文档编码：MT-YF-S610620-0028

通信协议

——充电桩读卡器底层通讯协议

文件状态： ［ ］草稿 [] 正式发布 ［ ］正在修改	文件标识：	
	当前版本：	1.0
	作　　者：	Lii
	完成日期：	2010-10-20

目录

一、更改记录

版本/状态	作者	参与者	起止日期	备注
1.0/N	Lii		2010-10-20	新建读卡器底层协议
1.1/A	Lii		2012-12-6	增加 MF1 部分协议的描述

N-->新建

M-->修改

A -->添加

二、规约定义

该协议有深圳市铭特科技有限公司定义，为读卡器与充电控制器之间的应用通信协议。

2.1、通讯格式

采用 RS232、全双工通讯方式,读卡器接收到完整数据包 10ms 后响应。
波特率: 默认 9600、数据格式: 1 位起始位，8 位数据位，1 位停止位。
数据帧之间的发送时间间隔>20ms。

2.2、通讯数据帧格式

表 2.1 数据包定义格式

序号	字节数	
1	1	STX
2	2	长度<LENGTH>
3	1	命令字
4	1	命令参数
5	LENGTH-2	数据
6	1	ETX
7	1	BCC

各字节定义详细请参考以下几节说明。

表 2.2 卡机返回数据包定义格式

序号	字节数	说明
1	1	STX
2	2	长度<LENGTH>
3	1	命令字
4	1	命令参数
5	1	状态字
6	LENGTH-2	数据
7	1	ETX
8	1	BCC

2.3、STX和ETX

定义发送开始字节 STX<x02>和 ETX<0x03>

2.4、长度<LENGTH>

发送长度<LENGTH>:长度<LENGTH>=命令字<1>+命令参数<1>+数据<length-2>
接收长度<LENGTH>:长度<LENGTH>=命令字<1>+命令参数<1>+状态字<1>+数据<length-2>

2.5、命令参数

表 2.2 命令参数定义表

命令	命令字CM	命令参数PM	描述
SIM卡	0x3d	0x40	复位(上电)
		0x41	
		0x42	休眠 (下电)
		0x43	APDU通信
		0x44	
射频 M1 卡操作	0x34	0x30	寻射频卡
		0x31	获取Mefare1 卡序列号
		0x32	验证Key_A密码
		0x39	验证Key_B密码
		0x33	读扇区块数据
		0x34	写扇区块数据
		0x35	更改密码
		0x37	增值操作
		0x38	减值操作
TYPE A CPU卡	0x34	0x40	激活射频卡(TYPE A)
		0x41	APDU通信(TYPE A)
		0x42	Deselect(TYPE A)
TYPE B CPU卡	0x35	0x40	激活射频卡(TYPE B)
		0x41	APDU通信(TYPE B)
		0x42	Deselect(TYPE B)

注：发送和接收命令字相同。

2.6、返回状态字

表 2.3 返回状态字定义表

命令	说明
0x59	命令操作成功
0x4E	命令操作失败

2.7、数据

根据不同的命令存不同的数据。具体参考下章节定义。

2.8、BCC数据异或校验

BCC 为数据帧的校验，算法为异或。校验区为 STX 至 ETX。

三、读卡器

此章针对读卡器的各个命令分析。

3.1 非接A卡

激活命令

HOST 发送：

0x02	0x00	0x02	0x34	0x40	0x03	BCC

READER 返回：

0x02	通讯包长度 2BYTE	0x34	0x40	操作状态 P	ATS 长度 H	ATS 长度 L	ATS 数据	0x03	BCC

操作状态字 P=‘Y’（0x59） 卡激活成功
P=‘N’（0x4E） 卡激活不成功
P=‘E’（0x45） 卡机内无卡 （610 型号）
P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

C-APDU应用命令

HOST 发送：

0x02	通讯包长度 2BYTE	0x34	0x41	APDU 包长度 H	APDU 包长度 L		APDU	0x03	BCC

READER 返回：

0x02	通讯包长度 2BYTE	0x34	0x41	操作状态 P	响应数据长度 H	响应数据长度 L	响应数据	0x03	BCC

操作状态字 P=‘Y’（0x59） APDU 成功
P=‘N’（0x4E） APDU 不成功
P=‘E’（0x45） 卡机内无卡 （610 型号）
P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

DESELECT命令

HOST 发送：

0x02	0x00	0x02	0x34	0x42	0x03	BCC

READER 返回：

0x02	通讯包长度 2BYTE	0x34	0x42	操作状态 P	0x03	BCC

操作状态字 P=‘Y’（0x59） DESELECT 成功
P=‘N’（0x4E） DESELECT 不成功
P=‘E’（0x45） 卡机内无卡 （610 型号）
P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

3.2 非接B卡

激活射频卡

HOST 发送：

0x02	0x00	0x02	0x35	0x40	0x03	BCC

READER 返回：

0x02	通讯包长度 2BYTE	0x35	0x40	操作状态 P	ATS 长度 H	ATS 长度 L	ATS 数据	0x03	BCC

操作状态字 P=‘Y’（0x59） 卡激活成功
P=‘N’（0x4E） 卡激活不成功
P=‘E’（0x45） 卡机内无卡 （610 型号）
P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

C-APDU应用命令

HOST 发送：

0x02	通讯包长度 2BYTE	0x35	0x41	APDU 包长度 H	APDU 包长度 L	APDU	0x03	BCC

READER 返回：

0x02	通讯包长度 2BYTE	0x35	0x41	操作状态 P	响应数据长度 L	响应数据长度 H	响应数据	0x03	BCC

操作状态字 P=‘Y’（0x59） APDU 成功
P=‘N’（0x4E） APDU 不成功
P=‘E’（0x45） 卡机内无卡 （610 型号）
P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

DESELECT命令

HOST 发送：

0x02	0x00	0x02	0x35	0x42	0x03	BCC

READER 返回：

0x02	通讯包长度 2BYTE	0x35	0x42	操作状态 P	0x03	BCC

操作状态字 P=‘Y’（0x59） DESELECT 成功
P=‘N’（0x4E） DESELECT 不成功
P=‘E’（0x45） 卡机内无卡 （610 型号）
P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

3.3 ESAM/PSAM卡

复位命令

HOST 发送：

0x02	0x00	0x03	0x3D	Pm	SIM 卡座号	0x03	BCC

Pm= 0x40 对工作电压是 3.0 V 的 SIM 卡进行复位操作
Pm= 0x41 对工作电压是 5.0 V 的 SIM 卡进行复位操作
Reader 操作成功返回： T=0 SIM 卡复位成功返回操作状态字 P=‘Y’（0x59）

0x02	通讯包长度 2 byte	0x3D	Pm	SIM 卡座号	操作状态字 P	复位数据包长度 2 byte	复位数据 n byte	0x03	BCC

通讯包长度=6+ 复位数据长度 n
Reader 操作成功返回： T=1 SIM 卡复位成功返回操作状态字 P=‘Z’（0X5A）

0x02	通讯包长度 2 byte	0x3D	Pm	SIM 卡座号	操作状态字 P	复位数据包长度 2 byte	复位数据 n byte	0x03	BCC

通讯包长度=6+ 复位数据长度 n
SIM 卡座号 =0x30 操作 SIM 卡 1
=0x31 操作 SIM 卡 2
=0x32 操作 SIM 卡 3 （610 型号）

=0x33 操作 SIM 卡 4 （610 型号）

Reader 操作失败返回：

0x02	0x00	0x04	0x3D	Pm	SIM 卡座号	操作状态字 P	0x03	BCC

操作状态字 P=‘N’（0x4E） 复位不成功

注：对 SIM 卡进行操作，只有复位成功后才能进行 C-APDU 包操作。使用 SIM 卡时请核对 SIM 卡工作电压，否则有可能损坏 SIM 卡。

下电命令

Host 发送:

0x02	0x00	0x02	0x3D	0X42	0x03	BCC

Reader 返回：

0x02	0x00	0x03	0x3D	0X42	操作状态字 P	0x03	BCC

操作状态字 P=‘Y’（0x59） 操作成功

P=‘N’（0x4E） 操作失败

P=‘E’（0x45） 卡机内无卡 （610 型号）

P=‘W’（0x57） 卡不在允许操作的位置上（610 型号）。

注：当卡不在有持卡位置上或不在卡机内时再执行 IC 卡下电命令时，将返回“卡不在允许操作位置”的信息上。

无 IC 卡机型执行 IC 卡下电命令时，读卡器将返回“命令不能执行”的信息,进行 IC 卡下电操作位无效。

C-APDU应用命令

0x02	通讯包长度 2 byte	0x3D	0x43	SIM 卡座号	C-APDU 包长度 2 byte	C-APDU 包 n byte	0x03	BCC

通讯包长度=5+ C-APDU 包长度 n (n=4--263byte)

Reader 操作成功返回： 操作状态字 P=‘Y’（0x59）

0x02	通讯包长度 2 byte	0x3D	043	SIM 卡座号	操作状态字 P	C-APDU 操作返回包长度 2 byte	C-APDU 操作返回包 n byte	0x03	BCC

通讯包长度=6+ C-APDU 返回包长度 n (n=4—263byte)

Reader 操作失败返回：

0x02	0x00	0x04	0x3D	0x43	SIM 卡座号	操作状态字 P	0x03	BCC

操作状态字 P=‘N’（0x4E） 操作不成功

3.4 射频M1卡操作

寻射频卡

HOST 发送：

0x02	0x00	0x02	0x34	0x30	0x03	BCC

READER 返回：

0x02	0x00	0x03	0x34	0x30	操作状态 P	0x03	BCC

操作状态字 P=‘Y’（0x59） 寻卡成功

P=‘N’（0x4E） 寻卡不成功

寻卡并获取序列号

HOST 发送：

0x02	0x00	0x02	0x34	0x31	0x03	BCC

READER 操作返回：

0x02	0x00	0x07	0x34	0x31	操作状态 P	4 byte hex 卡序列号	0x03	BCC

操作状态字 P=‘Y’（0x59） 获取卡序列号成功，并返回卡序列号

P=‘N’（0x4E） 获取卡序列号失败，并返回空序列号（0X00，0X00，0X00，0X00）

4byte 卡序列号用十六进制传送：如“ C6B272AE”

例：上传的通讯包为：0x02 0x00 0x06 0x35 0x31 0xC6 0xB2 0x72 0xAE 0x03 BCC

验证Key_A密码

HOST 发送：

0x02	0x00	0x09	0x34	0x32	扇区号	6 byte hex 密码	0x03	bcc

READER 操作返回：

0x02	0x00	0x04	0x34	0x32	扇区号	操作状态字 P	0x03	bcc

操作状态字 P=‘Y’（0x59） 下载密码成功

P=‘0’（0X30） 寻不到射频卡

P=‘3’（0X33） 密码错误

验证Key_B密码

HOST 发送：

0x02	0x00	0x09	0x34	0x39	扇区号	6 byte hex 密码	0x03	bcc

READER 操作返回：

0x02	0x00	0x04	0x34	0x39	扇区号	操作状态字 P	0x03	bcc

操作状态字 P=‘Y’（0x59） 验证密码成功

P=‘0’（0X30） 寻不到射频卡

P=‘3’（0X33） 密码错误

注： 扇区号= 0x00 ~0x28 （其中 S50 卡片扇区号是 0x00 ~0x0F，S70 卡片扇区号是 0x00 ~0x28）
块号= 0x00 ~0x0F （其中 S50 卡片每个扇区有 4 个地块，块号分别是 0x00 0x01 0x02 0x03，S70 卡片第 0-31 扇区中每一扇区有 4 个块，块号分别是 0x00 0x01 0x02 0x03，第 32-39 扇区每一扇区有 16 个块，块号分别是 0x00~0x0F）
要对扇区块数据进行读、写、值操作必须验证该扇区密码成功后才能进行。

读扇区块数据

HOST 发送：

0x02	0x00	0x04	0x34	0x33	扇区号	块号	0x03	BCC

当卡片为 S50 时，扇区号= 0x00~0x0F（S50 卡有 16 个扇区）

当卡片为 S70 时，扇区号= 0x00~0x28（S70 卡有 40 个扇区）

块号＝ 0x00 0x01 0x02 0x03 （S50 卡片块号,S70 卡片的块号=0x00~0x0F）

READER 读数据块操作成功返回： P=‘Y’（0x59）

0x02	0x00	0x15	0x34	0x33	扇区号	块号	操作状态字 P	16 byte 数据	0x03	BCC

读扇区块数据成功,并上传 16BYTE 读出的数据

READER 读扇区块操作错误返回：

0x02	0x00	0x05	0x34	0x33	扇区号	块号	操作状态字 P	0x03	BCC

操作状态字 P=‘0‘（0X30） 寻不到 RF 卡

P=‘1’（0X31） 操作扇区号错（不是验证密码后的扇区）

P=‘2’（0X32） 操作的卡序列号错

P=‘3’（0X33） 密码验证错

P=‘4’（0X34） 读数据错

注： 扇区号= 0x00 ~0x28 （其中 S50 卡片扇区号是 0x00~0x0F，S70 卡片扇区号是 0x00~0x28）
块号= 0x00 ~0x0F （其中 S50 卡片每个扇区有 4 个地块，块号分别是 0x00 0x01 0x02 0x03，S70 卡片第 0-31 扇区中每一扇区有 4 个块，块号分别是 0x00 0x01 0x02 0x03，第 32-39 扇区每一扇区有 16 个块，块号分别是 0x00~0x0F）

写扇区块数据

HOST 发送：

0x02	0x00	0x14	0x34	0x34	扇区号	块号	16 byte hex 数据	0x03	BCC

READER 写扇区块操作返回：

0x02	0x00	0x05	0x35	0x33	扇区号	块号	操作状态字 P	0x03	BCC

操作状态字 P=‘0 ‘（0X30） 寻不到 RF 卡

P=‘1’（0X31） 操作扇区号错（不是验证密码后的扇区）

P=‘2’（0X32） 操作的卡序列号错

P=‘3’（0X33） 密码验证错

P=‘4’（0X34） 校验写入块数据错

P=‘Y ‘（0X59） 操作成功

注： 扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00~0x0F，S70 卡片扇区号是 0x00~0x28）
块号= 0x00~0x0F （其中 S50 卡片每个扇区有 4 个地块，块号分别是 0x00 0x01 0x02 0x03，S70 卡片第 0-31 扇区中每一扇区有 4 个块，块号分别是 0x00 0x01 0x02 0x03， 第 32-39 扇区每一扇区有 16 个块，块号分别是 0x00~0x0F）
S50，S70 第 0-31 扇区中每个扇区的第 0X03 块，S70 第 32-40 扇区中第 0X0F 块是 KEYA、控制字、KEYB 的存储区域，对其进行写操作可能会遭成卡片锁死报废，需要谨慎操作，详见飞利浦 M1 卡片技术资料。

更改密码

执行该命令只能对 KEYA 的密码更改操作，并对 KEYB 密码的改写成：“0xFF, 0xFF, 0xFF,0xFF,0xFF,0xFF”同时控制字写成：“0xFF, 0x07, 0x80, 0x69” （卡片出厂的默认值）.。

HOST 发送：

0x02	0x00	0x09	0x34	0x35	扇区号	6 byte hex 密码	0x03	bcc

扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00~0x0F，S70 卡片扇区号是 0x00 ~0x28）

READER 返回：

0x02	0x00	0x04	0x34	0x35	扇区号	操作状态字 P	0x03	bcc

操作状态字 P=‘Y’（0x59） 更改密码成功

P=‘0‘(0X30) 寻不到 RF 卡
P=‘1’(0X31) 操作扇区号错（不是验证密码后的扇区）
P=‘2’(0X32) 操作的卡序列号错
P=‘3’(0X33) 密码验证错

要完全对扇区操作密码（KeyA 或 KeyB）和扇区存取控制字修改，在验证操作密码成功后对每扇区的块 3 进行写扇区块数据命令操作来完成。其格式如下（详见飞利浦 M1 卡片技术资料）：

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
6 byte KeyA 密码字节						4 byte 扇区存取控制字				6 byte KeyB 密码字节					

初始化值

如果区块要就进行值操作，在第一次使用之前要对要进行值操作的区块初始化。
HOST 发送：

0x02	0x00	0x08	0x34	0x36	扇区号	块号	4 byte hex 数据	0x03	BCC

READER 返回：

0x02	0x00	0x05	0x34	0x36	扇区号	块号	操作状态字 P	0x03	BCC

4 byte hex 数据为指定的扇区的指定块的初始化的值（低字节在前高字节在后）。如第 5 扇区块 0 初始化为 0x10，发送的 4 byte hex 数据为：“ 0x10, 0x00, 0x00, 0x00 ”

操作状态字
P=‘1’(0X31) 操作扇区号错（不是验证密码后的扇区）
P=‘3’(0X33) 密码验证错
P=‘Y’(0x59) 操作成功
P=‘Y’(0x4E) 操作失败

扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00 ~0x0F， S70 卡片扇区号是 0x00 ~0x28）
块号= 0x00 ~0x0E （其中 S50 卡片块号范围是 0x00--0x02，S70 卡片第 0-31 扇区块号范围是 0x00--0x02，第 32-39 扇区块号范围是 0x00 ~0x0E）
每一扇区的最后一块不能进行值操作。

增值操作

HOST 发送：

0x02	0x00	0x08	0x34	0x37	扇区号	块号	4 byte hex 数据	0x03	BCC

4 byte hex 数据为指定的扇区的指字块的值要增加的值（低字节在前高字节在后）。如第 5 扇区块 0 要增加 0x10，发送的 4 byte hex 数据为：“ 0x10, 0x00, 0x00, 0x00 ”

READER 返回：

0x02	0x00	0x05	0x34	0x37	扇区号	块号	操作状态字 P	0x03	BCC

操作状态字 P=‘0‘(0X30) 寻不到 RF 卡

P=‘1’（0X31） 操作扇区号错（不是验证密码后的扇区）

P=‘2’（0X32） 操作的卡序列号错

P=‘3’（0X33） 密码验证错

P=‘4’（0X34） 块数据格式错误（该块存贮数据没有写成值数据形式）

P=‘5’（0X35） 增值溢出

P=‘Y’（0x59） 操作成功

扇区号= 0x00~0x28 （其中 S50 卡片扇区号是 0x00 ~0x0F， S70 卡片扇区号是 0x00 ~0x28）

块号= 0x00 ~0x0E （其中 S50 卡片块号范围是 0x00 0x01 0x02， S70 卡片第 0-31 扇区块号范是 0x00 0x01 0x02， 第 32-39 扇区块号范围是 0x00 ~0x0E）

每一扇区的最后一块不能进行增减值操作。

减值操作

HOST 发送：

0x02	0x00	0x08	0x34	0x38	扇区号	块号	4 byte hex 数据	0x03	BCC

4 byte hex 数据为指定的扇区的指字块的值要减的值（低字节在前高字节在后）。不允许为 0 值，否则操作不成功。

READER 返回：

0x02	0x00	0x05	0x34	0x38	扇区号	块号	操作状态字 P	0x03	BCC

操作状态字 P=‘0‘（0X30） 寻不到 RF 卡

P=‘1’（0X31） 操作扇区号错（不是验证密码后的扇区）

P=‘2’（0X32） 操作的卡序列号错

P=‘3’（0X33） 密码验证错

P=‘4’（0X34） 块数据格式错误（该块存贮数据没有写成值数据形式）

P=‘5’（0X35） 减值溢出

P=‘Y’（0x59） 操作成功

扇区号= 0x00 ~0x28 （其中 S50 卡片扇区号是 0x00 0x01 0x02 ……0x0F， S70 卡片扇区号是 0x00 0x01 0x02 ……0x28）

块号= 0x00 ~0x0E （其中 S50 卡片块号范围是 0x00 0x01 0x02，S70 卡片第 0-31 扇区块号范是 0x00 0x01 0x02，第 32-39 扇区块号范围是 0x00 ~0x0E）,每一扇区的最后一块不能进行增减值操作。