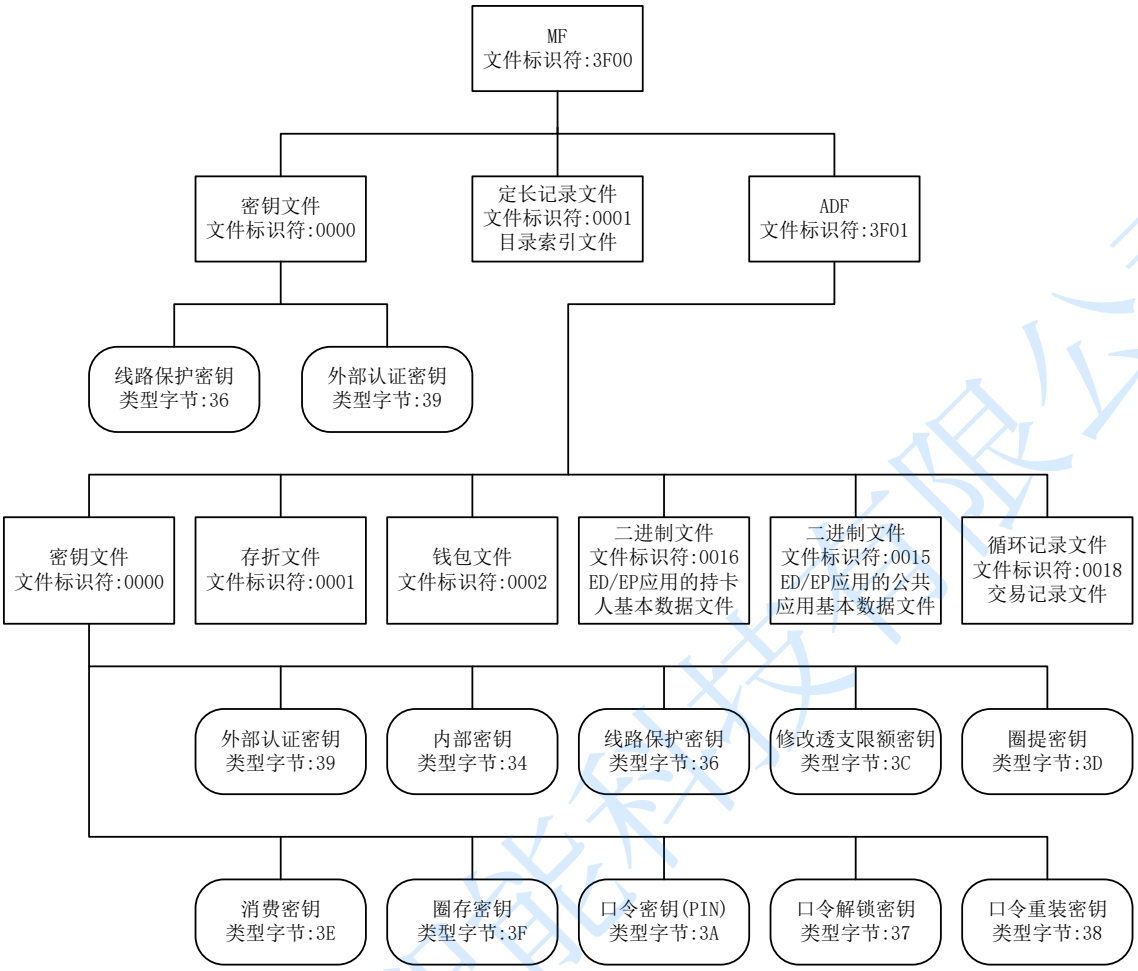
FM1208 CPU卡之PBOC操作实例

1　符合PBOC(中国人民银行)标准的CPU卡结构



MF(3F00)为根目录，不可删除，它下面目录、文件可删除。一张空白的CPU卡需先创建密钥文件及增加密钥，然后创建定长记录文件，最后创建ADF(3F01)文件。MF(3F00)下可创建多个DF，每个DF下必须创建密钥文件并增加密钥。每个DF是独立应用的，各自DF下的密钥只管理各自DF下其它文件的权限。

2　FMCOS安全体系介绍

2.1　安全状态

安全状态是指卡当前所处的一种安全级别，是否允许读、写、删除等操作。FMCOS的根目录和应用目录分别具有16种不同的安全状态，可以是0至F之间的某一值，卡片复位成功后它的状态值为0(缺省值为 0)。

2.2　安全属性

安全属性又称访问权限，有使用权、修改权、读权限、写权限等，在建立文件时用一个字节XY表示，X的取值范围为0~F，Y的取值范围为0~F。

访问权限为XY时有以下4种情况：

- 0Y时，表示要求MF的安全状态寄存器的值大于等于Y。如某文件读的权限为05，表示在对该文件进行读之前必须使MF的安全状态值大于等于5。
- X>Y时，表示要求当前目录的安全状态值大于等于Y且小于等于X。

- X=Y时，表示要求当前目录的安全状态值等于X，这里就只有一个取值了，如访问权限为AA，那么只有当前目录的安全状态值等于A才能访问了。
- X<Y时(X不为0)，表示禁止访问。

例子：设一个访问权限X的值=F,Y任意，即FY，表示要求安全状态值大于等于Y才能访问。

- 如某文件的读权限为F5，表示在对该文件进行读之前，必须使安全状态值大于等于5，即安全状态值只要是5~F这些值都可以访问该文件。
- 如某文件的读权限为F0，表示在对该文件进行读之前，必须使安全状态值大于等于0，即 0~F 所有值都可以，那就是说明没有权限权制了，随便读。

2.3 安全机制

安全机制是指某种安全状态转移为另一种安全状态所采用的方法和手段。FMCOS通过核对口令和外部认证来改变安全状态值。

当建立口令或者外部认证密钥时，参数的后续状态表示该口令核对成功或者外部认证成功后，置当前目录的安全状态值为后续状态。如某口令的后续状态为01表示对该口令核对成功后，当前目录安全状态值为1。当上电复位后或者从父目录进入子目录或退回上级目录时，当前目录的安全状态值均自动被置为0。

例如卡中某目录下有一个二进制文件，定义读二进制文件的权限为F1，写二进制文件权限为F2，那么这个二进制文件在后续状态为1~F时可以读，在后续状态为2~F时可以写。假如该目录下有一个口令密钥，后续状态为1，那么口令密钥验证通过后就可以读这个二进制文件了;假如该目录下还有一个外部认证密钥，使用权限为11(那么要先通过口令密钥验证后才能用这个外部认证密钥)，后续状态为2，那么外部认证密钥验证通过后就可以写上面的二进制文件了。

2.4 错误计数

用一个字节表示，高4位表示有多少次出错的机会，低4位表示当前还剩多少可出错的次数。比如我们的银行卡，在ATM机子上输入密码，如果连续输入3次密码错误即锁卡了，要实现这样的功能，使口令密钥或其它密钥指令里面的“错误计数”这一项为33即可，高4位为3表示有3次机会，低4位为3表示当前还有3次，如果输入口令错误CPU卡返回63C2(这里的2表示还有2次机会)，再错返回63C1(还有1次机会)，又再错返回63C0,这时表示没机会了，如果再输入错误即锁卡了。在调试时，建议把错误计数设为FF，即有16次的机会。

3 FM1208卡建立符合PBOC标准的结构

FM1208卡出厂时默认外部认证密钥为FFFFFFFFFFFFFFFF。须在卡片复位成功后进行下面的操作。

3.1 擦除FM1208卡所有数据

3.1.1 外部认证

(1)取4字节随机数

命令报文：0084000004，说明如下

00	84	00	00	04
CLA	INS	P1	P2	Le

(2)用密码“FFFFFFFFFFFFFFFF”对“4字节随机数+00000000”进行DES加密生成8字节加密数据。

例如4字节随机数为58001218，FFFFFFFFFFFFFFFF和5800121800000000进行DES加密后生成3C66F4E8F9DB86FA。

(3)发送00820000083C66F4E8F9DB86FA

指令说明：

00	82	00	00	08	3C66F4E8F9DB86FA
CLA	INS	P1	P2	Lc	加密数据

3.1.2 擦除MF下的数据

命令报文：800E000000，说明如下

80	0E	00	00	00
CLA	INS	P1	P2	Lc

3.2 MF下建立密钥文件及增加密钥

3F00这个根目录在出厂已建立，不可删除。

选择MF文件的命令报文：00A40000023F00，说明如下

00	A4	00	00	02	3F00
CLA	INS	P1	P2	Lc	文件标识符

3.2.1 建立密钥文件

命令报文：80E00000073F005001F0FFFF，说明如下

80	E0	0000	07
CLA	INS	文件标识	Lc

3F	00	50	01	F0	FF	FF
密钥文件	文件空间(字节)	短文件标识	增加密钥的权限		保留	保留

3.2.2 增加密钥

3.2.2.1增加线路保护密钥

命令报文：80D401000D36F0F0FF33FFFFFFFFFFFFFFFF，说明如下

80	D4	01	00	0D
CLA	INS	P1	密钥标识	数据长度

36	F0	F0	FF	33	FFFFFFFFFFFFFFFF
线路保护密钥	使用权	更改权	保留	错误计数器	8字节密钥

3.2.2.2 增加外部认证密钥

命令报文：80D401001539F0F0AA88FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF，说明如下

80	D4	01	00	15
CLA	INS	P1	密钥标识	数据长度

39	F0	F0	AA	88	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
外部认证密钥	使用权	更改权	后续状态	错误计数器	16字节密钥

3.3 MF下建立定长记录文件

命令报文：80E00001072A0213F000FFFF，说明如下

80	E0	0001	07
CAL	INS	文件标识	LC

2A	0213	F0	00	FFFF
定长记录文件	文件空间(字节)	读权限	写权限	保留

注：文件空间第一个字节 02为记录总个数，即可存 2条记录 ，第二个字节 13 为记录长度，即一条记录的内容为 13 个字节

增加记录内容：

命令报文：00E200081361114F09A000000003869807015004504 24F43，说明如下

00	E2	00	08	13	61114F09A000000003869807015004504 24F43
CAL	INS	P1	当前文件	LC	记录的信息内容为目录名及PBOC的ASCII码

注：这是一个TLV格式的记录，

61-11:(4F-09:A00000000386980701,50-04:50424F43),

其中A00000000386980701为目录名,50424F43为 PBOC的 ASCII码。

3.4 MF下建立DF文件及选择该文件

3.4.1 建立DF文件

命令报文：80E03F011138036FF0F095FFFFA00000000386980701，说明如下

80	E0	3F01	11
CLA	INS	文件标识	Lc

38	036F	F0	F0	95	FFFF	A00000000386980701
目录文件DF	文件空间(字节)	建立权限	擦除权限	应用ID	保留	DF名称

3.4.2 选择DF文件

命令报文：00A40000023F01，说明如下

00	A4	00	00	02	3F01
CLA	INS	P1	P2	Lc	文件标识

3.5 DF下建立密钥文件及增加密钥

3.5.1 建立密钥文件

命令报文：80E00000073F018F95F0FFFF ，说明如下

80	E0	0000	07
CLA	INS	文件标识	Lc

3F	018F	95	F0	FFFF
密钥文件	文件空间(字节)	短标识符	增加权限	保留

3.5.2 增加外部认证密钥

命令报文：80D401001539F00244FF393939393939393939393939393939，说明如下

80	D4	01	00	15
CLA	INS	P1	密钥标识	数据长度

39	F0	02	44	FF	3939393939393939393939393939393939

外部认证密钥	使用权	更改权	后续状态	错误计数器	16字节的密钥

3.5.3 增加内部密钥

命令报文：80D401001534F00200013434343434343434343434343434343434，说明如下

80	D4	01	00	15
CLA	INS	P1	密钥标识	数据长度

34	F0	02	00	01	3434343434343434343434343434343434
内部密钥	使用权	更改权	密钥版本号	算法标识	16字节密钥

3.5.4 增加线路保护密钥

命令报文：80D401001536F002FF33363636363636363636363636363636363636 ，说明如下

80	D4	01	00	15
CLA	INS	P1	密钥标识	数据长度

36	F0	02	FF	33	3636363636363636363636363636363636
线路保护密钥	使用权	更改权	保留	错误计数器	16字节密钥

3.5.5 增加修改透支限额密钥

命令报文：80D401021**53C**F00201003C023C023C023C023C023C023C023C023C02 ，说明如下

80	D4	01	02	15
CAL	INS	P1	密钥标识	数据长度

3C	F0	02	01	00	3C023C023C023C023C023C023C023C023C02
修改透支限额密钥	使用权	更改权	密钥版本号	算法标识	16字节密钥

3.5.6 增加圈提密钥

命令报文：80D401021**53D**F00201003D023D023D023D023D023D023D023D023D02 ，说明如下

80	D4	01	02	15
CAL	INS	P1	密钥标识	数据长度

3D	F0	02	01	00	3D023D023D023D023D023D023D023D023D02
圈提密钥	使用权	更改权	密钥版本号	算法标识	16字节密钥

3.5.7 增加消费密钥

命令报文：80D40102153EF00200013E023E023E023E023E023E023E023E02，说明如下

80	D4	01	02	15
CAL	INS	P1	密钥标识	数据长度

3E	F0	02	00	01	3E023E023E023E023E023E023E023E023E02
消费密钥	使用权	更改权	密钥版本号	算法标识	16字节密钥

3.5.8 增加圈存密钥

命令报文：80D40102153FF00200013F023F023F023F023F023F023F023F02，说明如下

80	D4	01	02	15
CAL	INS	P1	密钥标识	数据长度

3F	F0	02	00	01	3F023F023F023F023F023F023F023F02
圈存密钥	使用权	更改权	密钥版本号	算法标识	16字节密钥

3.5.9 增加口令 密钥(PIN)

命令报文：80D401000D3AF0EF0155123456FFFFFFFFFF，说明如下

80	D4	01	00	0D
CLA	INS	P1	密钥标识	数据长度

3A	F0	EF	01	55	123456FFFFFFFFFF
口令密钥	使用权	/	后续状态	错误计数器	3字节密钥，后面补FF

3.5.10 增加口令解锁密钥

命令报文：80D401001537F002FF33373737373737373737373737373737，说明如下

80	D4	01	00	15
CLA	INS	P1	密钥标识	数据长度

37	F0	02	FF	33	3737373737373737373737373737373737
口令解锁密钥	使用权	更改权	/	错误计数器	16字节密钥

3.5.11 增加口令重装密钥

命令报文：80D401001538F002FF33383838383838383838383838383838，说明如下

80	D4	01	00	15
CLA	INS	P1	密钥标识	数据长度

38	F0	02	FF	33	3838383838383838383838383838383838
口令解锁密钥	使用权	更改权	/	错误计数器	16字节密钥

3.6 DF下建立公共应用基本数据文件

3.6.1 建立二进制文件(带线路保护读写)

命令报文：80E0001507A8001EF0F0FFFF，说明如下

80	E0	0015	07
CLA	INS	文件标识	Lc

A8	001E	F0	F0	FFFF
二进制文件带MAC线路保护	文件空间(字节)	读权限	写权限	保留

3.6.2 写二进制文件

在该文件中写入公共应用基本数据：

数据长度(30字节)	数据说明	数据
8	发卡方标识	1111222233330006
1	应用类型标识	03
1	应用版本	01
10	应用序列号	00062016010100000030
4	启动日期	20160110
4	有效日期	20200110
2	发卡方自定义FCI	5566

注意：写二进制时必须使用DAMK 进行线路保护，如连续三次执行此命令失败，IC卡回送9303即应用永久锁定。

命令报文：

04D695002211112222333300060301000620160101000000302016011020200110556 69A47F249，说明如下

04	D6	95	00	22
CLA	INS	0015的短文件标识符	偏移量	LC(数据长度1E + 4 字节的 MAC)

1111222233330006030100062016010100000030201601102020011055 66	9A47F249
数据	MAC

MAC计算过程：

用线路保护密钥与线路保护数据进行MAC运算，MAC初值取4个字节的随机数并补0，然后计算得到 MAC的8个字节取前4字节。

- 初始值：假设取得随机数为F2C5FAE4，补0后为F2C5FAE400000000
- 线路保护数据：

04D695002211112222333300060301000620160101000000302016011020200110556 6

- 线路保护密钥：36363636363636363636363636363636
- MAC运算结果：9A47F249(取前4字节)

3.7 DF下建立ED/EP持卡人基本信息数据的文件

3.7.1 建立二进制文件(带线路保护读写)

命令报文：80E0001607A80027F0F0FFFF，说明如下

80	E0	0016	07
CLA	INS	文件标识	Lc

A8	0027	F0	F0	FFFF
二进制文件带MAC线路保护	文件空间(字节)	读权限	写权限	保留

3.7.1 写二进制文件

在该文件写入持卡人基本信息数据:

数据长度(39字节)	写入的数据说明	写入的数据
1	卡类型标识	00
1	本行职工标识	00
20	持卡人姓名	小柯(5C0F67EF)
16	持卡人证件号码	31313031303239383132313830303130

1	持卡人证件类型	05

注意：写二进制时必须使用DAMK进行线路保护，如连续三次执行此命令失败，IC卡回送 9303 即应用永久锁定。

命令报文：

04D696002B00005C0F67EF00000000000000000000000000000000313130313032393831323138303030313005926ACE48，说明如下

04	D6	96	00	2B
CAL	INS	P1(0016短文件标识)	偏移量	LC(数据长度39字节+4字节MAC)

00005C0F67EF0000000000000000000000000000003131303130323938313231383030313005	926ACE48
数据	MAC

MAC计算过程：

用线路保护密钥与线路保护数据进行MAC运算，MAC初始值取4个字节随机数并补0，然后计算得到MAC的8个字节取前4位。

- 初始值：假设取得随机数为F5C55AAC，补0后为F5C55AAC00000000
- 线路保护数据：
  04D696002E00005C0F67EF00000000000000000000000000000000313130313032393831323138303030313005
- 线路保护密钥：36363636363636363636363636363636
- MAC运算结果：926ACE48(取前4字节)

3.8 DF下建ED/EP应用的交易明细循环记录文件

命令报文：80E00018072E0A17F1EFFFFF ，说明如下

80	E0	0018	07
CLA	INS	文件标识	Lc

2E	0A17	F1	EF	FFFF
循环记录文件	文件空间(字节)	读权限	写权限	保留

只要把这个文件建好，当消费成功后COS系统会自动把每一笔消费记录写入该文件，无需手动写入。

3.9 DF下建立电子存折文件

命令报文：80E00001072F0208F100FF18，说明如下

80	E0	0001	07
CLA	INS	文件标识	Lc

2F	0208	F1	00	FF	18
PBOC ED/EP文件	PBOC	读权限	保留	保留	交易记录短标识

3.10 DF下建立电子钱包文件

命令报文：80E00002072F0208F000FF18，说明如下

80	E0	0002	07
CAL	INS	文件标识	LC

2F	0208	F0	00	FF	18
PBOC ED/EP文件	PBOC	读权限	保留	保留	交易记录短标识

4 FM1208卡电子钱包的圈存、消费、读余额

须在卡片复位成功后进行下面的操作。

4.1 选择电子钱包文件夹

命令报文：00A40000023F0100，说明如下

00	A4	00	00	02	3F01	00
CLA	INS	P1	P2	LC	文件标识	Le

4.2 验证PIN口令

对于电子钱包：圈存操作需要验证PIN，消费、读余额可以不验证PIN。

对于电子存折：圈存、消费需要验证PIN，读余额可以不验证PIN。

命令报文：0020000003123456，说明如下：

00	20	00	00	03	123456
CLA	INS	P1	口令密钥标识符	Lc	口令密钥

4.3 圈存

注：要想进行圈存交易首先必须进行圈存初始化。

4.3.1 电子钱包圈存初始化

命令报文：805000020B0200000064112233445566，说明如下

80	50	00	02	0B	02	00000064	112233445566
CLA	INS	P1	电子钱包	LC	密钥标识符	交易金额	终端机编号

响应报文数据域：00000000000000001688AC6F68F0E778F，说明如下

00000000	0000	00	01	688AC6F6	8F0E778F
旧余额	联机交易序号	密钥版本号	算法标识	伪随机数	MAC1

过程密钥的计算：

过程密钥由密钥标识符指定的圈存密钥对(4字节伪随机数+2字节联机交易序号+8000)数据进行3DES加密生成。

- 数据：688AC6F600008000
- 圈存密钥：3F023F023F023F023F023F023F023F02
- 进行3DES加密得出过程密钥：A305D2DCFC130935

MAC1的计算：

MAC1由过程密钥与(4字节旧余额+4字节交易金额+1字节交易类型标识+6字节终端机编号)数据进行MAC运算生成。其中交易类型标识的取值如下，电子存折圈存为01，电子钱包圈存为02。

- 取初始值为：0000000000000000
- 数据：00000000000000064021122334455 66
- 过程密钥：A305D2DCFC130935
- 进行MAC计算结果为：8F0E778F(取前4字节)，与卡片返回的MAC1相符。

4.3.2 电子钱包圈存

命令报文：805200000B201701151455105674 1ABA，说明如下

80	52	00	00	0B	20170115	145510	56741ABA
CLA	INS	P1	P2	Lc	交易日期	交易时间	MAC2

响应报文数据域：D2CD62D9，说明如下

D2CD62D9
交易验证码TAC

过程密钥的计算：

过程密钥由密钥标识符指定的圈存密钥对(4字节伪随机数+2字节联机交易序号+8000)数据进行3DES加密生成。

- 数据：688AC6F600008000
- 圈存密钥：3F023F023F023F023F023F023F023F02
- 进行3DES加密得出过程密钥：A305D2DCFC130935

MAC2的计算：

MAC2由过程密钥与(4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节交易日期+3字节交易时间)数据进行MAC运算生成。

- 取初始值为：0000000000000000
- 数据：00000064021122334455662017011514551 0
- 过程密钥：A305D2DCFC130935
- 进行MAC计算结果为：56741ABA(取前4字节)

交易验证码TAC的计算：

交易验证码TAC由内部密钥DTK左右8位字节异或运算结果与(4字节新余额+2字节联机交易序列号(加1前)+4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节交易日期+3字节交易时间)数据进行MAC运算生成。

- 取初始值为：0000000000000000
- 数据：0000006400000000006402112233445566201701151455 10
- 密钥计算：

  内部密钥：34343434343434343434343434343434

  内部密钥左右8位字节异或运算结果：0000000000000000
- 进行MAC计算结果为：D2CD62D9(取前4字节)，与卡片返回的交易验证码TAC相符。

4.4 消费

要想进行消费交易首先必须进行消费初始化，IC卡将INITIALIZE FOR PURCHASE响应报文回送给终端处理。如果IC卡回送的状态码不是“9000”，则交易中止。

4.4.1 消费初始化

命令报文：805001020B020000000211223344 5566，说明如下

80	50	01	02	0B	02	00000002	112233445566
CLA	INS	P1	电子钱包	Lc	密钥标识符	交易金额	终端机编号

响应报文数据域：000000640000000000000 1C410C94A，说明如下

00000064	0000	000000	00	01	C410C94A

旧余额	脱机交易序号	透支限额	密钥版本号	算法标识	伪随机数(IC卡)

4.4.2 消费命令

命令报文：805401000F000000002017011516551OB75CD851，说明如下

80	54	01	00	0F	00000000	20170115	165510	B75CD851
CLA	INS	P1	P2	Lc	终端交易序号	交易日期(终端)	交易时间(终端)	MAC1

响应报文数据域：5EAF3FFCA0F90116，说明如下

5EAF3FFC	A0F90116
交易验证码TAC	MAC2

过程密钥的计算：

过程密钥由与消费密钥相同的消费密钥对(4字节伪随机数+2字节脱机交易序号+终端交易序号的最右两个字节)数据进行3DES加密生成。

- 数据：C410C94A00000000
- 消费密钥：3E023E023E023E023E023E023E023E02
- 进行3DES加密得出过程密钥：530932241E167E21

MAC1的计算：

MAC1由卡中过程密钥与(4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节终端交易日期+3字节终端交易时间)数据进行MAC运算生成。其中交易类型标识的取值如下，电子存折消费为05，电子钱包消费为06。

- 取初始值为：0000000000000000
- 数据：00000002061122334455662017011516551O
- 过程密钥：530932241E167E21
- MAC计算结果为：B75CD851(取前4字节)

TAC的计算：

TAC由内部密钥DTK左右8位字节异或运算的结果与(4字节交易金额+1字节交易类型标识+6字节终端机编号+4字节终端交易序号+4字节终端交易日期+3字节终端交易时间)数据进行MAC运算生成。

- 取初始值为：0000000000000000
- 数据：000000020611223344556600000000020170115165510
- 密钥计算：

  内部密钥：34343434343434343434343434343434

  内部密钥左右8位字节异或：0000000000000000
- MAC计算结果为：F5DB9817(取前4字节)，与卡片返回的交易验证码TAC相符

MAC2的计算：

MAC2由过程密钥与(4字节交易金额)数据进行MAC运算生成。

- 取初始值为：0000000000000000
- 数据：00000002
- 过程密钥：530932241E167E21
- MAC计算结果：A0F90116(取前4字节)，与卡片返回的MAC2相符

4.5 读余额

命令报文：805C000204，说明如下

80	5C	00	02	04
CLA	INS	P1	电子钱包	Le

响应报文数据域：00000062，说明如下

00000062
余额