05
6	bStatus	1	00-FF	状态域
7	abData	ByteArray		数据域(长度为0则不存在)
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表1-2Host->Client协议解析

异或校验位 = 长度域+信息类型域/状态域+数据域的异或
如: FA FB FC FD 08 00 01 11 22 33 44 4D BB(十六进制)
4D(异或校验位) = $08 \oplus 00 \oplus 01 \oplus 11 \oplus 22 \oplus 33 \oplus 44$

表1-3 异或校验位计算方法

## 2 卡片指令集

### 2.1 接触CPU冷复位

#### Contect\_ColdReset

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	74	信息类型域
7	BSlot(abData)	1	0C\0D\0E\0F\10	卡座号（数据域）
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-1 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray	复位信息	数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-2 Client->Host

## 2.2 接触CPU热复位

### Contect\_WarmReset

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	75	信息类型域
7	BSlot(abData)	1	0C\0D\0E\0F\10	卡座号（数据域）
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-3 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray	复位信息	数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-4 Client->Host



## 2.3 接触CPU下电

### Contect\_PowerDown

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	73	信息类型域
7	BSlot(abData)	1	0C\0D\0E\0F\10	卡座号（数据域）
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-5 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray=0		数据域
7+ 0	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-6 Client-&gt;Host

## 2.4 接触CPUAPDU

### Contect\_APDU

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	72	信息类型域
7	BSlot(abData)	1	0C\0D\0E\0F\10	卡座号(数据域)
8	C-Apdu(abData)	ByteArray		APDU指令(数据域)
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-7 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	R-Apdu(abData)	ByteArray		APDU应答(数据域)
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-8 Client-&gt;Host

## 2.5 获取卡座状态

### Contect\_CardStatus

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	77	信息类型域
7	BSlot(abData)	1	0C~10	卡座号(数据域)
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	有卡未上电:03 无卡:02 有卡已上电:00	状态域
7	abData	ByteArray=0		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.6 4428卡上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	60	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.7 4428卡下电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	61	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.8 4428卡认证

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	64	信息类型域
7	BSlot(abData)	2		认证密钥
9	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.9 4428卡读数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	62	信息类型域
7	Offset	2	0000-0004	读取起始位置
9	Len	2	0000-0004	读取字节长度
11	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.10 4428卡写数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	63	信息类型域
7	Offset	2	0000-0004	读取起始位置
9	Len	2	0000-0004	读取字节长度
11	abData	ByteArray		数据域
11+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host



## 2.11 4428卡读保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	66	信息类型域
7	Offset	2		读取起始位置
9	Len	2		读取字节长度
11	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.12 4428卡写保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	67	信息类型域
7	Offset	2		读取起始位置
9	Len	2		读取字节长度
11	abData	ByteArray		数据域
11+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.13 4428卡修改密钥

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	65	信息类型域
7	Auth_Key	2		认证密钥
9	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.14 4428卡密钥剩余认证次数

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	68	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	1		剩余认证次数
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.15 4442卡上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	50	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.16 4442卡下电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	51	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.17 4442卡认证

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	54	信息类型域
7	BSlot(abData)	3		认证密钥
10	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.18 4442卡读数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	52	信息类型域
7	Offset	2		读取起始位置
9	Len	2		读取字节长度
11	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client->Host



## 2.19 4442卡写数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	53	信息类型域
7	Offset	2		读取起始位置
9	Len	2		读取字节长度
11	abData	ByteArray		数据域
11+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.20 4442卡读保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	56	信息类型域
7	Offset	2		读取起始位置
9	Len	2		读取字节长度
11	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	ByteArray		数据域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.21 4442卡写保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	57	信息类型域
7	Offset	2		读取起始位置
9	Len	2		读取字节长度
11	abData	ByteArray		数据域
11+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.22 4442卡修改密钥

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	55	信息类型域
7	Auth_Key	3		认证密钥
10	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.23 4442卡密钥剩余认证次数

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	58	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-11 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	abData	1		剩余认证次数
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-12 Client-&gt;Host

## 2.24 磁条卡读取

### MagCard\_Read

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	70	信息类型域
7	bTrackSelect(abData)	1	01/02/03	磁道号(数据域)
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-13 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7	(abTrackData)(abData)	ByteArray		磁道数据(数据域)
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-14 Client->Host

## 2.25 超时取消

### OVERTIME\_Handle

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	7B	信息类型域
7	bTypeSelect(abData)	1	获取密码超时:01 获取磁卡信息超时:02	磁道号(数据域)
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-15 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:1	状态域
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-16 Client->Host

## 2.26 Type A

### TYPE A上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	20	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-17 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	(abData)	ByteArray		UID+ATR
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-18 Client->Host

## 2.27 Type B

### TYPE B上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	21	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-19 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始





				帧和结束帧的 长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	(abData)	ByteArray		ATR
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-20 Client->Host



## 2.28 ISO14443 Protocol

### ISO14443 Protocol (APDU)

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	22	信息类型域
7	C-Apdu(abData)	ByteArray		APDU指令(数据域)
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-21 Host->Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	R-APDU (abData)	ByteArray		APDU应答(数据域)
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-22 Client->Host

## 2.29 M1认证

### Mifare one Auth

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	23	信息类型域
7	K_Mode(abData)	1		0- 2: KeyA; 4-



				6: KeyB, (读写器内部Key A、Key B各三套) 0x60或0x61表示从用户传输中加载KeyA或KeyB
8	SecNr	1	0-39	扇区号
9-14	Auth_Key	6		认证密钥(当使用读写器内部密钥时, Auth_Key设为全0)
15	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-23 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-24 Client-&gt;Host

## 2.30 M1读操作

### Mifare one Read

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	24	信息类型域
7	Block_Addr(abData)	1		块地址
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-25 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	Block_data	ByteArray		读取到块数据
7+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-26 Client-&gt;Host

## 2.31 M1写操作

### Mifare one Write

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	25	信息类型域
7	Block_Addr(abData)	1		块地址
8	Block_Data	16		写入块数据
24	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-27 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-28 Client-&gt;Host



## 2.32 M1增值

### Mifare one IncVal

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	26	信息类型域
7	Block_Addr(abData)	1		块地址
8	IncVal	4		增值数据, 低字节在前
12	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-29 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-30 Client-&gt;Host

## 2.33 M1减值

### Mifare one DecVal

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	27	信息类型域
7	Block_Addr(abData)	1		块地址
8	IncVal	4		减值数据, 低字节在前



12	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-31 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-32 Client-&gt;Host

## 2.34 M1装载密钥

### Mifare one Load Key

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	28	信息类型域
7	Key_Mode(abData)	1		0-2: KeyA; 4-6: KeyB(各3套密钥)
8	Load_key	6		加载密钥
14	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表2-33 Host-&gt;Client

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	FA FB FC FD	起始帧
4	dwLength	2	0000-FFFF	长度域(除起始帧和结束帧的长度)
6	bStatus	1	成功:0 失败:非0	状态域
7	bParity	1		异或校验位



Last Byte	bEndFrame	1	BB	结束帧
-----------	-----------	---	----	-----

表2-34 Client->Host