RF-POS Specification

Version 5.0

文档版本号：**1.0.5**

2008 年 07 月

目录

01. 帧类别及命令收发

01.01. 帧格式

帧类别(1 Byte)	帧长度(1 Byte)	帧数据(N byte)	可选效验和(累加和 + 异或和)

注:

帧类别的 Bit0 为帧长度的扩展，帧长度最大可为 0x104（帧数据长度）。
帧类别的 Bit1 为帧是否带效验和，1 为带校验和。
校验和的格式:累加和+异或和。

01.02. 帧类别

帧类别值	用途	备注
80	发往 RF-POS 的 APDU 指令	指令只作用于 RF-POS 本身
90	APDU 响应	
B0	被动消息	
A0	发往 RF-UIM 的 APDU 指令	指令经 RF-POS 转发给远端的 RF-UIM 并作用于 RF-UIM
70	ID 卡刷卡时用	纯 ID(ID 刷卡)
68	读取照片	照片结束(照片传送结束)
60	读取照片	照片(数据)
E0	操作 PSAM 卡	操作外接的 PSAM 卡

01.03. 命令收发

先发,如下所示：

帧类别	帧长度	帧数据
80	05	90E6000008

如：800590E6000008

后收：

帧类别	帧长度	帧数据
90	0A	11223344556677889000

如：900A11223344556677889000

帧数据里一般是 APDU 指令数据或 APDU 响应数据，响应数据的最后两个字节是状态字。

01.04. 状态字

响应数据的最后 2 个字节是状态字，常用状态字如下表：

SW	说明
9000	成功
9C02	RF 已经连接上
9C03	RF 没有连接上

01.05. 校验和

校验和是可选的，如有校验和为 2 个字节，校验和字节数不包括在帧长度内

	说明
Check1	帧数据的累加和
Check2	帧数据的异或和

02. RF 接口

02.01. RF 参数

在 RF-POS 内部，有下述一个结构数据块控制 RF 的行为：

Field	Len	Value	Note
SelectID	8		指定连接卡 ID,在 Flag 的指定 ID 方式时启用,拷贝卡号 8 字节,只有低 5 字节有效
nR1	1	0x00	保留
Term	1	0x00	00::连接失败后不继续重新连接 01:连接失败后继续重新连接
Channel	1	0x01	数据通讯频道（保留频道不对外开放,具体见.频道定义表）
Delay	1	0x00	刷卡之间的延迟时间，以 100ms 为单位（若此时间小于当前刷卡速度下的刷卡间隔则忽略）
FireFlag	1	SHNM100,SHR600, SHNM202 类型读头一定要有 0x08	感应方式： 0x01：取 ID(普通模式) 0x02：取 ID(汽车模式) 0x08：功率敏感(FAM 模式) 0x10： SelectID 是指定对象 CardID 的低 5 字节 0x20：修正手机灵敏度
FireMode	1	0x00	SHR200 读头近距离时为 0x02 其它情况为 0x00
nR2	1	0x00	保留
FirePower	1	0x00-0x03	Fire 包发送功率(缺省值为 0x03)
nR3	1	0x00	保留
Applet	1		00 无默认应用 0xA0 广播器 0xA1 门禁控制器 0xA2 Accounter 0xA3 Merchant 0xA5 高速公路收费 0xA6 我的 E 券
Select	1	0x00	选择 RF 通道(0:基本应用 ; 1:扩展应用如卡商的 PBOC 应用)
Collision	1	0x00	多卡防冲突掩码 bit 的个数(取值范围:0~8,其中 0:表示不防冲突,1~8 表示掩码为 0x01~0xff,能扫描 1~255 范围的 POS,但是同一个卡的扫描时间变长了.)
Message	1	0x00	连接和断开时用消息通知上层（0：表示不通知，1：表示通知）
nR4	1	0x00	保留
nR5	1	0x00	保留
nR6	1	0x00	保留

02.02. 打开 RF

Describe：

打开读头的 RF 功能，以便能够连接上 RF-UIM 卡。

Detail:

Field	Len	Value	Note
Class	1	90	
Ins	1	B0	Reader 指令
P1	1	01	打开 RF
P2	1	00	80:保存 RF 设置到 E2(后面要跟 RF 配置数据);否则不保存
Lc	1	00 或 18	00:不带 RF 配置参数，使用内部缺省的参数 18:带 RF 配置参数,具体格式见 RF 参数表 02.01 **例如操作 PBOC 的完整指令：** 90 B0 01 00 18 00 00 00 00 00 00 00 00 00 00 00 08 00 00 03 00 00 **01** 00 00 00 00 00

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

如果 RF-POS 的默认应用在 RF 连接后有自动执行功能，此命令会使其失效，故发送此命令后需重新选择应用连接成功后，如果连续 5 秒没有收到命令，则会自动断开本次连接，之后根据参数决定是否自动重连。

说明：请注意如果需要修改默认的参数，请先读出，然后只修改要改的部分，然后再写入。

02.03. 断开 RF

Describe：

关闭 POS 的 RF，确保与当前的 RF-UIM 卡完全断开连接

Detail:

Field	Len	Value	Note
Class	1	90	

Ins	1	B0	Reader 指令
P1	1	00	断开 RF
P2	1	00	
Lc	1	00	

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

02.04. 读取 RF 配置参数

Describe:

关闭 RF

Detail:

	Len	Value	Note
Class	1	90	
Ins	1	B0	Reader 指令
P1	1	03	读取 RF 配置参数
P2	1	00	
Lc	1	00	

Return:

返回数据参见 RF 参数(格式见 02.01)

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

02.05. 查询 RF

Describe：

查询是否与某个 RF-UIM 卡连接成功。

Detail:

Field	Len	Value	Note
Class	1	90	
Ins	1	B0	Reader 指令
P1	1	04	查询 RF
P2	1	00	这个值保留为 0，对于双频读头可以用来设置询卡方式： 1：0x52 寻卡模式要求操作的卡在读写完成后卡片只需关闭后又可读写 2：0x26 寻卡模式要求操作的卡在读写完成后要离开感应区才能再读写
Lc	1	00	

Return:

Field	Len	Value	Note
状态字	2	9C02	这个状态字是兼容老的直接读第一个返回数据的程序
卡类型和数据长度	1	XX	通道类型在高 4bit。卡类型如下： 1:：2.4G 4：Mifare (iso1443a)(必须读头上有支持 13.56M 的硬件) 低 4bit 表示卡号字节数+1（UID）： 5 或 9 字节，其他目前未用
卡号（UID）	XX	XXXX….	连接卡的卡 ID（长度在前一字节的低 4bit 指示数减一） 目前 2.4G 卡的 ID 是 8 字节，Mifare 是 4 字节
ATQA	2	XXXX	卡类型 0x0400 = Mifare_One(Mifare One S50) 0x0200 = Mifare_One(S70) 0x0800 = Mifare_Pro(X) 0x4400 = Mifare_UltraLight 0x4403 = Mifare_DESFire 这个数据由 Mifare 卡给出，请参见 Mifare 卡的芯片资料（2.4G 卡没有这个数据项）
SAK	1	XX	08：MifareOne，

			28：Mifae cpu 卡 这个数据也是 Mifare 卡给的，请参见 Mifare 卡的芯片资料（2.4G 卡没有这个数据项）

SW:

SW	Note
9C02	RF 已经连接上
9C03	RF 没有连接上
	其它请参考【常见状态字定义】

Notes:

此指令发送之后只表示本次查询的结果。实际使用中需要不断的发送本指令(间隔 100ms)。
注意：Mifare 操作不能使用此指令来寻卡。

02.06. 取连接数据

Describe：

取 RF 连接后的相关数据(本指令可以获取 RF-UIM 卡的 ID 号码)

Detail:

	Len	Value	Note
Class	1	90	
Ins	1	B0	Reader 指令
P1	1	05	取连接数据
P2	1	00	
Lc	1	00	

Return:

Field	Len	Value	Note
TermID	8		RF-POS 的 ID
Random	8		本次连接的随机数
保留	4		保留
	1		保留
	1		保留
	1		保留
	1		保留
	1		RF 连接状态: 零-未连接; 非零:RF 已经连接,这个值表示 RF 连接的序列号
	1		保留
	6		
	24		保留

CardID	8		RF-UIM 的 ID 号码(全球唯一编号)

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

02.09. 读取 POS 时间

Describe:

控制 Reader 的蜂鸣器

Detail:

	Len	Value	Note
Class	1	90	
Ins	1	B0	Reder 指令
P1	1	10	设置 POS 的时间
P2	1	00	
Lc	1	00	

Return:

Field	Len	Value	Note
秒	1	XX	
分	1	XX	
时	1	XX	
星期几	1	0X	(1~7:代表:周日,周一,周二……周六的顺序)
日	1	XX	
月	1	XX	
年	1	XX	以 2008 年对应 00,2009 对应 01……..

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

1:硬件配置问题:
(1)当 POS 有硬件 RTC 时时间保存到硬件 RTC 电路,POS 重新上电时间不会丢失.
(2)当 POS 没有硬件 RTC 时采用模拟计时,POS 控制端(PC 或其他主机)至少要在一天内再次设置时间,软件会在设置后的时间基础上继续计时,掉电后时间丢失.
2:BCD 码的格式:
比如:10 进制的 44 秒对应的 BCD 码格式是 16 进制的 44
例如: 2008 年 7 月 14 日星期一 10 点 40 分 55 秒对应的数据为:55 40 10 02 14 07 00
上面数据的每个字节对应的格式为:秒/分/时/星期几/日/月/年

3:星期几的 1~7 对应周日开始到周六
4:年的对应时间从 2008 年起始.

02.10. 收发指令

前面的几个指令都是 RF-POS 的本地指令，只作用于 RF-POS 自身，要将其它的 APDU 指令发往远端的 RF-UIM 并收回响应数据及状态字,必须注意将帧类别设为 A0。参见:帧类别及命令收发

先发,如下所示：

帧类别	帧长度	帧数据(APDU 指令)
A0	05	90E6000008

后收：

帧类别	帧长度	帧数据(APDU 响应)
90	0A	11223344556677889000

帧数据里是 APDU 指令数据或 APDU 响应数据

02.11. 读取 POS 版本

Describe:

读取 POS 的版本数据

Detail:

	Len	Value	Note
Class	1	90	
Ins	1	B0	Reder 指令
P1	1	12	设置 POS 的扩展配置参数

P2	1	00	
Lc	1	14	要读取数据的长度

Return:

Field	Len	Value	Note
第一版本号	1	XX	主版本号
第二版本号	1	XX	从版本号
第三版本号	1	XX	次版本号
保留	1	XX	
编译时间	4	XXXXXXXX	4 字节小端在前存储,表示,例如: 0801020d 表示 2008 年 1 月 2 日 13 日
保留	12		

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

02.12. 卡商应用却换

Describe:

切换到卡商的其他应用;

Detail:

	Len	Value	Note
Class	1	90	
Ins	1	B0	Reder 指令
P1	1	17	设置 POS 的扩展配置参数
P2	1	XX	XX -0:elitel XX -1：卡商
Lc	1	00	

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

03. Message 接口

在 RF 工作过程中，RF-POS 可主动向主机提供一些消息，这种特性可方便主机应用程序的开发。要得到 Message，必须配置 RF 参数中的 Message 字段为 1。

03.01. 连接消息

Field	Len	Value	Note
消息类型	1	00	0: 表示连接成功。
CardID	8	00	RF-UIM 卡 ID 号码（全球唯一编号）。

03.02. 断开消息

Field	Len	Value	Note
消息类型	1	01	1: RF 断开
保留	8	00	保留

03.03. RF-POS 消息开关

Describe：

设置 RF-POS 主动连接 RF-UIM 卡功能。

Detail:

Field	Len	Value	Note
Class	1	90	
Ins	1	B0	
P1	1	19	
P2	1	00 or 01	01：打开消息功能　00：关闭消息功能
Lc	1	00	

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

04. 常用指令

下面是一些基础指令，有些其它的指令需要这些指令配合。

04.01. 取随机数

Describe：

取随机数(根据帧类别的不同，获取的对象可以是 RF-POS 和 RF-UIM 卡)

Detail:

Field	Len	Value	Note
Class	1	90	
Ins	1	E6	
P1	1	00	
P2	1	00	
Lc	1	XX	获取的随机数长度

Return:

Field	Len	Value	Note
Random	XX		随机数

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

XX 不能大于 10

04.02. 显示单文本

Describe：

用于 UTK 显示单文本(执行成功之后在手机上显示指令中的文本信息)

Detail:

	Len	Value	Note
Class	1	90	
Ins	1	F8	

P1	1	01	
P2	1	00	
Lc	1	XX	
Data	XX		文本内容(UTK 字符串)，请参照说明

Return:

无

SW:

SW	Note
9000	执行成功
9A32	忙

Notes:

此命令应发向 RF-UIM 卡**(帧类别为 0XA0)**。

说明：文本内容请参照如下格式：
长度+编码(0x80：UCS-2 编码；0x00：ASCII 编码)+文本内容
列如：
A0 0F 90 F8 01 00 0A 08(数据长度) 80(UCS-2 编码) 6F 14 79 3A 4F E1 60 6F(演示信息)

04.03. 修改波特率

Describe:

修改 pos 的波特率

Detail:

Field	Len	Value	Note
Class	1	90	
Ins	1	B0	Reader 指令
P1	1	1F	修改波特率
P2	1	xx	xx 波特率的索引值(00：115200, 01：38400, 02：19200, 03：9600, 04：57600)
Lc	1	00	

Return:

Field	Len	Value	Note
index	1	xx + 0x10	波特率的索引值

SW:

SW	Note
90 00	命令操作成功
9A 10	索引值超出范围

Notes:

注：POS 只有 05.05.19 以后的版本才兼容该指令

04.04. 设置 Mifare 应用 ID

Describe:

设置 RF-Pod 内，用于连上卡后自动选择的 MifareID

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	0C	
P1	1	04	
P2	1	00	
Lc	1	0C	
Data	12	XX	修改读头缺省 AID

Return:

无

SW:

SW	Note
9000	命令操作成功
9A24	此功能已被锁

Notes:

注：设置时 Mifare 接口需为解锁状态，POS 只有 05.05.19 以后的版本才兼容该指令

05. Mifare 接口

RF-UIM 卡内部有一张或多张逻辑加密卡，它与 Mifare 1K 及 Mifare 4K 兼容，并在此基础上对其进行了扩展，如空中充值接口、自动生成交易记录等。

RF-POS 支持 Mifare 接口，需使用 Accounter 应用，且类别为“外部主机”。为了方便应用开发和密钥管理，RF-POS 在内部提供相应的 Sam 功能，一方面，解决了密钥管理，另一方面也降低的应用开发难度，下面是操作 Mifare 接口的相关的数据结构和控制命令。

说明：针对建设部标准的 Mifare 或者定制的 Mifare，Mifare 卡头结构功能相应的要弱化，具体请参照定制的附加说明文档。

在 Mifare 接口中所用到的结构：

A. DataMifare_Head（RF-UIM 卡上 Mifare 应用头结构）

Field	Len	Value	Note
ServerNo	4	0x00	OTA 序列号
Reserved	8		保留
Sector	1	0x10（16 或 40）	扇区数
Flag	1	0x83 **(建议不要修改)**	属性（位标识） 0x01：允许空中充值 0x02：记录消费记录 0x04：允许一直透支 0x08：允许一次透支 0x80：消费额度菜单
Lock	1	0x00	冻结 0x01：冻结 0x00：未冻结
Remote	1	0x00	远程开关 0x01：开 0x00：关
Trade_Sector	**1**	**0x0A (建议不要修改)**	**交易记录所在的起始扇区（应在钱包所在扇区之后）**
Trade_Count	**1**	**0x09 (建议不要修改)**	**交易记录所占用的块数**
Trade_Index	1		交易记录循环索引
Money	**1**	**0x02 (建议不要修改)**	**金额单位（小数点位数）**
SmsNo	12		短消息中心

特别说明：缺省的 Mifare 应用，第 10，11，12 共 3 个扇区用来存放交易记录，请在规划扇区的时候避开这 3 个扇区。

A.1 读 Mifare 应用头结构指令

Field	Len	Value	Note
Class	1	40	
Ins	1	06	
P1	1	00	
P2	1	00	
Lc	1	20	
Data	00	00	

Return:

块的 32 个字节 Mifare 应用头结构

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

A.2 写 Mifare 应用头结构指令

Field	Len	Value	Note
Class	1	40	
Ins	1	06	
P1	1	04	
P2	1	00	
Lc	1	20	
Data	32	XX	Mifare 应用头应用结构。

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

特别说明：在使用【A.2 写 Mifare 应用头结构指令】之前，必须先使用【A.1 读 Mifare 应用头结构指令】，获取目前的应用头数据内容，然后在做相应的修改。

B. DataAccounter_Head（RF-POS 上 Accounter 应用头结构）

Field	Len	Value	Note
Mifare_ID	12	Mifare App（缺省值）	Mifare 钱包的应用号，RF-POS 用来自动选择卡上应用
Value	4		自动扣款值（Type 为 80 时使用）
License_Inc	4		加钱许可
License_Dec	4		扣钱许可
Type	1	0x00 (建议不要修改)	0x 00：外部主机 0x 01：外部主机 1 0x 02：外部主机 2 0x 03：外部主机 3 0x80：直接按 nValue 扣一次款 0x81：欢迎程序(Beep) 0x82：发(写)优惠券 0x83：取(读)优惠券

			0x84：输出 SIM 卡 ID 0x85：输出维根ID 0x86：输出 Wap Url 0x87：输出 Sms 0x88：售货机 0x89：外部超快刷卡触发器 0x8A ： Syris485 **请确认该值为 0x00**
Delay	1	0x00	同一张卡两次刷卡之间的间隔 （因 RF 参数已有，该字节未使用）
Attribute	1	0x00	属性（位标识） 0x01：使用前需要密码认证 0x02：Inc 需要 License 0x04：Dec 需要 License 0x08：AB 密钥分散
Lock	1	0x00	0x01：锁定 0x00：未锁定
Sector_No	1		自动扣款钱包所在扇区号(Type 为 80 使用)
Sector_AB	1	0x03	A、 B 密钥使用权限（位标识） 0x01：允许使用 A 密钥认证 0x02：允许使用 B 密钥认证
Block_Burse	1		自动扣款钱包所在块号(Type 为 80 时使用)
Block_Record	1		信息块

B.1 读 RF-POS Mifare 应用头结构指令

Field	Len	Value	Note
Class	1	40	
Ins	1	0C	
P1	1	82	
P2	1	00	
Lc	1	20	
Data	00	00	

Return:

块的 32 个字节 RF-POS Mifare 应用头结构

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

B.2 写 RF-POS Mifare 应用头结构指令

Field	Len	Value	Note

Class	1	40	
Ins	1	0C	
P1	1	00	
P2	1	00	
Lc	1	20	
Data	32	XX	RF-POS Mifare 应用头应用结构。

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

特别说明：在使用【B.2 写 RF-POS Mifare 应用头结构指令】之前，最好先使用【B.1 读 RF-POS Mifare 应用头结构指令】，获取目前的应用头数据内容，然后在做相应的修改。

05.01. 选择 Accounter 应用（Select）

Describe：

选择 RF-POS 的 Accounter 应用 (Mifare 的电子钱包一定要使用本条指令)

Detail:

Field	Len	Value	Note
Class	1	A0	

Ins	1	A4	
P1	1	04	
P2	1	00	
Lc	1	10	
Data	16	Accounter App	值为字符串，不足 16 字节的补零

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

Mifare 的其它操作功能必须在激活 Accounter 应用后才能使用。 如果默认应用是 Accounter（可以通过 RF 参数查看，见 02 RF 接口），则不用选择，但是如果使用了带参数打开 RF 命令时，参数没有指定 Accounter 应用，则必须使用本指令。

05.02. 读取 Mifare 接口的配置参数（Report）

Describe：

读回 RF-POS 内 Mifare 接口，返回 32 个字节。最前 12 个字节为 AID。

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	0C	
P1	1	82	
P2	1	00	
Lc	1	00	

Return:

SW:

SW	Note
9000	命令操作成功

9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

此指令需要执行了【05.01.　选择 Accounter 应用】指令之后执行。

05.03.　初始化 Mifare 接口（Format）

Describe：

初始化 RF-POS 内 Mifare 接口。可以用来修改读头缺省的 AID，使之和卡片对应的 Mifare 匹配。
特别注意：操作执行请一定要先执行【05.02 读取 Mifare 接口的配置参数（Report）】这个指令。然后只需要修改最前面的 12 个字节，其它的不要改动(以后的读头会有一个专门的指令来修改)。

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	0C	
P1	1	00	
P2	1	00	
Lc	1	20	
Data	20	XX	

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

确保 Mifare 接口为解锁状态，且必须被初始化后才能正常工作，成功后需锁定。参见 12.06

05.04. 设置 AB 密钥（SetAB）

Describe：

加载 RF-POS 内 Mifare 接口保存的某扇区的 AB 密钥及控制字(完整的控制块内容)

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	0C	
P1	1	02	
P2	1	XX	对应 Mifare 扇区的控制块
Lc	1	10	
Data	16	XX	格式为：A 密钥(6 BYTE) Ctrl (4 BYTE)B 密钥(6 BYTE)

Return:

无

SW:

SW	Note
9000	命令操作成功
9A24	此功能已被锁
9C00	目标不存在(扇区号太大)

Notes:

设置时 Mifare 接口需为解锁状态

05.05. 分配卡头和卡号（Asign）

Describe：

给空卡分配与 Mifare 兼容的卡头和卡号,初始化 Mifare 第 0 个扇区第 0 块

Detail:

Field	Len	Value	Note

Class	1	40	
Ins	1	06	
P1	1	02	
P2	1	00	00
Lc	1	10	
Data	16		

Return:

无

SW:

SW	Note
9000	命令操作成功
9A24	卡被冻结

Notes:

需要寻卡成功后，方可修改成功！

05.06. 查询（Request）

Describe:

Mifare 专用的寻卡指令(类似于 RF-POS 封装的一套寻找 Mifare 应用的指令)

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	0A	
P1	1	00 or 80	80：重新启动**(尽量少用 80)**
P2	1	00	
Lc	1	00	

Return:

当返回状态字为 9000 时 **电信集团规范:** 成功：90 28 Data 90 00 失败：90 02 9C 00 Data：

内容	长度（byte）	备注
卡号	4	Mifare 卡号
黑名单	1	公共信息区的黑名单标志
保留	1	
发行数据	32	发行区 0、1 块数据

普通的卡:

成功：90 12（0 扇区 0 块的 16 字节数据）90 00

失败：90 02 9C 00

说明： 如果返回 0x9C03，那么需要延时 100MS 再重发寻卡指令。

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

此指令发送之后只表示本次查询的结果。实际使用中需要不断的发送本指令(间隔 100ms)。

05.07. 认证（Authentication）

Describe:

对卡的某个扇区进行认证。
使用 POS 内部密钥认证时，如果 AB 密钥分散功能打开了，则 RF-POS 使用内部分散算法产生与卡号相关的 A,B 密钥，否则直接使用内部密钥认证。

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	08	
P1	1	XX	扇区号
P2	1	00-01	00：B, 01：A
Lc	1	00 or 06	00：使用 POS 内部密钥认证，06：使用指令所含密钥认证
Data	0 or 6		Lc 为 6 时，填密钥 A 或 B 的值

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

认证后 5 秒内如果无命令，会因连接自动断开导致本次认证失效，参见 6.2 说明

05.08. 读块数据（Read）

Describe:

读卡的某个块

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	02	
P1	1	01	
P2	1	XX	块号（已认证扇区内相对块号，非总块号）
Lc	1	00	

Return:

块的 16 个字节

SW:

SW	Note
9000	成功

Notes:

无

05.09. 写块数据（Write）

Describe：

写卡的某个块

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	02	
P1	1	02	
P2	1	XX	（已认证扇区内相对块号，非总块号）
Lc	1	10	
Data	16		块数据

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

05.10. 加值（Increment）

Describe：

加值

Detail:

Field	Len	Value	Note
Class	1	40	

Ins	1	02	
P1	1	03	
P2	1	XX	（已认证扇区内相对块号，非总块号）
Lc	1	10	
Data	4	XX	要充值的金额
	4	XX	日时分秒，BCD 格式
	4	XX	机具号
	1	88	充值(请参考建设部 M1 交易类型编码)
	1	01	交易进度标志(开始标志)
	2	XX	保留

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

05.11. 减值（Decrement）

Describe:

减值

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	02	
P1	1	04	
P2	1	XX	（已认证扇区内相对块号，非总块号）
Lc	1	10	
Data	4	XX	要减值的金额
	4	XX	日时分秒，BCD 格式

	4	XX	机具号
	1	01	公交消费(请参考建设部 M1 交易类型编码)
	1	01	交易进度标志(开始标志)
	2	XX	保留

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

05.12. 复制（Restore）

Describe:

复制钱包块的内容到钱包备份块(需要有 DEC 指令权限，只能在钱包块之间使用)。

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	02	
P1	1	05	
P2	1	XX	（已认证扇区内相对块号，非总块号）
Lc	1	00	

Return:

无

SW:

SW	Note
9000	命令操作成功

9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

无

05.13. 传送（Transfer）

Describe:

加值，减值，复制指令的配套指令

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	02	
P1	1	06	
P2	1	XX	（已认证扇区内相对块号，非总块号）
Lc	1	00 或 07	为 07 时带时间，用于交易记录
Data	0 或 7	XXXXX	BCD 码，依次为秒，分，时，星期(未用)，日，月，年(减 08) 如 2008-9-1 10:58:30 为 30 58 10 XX 01 09 00

Return:

返回传送块的数据（比如返回钱包块数据）。

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

说明：自动产生交易记录的格式(建设部或其它定制 Mifare 不适用)： Long Int：Date(交易时间) + Long Int：Value(交易金额) + Byte (交易类型: 02 消费，03：充值) + Byte (绝对块号) + 6Byte(POS ID) Date: 从 2008 年开始计算(比如：2009-2008)，具体的格式如下： Year ：6bit (最高位)

Month ： 4bit
Day ： 5bit
Hour ： 5bit
Minute ： 6bit
Second ： 6bit

05.14. 中断（Halt）

Describe：

断开 RF 连接

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	04	
P1	1	80 或 00	80 完全关闭 RF；00 先断开 RF，然后 RF-POS 再开启 RF
P2	1	00	
Lc	1	00	

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

建议采用 P1 为 0X80(完全关闭的模式)，RF-POS 是否开启 RF 有流程来控制。

05.15. 钱包名称（UTK Name）

Describe：

UTK 钱包名称(主要描述钱包名称的格式以及 UTK 显示的条件)

钱包名块一定要放在钱包块的下一块(比如钱包块放在第 0 块，那钱包名块一定要放在第 1 块)

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	02	
P1	1	02	写数据块
P2	1	XX	钱包名存放的位置块(已认证扇区内相对块号，非总块号)
Lc	1	10	16 字节的块数据,也就是钱包数据; 钱包名称须转化成 UIM 卡的字符串， 数据格式：E8 20 **XX** (00/80) **XXXX** 0 E8 钱包名称格式 1 20 钱包类型 2 XX 转换后的钱包数据长度 3 00 or 80 数据编码(00:ASCII, 80：UCS-2 编码 。。。 转换后的钱包数据 15 **特别说明：钱包名称必须放在钱包块的下一块(或者说 UTK 自动会寻找钱包块的下一块是否满足钱包名称的格式要求)**

Return:

无

SW:

SW	Note
9000	命令操作成功
9A03	通讯错误
	其它请参考【常见状态字定义】

Notes:

如果钱包块的下一块要内部使用，请一定不要和钱包名称定义的格式冲突，否则可能 UTK 看到的钱包名有可能是乱码(因为符合钱包名格式，可是钱包名内容不符合字符串格式)。

06．13.56MHz Mifare One 接口 （硬件双频读头、软件 V6 以上 ）

说明：这些指令只有在盛华双频读头，型号(SHRM202)的读头上，才可以正确的执行。

06.01．向支持 ISO1443A-4 的卡发送 RATS 指令

Describe：

发送 RATS 指令；

Detail:

向支持 ISO1443A-4 的卡发送 RATS 指令，读取卡的复位信息。

Field	Len	Value	Note
Class	1	40	
Ins	1	50	RATS 指令（向支持 iso1443a-4 的卡 前面 13.56M 选卡指令或联合询卡指令 90b004xx00 返回的 SAK 数据位 2X 的卡支持这个协议）
P1	1	0X	低 4bit 表示要设定该卡的 CID（为 0 表示不选定）
P2	1	00	
Lc	1	00	
Data	0		

Return:

卡的 ATS 数据（复位数据参见 iso1443a-4）

SW:

SW	Note
XXXX	其他卡的响应
9a12	传送错误（执行超时没有得到响应）
9000	成功

Notes:

06.02．Tranceive_Cos_Apdu 指令

Describe：

此指令可以做为相应卡的指令的转发通道；

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	53	把上层的指令和数据转发到卡（有把上层数据打包）
P1	1	XX	指定 CID（当卡不支持时，读头把这个标志清掉）
P2	1	XX	指定 AID（当卡不支持时，读头把这个标志清掉）
Lc	1	XX	13.56M 传输到卡的指令及数据的总长度
Data	Lc		13.56M 传输到卡的指令及数据

Return:

指令执行的数据和结果

SW:

SW	Note
XXXX	其他卡的响应
9a12	传送错误（执行超时没有得到响应）

Notes:
这条指令把读头当做 13.56M 的透明传输通道，向卡传输指令。（执行条件是在卡的 SELECT 之后执行，且卡也要支持 iso1443-4 协议层）

06.03. 取消选择指令

Describe:

停止选卡操作， 必须调用这条指令，才可以重新寻卡；

Detail:

Field	Len	Value	Note
Class	1	40	
Ins	1	51	取消选择 Deselect 指令和前面的选卡 Select 指令相对
P1	1	XX	低 4bit 指定 CID
P2	1	00	
Lc	1	00	
Data	0		

Return:

指令执行结果

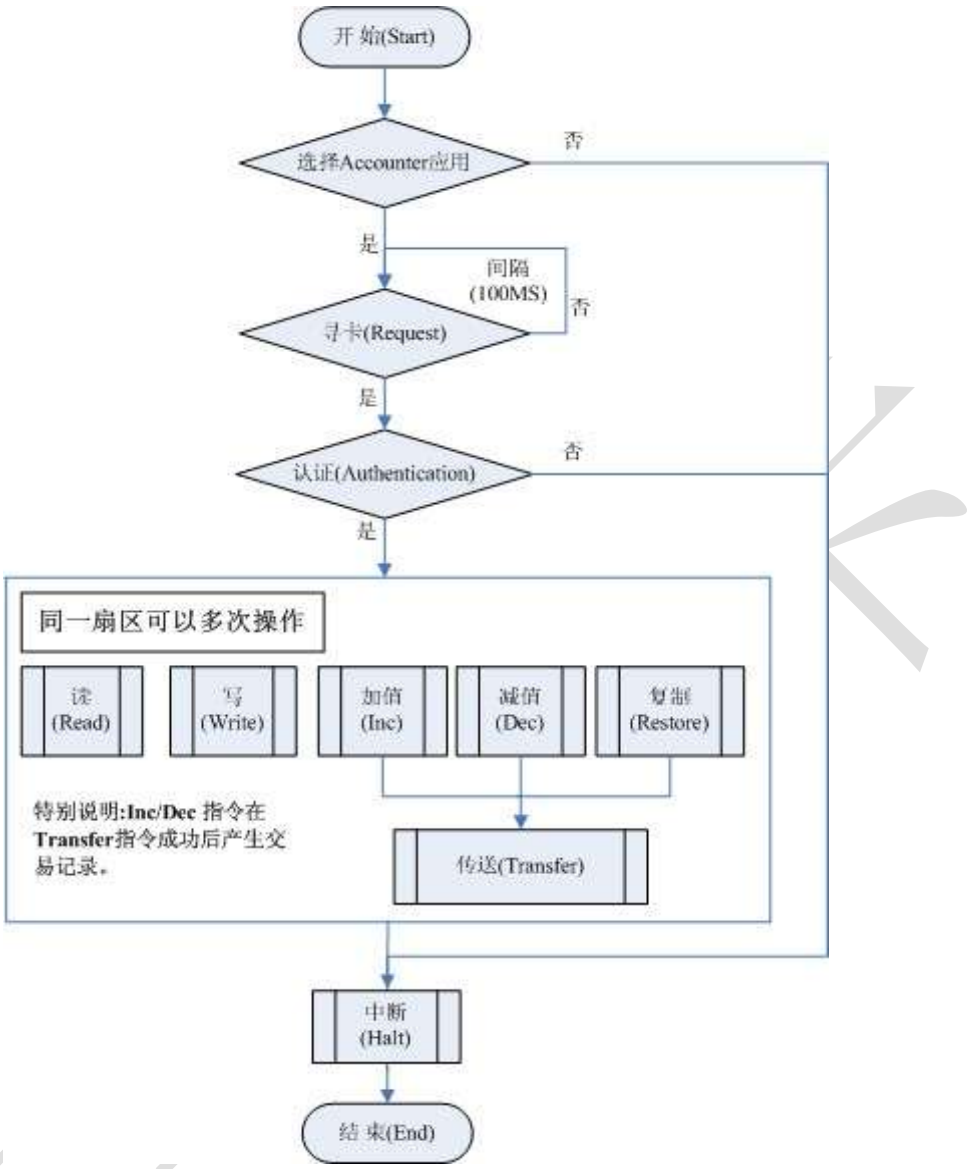
SW:

SW	Note
9000	指令执行完毕
9a12	传送错误（执行超时没有得到响应）

Notes:

执行条件是在卡的 SELECT 之后执行，且卡也要支持 iso1443a-4 协议层，本条指令执行后退出 iso1443a-4 协议层，可以重新寻卡。否则再次寻卡的话会失败。

07. 典型使用 Mifare 卡流程图



注：

1：在执行【Request】指令前，请先执行【选择 Accounter 应用】(必须执行)。

2：在执行【Request】时如果返回时没有连接上 RF-UIM 卡，则需要延时 100MS，再重发【Request】指令。

08. 常见状态字定义

状态字	描述
9000	成功

6200	No information given, state of non volatile memory unchanged
6281	Part of returned data may be corrupted
6282	End of file/record reached before reading Le bytes
6283	Selected file invalidated
6400	No information given, state of non-volatile memory unchanged
6500	No information given, state of non-volatile memory changed
6581	Memory problem
6700	Wrong length
6800	No information given
6881	Logical channel not supported
6882	Secure messaging not supported
6900	No information given
6981	Command incompatible with file structure
6982	Security status not satisfied
6983	Authentication/PIN method blocked
6984	Referenced data invalidated
6985	Conditions of use not satisfied
6986	no EF selected
6A80	Incorrect parameters in the data field
6A81	Function not supported
6A82	File not found
6A83	Record not found
6A86	Incorrect parameters P1-P2
6A87	Lc inconsistent with P1-P2
6A88	Referenced data not found
6A84	not enough memory
6B00	Wrong parameter(s) P1-P2
6D00	Instruction code not supported or invalid
6E00	Class not supported
6F00	Technical problem, no precise diagnosis
9240	memory problem
9850	INCREASE cannot be performed, max value reached
9862	Authentication error, application specific
9A00	指令不存在
9A01	卡头不存在
9A02	没有定义的用法
9A03	通信错误
9A04	没有认证
9A05	已经存在
9A06	空间不足
9A07	认证不对
9A08	无根目录
9A09	P1 错误

9A10	P2 错误
9A11	Lc 错误
9A24	应用被锁
9A26	重复子目录
9A27	存在相同的文件 ID
9A28	还有子目录存在
9A29	文件不存在
9A2A	无权限
9A2B	无此块
9A2C	无此密钥
9A2D	钱包字段出错
9A2E	到期
9A2F	系列号错
9A30	条件不足
9A31	通道正在执行其他指令
9A32	忙
9A33	天线不对
9A34	应用状态错误
9A35	未完，继续操作
9A40	钱包 0 扇区 0 块不能写
9A41	超出最大值
9A42	不允许透支
9A43	不允许最后一次透支
9A44	充值金额小于等于零
9B00	应用没选择
9B01	没有许可
9B02	没有选择
9B03	没有 PIN 认证
9C00	目标不存在
9C01	Key 不存在
9C02	RF 已经连接上
9C03	RF 没有连接上
9C04	RF 通信错误
9C05	RF 没有数据
9C06	正在等 ACK
9C07	发送成功
9C08	发送失败
9C0A	spi 通讯超时

9D01	处理失败
9D02	权限不够，需发卡方验证
9D03	权限不够，需 POS 或用户密码验证
9D04	地址不可读
9D05	地址不存在
9D06	空间不足
9D07	密钥不存在
9D08	功能不支持
9D09	指令错误
9D0A	配置信息错误
9D0B	数据错误
9E00	MAC 错误
9E01	应用没有注册
9E02	应用已注册
9E03	应用已停用
9E04	版本号不对
9E05	卡锁定
9E06	余额不足
9E07	积分锁定
9E08	CardID 不匹配
9E09	数目不匹配
9E0A	状态字不匹配
9E0B	VIP 许可数量超界
9E0C	币值为 0
9E0D	TAC 错误
9E0E	数据有错
9E10	传送门禁卡信息失败
9E11	黑名单不能开门
9E12	门禁选择钥匙出错
9E13	临时钥匙使用出错
9E14	开门失败
9E15	选择应用失败
9E16	门禁操作未认证
9EA0	IBC 解密失败
9EA1	IBC 加密失败
9EA2	IBC 签名失败
9EA3	IBC 验签失败

附录 A. 编制历史

版本号	更新时间	修改人	主要内容或重大修改
V1.0.0	2008-01-24	simon	编制规范
V1.0.1	2008-02-26	xicy	修改
V1.0.2	2008-05-06	xicy	修改
V1.0.3	2008-07-16	xicy	修改
V1.0.4	2009-03-06	huhq	修改
V1.0.5	2009-12-05	huhq	修改
V1.0.6	2010-03-18	huangzn	修改

Select	1	0x00	选择 RF 通道(0:基本应用 ；1:扩展应用如卡商的 PBOC 应用)