Fudan Microelectronics CPU card issuance process

 Top One line of Java Posted on 2016-11-23 14:14:01 Reading volume 1.7w Favorites 108 Likes 15

Category Column: CPU card Article Tags: CPU card Fudan micro E-wallet issuance PBOC E-wallets

preface

Recently, I have been doing CPU card-related applications, and I also know how to simply manipulate CPU card-related data, but I don't really have a deep understanding of CPU-related things; Recently, I collected some information, carefully read the **pboc3.0 specification** and **Fudan FM1208 technical manual** and other related documents, and found a few Fudan white cards on Taobao, and spent a whole week, and finally sent a few test cards and successfully recharged and consumed the operation, so it is also a good note to share the results of the study, so that it is easy to view and review in the future.

Instruction list

The list of FMCOS commands is shown in the figure below:

表 1.1 FMCOS 2.0 命令表

编号	指令	指令类别	指令码	功能描述	兼容性
	VERIFY	00	20	验证口令	ISO&PBOC
	EXTERNAL AUTHENTICATE	00	82	外部认证	ISO&PBOC
	GET CHALLENGE	00	84	取随机数	ISO&PBOC
	INTERNAL AUTHENTICATE	00	88	内部认证	ISO&PBOC
	SELECT	00	A4	选择文件	ISO&PBOC
	READ BINARY	00	B0	读二进制文件	ISO&PBOC
	READ RECORD	00	B2	读记录文件	ISO&PBOC
	GET RESPONSE	00	C0	取响应数据	ISO&PBOC
	UPDATE BINARY	00/04	D6/D0	写二进制文件	ISO&PBOC
	UPDATE RECORD	00/04	DC/D2	写记录文件	ISO&PBOC
	CARD BLOCK	84	16	卡片锁定	PBOC
	APPLICATION UNBLOCK	84	18	应用解锁	PBOC
	APPLICATION BLOCK	84	1E	应用锁定	PBOC
	PIN UNBLOCK	80/84	24	个人密码解锁	PBOC
	UNBLOCK	80	2C	解锁被锁住的口令	PBOC
	INITIALIZE	80	50	初始化交易	PBOC/建设部
	CREDIT FOR LOAD	80	52	圈存	PBOC
	DEBIT FOR PURCHASE/CASE WITHDRAW/UNLOAD	80	54	消费/取现/圈提	PBOC
	UPDATE OVERDRAW LIMIT	80	58	修改透支限额	PBOC
	GET TRANSCATION PROVE	80	5A	取交易认证	PBOC/建设部
	GET BALANCE	80	5C	读余额	PBOC
	RELOAD/CHANGE PIN	80	5E	重装/修改个人密码	PBOC
	ERASE DF	80	0E	擦除 DF	专有
	PULL	80	30	专用消费	建设部
	CHARGE	80	32	专用充值	建设部
	WRITE KEY	80/84	D4	增加或修改密钥	专有
	CREATE	80	E0	建立文件	专有
	WRITE EEPROM	00	00	写数据 EEPROM	生产测试
	READ EEPROM	00	04	读数据 EEPROM	生产测试
	INITIAL EEPROM	00	02	初始化 EEPROM	生产测试
	READ ROM	00	0C	读程序 ROM	生产测试
	CALCULATE ROM CRC	00	0A	计算程序 ROM CRC	生产测试

Issuing

Simple and rude, directly on the specific card issuance process, because the specific CPU card-related theories still need a while to understand, not I can explain clearly in one or two sentences here; According to my personal experience, at the beginning of the research (entry), it is more necessary to know what to do, and then go back to the theory to understand faster, so here is directly to the dry goods; If you want to know more about the theory, you can go directly to Baidu's "PBOC3.0 Specification" to see the document.
The operation of card issuance is divided into the following steps:

1. Transport Authentication (External Authentication)
2. Card erasure
3. Create and write directory files and user keys
4. Writing of data (binary data, record data).

> For the authentication of the transmission channel, I personally think that the most popular understanding is to obtain read and write permissions, allowing the operation of adding, deleting and modifying the information inside; The default transfer key is an 8-byte 0xFF, i.e., FFFFFFFFFFFFFFFF

- **Card power-on reset**
  The personal front-end is to use the mobile phone NFC for card operation, so the card is pasted to the NFC sensing area of the mobile phone that it has been powered on and reset, and the next operation can be carried out after the card connection is established.
- **Get Random Number**
  Send Command: **0084000008** (Get 8 Bytes Random Number)
  Command Reply: 53fd1f262ec4e6e29000 (Get Random Number: 53fd1f262ec4e6e2).
  Instruction Description: 00 (CLA) 84 (INS) 00 (P1) 00 (P2) 08 (Le)
- **DES encryption for random numbers**
  Encrypted data: 53fd1f262ec4e6e2
  Encryption key: FFFFFFFFFFFFFFFF (external authentication key)
  Processing result: A0DBBFC1192FF24A
- **Transmission Authentication (External Authentication)**
  Send command: **0082000008A0DBBFC1192FF24A** (the data part is the result of the DES processing in the previous step)
  Command reply: 9000 (authentication successful).
  Command description: 00 (CLA) 82 (INS) 00 (P1) 00 (P2 external authentication key identifier 00/01) 08 (Lc) A0DBBFC1192FF24A (random number after data 8-byte encryption)
  Possible error responses:
  - The 6188
    authentication key does not exist, it may be a card that has been authenticated and erased, you can directly try to erase the card to see if it is successful, and if it is successful, you can do subsequent actions.
  - 63Cx
    authentication failed, x is the number of allowed reattempts; There are two possible reasons for this error, one is the wrong key; The other is that there is an error in DES encryption;

  > **There may be differences in the card authentication methods of different manufacturers, such as when Taobao Taoka, it will be clear that he has this card authentication method.**

Card erasure

> Erase all data in the card, and after the erasure is successful, the card becomes a blank card

Send command: **800E0000000**
Command reply: 9000 (erase successful)
Command description: 80 (CLA) 0E (INS) 00 (P1) 00 (P2) 00 (Lc)

Create and write directory files and user keys

This mainly includes the creation of the main file, the creation of the key file, the creation of binary files and record files, and the writing of user keys

Command packet data field

- Catalog file DF (including MF)

file type	File space	Establish permissions	Erase permissions	App file ID	reserved word	DF name
38	2 bytes	1 byte	1 byte	XX	FFFF	5-16 bytes

- Basic file EF

	Command packet data field					
file type	BYTE1	BYTE2-3	BYTE4	BYTE5	BYTE6	BYTE7
binary file	28	File space	Read permissions	Write permissions	FF	See description
Fixed-length recording file	2A	File space	Read permissions	Write permissions	FF	See description
Loop files	2E	File space	Read permissions	Write permissions	FF	See description
PBOC ED/EP	2F	02 08	Usage Rights	Reserved (00)	FF	Transaction details file short indication
Variable-length record files	2C	File space	Read permissions	Write select all	FF	See description
Key file	3F	File space	DF file short identifier	Intermediate permissions	FF	FF

  - If you want to use plaintext MAC to write BYTE1, you need to set the highest bit of BYTE1 to 1 ("28" becomes "A8")
    If you want to use encrypted write, the highest position of BYTE1 ("28" becomes "68")
  - The last byte of the reserved word for the basic EF file (except for the key file and PBOC ED/EP file) is defined as follows: (let the byte be defined as b8 ~ b1)

b8	b7	b6	b5	b4	b3	b2	b1	meaning	
1	-	-	-	-	-	-	-	The file does not support wire-protected reads	
0	-	-	-	-	-	-	-	The file must be read using line protection	
-	1	1	1	-	-	-	-	Leave it at 1	
-	-	-	-	1	1	-	-	The ID of the key used for the read operation	A key identified as 00
-	-	-	-	1	0	-	-		The key identified as 01
-	-	-	-	0	1	-	-		The key identified as 02
-	-	-	-	0	0	-	-		The key identified as 03
-	-	-	-	-	-	1	1	The key identifier used for the write operation	A key identified as 00
-	-	-	-	-	-	1	0		The key identified as 01
-	-	-	-	-	-	0	1		The key identified as 02
-	-	-	-	-	-	0	0		The key identified as 03

  - For record files (including fixed-length files, wallet files, and circular files), the **first byte of the file space is the total number of records, and the second byte is the length of the record**: the total number of physical spaces (number of records * (record length + 1) + 8).
  - For the so-called **DF short file identifier** for the key file, the instructions are as follows: **DDF when the upper three digits are 000**, and **ADF short file identification number when the upper three digits are 100**.
  - For PBOC ED/EP, the so-called TAC key identifier refers to the identifier of the key type '34' used by the ED/EP in the calculation of TAC; The so-called transaction details file refers to the short file identifier used by ED/EP to record transaction details.
  - All files cannot be selected automatically after they have been created.

- The type of key

type	significance
34	Internal keys
36	File line protection key

type	significance
38	The key to reinstall the password key
39	External authentication key
3A	Password key
3B	Unlock the password key
3C	Modify your overdraft limit
3D	Circle mention
3E	consume
3F	Trap keys

A list of instruction sets

```
800E000000
80E03F000D38FFFFF0F001FFFFFFFFFFFFF
80E00000073F005001F0FFFF
80D401000D36F0F0FF33FFFFFFFFFFFFFFF
80D401001539F0F0AA33FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
80E00001072A0213F000FFFF
80E0000507A80030F0F0FFFF
00E200081361114F09A000000003869807015004504 24F43
80E03F011138036FF0F095FFFFA00000000386980701
00A4040009A00000000386980701
80E00000073F018F95F0FFFF
80D401001534F00200013434343434343434343434343434343434
80D401001536F002FF33363636363636363636363636363636363636
80D401001537F002FF33373737373737373737373737373737373737
80D401001538F002FF33383838383838383838383838383838383838
80D401001539F00244333939393939393939393939393939393939
80D40101153EF00200013E013E013E013E013E013E013E013E01
80D40102153EF00200013E023E023E023E023E023E023E023E02
80D40101153FF00200013F013F013F013F013F013F013F013F01
80D40102153FF00200013F023F023F023F023F023F023F023F02
80D40101153DF00201003D013D013D013D013D013D013D013D01
80D40102153DF00201003D023D023D023D023D023D023D023D02
80D40101153CF00201003C013C013C013C013C013C013C013C01
80D40102153CF00201003C023C023C023C023C023C023C023C02
80D401000D3AF0EF013312345FFFFFFFFFF
80E0001507A8001EF0F0FFFF
80E0001607A80027F0F0FFFF
80E00017072805DCF0F0FFFF
80E00018072E0A17F0EFFFFF
80E00001072F0208F100FF18
80E00002072F0208F000FF18
```

Instruction set description

- **MF file creation**
  Send command: **80E03F000D38FFFFF0F001FFFFFFFFFFFFF**
  Command reply: 9000 (file created successfully).
  Instruction Description: 80 (CLA) E0 (INS) 3F00 (P1 P2 File ID) 0D (Lc) 38 (File Type) FFFF (File Space) F0 (Establish Permission) F0 (Erase Permission) 01 (App File ID) FFFF (Reserved Word) FFFFFFFFFFFF (DF Name)
- **Create a key file**
  Send command: **80E00000073F005001F0FFFF**
  Command reply: 9000 (created successfully).
  Instruction Description: 80 (CLA) E0 (INS) 0000 (P1P2 file identifier) 07 (Lc) 3F (file type) 0050 (file space) 01 (DF file short identifier) F0 (add permission) FF (default) FF (default)
- **Add a line protection key**
  Send command: **80D401000D36F0F0FF33FFFFFFFFFFFFFFF**
  Command reply: 9000 (successful).
  Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 0D (Lc) 36 (Key ID) F0 (Right to Use) F0 (Right to Change) FF (Default) 33 (Error Counter) FFFFFFFFFFFFFFFF (Key)

- **Add an external authentication key**
  Send command:
  80D401001539F0F0AA33FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

  Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 15 (Lc) 39 (Key ID) F0 (Right to Use) F0 (Right to Change) AA (Subsequent State) 33 (Error Counter)
  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
  FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
- **Create a fixed-length file**
  Send command: **80E00001072A0213F000FFFF**
  Command reply: 9000 (successful).
  Command description: 80 (CLA) E0 (INS) 0001 (P1P2 file identifier) 07 (Lc) 2A (fixed-length file) 0213 (file space) F0 (read permission) 00 (write permission) FF (default) FF (default)
- **Create 05 file**
  Send command: **80E0000507A80030F0F0FFFF**
  Command reply: 9000 (success)
  Command description: 80 (CLA) E0 (INS) 0005 (P1P2 file ID) 07 (Lc) A8 (binary 28–> A8) 0030 (file space) F0 (read permission) F0 (write permission) FF (default) FF (default)
  Note: **28–> A8 28 = 00101000 high bit change 1, that is: 10101000 = A8 (plaintext + MAC verification).**
- **Add File Records**
  Send Command: **00E200081361114F09A00000000386980701500450424F43**
  Command Reply: 9000 (Added successfully)
- **Create EF (Basic File)**
  Send command: **80E03F011138036FF0F095FFFFA00000000386980701**
  Command reply: 9000 (created successfully).
  Instruction Description: 80 (CLA) E0 (INS) 3F01 (P1 P2 File ID) 11 (Lc) 38 (File Type (Directory File)) 036F (File Space) F0 (Establish Permission) F0 (Erase Permission) 95 (Apply File ID) FFFF (Reserved Field) A00000000386980701 (DF Name AID)
- **Select EF**
  Send Command: **00A4040009A00000000386980701**
  Command Reply: 6f0b8409a000000003869807019000 (successfully selected).
  Instruction description: 00 (CLA) A4 (INS) 04 (P1) 00 (P2) 09 (Lc) A00000000386980701 (Data AID)
  Reply description: 6f (record ID of the file control information section) 0b (length) 84 (record ID of DF name) 09 (DF name record data length) a00000000386980701 (name of ADF) 9000 (SW1 SW2)
- **Create a key file**
  Send command: **80E00000073F018F95F0FFFF**
  Command reply: 9000 (created successfully)
  Command description: 80 (CLA) E0 (INS) 0000 (P1P2.) File ID) 07 (Lc) 3F (File Type) 018F (File Control) 95 (DF File Short Identifier) F0 (Add Permissions) FF (Default) FF (Default)
- **Add an internal key**
  Send command: **80D401001534F002000134343434343434343434343434343434**
  Command reply: 9000 (created successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 15 (Lc) 34 (key identification) F0 (use right) 02 (change right) 00 (key version number) 01 (algorithm identification) 34343434343434343434343434343434 (key)
- **Add the line protection key** (the line key here is different from the file protected by the previous one)
  Send the command: **80D401001536F002FF3336363636363636363636363636363636**
  Command reply: 9000 (added successfully).
  Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 15 (Lc) 36 (Key ID) F0 (Right to Use) 02 (Right to Change) FF (Default FF) 33 (Error Counter) 36363636363636363636363636363636 (Key)
- **Add a password unlock key**
  Send command: **80D401001537F002FF3337373737373737373737373737373737**
  Command reply: 9000 (added successfully).
  Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 15 (Lc) 37 (Key ID) F0 (Right to Use) 02 (Right to Change) FF (Default FF) 33 (Error Counter) 37373737373737373737373737373737 (Key)
- **Add password to reinstall key**
  Send command: **80D401001538F002FF3338383838383838383838383838383838**

Command reply: 9000 (added successfully).
Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 15 (Lc) 38 (Key ID) F0 (Right to Use) 02 (Right to Change) FF (Default FF) 33 (Error Counter) 38383838383838383838383838383838 (Key)

- **External authentication key**
  Send command: **80D401001539F00244333939393939393939393939393939**
  Command reply: 9000 (added successfully).
  Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 15 (Lc) 39 (Key ID) F0 (Right to Use) 02 (Right to Change) 44 (Subsequent State) 33 (Error Counter) 39393939393939393939393939393939 (Key)
- **Consumption key 01**
  Send command: **80D40101153EF00200013E013E013E013E013E013E013E013E013E01**
  Command reply: 9000 (added successfully).
  Instruction Description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3E (Key ID) F0 (Right to Use) 02 (Right to Change) 00 (Key Version Number) 01 (Algorithm ID) 3E013E013E013E013E013E013E013E013E
- **Consumption key 02**
  Send command: **80D40102153EF00200013E023E023E023E023E023E023E023E023E02**
  Command reply: 9000 (added successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 02 (P2) 15 (Lc) 3E (key ID) F0 (right to use) 02 (right to change) 00 (key version number) 01 (algorithm ID) 3E023E023E023E023E023E023E023E023E02 (key)
- **Trap key 01**
  Send command: **80D40101153FF00200013F013F013F013F013F013F013F013F01**
  Command reply: 9000 (added successfully).
  Command description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3F (key ID) F0 (right to use) 02 (right to change) 00 (key version number) 01 (algorithm ID) 3F013F013F013F013F013F013F013F013F013F (key)
- **Trap key 02**
  Send command: **80D40102153FF00200013F023F023F023F023F023F023F023F023F02**
  Command reply: 9000 (added successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3F (key ID) F0 (right to use) 02 (right to change) 00 (key version number) 01 (algorithm ID) 3F023F023F023F023F023F023F023F023F023F (key)
- **Circle key 01**
  Send command: **80D40101153DF00201003D013D013D013D013D013D013D013D013D01**
  Command reply: 9000 (added successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3D (key identification) F0 (right to use) 02 (right to change) 01 (key version number) 00 (algorithm identification) 3D013D013D013D013D013D013D013D013D013D01 (key)
- **Circle key 02**
  Send command: **80D40102153DF00201003D023D023D023D023D023D023D023D023D02**
  Command reply: 9000 (added successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3D (key ID) F0 (right to use) 02 (right to change) 01 (key version number) 00 (algorithm ID) 3D023D023D023D023D023D023D023D023D023D (key)
- **Add and modify overdraft limit key 01**
  Send command: **80D40101153CF00201003C013C013C013C013C013C013C013C013C01**
  Command reply: 9000 (added successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3C (key ID) F0 (right to use) 02 (right to change) 01 (key version number) 00 (algorithm ID) 3C013C013C013C013C013C013C013C013C013C
- **Add and modify the overdraft limit key 02**
  Send command: **80D40102153CF00201003C023C023C023C023C023C023C023C023C02**
  Command reply: 9000 (added successfully).
  Instruction description: 80 (CLA) D4 (INS) 01 (P1) 01 (P2) 15 (Lc) 3C (key ID) F0 (right to use) 02 (right to change) 01 (key version number) 00 (algorithm ID) 3C023C023C023C023C023C023C023C023C02 (key)
- **Add PIN**
  Send command: **80D401000D3AF0EF013312345FFFFFFFFFF**
  Command reply: 9000 (added successfully
). Instruction description: 80 (CLA) D4 (INS) 01 (P1) 00 (P2) 0D (Lc) 3A (password key) F0 (right to use) EF (default EF) 01 (subsequent state) 33 (error counter) 12345FFFFFFFFFFF (password)
- **Create File 15 (binary)**
  Send command: **80E0001507A8001EF0F0FFFF**
  Command reply: 9000 (created successfully).
  Instruction description: 80 (CLA) E0 (INS) 0015 (P1 P2 file ID) 07 (Lc) A8 (plaintext MAC 28 (binary bit change 1) –> A8) 001E (file space) F0 (read

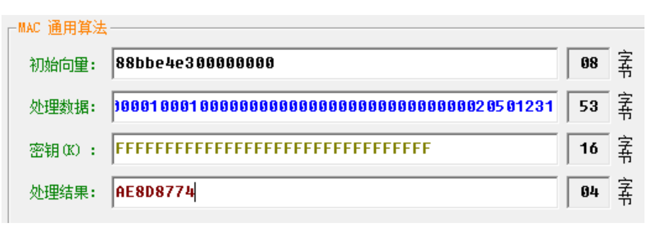
permission) F0 (add permission) FF (default FF) FF (default FF)
Note: **28–>A8 28=00101000 high bit change 1 i.e.: 10101000=A8 (plaintext + MAC address).**

- **Create Document 17 (binary)**
  Send command: **80E00017072805DCF0F0FFFF**
  Command reply: 9000 (created successfully).
  Instruction Description: 80 (CLA) E0 (INS) 0017 (P1 P2 File ID) 07 (Lc) 28 (Binary) 05DC (File Space) F0 (Read Permission) F0 (Add Permission) FF (Default FF) FF (Default FF)
- **Create Document 18 (Circular File)**
  Send Command: **80E00018072E0A17F0EFFFFFFF**
  Command Reply: 9000 (Created Successfully).
  Instruction Description: 80 (CLA) E0 (INS) 0018 (P1 P2 File ID) 07 (Lc) 2E (Loop File) 0A17 (File Space) F0 (Read Permission) EF (Add Permission) FF (Default FF) FF (Default FF)
- **Create a wallet file (electronic passbook)**
  Send command: **80E00001072F0208F100FF18**
  Command reply: 9000 (created successfully).
  Instruction Description: 80 (CLA) E0 (INS) 0001 (P1 P2 File ID) 07 (Lc) 2F (PBOC ED/EP) 0208 (Default 0208) F1 (Right to Use) 00 (Reserve 00) FF (Default FF) 18 (Transaction Details File Short ID)
- **Create a wallet file (e-wallet)**
  Send command: **80E00002072F0208F000FF18**
  Command reply: 9000 (created successfully).
  Instruction Description: 80 (CLA) E0 (INS) 0002 (P1 P2 File ID) 07 (Lc) 2F (PBOC ED/EP) 0208 (Default 0208) F0 (Right to Use) 00 (Reserved 00) FF (Default FF) 18 (Transaction Details File Short ID)

Writing of data (binary data, record data).

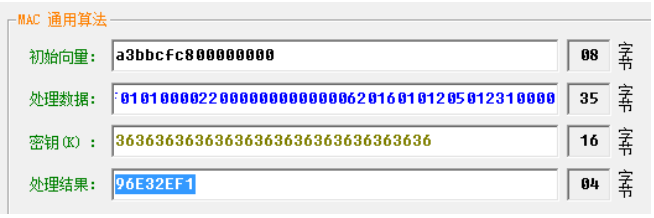
MF is written to file 05

- **Select MF**
  Send command: 00A40000023F00
  Command reply: 6f15840e315041592e5359532e4444463031a5038801019000
- **Take the random number**
  Send the instruction: 0084000004
  Command reply: 88bbe4e39000
- **Calculate MAC by writing data**
  Calculate MAC The MAC calculation method can be searched by Baidu for PBOC MAC calculation tool
  Data source: 04D6850034000122000001FFFF2200000000000000600012016102800000000000001000100000000000000000000000000020501231
  Initial vector: 88bbe4e3000000000 (random number +00000000).
  Key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AE8D8774 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFFFF
  Send command:
  04D6850034000122000001FFFF2200000000000000600012016102800000000000001000100000000000000000000000000020501231AE8D8774 (instruction + MAC)
  Command reply: 9000 (added successfully).
  Instruction description: 04 (CLA) D6 (INS) 85 (file ID) 00 (write data offset) 34 (Lc data + MAC) 000122000001FFFF2200000000000000600012016102800000000000001000100000000000000000000000000020501231 (data write according to the situation, You can arbitrarily define) AE8D8774 (MAC)
  MAC calculation as shown in the following figure:



EF files are written under 15

- **Select MF**
  Send command: 00A40000023F00
  Command reply: 6f15840e315041592e5359532e4444463031a5038801019000
- **Select EF**
  to send the command: 00A4040009A00000000386980701
  Command Reply: 6f328409a00000000386980701a5259f0801029f0c1e0000000000000000000000000000000000000000000000000000000000000000009000
- **Take the random number**
  Send the instruction: 0084000004
  Reply to the instruction: a3bbcfc89000
- **Calculate MAC by writing data**
  Calculate MAC The MAC calculation method can be searched by Baidu PBOC MAC calculation tool
  Data source: 04D695002200012200000 1FFFF0101000022000000000000062016010120501231000 0
  Initial vector: a3bbcfc800000000 (random number + 00000000)
  Key: 36363636363636363636363636363636 (line protection key under the respective file)
  Result: 96E32EF1
  Send command: 04D695002200012200000 1FFFF0101000022000000000000062016010120501231000096E32EF1 (instruction + MAC)
  Command reply: 9000 (added successfully).
  Command description: 04 (CLA) D6 (INS) 95 (file identifier) 00 (write data offset) 22 (Lc Date+Mac)
  000122000001FFFF0101000022000000000000062016010120501231000 0 (data can be defined as needed) 96E32EF1 (MAC)
  The MAC is calculated as follows:



At this point, a CPU that can be recharged and consumed normally has been sent.