建设部 PSAM 卡

参考手册

2008 年 12 月

目录

1 消费交易流程

消费交易是在终端上以脱机的形式进行的，PSAM 卡存放在执行消费交易的终端中，交易流程如下图所示：

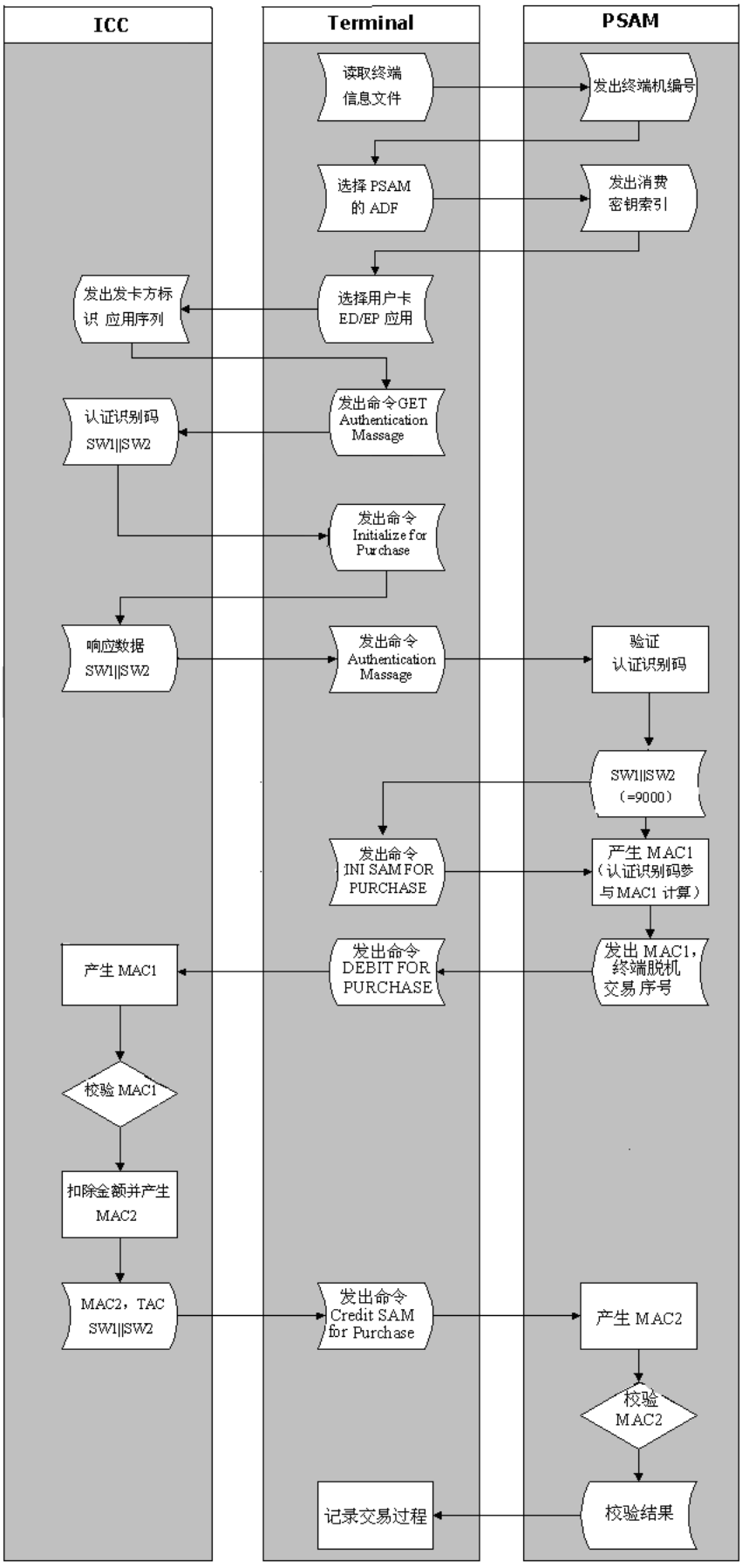
ICC
Terminal
PSAM
读取终端信息文件
发出终端机编号
选择 PSAM 的 ADF
发出消费密钥索引
发出发卡方标识 应用序列
选择用户卡 ED/EP 应用
认证识别码 SW1||SW2
发出命令GET Authentication Massage
发出命令 Initialize for Purchase
响应数据 SW1||SW2
发出命令 Authentication Massage
验证 认证识别码
SW1||SW2 (=9000)
发出命令 INI SAM FOR PURCHASE
产生 MAC1（认证识别码参与MAC1 计算）
产生 MAC1
发出命令 DEBIT FOR PURCHASE
发出 MAC1，终端脱机交易 序号
校验 MAC1
扣除金额并产生 MAC2
MAC2，TAC SW1||SW2
发出命令 Credit SAM for Purchase
产生 MAC2
校验 MAC2
记录交易过程
校验结果

图 4-1 消费交易流程图

2 命令

q 传输协议 T=1，参数 L_e =0 时，发送所有响应数据。

SM 命令传输

如果命令以安全报文方式(SM)传输，命令结构将不会改变；安全报文编码为命令数据域的一部分。

响应

卡通过响应向终端命令作出反应。响应至少包含两个状态字节(尾标)，附加数据部分根据不同命令包含所需要的不同数据。

表 7-2 响应结构

Body	Trailer	
DATA	SW1	SW2

命令执行成功后，典型的响应报文为 SW1=‘90’和 SW2=‘00’。

2.1 建设部 PSAM 卡命令简介

2.1.1 响应一览表

下表列出建设部 PSAM 卡对命令作出的全部响应。

表 7-3 建设部 PSAM 卡的响应列表

	代码	说明
正常操作	’90 00’	正常处理
	’61 xx’	正常处理；‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
警告	’63 Cx’	‘x’为计数器值,准确意义根据命令而定
执行错误	’64 00’	标志状态位未变
	’65 81’	内存失败
校验错误	’67 00’	长度错误
	’68 82’	不支持安全报文
	’69 00’	无法处理
	’69 01’	无效状态
	’69 81’	命令与文件结构不兼容
	’69 82’	不满足安全状态
	’69 83’	认证方法锁定 或 个人密码锁定
	’69 84’	引用数据无效
	’69 85’	不满足使用条件
	’69 86’	不满足命令执行的条件(不是当前 EF)
	’69 87’	安全报文数据项丢失
	’69 88’	安全报文数据项不正确
	‘6A 80’	数据域参数不正确
	‘6A 81’	功能不支持；应用被锁定
	‘6A 82’	未找到文件
	‘6A 83’	未找到记录
	‘6A 84’	文件内存空间不足
	‘6A 86’	参数 P1/P2 不正确
	‘6A 88’	未找到引用数据

	‘6B 00’	参数不正确；偏移地址超出 EF
	‘6C xx’	Le 长度错误；SW2 标明准确长度
	‘6F 00’	判断不准确；数据无效
	‘6F 01’	公钥不完整
	‘6F 08’	KFL 长度不正确
	‘6F 81’	系统错误
	’93 02’	MAC 不正确
	’93 03’	应用永久锁定
	’94 01’	金额不足
	’94 03’	密钥索引不支持

2.1.2 APPLICATION UNBLOCK（应用解锁）命令

如果 MAC 正确且应用未被永久锁定，*APPLICATION UNBLOCK* 命令将恢复当前被锁的应用。命令成功执行后，MAC 的错误计数器将被重置。

注

- 该命令需要计算安全报文鉴别码 SM-MAC，SM-MAC 由应用维护密钥（AMK）对相关数据加密而得。
- 如果当前应用未被锁定，*APPLICATION UNBLOCK* 命令将仍然可以执行。
- 如果 *APPLICATION UNBLOCK* 命令的执行失败三次，则当前的应用将被永久锁定。

  先前状态： 当前应用的状态

  后续状态： 状态将不会改变

命令

CLA	INS	P1	P2	Lc	DATA
‘84’	‘18’	‘00’	‘00’	‘04’	SM-MAC（4 字节）

DATA

SM-MAC 的计算参见 6.2 节

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
‘6x xx’	正确执行(61 XX)或 SM-MAC 错误(63 CX)

’69 83’	认证方法(应用维护密钥)被锁定
’93 03’	应用被永久锁定
’69 82’	安全条件不满足

2.1.3 AUTHENTICATION MASSAGE 命令

每次执行 MAC1 计算（*INT_SAM_FOR_PURCHASE*）命令前，卡片必须先执行 *AUTHETICATION MASSAGE* 命令，否则执行 *INT_SAM_FOR_PURCHASE* 命令时将返回错误状态码‘6985’。

注

- 为使用该命令，必须在密钥文件中定义一个新的密钥用途，PK=0x1B(VK=0x01)，用于装载和使用对应密钥 MCK；
- 执行该命令时，卡片用 MCK 对输入的 5 个字节数据（MID||UID0UID1UID2UID3）进行特定的计算得出认证识别码，再用计算得到认证识别码与送入的认证识别码比对，若正确才允许执行 *INT_SAM_FOR_PURCHASE*（MAC1 计算）命令；
- 该命令允许永远尝试下去，不设置尝试计数器。

命令

CLA	INS	P1	P2	Lc	DATA
‘80’	‘CA’	‘00’	‘00’	‘09’	MID||UID0UID1UID2UID3||认证识别码

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
’63 00’	认证识别码出错
’67 00’	长度错误
’6A 80’	数据域结构错误
’6A 86’	P1/P2 出错
’6D 00’	INS 错误或不支持
6E 00’	CLA 错误或不支持

2.1.4 CACULATE KEY(计算密钥)命令

CALCULATE KEY 命令是标准的建设部 SAM 专用命令，是实现在 SAM 卡的控制下，使用 MIFARE ONE 卡作为用户卡，计算逻辑加密卡的扇区密钥。

注

- 计算得到的密钥按顺序在响应报文中送出。
- 标准的建设部 SAM 专用命令的使用
  - 所有算法均采用 TripleDES（3DES），通讯速率为 38400bps，通讯协议为 T=0。
  - 根据 P2 指定的 KID 查找逻辑加密卡专有密钥
  - 用查找到的密钥对数据域的前 8 个字节加密
  - 比较加密结果前 4 个字节和数据域中的 MAC，如果不同则返回错误
  - 再用此密钥对以下数据加密：
    唯一号（4 字节）+流水号（2 字节）+MAC 高字节（1 字节）+ 扇区标识 1（1 字节）
  - 取加密结果的高 6 字节为 MIFARE 的一组密钥
  - 将加密数据中的扇区标识 1 换成扇区标识 2、3、4、5（如果有），计算相应 的密钥。
  - 例如：设卡中有 KID=‘01’，密钥值‘12 34 56 78 9A BC DE F0 12 34 56 78 9A BC DE F0’的逻辑加密卡专有密钥；因此发向 SAM 卡的命令为 80 FC 00 01 0E FE DC BA 98 76 54 32 10 4A B6 5B 3D 01 02　则返回结果为 6C DF 72 41 82 27　　18 41 9D 72 D0 C9
- 扩展的建设部 SAM 专用命令的使用
  - P1 必须不等于‘00’
  - COS 内部按 P1 指定的 KID 查找逻辑加密卡认证密钥
  - 使用查找到的逻辑加密卡认证密钥对数据域的前 8 个字节加密
  - 比较加密结果前 4 个字节和数据域中的 MAC，如果不同则返回错误
  - 根据 P2 指定的 KID 查找逻辑加密卡专有密钥
  - 用查找到的逻辑加密卡专有密钥对以下数据加密：
    唯一号（4 字节）+流水号（2 字节）+MAC 高字节（1 字节）+ 扇区标识 1（1 字节）
  - 取加密结果的高 6 字节为 MIFARE 的一组密钥；
  - 将加密数据中的扇区标识 1 换成扇区标识 2、3、4、5（如果有），计算相应 的密钥。
  - 例如：设卡中有 01 号的逻辑加密卡专有密钥 12 34 56 78 9A BC DE F0 12 34 56 78 9A BC DE F0；有 01 号的逻辑加密卡认证密钥 00 11 22 33

44 55 66 77 88 99 AA BB CC DD EE FF；发向 SAM 卡命令为：80 FC 01 01 0E FE DC BA 98 76 54 32 10 69 1C 58 65 01 02　　则返回结果为：F2 49 55 7A 78 50　E1 1B 8C 30 70 9B

命令

CLA	INS	P1	P2	Lc	DATA	Le
‘80’	‘FC’		KID	‘0D’ ~ ‘11’		‘06’ ~ ‘1E’

P1

P1=‘00’—标准模式，按标准的建设部 SAM 专用命令进行认证及扇区密钥的计算

P1≠‘00‘—扩展模式，按扩展的建设部 SAM 专用命令进行认证及扇区密钥的计算，P1 为逻辑加密卡认证密钥的标识

P2

KID　逻辑加密卡专用密钥的标识

DATA

IND_CT　城市代码(2 字节)

CSN　卡片唯一号(4 bytes)

SN　流水号(2 bytes)

MAC　认证 MAC (4 bytes)

IND_sec1　扇区标识 1 (1 byte)

IND_sec2　扇区标识 2 (1 byte)

IND_sec3　扇区标识 3 (1 byte)

IND_sec4　扇区标识 4 (1 byte)

IND_sec5　扇区标识 5 (1 byte)

响应

DATA	SW1	SW2
	‘90’	‘00’

DATA

KV1　扇区 1 的密钥值(6 bytes)

KV2　扇区 2 的密钥值(6 bytes)

KV3　扇区 3 的密钥值(6 bytes)

KV4　扇区 4 的密钥值(6 bytes)

KV5　扇区 5 的密钥值(6 bytes)

状态码

代码	说明
’61 xx’	命令正确执行，‘xx’ 为要取响应的长度
’67 00’	数据长度错误
’69 85’	使用条件不满足(应用临时被锁定)
‘6A 81’	功能不支持(文件不可建立在 MF 或 DF)
‘6A 86’	P1 或 P2 参数不正确
‘6D 00’	不正确的 INS
‘6E 00’	不正确的 CLA
’93 03’	应用永久锁定
’94 03’	密钥索引不支持

2.1.5 CREDIT_SAM_FOR_PURCHASE（校验 MAC2）命令

CREDIT_SAM_FOR_PURCHASE 命令利用 *INIT_SAM_FOR_PURCHASE* 命令产生的过程密钥 SESPK 校验 MAC2。

注

- 检查 MAC2 尝试计数器；
- PSAM 在其内部用 SESPK 对交易金额加密得到 MAC2；
- 加密产生的 MAC2 与用户卡送出的 MAC2 进行比较；
- 如命令执行不成功，PSAM 卡将 MAC2 尝试计数器减 1，并返回状态码‘63 CX’， 这里‘X’ 是 MAC2 尝试计数器的新值；
- 若命令执行成功，PSAM 卡将应用中的终端脱机消费交易序号加 1
  先前状态 = 准备执行 *CREDIT_SAM_FOR_PURCHASE* 命令状态
  后续状态 = 空闲状态

命令

CLA	INS	P1	P2	Lc	DATA
‘80’	‘72’	‘00’	‘00’	‘04’	MAC_2（4 字节）

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
’63 Cx’	MAC2 错误
’65 81’	内存失败

’67 00’	长度错误
’69 01’	命令不接受(无效状态)
’69 85’	使用条件不满足(应用被锁定)
’69 87’	MAC2 丢失
‘6A 80’	参数错误
‘6A 81’	应用被锁定
‘6A 86’	P1 或 P2 不正确
‘6D 00’	INS 不正确
‘6E 00’	CLA 不正确
’93 03’	应用被永久锁定

2.1.6 DES CRYPT（通用 DES 计算）命令

DES CRYPT 命令利用指定的密钥来进行运算。

注

- 若一条命令无法传输所有的待处理数据，可分几条命令输入；
- 加密计算采用 ECB 模式，数据的填充在卡片的外面进行，卡片只支持长度为 8 的整数倍的数据加密与 MAC 计算；
- *DES CRYPT* 命令必须在 *INIT_FOR_DESCRYPT* 命令执行成功后才能执行。若 MAC 的计算无后续数据块，则卡片的状态复原为通用 DES 计算初始化执行前的状态。MAC 计算参见 5.2 节；
- 本命令执行成功后，直到发送下一个 *DES CRYPT* 命令，临时密钥寄存器中的密钥保持有效；
- 当 P1 = xxxxx001 时，该命令也可用于计算圈存 MAC2，此时，命令使用密钥用途为 0x0B 的密钥，其输入数据为：
  - 用户卡伪随机数（4 字节）
  - ED/EP 联机交易序号（2 字节）
  - 交易金额（4 字节）
  - 交易类型标识（1 字节）
  - 终端机编号（6 字节）
  - 交易日期（4 字节）
  - 交易时间（3 字节）

  卡片收到这些数据后，首先用 INIT_FOR_DESCRYPT 命令产生的圈存子密钥对伪随机数||ED/EP 联机交易序号||‘8000’加密产生过程密钥，然后用该过程密钥对交易金额||交易类型标识||终端机编号||交易日期||交易时间按 PBOC 要求计算出用户卡圈存时的 MAC2。

命令

CLA	INS	P1	P2	Lc	DATA
‘80’	‘FA’		‘00’		

P1 值详细表示：

- P1 = xxxxx000　无后续块加密
- P1 = xxxxx001　最后一块 MAC 计算或计算圈存 MAC2
- P1 = xxxxx010　有后续块加密
- P1 = xxxxx011　下一块 MAC 计算
- P1 = xxxxx101　唯一一块 MAC 计算
- P1 = xxxxx111　第一块 MAC 计算
- P1 = 其他值保留

---

q *DES CRYPT* 命令使用 P1 = xxxxx001 参数计算圈存 MAC2 时，其初始向量为 8 字节的 0x00。

Lc

Lc 必须是 8 的模。

DATA

命令报文数据域包括要加密的数据。在 P1 的 bit3 位为 1 时，待处理数据的前 8 字节为计算 MAC 的初始向量，即 Data = Init_value || Block_1|| Block_2 || ……。

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
’63 Cx’	MAC2 错误
’65 81’	内存失败
’67 00’	长度错误
’69 01’	命令不接受(无效状态)
’69 85’	使用条件不满足(应用被锁定)
‘6A 80’	参数错误

‘6A 81’	应用被锁定
‘6A 86’	P1 或 P2 不正确
‘6D 00’	INS 不正确
‘6E 00’	CLA 不正确
’93 03’	应用被永久锁定

2.1.7 EXTERNAL AUTHENTICATION（外部认证）命令

PSAM 卡用 ***EXTERNAL AUTHENTICATION*** 命令通过 3DES 加密算法对卡片外部进行安全认证。终端对卡返回的随机数进行加密来进行认证。

注

- 执行 ***EXTERNALAUTHENTICATE*** 命令前要求从 PSAM 卡取回一个 4 或 8 字节的随机数，且随机数必须有效。若此随机数为 4 字节，终端对 4 字节随机数+‘00000000’进行加密得到 8 字节密文，若此随机数为 8 字节，则终端直接对 8 字节随机数进行加密得到 8 字节密文；
- 命令的 P2 参数表示外部认证使用的密钥的 KID，若 P2=0x00，表示使用默认的外部认证密钥(在建设部 PSAM 卡中,默认外证密钥即 CCK/ACK)；
- 指定使用的密钥必须支持外部认证功能，即其 PK 必须为 0x0E；
- 外部认证密钥的尝试计数器必须大于 0，表示密钥为可用状态，未锁定。如果卡片校验执行错误，尝试计数器减 1，当尝试计数器为 0 时，表示密钥被锁定，无法使用；
- 成功执行命令后，卡的状态将变为密钥定义的后续状态。

命令

CLA	INS	P1	P2	Lc	DATA
‘00’	‘82’	‘00’	KID	‘08’	DataEnc（8 字节）

DATA

DataEnc (8 字节) 即对随机数进行加密所得的 8 个字节数据。

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
’63 CX’	外部认证错误。X 表示剩余的尝试次数
’67 00’	长度错误
’69 82’	安全条件不满足

’69 83’	认证方法锁定
’69 85’	使用条件不满足，密钥类型错误
‘6A 81’	P1 或 P2 不正确
‘6A 88’	相关数据未找到，找不到指定的密钥

2.1.8 GET CHALLENGE（取随机数）命令

终端用 *GET CHALLENGE* 命令从 PSAM 卡中取回一个随机数，用于安全交易过程。

注

- 随机数通常是 4 或 8 个字节。
- 被返回的随机数同时也保存在 PSAM 卡内存 RAM 中，直到：
  - 又发出一个 *GET CHALLENGE* 命令；
  - 执行 *SELECT* 命令；
  - PSAM 卡下电。

命令

CLA	INS	P1	P2	Le
‘00’	‘84’	‘00’	‘00’	

响应

DATA	SW1	SW2
随机数	‘90’	‘00’

状态码

代码	含义
‘6A 81’	不支持此功能，应用被锁定
‘6A 86’	P1 或 P2 不正确

2.1.9 GET RESPONSE（取响应数据）命令

终端用 *GET RESPONSE* 命令从 PSAM 卡中取回响应报文。传输协议为 T=0 时，第四种情况的命令不能同时传送和接收数据，因此，根据 SO/IEC7816-4 的规定，在执行这种命令时，必须用 *GET RESPONSE* 命令来得到它的响应报文。

如果第二种情况的命令或第四种情况的命令使用安全报文的形式传送数据，命令执行后必须用命令 *GET RESPONSE* 取回响应报文。

注

- PSAM 卡确认应用命令执行正确则返回代码’61 xx’。

- 响应数据可以用一次或多次命令 ***GET RESPONSE*** 来取回响应报文。
- 当读文件命令 ***READ BINARY*** 超出文件的长度时，若 T=1 时则响应报文状态码为 ‘62 82’，若 T=0 时,状态码为 ’61 xx’。

命令

CLA	INS	P1	P2	Le
‘00’	‘C0’	‘00’	‘00’	xx

响应

DATA	SW1	SW2
响应报文数据	‘90’	‘00’

状态码

代码	说明
‘62 81’	回送的数据可能有错
‘64 00’	标识状态位未变
‘67 00’	长度错误
‘6A 86’	P1 或 P2 不正确
‘6C xx’	长度错误(Le 不正确，‘XX’表示实际长度)
‘6F 00’	数据无效

2.1.10 INTERNAL AUTHENTICATION（内部认证）命令

通过 ***INTERNAL AUTHENTICATION*** 命令，终端设备可以采用 DES 加密算法来对 PSAM 卡片进行认证。对于这个认证，卡片需要对接收到的随机数进行加密，并将加密结果返回到终端设备。

注

- ***INTERNAL AUTHENTICATION*** 命令是由终端来执行校验，因此所使用的密钥的尝试计数器不会改变。但内部认证密钥的尝试计数器必须大于 0，表示该密钥未被锁定；
- 命令中的 P2=KID，如果 P2=0x00，表示使用默认的内部认证密钥进行认证（在建设部 PSAM 卡中，默认内证密钥即 CCK/ACK）；
- KID 指定使用的密钥必须支持内部认证功能，即 PK=0x0F；
- 卡片直接对 8 字节的终端随机数采用 3DES 算法进行计算，得到 8 字节密文数据，不使用任何初始向量和填充字符。

命令

CLA	INS	P1	P2	L_c	DATA	Le
‘00’	‘88’	‘00’	KID	‘08’		‘00’/‘08’

DATA

8 字节终端随机数。

响应

DATA	SW1	SW2
密文数据	‘90’	‘00’

状态码

代码	说明
‘6700’	Lc 长度错误
‘6982’	安全条件不满足
‘6983’	密钥已锁定
‘6985’	使用条件不满足，密钥类型错误
‘6A80’	数据域参数不正确
‘6A81’	参数 P1/P2 不正确
‘6A88’	未找到密钥

2.1.11 INIT_FOR_DESCRYPT（通用 DES 计算初始化）命令

INIT_FOR_DESCRYPT 命令用来初始化通用密钥计算过程。PSAM 卡将利用卡中指定的密钥进行运算，产生一个临时密钥。运算方式由指定的密钥类型、密钥分散级数和密钥算法标识确定。

注

- 以下三种类型的密钥不能产生临时密钥：
  - 主控密钥
  - 维护密钥
  - 消费密钥
- 产生双长度临时密钥的双长度密钥类型有：
  - PIN 解锁密钥
  - 用户卡应用维护密钥
- 双长度密钥左右异或产生单长度临时密钥的密钥类型有：
  - 重装 PIN 密钥

  TEMP_KEYreload =密钥左 8 位 ⊕ 密钥右 8 位
- 双长度密钥产生双长度临时密钥，单长度密钥产生单长度临时密钥的密钥类型有：
  - MAC 密钥

– 加密密钥
– MAC、加密密钥

指定密钥处理级数由分散级数和 Lc 确定，若二者不一致，则返回错误信息。

---

q 临时密钥在 PSAM 卡下电后自动无效，不允许读取。

命令

CLA	INS	P1	P2	Lc	DATA	Le
‘80’	‘1A’	PK	VK	N*8	待处理的数据	NP

Lc

Lc = Nx8 (数据长度 Lc 应跟密钥用途 PK 的高三位相匹配)

如果数据长度 Lc = 0, 则临时密钥跟原始密钥相同。

DATA

DATA= Data_n||… Data_2|| Data_1||

数据 1(Data_1)将首先被使用，然后是数据 2(Data_2) ….数据 n(Data_n);

当算法标识最高位置 1 时，过程密钥将在这条命令中产生。

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
‘65 81’	内存失败
‘67 00’	长度错误
‘69 85’	使用条件不满足(应用被锁定)
‘6A 80’	参数错误
‘6A 81’	应用被锁定
‘6A 86’	P1 或 P2 不正确
‘6A 88’	引用数据未找到
‘69 01’	命令不接受(无效状态)
‘6D 00’	INS 不正确
‘6E 00’	CLA 不正确
‘93 03’	应用被永久锁定

2.1.12 INIT_SAM_FOR_PURCHASE（MAC1 计算初始化）命令

INIT_SAM_FOR_PURCHASE 命令支持多级消费密钥分散机制。

注

- 产生 MAC1。分散的次数依赖于密钥文件中定义的主密钥用途(PK)；

  产生 MAC1 的过程：

  第一步： BMPK = (DMPK, PC_ID)

  第二步： MPK = (BMPK, BB_ID)

  第三步： DPK = (MPK, APP_NR)

  第四步： SESKEY = (DPK, (R_icc||NT_OFF_xx||NT_TERM))

  第五步： MAC1 = (SESKEY,

  （M_PUA||TT_IND||ID_TERM||DATE_T||TIME_T||安全认证数据))

- MAC1 计算中的安全认证数据（9 字节）为 *AUTHENTICATION MASSAGE* 命令的输入数据。

  先前状态. = 空闲状态

  后续状态 = *CREDIT_SAM_FOR_PURCHASE* 命令备用状态

命令

CLA	INS	P1	P2	Lc	DATA	Le
‘80’	‘70’	‘00’	‘00’	‘14’+8*N		‘08’

Lc

Lc = 14h + 8xN

N=1：只有应用序列号 APP_NR

N=2：只有应用序列号 APP_NR 和银行标识符 BANK_ID

N=3：有应用序列号 APP_NR、银行标识符 BANK_ID 以及城市标识符 CITY_ID。

DATA

数据域=用户卡随机数 R_icc(4bytes) || 用户卡脱机交易序列号 NT_OFF_XX(2 bytes) || 交易金额 M_P(4bytes) || 交易类型标识 NT_IND(1byte) || 终端交易日期 DATE_TERM(4bytes) || 终端交易时间 TIME_TERM(3bytes) ||消费密钥版本号 VK(1byte) || 消费密钥算法标识 ALGK(1byte) || 应用序列号 APP_NR (8bytes) || 银行标识符 BANK_ID(8 bytes) || 城市标识符 CITY_ID(8 bytes)

响应

DATA	SW1	SW2
	‘90’	‘00’

如果命令执行成功，从用户卡(ICC)返回 8 字节的响应报文数据：

- 4 字节终端脱机交易序号
- 4 字节报文校验码 MAC1

状态码

代码	说明
‘6A 86’	P1 或 P2 不正确
‘67 00’	长度错误
‘6A 80’	数据参数不正确(如：密钥分散级数与数据不符)
‘6A 81’	应用被锁定
‘6A 88’	引用数据未找到
‘69 88’	MAC 不正确
‘93 03’	应用被永久锁定
‘94 03’	密钥版本不支持
‘61 xx’	需发出 GET RESPONSE 命令
‘69 85’	使用条件不满足(应用被锁定)
‘69 01’	命令不接受(无效状态)
‘94 02’	交易序列号已达最大

2.1.13 MANAGE SECURITY ENVIRONMENT（安全环境管理）命令

在建设部 PSAM 卡中，*MANAGE SECURITY ENVIRONMENT* 命令在 *WRITE RSA KEY* 命令前使用，用于指定修改 PSAM 卡中的哪个 RSA 密钥对的公钥。

注

- 当在一个密钥在 *MANAGE SECURITY ENVIRONMENT* 命令数据域中被指定后，PSAM 卡将首先作如下操作：
  - 验证指定的密钥是否与输入的 CHR 一致；
  - 验证指定的密钥是否支持加/解密等功能；
  - 验证指定的密钥是否完整。

命令

CLA	INS	P1	P2	Lc	DATA

‘00’	‘22’	‘41’	‘B8’	‘06’—‘0D’	TLV 数据块

DATA

– CHR 的 TLV 结构：

T	L	V
‘83’	‘01’--‘08’	CHR

– 算法号的 TLV 结构（固定值）：

T	L	V
‘80’	‘01’	‘03’

响应

SW1	SW2
90	00

状态码

代码	说明
‘65 81’	内存失败
‘67 00’	长度错误
‘69 81’	命令与文件结构不相容，当前文件非所需文件
‘69 84’	相关数据无效
‘69 85’	使用条件不满足
‘6A 80	数据域结构不正确
‘6A 81’	P1/P2 出错
‘6A82’	该文件未找到
‘6A88’	找不到密钥
‘6F 01’	公钥不完整
‘6F 08’	KFL 长度不正确
‘6F 81’	系统出错

2.1.14 READ BINARY（读二进制文件）命令

READ BINARY 命令用于读取二进制文件中内容或部分内容。

被读取的 EF 文件可以通过 ***SELECT*** 等命令进行显式选择，也可以通过 ***READ BINARY*** 命令的 P1 字节进行隐式选择。

READ BINARY 命令只有在创建 EF 文件时设置的 AC READ 条件得到满足后，才能执行。

注

- 文件可以通过以下命令被选择：
  - *CREATE* 命令
  - *SELECT* 命令
  - *READ BINARY* 或 *UPDATE BINARY* 命令
- 若 P1 字节包含一个 EF 文件的短文件标识 SFI，则这个 EF 文件必定是当前 DF 下的文件。

命令

CLA	INS	P1	P2	Lc	DATA	Le
‘00’/’04’	‘B0’	OH	OL			

对于显式选择，OH 字节的编码如下：

b8	b7	b6	b5	b4	b3	b2	b1	说明
0								
	x	x	x	x	x	x	x	偏移量高字节

OL 表示偏移量低字节

偏移量=OH×‘100’+OL

对于隐式选择，OH 字节的编码如下：

b8	b7	b6	b5	b4	b3	b2	b1	说明
1	0	0						
			x	x	x	x	x	EF 文件的 SFI（1-31）

OL 字节表示偏移量

DATA

当 CLA= ‘00’时，不存在 Lc 字节和数据域

当 CLA=‘04’时，Lc=‘04’，DATA=MAC

Le

表示要读取的字节数，Le=‘00’表示读取文件的所有字节。

响应

DATA	SW1	SW2
读取的数据	90	00

状态码

代码	说明
‘65 81’	内存失败
‘67 00’	长度错误
‘69 81’	命令与文件结构不相容，当前文件非所需文件
‘69 82’	操作条件不满足
‘69 86’	不满足命令执行条件，当前文件不是 EF
‘6A 81’	应用被锁定
‘6A82’	该文件未找到
‘93 03’	应用被永久锁定

2.1.15 EAD RECORD（读记录文件）命令

READ RECORD 命令用于读取非二进制文件中内容。被读取的 EF 文件可以通过 *SELECT* 等命令进行显式选择，也可以通过 *READ RECORD* 命令的 P2 字节进行隐式选择。

READ RECORD 命令只有在创建 EF 文件时设置的 AC READ 条件得到满足后，才能执行。

注

- 文件可以通过以下命令被选择：
  - *CREATE* 命令
  - *SELECT* 命令
  - *READ RECORD/UPDATE RECORD* 命令
- 只有在读取条件满足时，才能执行 *READ RECORD* 命令；
- *READ RECORD* 命令一次只能读取一条记录；
- 若 P2 字节包含一个 EF 文件的短文件标识 SFI，则这个 EF 文件必定是当前 DF 下的文件。
-

命令

CLA	INS	P1	P2	Lc	DATA	Le
‘00’/’04’	‘B2’	NR	AM	‘00’/’04’	MAC(4 字节)	00

NR—Number

NR = 记录号（‘01’~‘FE’）

AM—访问模式

b8	b7	b6	b5	b4	b3	b2	b1	说明
0 x	0 x	0 x	0 x	0 x				文件选择： 当前已经被选择的文件 短文件标识符（SFI）
					1	0	0	P1 为记录序号

Lc

当 CLA = ‘00’时， Lc 不存在

当 CLA = ‘04’时， Lc = ‘04’

DATA

当 CLA =‘00’时，数据域不存在

当 CLA =‘04’时，数据域为 SM-MAC(4 字节)

响应

DATA	SW1	SW2
读取的记录	‘90’	‘00’

状态码

代码	说明
‘67 00’	长度错误
‘6A 81’	应用被锁定
‘6A 82’	该文件未找到
‘6A 83’	记录未找到

2.1.16 SELECT（选择文件）命令

本命令是 ISO7816-4 中 ***SELECT*** 命令的一个细分，由 STARCOS S2.1 SELECT 命令演化而来。它用来激活一个存在的文件或文件层。使用应用标识(AID)进行选择。

注

- ***SELECT*** 命令只能用来选择已经完全安装的相应文件；
- ***SELECT*** 命令自动激活新选择的应用，并终止先前的应用；
- 可以用应用标识(AID)来选择专用文件；也可以用应用标识(AID)的短标识来选择；
- 可以用文件标识(FID)来选择文件；

- 当采用 AID 方式选择应用文件时，通常响应报文中返回文件控制信息(FCI)。

先前状态：　　任何状态

后续状态：　　应用被激活或空状态 (MF or PSE 被选择)

命令

CLA	INS	P1	P2	Lc	DATA	Le
‘00’	‘A4’	‘00’/‘02’/‘04’	‘00’			xx

P1

P1=‘00’，表示用 FID 来选择 DF 文件或 EF 文件，Lc=‘02’；

P1=‘02’，表示用 FID 来选择 EF 文件，Lc=‘02’；

P1=‘04’，表示用 AID 来选择文件，Lc=‘01’-‘10’。

DATA

AID – 应用标识(1 – 16 bytes)

FID – 文件标识（2 bytes）

响应

DATA	SW1	SW2
FCI	‘90’	‘00’

成功选择 DDF 后回送的 FCI：

FCI 模板 (6F) || DF 名 (84) || FCI 专用数据 (A5) || 目录基本文件的 SFI (88)

成功选择 ADF 后回送的 FCI：

FCI 模板 (6F) || DF 名 (84) || FCI 专用数据 (A5) || 发卡方自定义数据的 FCI (9F0C)

状态码

代码	说明
‘65 81’	内存失败
‘67 00’	长度错误
‘6A 81’	应用被锁定
‘6A 82’	该文件未找到

2.1.17 UPDATE BINARY（写二进制文件）命令

UPDATE BINARY 命令用于更新二进制文件的内容(或部分内容)。

被读取的 EF 文件可以通过 *SELECT* 等命令进行显式选择，也可以通过 *UPDATE BINARY* 命令的 P1 字节进行隐式选择。

UPDATE BINARY 命令只有在创建 EF 文件时设置的 AC UPDATE 条件得到满足后，才能执行。

注

- 文件可以通过以下命令被选择：
  - *CREATE* 命令
  - *SELECT* 命令
  - *READ BINARY* 或 *UPDATE BINARY* 命令
- 若 P1 字节包含一个 EF 文件的短文件标识 SFI，则这个 EF 文件必定是当前 DF 下的文件；

命令

CLA	INS	P1	P2	Lc	DATA
‘00’/’04’	‘D6’	OH	OL		

对于显式选择，OH 字节的编码如下：

b8	b7	b6	b5	b4	b3	b2	b1	说明
0								
	x	x	x	x	x	x	x	偏移量高字节

OL 表示偏移量低字节

偏移量=OH×‘100’+OL

对于隐式选择，OH 字节的编码如下：

b8	b7	b6	b5	b4	b3	b2	b1	说明
1	0	0						
			x	x	x	x	x	EF 文件的 SFI（1-31）

OL 字节表示偏移量

Lc

若 CLA= ‘00’，Lc=更新数据的长度

若 CLA= ‘04’，Lc=更新数据的长度或更新数据密文的长度+4

DATA

若 CLA= ‘00’，DATA=更新数据

若 CLA= ‘04’，DATA=更新数据或更新数据密文+MAC

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
‘65 81’	内存失败
‘67 00’	长度错误
‘69 81’	命令与文件结构不相容，当前文件非所需文件
‘69 82’	操作条件不满足
‘69 86’	不满足命令执行条件，当前文件不是 EF
‘6A 81’	应用被锁定
‘6A 82’	该文件未找到
‘6B 00’	参数错误(偏移量超出 EF)
’93 03’	应用被永久锁定

2.1.18 UPDATE RECORD（写记录文件）命令

UPDATE RECORD 命令用于更新线性定长结构的文件记录。当前指定记录将被新记录覆盖。 该命令以整条记录的形式更新记录，不能只更新记录中的一部分。所更新的 EF 要求已经被选定或在 *UPDATE RECORD* 的命令参数 P2 中指定。

只有更新记录的权限满足时，才能执行命令 *UPDATE RECORD*。

注

- 文件可以通过以下命令被选择：
  - *CREATE* 命令
  - *SELECT* 命令
  - *READ RECORD/UPDATE RECORD* 命令
- 执行 *UPDATE RECORD* 命令，一次只能更新一条记录。
- *UPDATE RECORD* 命令不能用来更新二进制结构的文件。
- 若 P2 字节包含一个 EF 文件的短文件标识 SFI，则这个 EF 文件必定是当前 DF 下的文件。
-

命令

CLA	INS	P1	P2	L_C	DATA

‘00’/‘04’	‘DC’	NR	AM		

NR—Number

NR = 记录号（‘01’~‘FE’）；

AM—访问模式

B7	B6	B5	B4	B3	B2	B1	B0	说明
0 x	0 x	0 x	0 x	0 x				文件选择： 当前已经被选择的文件 短文件标识符（SFI）
					1	0	0	由 P1 指定记录号

Lc – 记录长度

当 CLA = ‘00’时， Lc = 更新数据长度，最大值为 PSAM 卡的 buffer 长度。

当 CLA = ‘04’时，Lc = 更新数据长度或更新数据的密文长度+ 4

DATA

当 CLA = ‘00’时，DATA = 更新数据

当 CLA = ‘04’时，Lc = 更新数据或更新数据的密文 + MAC

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
‘65 81’	内存失败
‘67 00’	长度错误
‘69 81’	命令与文件结构不相容，当前文件非所需文件
‘69 82’	操作条件不满足
‘69 86’	不满足命令执行条件，当前文件不是 EF
‘6A 81’	应用被锁定
‘6A 82’	该文件未找到
‘6A 83’	记录未找到

2.1.19 WRITE RSA KEY（写 RSA 密钥）命令

WRITE RSA KEY 命令用于更新 PSAM 卡中已经存在的 RSA 公钥。PSAM 卡接收到该命令后，首先使用卡片内被装载的旧 RSA 密钥对的公钥，对被私钥加密的新 RSA 密钥对的公钥分量 n 进行解密计算，然后进行自身 RSA 公钥的更

新。默认的公钥指数为 65537。

注

- 使用 ***WRITE RSA KEY*** 命令时必须确保卡内已经正确个人化一个 RSA 公钥；
- RSA 密钥模 n 的最高字节必须大于 0x80，确保其密钥的强度及更新的正确性；
- RSA 密钥对的密钥长度只支持 1024bit(128 字节)；
- 在该命令执行前，必须成功地执行 ***MANAGE SECURITY ENVIRONMENT*** 命令，用于指定哪个密钥参与运算；在本命令正确执行后，新的 RSA 公钥将代替旧 RSA 公钥；

命令

CLA	INS	P1	P2	Lc	DATA
‘80’	‘D2’	‘00’	‘00’	‘8C’	

DATA

– 新 RSA 公钥的分量结构

新的 RSA 公钥分量结构=0x60||0x01||8 字节 RND||RSA 公钥分量(n-11)||0xBC||0xFF

终端采用旧的 RSA 私钥对新的 RSA 公钥分量结构进行 RSA 加密计算，获得和旧的 RSA 公钥对长度相等的密文数据，作为命令数据域的输入；

– 新的 RSA 公钥余项

长度为 11 字节，值为新 RSA 密钥对分量 n 从最右开始按余项长度取得的所有数据的值。

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
‘67 00’	长度错误
‘69 85’	使用条件不满足，找不到 RSA 密钥
‘6A 80’	数据域错误，数据格式不正确
‘6A 81’	P1/P2 出错
‘6F 81’	系统错误

2.1.20 ATE KEY PROTECTED BY RSA 命令

UPDATE KEY PROTECTED BY RSA 命令用于装载 DES 应用密钥或更新已经存在的密钥，首先使用卡片内 RSA 密钥对的公钥，对被私钥加密的新 DES 密钥进行解密计算，然后进行 DES 密钥的装载或更新。

注

- 使用该命令时必须确保卡内已经正确个人化一个 RSA 公钥；
- 卡片接收到该命令后，通过判断 PK 与 VK 来确定该命令是装载模式还是更新模式：若 PK 与 VK 对应的密钥已经存在，则该命令用于更新对应密钥，若 PK 与 VK 对应的密钥不存在，则该命令用于装载新密钥；
- 命令数据域为采用 RSA 密钥对对应的私钥加密后的密文数据，受算法要求，其数据长度等于 RSA 密钥对的长度（128 字节）；
- 由于 RSA 非对称算法安全等级更高，所以不再使用 MAC 等基于对称算法的安全报文进行保护。
- 在执行该命令前，必须先执行 *MANAGE SECURITY ENVIRONMENT* 命令，该命令用于指定使用哪个公钥来进行解密计算。

命令

CLA	INS	P1	P2	Lc	DATA
‘80’	‘D8’	‘00’	‘00’	‘80’	

DATA

命令报文数据域为 RSA 私钥对如下数据加密后的密文，加密前的数据明文为：

- 0x60||0x00…..||0x01
- 8 字节 RND
- PK：表示密钥用途
- VK：表示密钥版本
- Algo：算法字节
- 新密钥值（8 或 16 字节）
- AC1||AC2：AC1 为密钥使用的状态机条件，AC2 为密钥通过认证后的状态机跳转目的状态（仅对外部认证密钥有效）
- KFPC||RFU（仅对外部认证密钥有效）
- 0xBC

响应

SW1	SW2
‘90’	‘00’

状态码

代码	说明
‘67 00’	长度错误
’69 82’	安全条件不满足
’69 83’	密钥已锁定
‘69 85’	使用条件不满足，找不到 RSA 密钥
‘6A 80’	数据域错误，数据格式不正确
‘6A 81’	P1/P2 出错
‘6F 81’	系统错误

3 附录一

本附录简单介绍了建设部 PSAM 卡的密钥结构及密钥的装载与更新。

建设部 PSAM 卡的密钥分两大类：DES 应用密钥（如 CCK、ACK 等）和 RSA 密钥。在介绍密钥的装载及修改之前，先介绍密钥文件和 IPF 文件。

在建设部 PSAM 卡中，密钥文件用于存放 DES 应用密钥，如 CCK、ACK 等；IPF 文件用于存放 RSA 密钥对的公钥。

密钥文件是一个定长记录文件，记录长度为 0x17。每个记录存放一条密钥，每条密钥由如下格式组成：PK||VK||Algo ||密钥值（8 字节或 16 字节）||ACV1||ACV2||KFPC||RFU。通常，对于没有外部认证功能的密钥，卡片只判断 PK、VK、Algo 字节及密钥值

– PK

PK 字节编码如下图 8-1 所示

表 8-1 PK 字节编码

b8	b7	b6	b5	b4	b3	b2	b1	定义
								离散次数
0	0	1						1 次
0	1	0						2 次
……..								…….
1	1	1						7 次
								密钥用途
0	0	0	0	0	0	0	0	CCK/ACK

0	0	0	0	0	0	0	1	MK
			0	0	0	1	0	Purchase
			0	0	0	1	1	PIN Unblock
			0	0	1	0	0	Reload PIN
			0	0	1	0	1	Card holder card AMK
			0	0	1	1	0	MAC
			0	0	1	1	1	Secure Messaging
			0	1	0	0	0	MAC & SM
			0	1	0	1	1	圈存 MAC2 计算密钥
			0	1	1	1	0	外部认证密钥
			0	1	1	1	1	内部认证密钥
			1	1	1	0	0	Mifare 1 专用密钥
			1	1	1	0	1	Mifare 1 认证密钥
			Other values					RFU

– VK

只有交易密钥的VK字节表示密钥版本，其他密钥的VK表示密钥标识，即KID。

– Algo

当密钥为 3DES 密钥时，Algo=0x00 或 0x80；

当密钥为 DES 密钥时，Algo=0x01 或 0x81。

– 密钥值（8 字节或 16 字节）

– ACV1

该字节编码参见 ***CREATE*** 命令中的表 7-4。

– ACV2

该字节表示密钥认证通过后的状态机跳转的目的状态，其编码见表 8-2

表 8-2 AC2 字节编码

bit1	bit2	bit3	bit4	bit5	bit6	bti7	bit8	说明
								后续状态（CS）
				0	0	0	0	最高状态
				1	1	1	1	最低状态

– KFPC

表 8-3 KFPC 字节编码

bit1	bit2	bit3	bit4	bit5	bit6	bti7	bit8	说明
x	x	x	x					尝试计数器初始值

				x	x	x	x	尝试计数器

– RFU

IPF 文件是一个 LV 结构的文件，该文件的第一个字节表示该文件存放的密钥个数，从第二个字节开始存放密钥。每个密钥由如下格式构成：

– PKID

PKID 用于标识 RSA 密钥对的公钥。

表 8-4 PKID 字节编码

bit1	bit2	bit3	bit4	bit5	bit6	bti7	bit8	说明
0 1								层次： 全局 当前
	0	0						RFU
			#	#	#	#	#	值（1-31）

– 密钥长度

表示密钥的长度，2 字节。

– ACV（2 字节）

该字节编码参见 ***CREATE*** 命令中的表 7-4 及本附录中表 8-2。

– RFU

– Algo

该字节用于指定密钥值在 IPF 文件中存储的顺序（高字节到低字节或低字节到高字节）以及在应用中将使用的算法，其编码如表 8-5。

表 8-5　Algo 字节编码

bit1	bit2	bit3	bit4	bit5	bit6	bti7	bit8	说明
								RFU
				0 1				密钥格式： 高字节到低字节 低字节到高字节
					0			RFU
						-- 	1	非对称算法： RSA

– AKD

表 8-6 AKD 字节编码

bit1	bit2	bit3	bit4	bit5	bit6	bti7	bit8	说明
0								RFU
	--							RFU
		0						RFU
			--	--	--			RFU
						1 0		是否允许加/解密： 是 否
							--	RFU

– 密钥指示器（2 字节）

密钥指示器相应于密钥长度，另外，其高字节的 bit8 表示密钥是否完成：若等于 1 表示完整，等于 0 表示不可用。

– 密钥

密钥由密钥格式列表（KFL）和密钥分量构成，见表 8-7。KFL 包含了密钥分量信息及其长度信息。由于建设部 PSAM 卡只需要 RSA 密钥对的公钥成分，故，这里只介绍关于 RSA 公钥的密钥格式及其编码。

表 8-7 密钥结构表

密钥格式列表 KFL							密钥分量		
KFL 长度（表示分量个数）	F1	L1	F2	L2	Fn	Ln	密钥分量 F1	密钥分量 F2	密钥分量 F3
1 字节	KFL 字节								

F 字节指示了密钥分量信息，其编码见表 8-8。

bit1	bit2	bit3	bit4	bit5	bit6	bti7	bit8	说明
0 1								密钥类型： 公钥 私钥
	0	0						RFU
			1					RSA 算法
				0				RFU
					0 0 0 0		1 0	RSA 公钥： CHR 模

					0	1	1	指数

由上表可知，对于 RSA 公钥，CHR 的 F 字节为 ‘01’（注意：对于 CHR，F 字节的 bit4 应置 0）；模的 F 字节为 ‘10’；指数的 F 字节为 ‘13’。

L 字节表示密钥分量的长度。其中，CHR 表示 RSA 公钥标识，由 1-8 个字节数据组成，且每个 RSA 公钥的 CHR 是唯一的；RSA 公钥的指数长度也是 4 个字节；RSA 公钥的模长度固定为 128 字节。

– RFU = 0x00。
– RFU = 0x00。

下面简单介绍 DES 应用密钥和 RSA 公钥的装载和更新流程。

对于 DES 应用密钥，首先应使用 ***CREATE*** 命令创建一个定长记录文件作为密钥文件，然后通过 ***UPDATE KEY PROTECTED BY RSA*** 命令按上述 DES 密钥格式装载或更新密钥；对于 RSA 公钥，首先应使用 ***CREATE*** 命令创建一个 IPF 文件，然后用户在卡片外部用特定工具生成 RSA 公私钥对，在外部保存私钥分量，同时把公钥分量通过 ***UPDATE BINARY*** 命令以上述格式写入 IPF 文件中。至此密钥的装载过程完成，注意，RSA 密钥的装载只能在 ***CREATE END*** 命令执行前完成。

在 PSAM 卡的应用过程中，使用 ***WRITE RSA KEY*** 命令完成 RSA 公钥的更新，详见具体命令。注意，这条密钥只存在更新模式。