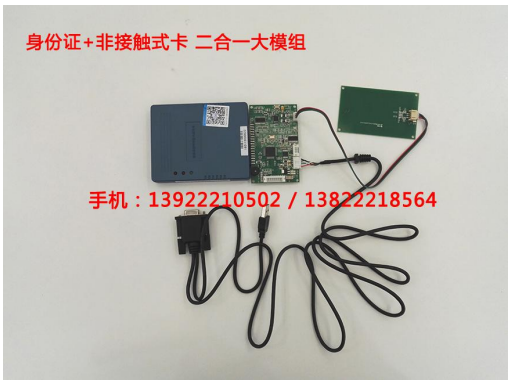
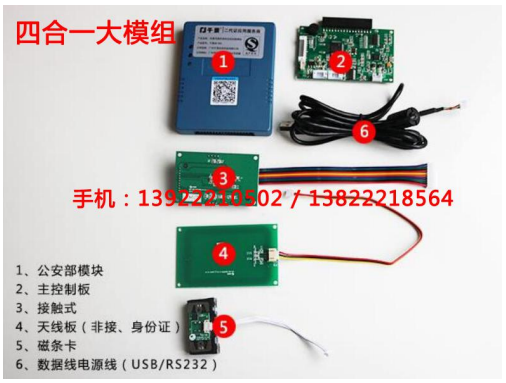
多功能读卡器串口通信协议

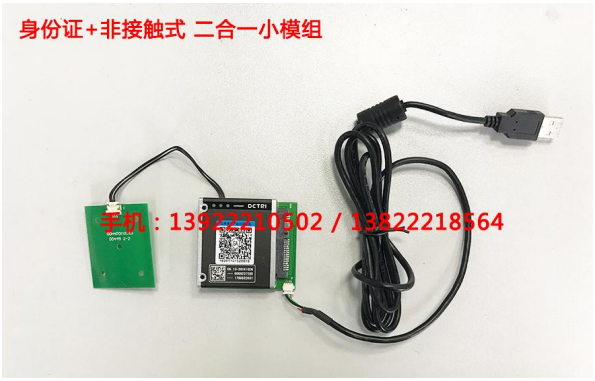
V2019.05.15 PE03F

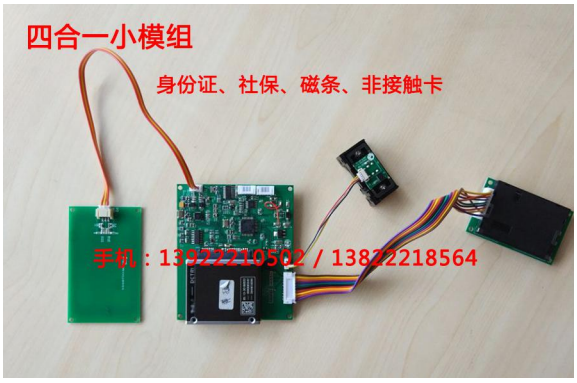
广东东信智能科技有限公司	
地址：	广东省广州科学城总部经济区观虹路 12 号
网址:	www.eastcoms.com

本协议适用以下几类产品









此为串口底层协议，适用 **Linux**、单片机、**Wince** 等嵌入式系统使用。

目录

1 串口通信协议简介

1.1 本章概述

读卡器为 Host，用户为 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
- 异或检验位：除去起始帧+异或校验位+结束帧，中间的全部异或

1.2 Client > Host-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	EA EB EC ED	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 1-1Client->Host 协议解析

1.3 Host -> Client 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	EA EB EC ED	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	bMessageType	1	00-FF	信息类型域
8	abData	ByteArray		数据域
8+ 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: EA EB EC ED 08 00 01 11 22 33 44 4D BB(十六进制) 4D(异或校验位) = 08^00^01^11^22^33^44

表 1-3 异或校验位计算方法

2 卡片指令集（信息类型）

2.1 接触 CPU 冷复位

Contect_ColdReset

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	74	信息类型域
8	abData	ByteArray	复位信息	数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-2 返回

社保卡冷复位：EA EB EC ED 05 00 74 0C 7D BB

返回：EA EB EC ED 16 00 00 74 3B 6D 00 00 00 81 54 40 00 86 60 44 01 00 6B 36 68 37 BB

2.2 接触 CPU 热复位

Contect_WarmReset

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	75	信息类型域
8	abData	ByteArray	复位信息	数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-4　返回

2.3 接触 CPU 下电

Contect_PowerDown

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	73	信息类型域
8	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　返回

2.4 接触 CPU APDU

Contect_APDU

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	72	信息类型域
8	R-Apdu(abData)	ByteArray		APDU 应答(数据域)
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-8　返回

2.6 蜂鸣器

Contect_CardStatus

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	起始帧
4	dwLength	2	04 00	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	A4	信息类型域
8	bParity	1	A0	异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-11　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	A4	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12　返回

2.7 身份证寻卡

Contect_CardStatus

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	起始帧
4	dwLength	2	04 00	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	B0	信息类型域
8	bParity	1	B4	异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-11　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	B0	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12　返回

发送：EA EB EC ED 04 00 B0 B4 BB

返回：EA EB EC ED 05 00 00 B0 B5 BB

2.8 身份证选卡

Contect_CardStatus

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	起始帧
4	dwLength	2	04 00	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	B1	信息类型域
8	bParity	1	B5	异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-11　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	B1	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12　返回

发送：EA EB EC ED 04 00 B1 B5 BB

返回：EA EB EC ED 05 00 00 B1 B4 BB

2.9 读取身份证

Contect_CardStatus

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	起始帧
4	dwLength	2	04 00	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	B4	信息类型域
7	bParity	1	B0	异或校验位
Last Byte	bEndFrame	1	BB	结束帧

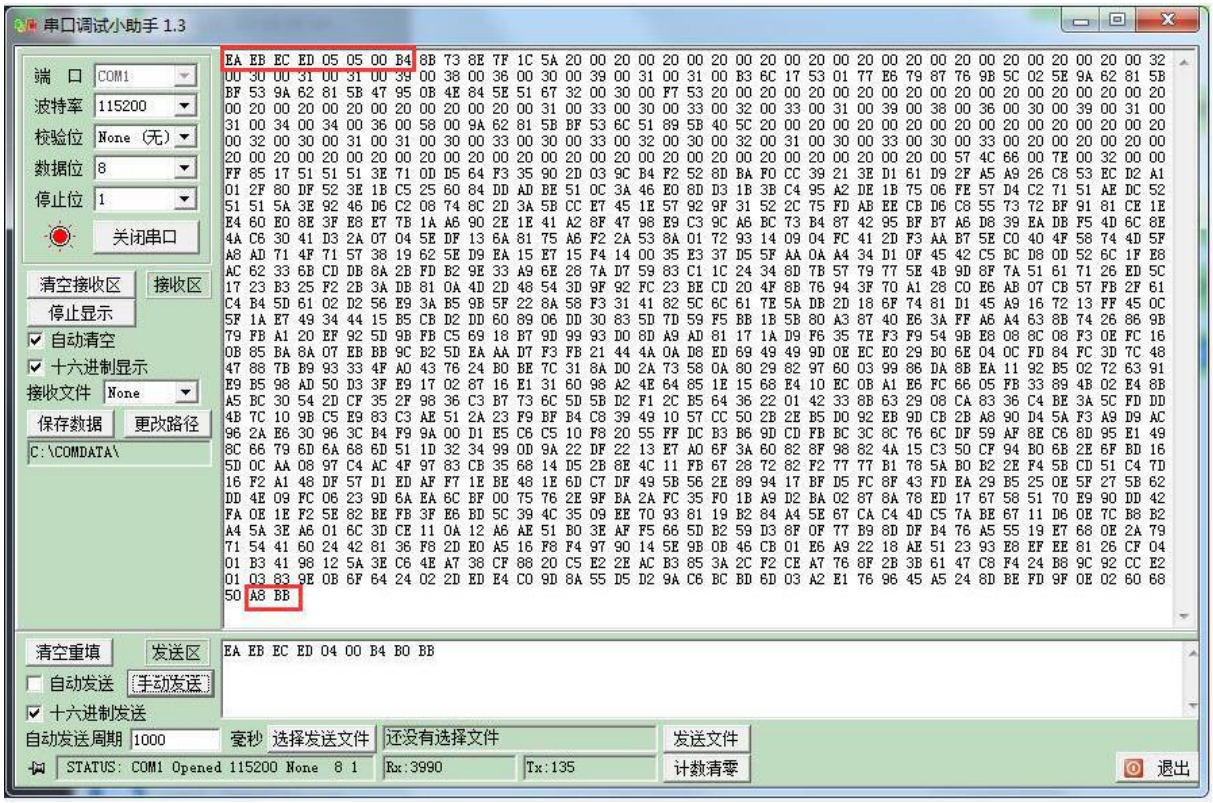
表 2-11　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	B4	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12　返回

发送：EA EB EC ED 04 00 B4 B0 BB

返回信息：



说明：

返回为 **1290** 字节的数据。其中身份证文字+照片数据为 **1280** 字节，具体解析见我司另外的东信智能身份证信息解析说明文件。

除去红色框以为内容，中间就是读取出来的身份证信息。

2.91 读取身份证物理 ID

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	起始帧
4	dwLength	2	04 00	长度域(除起始帧和结束帧的长度)
6	bMessageType	1	12	信息类型域
7	bParity	1	B0	异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-11　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	12	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12　返回

附：

读身份证物理卡号（UID）：

示例：**EA EB EC ED 04 00 12 16 BB**，返回数据：**EA EB EC ED 0F 00 00 12 31 31 27 22 40 19 0A C3 90 00 18 BB** ，其中 **31 31 27 22 40 19 0A C3** 就是身份证的 UID。

2.10 4428 卡上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	60	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.11 4428 卡下电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	61	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.12 4428 卡认证

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	64	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.13 4428 卡读数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	62	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.14 4428 卡写数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	63	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.15 4428 卡读保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	66	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.16 4428 卡写保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	67	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.17 4428 卡修改密钥

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	65	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.18 4428 卡密钥剩余认证次数

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	68	信息类型域
8	abData	1		剩余认证次数
9	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.19 4442 卡上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	50	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.20 4442 卡下电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	51	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.21 4442 卡认证

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	54	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.22 4442 卡读数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	52	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.23 4442 卡写数据

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	53	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.24 4442 卡读保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	56	信息类型域
8	abData	ByteArray		数据域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.25 4442 卡写保护区

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	57	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.26 4442 卡修改密钥

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	55	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.27 4442 卡密钥剩余认证次数

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	58	信息类型域
8	abData	1		剩余认证次数
9	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-12 返回

2.28 磁条卡读取

MagCard_Read

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	70	信息类型域
8	(abTrackData)(abData)	ByteArray		磁道数据(数据域)
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-14　返回

2.29 超时取消

OVERTIME_Handle

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	7B	信息类型域
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-16　返回

2.30 Type A

TYPE A 上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	20	信息类型域
8	(abData)	ByteArray		UID/ATS
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-18 返回

2.31 Type B

TYPE B 上电

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	21	信息类型域
8	(abData)	ByteArray		ATS
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-20　返回

2.32 CPU 卡发送 APDU

ISO14443 Protocol（APDU）

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	22	信息类型域
8	R-APDU (abData)	ByteArray		APDU 应答(数据域)
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-22 返回

2.33 M1 认证

Mifare one Auth

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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		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		认证的密钥（6 字节秘钥）
15	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-23　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	23	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-24　返回

2.34　M1 读操作

Mifare one Read

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

扇区跟块的对应关系：扇区号*4　+ 块号 = 块地址

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	24	信息类型域
8	Block_data	ByteArray		读取到块数据
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-26　返回

2.35　M1 写操作

Mifare one Write

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	25	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-28　返回

2.36 M1 增值

Mifare one IncVal

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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 发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	26	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-30 返回

2.37 M1 减值

Mifare one DecVal

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	27	信息类型域
8	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-32　返回

2.39　获取 M1 卡物理卡号

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	29	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-17　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	29	信息类型域
8	(abData)	ByteArray		UID
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 2-18　返回

3.2 Get Version

Get Version

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	A1	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 3-2-1　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	A1	信息类型域
8	Version	ByteArray		版本信息
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 3-2-2　返回

3.7 获取读写器编号

Get Reader SNR

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	A6	信息类型域
7	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 3-7-1　发送

Offset	Field	Size	Value(十六进制)	Description
0	dwStarFrame	4	EA EB EC ED	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	bMessageType	1	A6	信息类型域
8	SNR_Buf	ByteArray		读写器序列号
8+ ByteArray	bParity	1		异或校验位
Last Byte	bEndFrame	1	BB	结束帧

表 3-7-2　返回

4 错误代码

4.1 本章概述

4.2 非接触卡片操作错误代码

错误代码	名称	描述
0xfe	未找到该命令	
0xfd	TYPE A 寻卡错误	
0xfc	TYPE A 检测到多张卡片	
0xfb	TYPE A 防碰撞错误	
0xfa	TYPE A 选卡错误	
0xf9	TYPE A RATS 错误	
0xf8	Mifare one Auth 错误	
0xf7	TYPE B 寻卡错误	
0xf6	TYPE B attrib 错误	
0xf5	接收帧错误，要求重发	

附：卡片操作顺序

1.1 附 1：typeA CPU 卡操作顺序
1、TypeA 上电
2、APDU 命令

1.2 附 2：身份证
1、身份证寻卡
2、身份证选卡
3、身份证读卡

1.3 附 3：M1 卡操作顺序
1、TypeA 上电/获取 M1 卡物理卡号
2、认证密钥
3、读或写

1.4 附 4：4442/4428 卡片操作顺序
1 上电复位
2 认证
3 读或写

1.4 附 4：接触 CPU 卡操作顺序

1 冷复位
2 APDU 命令