FUDAN MICROELECTRONICS

复旦微电子

FMCOS2.0

专用技术手册

2009. 7

目 录

1 FMCOS 发卡命令

1.1 擦除目录文件 ERASE DF

1.1.1 定义和范围

ERASE DF 命令用于在满足目录擦除条件的情况下，擦除当前 DF 下所有文件（不包括目录本身）。

1.1.2 命令报文

ERASE DF 命令报文编码如下：

代码	值
CLA	80
INS	0E
P1	00
P2	00
Lc	00
Data	不存在
Le	不存在

1.1.3 命令报文数据域

命令报文数据域不存在。

1.1.4 响应报文数据域

响应报文数据域不存在。

1.1.5 响应报文状态码

此命令执行成功的状态码是'9000'。

IC 卡可能回送的错误状态码如下所示：

SW1 SW2	含 义
65 81	写 EEPROM 不成功
69 82	擦除权限不满足

说明：擦除当前 DF 下所有文件，擦除 DF 后即可任意在该 DF 下建立文件而不受建立权限的控制，当建立 KEY 文件后下次再进入 DF 将受权限控制，因此建议 DF 的擦除权限应设计为最高，若不允许擦除设为 EF 即可。擦除 DF 成功后，DF 下所有基本文件 EF 及下级目录文件 DF 都将丢失，成为一个空的 DF，但 DF 本身及其 DF 的各权限及空间大小均不变。

若当前目录为 MF，则除 MF 外卡上所有基本文件 EF 和目录文件 DF 均被删除。

1.2 增加或修改密钥 WRITE KEY

1.2.1 定义和范围

WRITE KEY 命令用于在密钥文件中增加或修改密钥

1.2.2 命令报文

WRITE KEY 命令报文如下

代码	值
CLA	80/84
INS	D4
P1	01：表示此条 WRITE KEY 命令 用来添加密钥
	XX：表示此条 WRITE KEY 命令 用来更新 P1 中指定类型的密钥
P2	密钥标识
Lc	见命令报文数据域
Data	
Le	不存在

1.2.3 命令报文数据域

- CASE1：内部认证密钥、TAC 密钥、消费、圈提、圈存、修改透支限额

CLA	INS	P1	P2	Lc	DATA					
80	D4	01	密钥标识	0D/15	30/34/3C/3D/3E/3F	使用权	更改权	密钥版本号	算法标识	8 或 10 字节密钥

- CASE2：增加外部认证密钥

CLA	INS	P1	P2	Lc	DATA					
80	D4	01	密钥标识	0D/15	39	使用权	更改权	后续状态	错误计数器	8 或 10 字节密钥

- CASE3：增加口令密钥

CLA	INS	P1	P2	Lc	DATA					
80	D4	01	密钥标识	07-0D	3A	使用权	EF	后续状态	错误计数器	02-08 字节口令

- CASE4：增加解锁口令密钥

CLA	INS	P1	P2	Lc	DATA					
80	D4	01	密钥标识	0D/15	37	使用权	更改权	FF	错误计数器	8 或 10 字节密钥

- CASE5：增加文件线路保护、重装口令密钥的密钥

CLA	INS	P1	P2	Lc	DATA					
80	D4	01	密钥标识	0D/15	36/38	使用权	更改权	FF	错误计数器	8 或 10 字节密钥

密钥类型	意义
30：	内部认证密钥（加密密钥）
34：	TAC 密钥
36：	文件线路保护密钥
37：	解锁口令密钥
38：	重装口令密钥的密钥
39：	外部认证密钥
3A：	口令密钥
3C：	修改透支限额

密钥类型	意义
3D：	圈提密钥
3E：	消费密钥
3F：	圈存密钥

增加密钥命令编码如下：

说明：

- 密钥标识不可为 FF；
- 口令密钥的长度可变（为 2-8 个字节）。
- 添加新密钥时只支持明文和密文 MAC 两种方式，不支持明文 MAC 方式
- 对于密钥也可以使用线路保护。如需进行线路保护，只需在安装密钥时将密钥类型次高位置 1 即可。如 PIN 类型由 3A 变为 7A。
- 对于密钥也可以使用线路加密保护。如需进行线路加密保护，只需在安装密钥时将密钥类型最高位置及次高位置均置 1 即可。如内部密钥类型由 30 变为 F0。

[注]：在一个应用下只能有一个文件线路保护密钥，一个密钥线路保护密钥，一个重装口令密钥的密钥。

如果该目录下某类型密钥只有一个,则其密钥标识原则上应为'00'，否则，应从'01'顺序开始。

- 使用权限：指该密钥在使用时如核对、认证、运算时所需满足的条件。
  例如：使用权为 41 表示在使用该密钥时当前目录安全状态寄存器值必须大于等于 1 且小于等于 4。
- 更改权限：指用 WRITE KEY 更改密钥内容的权限,在满足该条件时可使用 WRITE KEY 更改密钥内容，但不能改变错误计数器的值。
- 错误计数器：高半字节指出密钥可以连续错误的最多次数，低半字节指出还可以再试的次数。如果连续错误错超过规定的次数，密钥自动被锁死。
  例如：错误计数器的值为 33，表示该密钥最多可以连续错误 3 次，若输错一次则其值变为 32，再错一次之后变为 31，若下次核对或认证正确则该值变为 33。
  使用解锁口令时，解锁口令正确后错误次数低半字节被设置成高半字节值，同时口令被修改。解锁口令若错误，解锁口令允许再试次数减一，解锁口令和外部认证密钥锁死后无法被解锁。
- 后续状态：当口令核对成功或外部认证成功后，置安全状态寄存器值为后续状态的低半字节。

修改密钥命令编码如下：

- 在修改时密钥时，密钥头和密钥值等数据的长度必须和原有密钥相同。
- 并使用如下参数

P1	P2
密钥类型	密钥标识

数据域参数和添加密钥时相同。

1.2.4 响应报文数据域

响应报文数据域不存在。

1.2.5 响应报文状态码

此命令执行成功的状态码是'9000'。

IC 卡可能回送的错误状态码如下所示：

SW1 SW2	意 义
65 81	写 EEPROM 不成功
67 00	密钥长度错误

69 82	增加或修改权限不满足
69 83	密钥被锁死
6A 82	KEY 文件未找到
6A 88	密钥未找到
6A 84	KEY 文件空间已满
93 02	修改密钥时线路保护错误

[例 1]：在密钥文件中明文写入密钥标识为 00 的 39 密钥（主控密钥）和标识为 00 的 36 密钥（文件线路保护密钥），并且今后都使用明文更新这两条密钥。

写入 39 密钥的命令报文为：

80 D4 01 00 15 39 F0 FA AA 88 39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 01 39 01

卡片返回相应数据为：90 00

写入 36 密钥的命令报文为：

80 D4 01 00 0D 36 F0 FA FF 33 36 FF 36 FF 36 FF 36 01

命令中 39 密钥的使用权限为任意权限，修改权限为 A 到 F，外部认证后续状态为 A，密钥重试次数为 8 次，密钥值为“39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 01 39 01”。

命令中 36 密钥的使用权限为任意权限，修改权限为 A 到 F，密钥重试次数为 3 次，密钥值为“FF FF FF FF FF FF FF FF”。

[例 2]：修改上例密钥文件中的 00 的 39 密钥（主控密钥）和标识为 00 的 36

修改 39 密钥的命令为：

80 D4 39 00 15 39 F0 FA AA 88 39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 02 39 02

修改 36 密钥的命令为：

80 D4 36 00 0D 36 F0 F0 FF 66 36 FF 36 FF 36 FF 36 02

命令将 39 密钥的值修改为“39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 02 39 02”

命令将 36 密钥的值修改为“36 FF 36 FF 36 FF 36 02”，同时将 36 密钥的错误重试次数设定在了 6 次。

[例 3]：密文带 MAC 更新上例中的 39 密钥和 36 密钥。

首先将 39 密钥的密钥类型的高两位置 1，命令为：

80 D4 39 00 15 F9 F0 FA AA 88 39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 02 39 02

由于高两位置 1，明文修改将报错，此时需使用密文带 MAC 方式修改密钥，命令为：

84 D4 39 00 1C XX XX XX XX XX XX XX XX XX XX XX XX XX XX…..

（密文数据由以下数据加密而成 15 F9 F0 FA AA 88 39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 03 39 03 80 00，使用原 39 00 密钥“39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 02 39 02”，再使用同样密钥计算 MAC）

36 密钥按照 39 密钥同样方法更新，命令为：

80 D4 36 00 0D F6 F0 F0 FF 66 36 FF 36 FF 36 FF 36 02

80 D4 36 00 14 XX XX XX XX XX XX…….

（密文数据由以下数据加密而成 0D F6 F0 F0 FF 66 36 FF 36 FF 36 FF 36 03 80 00，使用原 39 00 密钥“39 FF 39 FF 39 FF 39 FF 39 FF 39 FF 39 02 39 02”，再使用同样密钥计算 MAC）

1.3 建立文件 CREATE FILE

1.3.1 定义和范围

CREATE FILE 命令用于建立文件系统，包括 MF、DF 和 EF。

1.3.2 命令报文

CREATE FILE 命令的报文如下：

代码	值
CLA	80
INS	E0
P1	文件标示 (File ID)
P2	
Lc	XX
Data	文件控制信息和 DF 名称

1.3.3 命令报文数据域

命令报文数据域包括文件控制信息，如果建立的文件为 DF，则还可能包括 DF 的名称。DF 的名称长度为 2~16 字节。各种文件的控制信息列表如下：

- 目录文件 DF（包括 MF）

文件类型	文件空间	建立权限	擦除权限	应用文件 ID	保留字	DF 名称
38	2 字节	1 字节	1 字节	XX	FF FF	5~16 字节

说明：建立 MF 时，P1 P2 参数固定为 3F 00，文件空间为 FF FF。保留字和 DF 名称域为卡片的传输代码，该传输代码事先约定，默认值为 8 字节 FF。

应用文件 ID：如在 Select File 时需要返回的文件为 0015，则此字节为 95。

目录文件（除 MF 外）建立后不能被自动选择。

- 基本文件 EF（包括密钥文件）

文件类型	命令报文数据域					
文件类型	BYTE1	BYTE2~3		BYTE4	BYTE5	BYTE6	BYTE7
二进制文件	28	文件空间		读权限	写权限	FF	见说明
定长记录文件	2A	文件空间		读权限	写权限	FF	见说明
循环文件	2E	文件空间		读权限	写权限	FF	见说明
PBOC ED/EP	2F	02	08	使用权限	保留（00）	FF	交易记录短标识
变长记录文件	2C	文件空间		读权限	写权限	FF	见说明
密钥文件	3F	文件空间		DF 文件短标识符	增加权限	FF	FF

- 如果希望使用明文 MAC 写 BYTE1 最高位需置 1（“28”变为“A8”）
  如果希望使用加密写，则 BYTE1 次高位需置 1（“28”变为“68”）
- 基本文件 EF（密钥文件、PBOC ED/EP 文件除外）的保留字的最后一个字节定义如下：（设该字节的为定义为 b8～b1）：

b8	b7	b6	b5	b4	b3	b2	b1	含 义
1	-	-	-	-	-	-	-	文件不支持带线路保护读
0	-	-	-	-	-	-	-	文件必须使用带线路保护读

b8	b7	b6	b5	b4	b3	b2	b1	含 义	
-	1	1	1	-	-	-	-	保留为 1	
-	-	-	-	1	1	-	-	读操作时使用的密钥标识	标识为 00 的密钥
-	-	-	-	1	0	-	-		标识为 01 的密钥
-	-	-	-	0	1	-	-		标识为 02 的密钥
-	-	-	-	0	0	-	-		标识为 03 的密钥
-	-	-	-	-	-	1	1	写操作时使用的密钥标识	标识为 00 的密钥
-	-	-	-	-	-	1	0		标识为 01 的密钥
-	-	-	-	-	-	0	1		标识为 02 的密钥
-	-	-	-	-	-	0	0		标识为 03 的密钥

- 对于记录文件（包括定长记录文件、循环文件、钱包文件），文件空间第一个字节为记录总个数，第二个字节为记录长度；物理空间总数为（个数*(记录长度+1) +8）。
- 对于密钥文件中所谓 DF 文件短标识符、说明如下：当高三位为 000 时，为 DDF 当高三位为 100 时为 ADF 的短文件标示符号。
- 对于 PBOC ED/EP 中所谓的 TAC 密钥标识是指该 ED/EP 在计算 TAC 时使用到的密钥类型为‘34’密钥的标识；所谓交易明细文件是指 ED/EP 在记录交易明细时用到的短文件标识符。
- 所有文件建立后不能自动被选择。

1.3.4 响应报文数据域

响应报文数据域不存在。

1.3.5 响应报文状态码

此命令执行成功的状态码是’9000’。

IC 卡可能回送的错误状态码如下所示：

SW1 SW2	意 义
67 00	错误的长度
69 82	建立权限不满足
6A 80	记录个数小于 2 或目录级数大于三级
6A 84	文件没有足够空间
6A 86	文件已存在

2 FMCOS 发卡范例

命令作用	命令代码
建立 MF	80E03F000D38FFFFF0F001FFFFFFFFFFFFFF
建立密钥文件	80E00000073F005001F0FFFF
线路保护密钥	80D401000D**36**F0F0FF33FFFFFFFFFFFFFFFF
外部认证密钥	80D401001**39**F0F0AA33FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
建立定长记录文件	80E00001072A0213F000FFFF
添加文件记录[注一]	00E200081361114F09A00000000386980701500450424F43
建立 EF	80E03F011138036FF0F095FFFFA00000000386980701
选择 EF（必须）	00A4040009A00000000386980701
建立密钥文件	80E00000073F018F95F0FFFF
内部密钥	80D401001**34**F00200013434343434343434343434343434343434
线路保护密钥	80D401001**36**F002FF33363636363636363636363636363636363636
口令解锁密钥	80D401001**37**F002FF33373737373737373737373737373737373737
口令重装密钥	80D401001**38**F002FF33383838383838383838383838383838383838
外部认证密钥	80D401001**39**F00244333939393939393939393939393939393939
消费密钥	80D40101153**E**F00200013E013E013E013E013E013E013E013E013E01
消费密钥	80D40102153**E**F00200013E023E023E023E023E023E023E023E023E02
圈存密钥	80D40101153**F**F00200013F013F013F013F013F013F013F013F013F01
圈存密钥	80D40102153**F**F00200013F023F023F023F023F023F023F023F023F02
圈提密钥	80D40101153**D**F00201003D013D013D013D013D013D013D013D013D01
圈提密钥	80D40102153**D**F00201003D023D023D023D023D023D023D023D023D02
修改透支限额密钥	80D40101153**C**F00201003C013C013C013C013C013C013C013C013C01
修改透支限额密钥	80D40102153**C**F00201003C023C023C023C023C023C023C023C023C02
口令(PIN)	80D401000D**3A**F0EF013312345FFFFFFFFFF
建立二进制文件[注二] (线路保护读写)	80E0001507A8001EF0F0FFFF
写二进制文件	MAC1(04D69500,1E,1111222233330006030100061998081700000030199808151998121555 66,,3636363636363636363636363636363636)
建立二进制文件[注三]	80E0001607A80027F0F0FFFF
写二进制文件	MAC1(04D69600,27,000053414D504C4520434152442041444631000000003131303130323938313231383030313005,,363636363636363636363636363636)
建立二进制文件	80E00017072805DCF0F0FFFF
写二进制文件	04D69700(长度)（照片数据）
建立循环文件	80E00018072E0A17F1EFFFFF
建立钱包文件 (电子存折)	80E00001072F0208F100FF18
建立钱包文件 (电子钱包)	80E00002072F0208F000FF18

注一：
定长记录文件内容为“文件控制信息（file control information）”
61-11:(4F-09:A00000000386980701);50-04:(50424F43)
50 42 4F 43 为 PBOC 的 ASC 码
如果需要采用线路保护写数据，则用以下命令：

MAC1(04E20008,13,61114F09A00000000386980701500450424F43,,FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)

注二：
文件标识为 15，此文件为 ED/EP 应用的公共应用基本数据文件
在下一条命令中写入的二进制文件数据格式内容为：

文件标识		‘15’(十六进制)
文件类型		二进制文件
文件大小		59
字节	数据元	长度
1-8	发卡方标识	8
9	应用类型标识	1
10	应用版本	1
11－20	应用序列号	10
21－24	应用启动日期	4
25－28	应用有效日期	4
29-30	发卡方自定义 FCI 数据	2

注三：
文件标识为 16，此文件为 ED/EP 应用的持卡人基本数据文件
在下一条命令中写入的二进制文件数据格式内容为：

文件标识		‘16’(十六进制)
文件类型		二进制文件
文件大小		31
字节	数据元	长度
1	卡类型标识	1
2	本行职工标识	1
3-22	持卡人姓名	20
23-30	持卡人证件号码	16
31	持卡人证件类型	1

注四：
文件标示为 17，此文件保存持卡人照片信息

文件标识		‘17’(十六进制)
文件类型		二进制文件
文件大小		1．5K
字节	数据元	长度
1-5DC	照片信息	1.5K

版本信息

版本号	更新日期	修改人	更新内容
1.0	2008-7-16	陆俊	初稿
1.1	2009-5-13	陆俊	整理现有手册版本，去除通用手册中重复部分。

上海复旦微电子股份有限公司销售及服务网点

上海复旦微电子股份有限公司
地址：上海市国泰路 127 号 4 号楼
邮编：200433
电话：(86-21) 6565 5050
传真：(86-21) 6565 9115

上海复旦微电子（香港）股份有限公司
地址：香港九龙尖沙咀东嘉连威老道 98 号东海商业中心 5 楼 506 室
电话：(852) 2116 3288　2116 3338
传真：(852) 2116 0882

北京办事处
地址：北京市东城区东直门北小街青龙胡同 1 号歌华大厦 B 座 419E 室
邮编：100007
电话：（86-10）8418 6608　8418 7486
传真：（86-10）8418 6211

深圳办事处
地址：深圳市华强北路圣廷苑酒店世纪楼 1301 室
邮编：518028
电话：(86-755) 8335 3211　8335 6511
传真：(86-755) 8335 9011

公司网址：**http://www.fmsh.com/**