

高速公路区域联网不停车收费示范工程暂行技术要求 第 4 部分

联网电子收费 PSAM 卡应用指南

2008 年 8 月

目 次

1 范围.....	1
2 规范性引用文件.....	1
3 缩略语和符号.....	1
4 文件结构.....	2
4.1 PSAM 卡详细文件结构说明	3
4.2 MF 下的卡片公共信息文件结构.....	3
4.3 MF 下的终端信息文件.....	3
4.4 DF01 下的应用公共信息文件	4
5 密钥说明.....	4
5.1 DF01 下的密钥文件结构	5
6 安全管理.....	5
6.1 安全计算方法.....	5
6.1.1 密钥分散计算方法.....	5
6.1.2 数据加密的计算方法.....	7
6.1.3 安全报文的计算方法.....	7
6.2 数据的安全计算步骤.....	9
7 应用系统的兼容性.....	10
7.1 密钥分散.....	10
7.2 扩展目录使用.....	10
8 命令.....	10
8.1 基本命令.....	10
8.1.1 EXTERNAL AUTHENTICATE 命令	10
8.1.2 SELECT FILE 命令.....	11
8.1.3 READ RECORD 命令.....	13
8.1.4 UPDATE RECORD 命令	14
8.1.5 READ BINARY 命令	15
8.1.6 UPDATE BINARY 命令.....	16
8.1.7 GET CHALLENGE 命令	17
8.1.8 GET RESPONSE 命令	18
8.2 扩展命令.....	19
8.2.1 APPLICATION UNBLOCK 命令	19
8.2.2 CIPHER DATA 命令	20
8.2.3 CREDIT SAM FOR PURCHASE 命令（校验 MAC2）	21
8.2.4 DELIVERY KEY 命令	21
8.2.5 INIT SAM FOR PURCHASE 命令（计算 MAC1）	22
8.2.6 WRITE KEY 命令.....	23
9 附录.....	25

1 范围

本指南用于说明联网电子收费PSAM卡密钥的导入，在应用系统中使用的技术要求等。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本规范，然而，鼓励根据本规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本规范。

GB/T 20851.4-2007 电子收费 专用短程通信 第4部分：设备应用

JR/T 0025-2005 中国金融集成电路 IC 卡规范

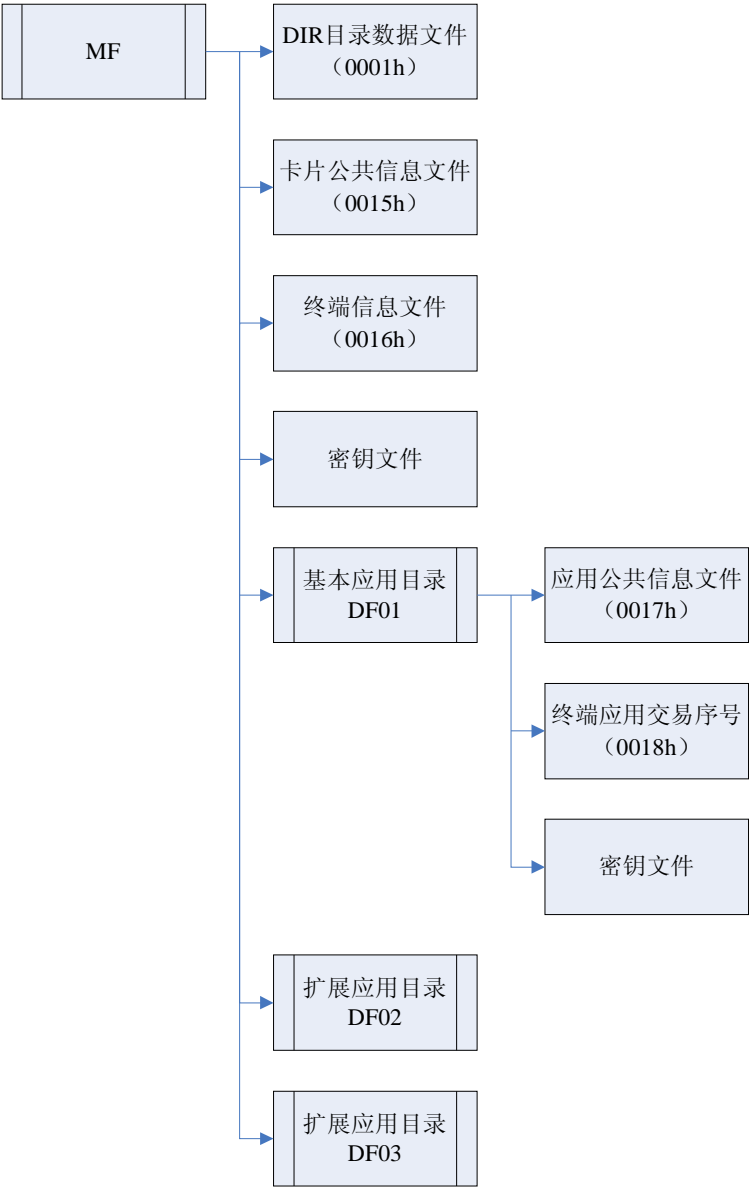
收费公路联网收费技术要求，交通部 2007 年第 35 号公告

3 缩略语和符号

ADF	应用数据文件（Application Definition File）
AID	应用标识符（Application Identifier）
an	字母数字型（Alphanumeric）
ans	字母数字及特殊字符型（Alphanumeric Special）
APDU	应用协议数据单元（Application Protocol Data Unit）
ATR	复位应答（Answer to Reset）
b	二进制（Binary）
CLA	命令类别（Chip Card Payment Service）
CLK	时钟（Clock）
cn	压缩数字（Compressed Numeric）
DIR	目录（Directory）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
f	频率（Frequency）
INS	命令报文的指令字节（Instruction Byte of Command Message）
I/O	输入/输出（Input/Output）
Lc	终端发出的命令数据的实际长度（Exatct Length of Data Sent）
Le	响应数据中的最大期望长度（Maximum Length of Data Expected）
MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件（Mater File）

N	数字型 (Numeric)
P1	参数 1 (Parameter 1)
P2	参数 2 (Parameter 2)
RFU	保留为将来所用 (Reserved for Future Use)
SW1	状态码 1 (Status Word One)
SW2	状态码 2 (Status Word Two)

4 文件结构



4-1联网电子收费PSAM卡结构

注：本文以《收费公路联网收费技术要求》第四章，“编码和数据交换格式”中的PSAM卡的数据格式为依据，考虑到在测试过程中的便利性及各地区未来应用需求的差异性，对原有PSAM卡片结构稍加扩充。

4.1 PSAM 卡详细文件结构说明

表4-1 PSAM卡详细文件结构

文件名称		文件类型	文件标识符	读权	写权	备注
MF		主文件	3F00	建立权: MK _{MF}		厂商交货时已经建立
	密钥文件	密钥文件	--	禁止	增加密钥权: MK _{MF}	通过卡片主控密钥 MK _{MF} 采用密文+MAC 方式写入密钥
	DIR 目录数据文件	变长记录	0001	自由	AMK _{MF}	自由读, 写时使用卡片维护密钥进行线路保护 (明文+ MAC)
	卡片公共信息文件	二进制文件	0015	自由	AMK _{MF}	自由读, 写时使用卡片维护密钥进行线路保护 (明文+ MAC)
	终端信息文件	二进制文件	0016	自由	AMK _{MF}	自由读, 写时使用卡片维护密钥进行线路保护 (明文+ MAC)
	DF01 CPU 卡应用和 OBU 认证目录	目录文件	DF01	建立权: MK _{MF}	擦除权: MK _{MF}	卡片主控密钥 MK _{MF} 认证通过后可以建立和擦除文件
	密钥文件	密钥文件	--	禁止	增加密钥权: MK _{DF01}	PSAM 卡应用 1 主控密钥 MK _{DF01} 采用密文+MAC 方式写入密钥
	应用公共信息文件	二进制文件	0017	自由	AMK _{DF01}	自由读, 写时使用 PSAM 卡应用 1 维护密钥 AMK _{DF01} 进行线路保护 (明文+ MAC)
	终端应用交易号数据元	二进制文件	0018	自由	不可写, COS 维护	用于存储终端交易序号, 由 COS 维护
	DF02 CPU 卡应用和 OBU 认证目录	目录文件	DF02	建立权: MK _{MF}	擦除权: MK _{MF}	卡片主控密钥 MK _{MF} 认证通过后可以建立和擦除文件
	DF03 CPU 卡应用和 OBU 认证目录	目录文件	DF03	建立权: MK _{MF}	擦除权: MK _{MF}	卡片主控密钥 MK _{MF} 认证通过后可以建立和擦除文件

4.2 MF 下的卡片公共信息文件结构

表4-2 MF下卡片公共信息文件结构

文件标识		0015
文件类型		二进制文件
文件大小		14 字节
文件存取控制	读=自由	改写=AMK _{MF} 线路保护写 (明文 + MAC)
字节	数据元	长度 (字节)
1-10	PSAM 序列号	10
11	PSAM 版本号	1
12	密钥卡类型	1
13-14	发卡方自定义 FCI 数据	2

4.3 MF 下的终端信息文件

表4-3 MF下的终端信息文件

文件标识		0016
文件类型		二进制文件
文件大小		6 字节
文件存取控制	读=自由	改写=AMK _{MF} 线路保护写（明文 + MAC）
字节	数据元	长度（字节）
1-6	终端机编号	1-6

4.4 DF01 下的应用公共信息文件

表4-4 DF01下的应用公共信息文件

文件标识		0017
文件类型		二进制文件
文件大小		25 字节
文件存取控制	读=自由	改写=AMK _{DF01} 线路保护写（明文 + MAC）
字节	数据元	长度（字节）
1	密钥索引号	1
2-9	发行方标识	8
10-17	应用区域标识	8
18-21	应用启用日期	4
22-25	应用有效日期	4

5 密钥说明

联网电子收费 PSAM 卡中，除主控密钥 MK 存储在 MF 或 ADF 缺省的位置上外，其余所有密钥都以记录的形式存储在密钥文件中。每一条密钥包括用途、标识/版本、算法和密钥数据等参数信息。

PSAM 卡中包括以下几种密钥类型：

- l 02h: 消费密钥，能进行消费交易；
- l 06h: MAC 密钥，能进行 MAC 计算；
- l 08h: MAC、加密密钥，能进行 MAC 和数据加密运算；
- l 09h: 圈存密钥，能进行圈存交易；
- l 19h: MAC、解密密钥，能进行 MAC 和数据解密运算；

5.1 DF01 下的密钥文件结构

表5-1 DF01下的密钥文件结构

密钥名称	密钥用途	密钥标识	密钥大小	算法标识	错误计数器
PSAM 卡应用 1 主控密钥 MK_DF01	--	00	10H	00	15
PSAM 卡应用 1 维护密钥 AMK_DF01	--	01	10H	00	15
CPU 卡外部认证密钥 UK_DF01	48	01	10H	00	--
CPU 卡消费密钥 1 PK1	42	01	10H	00	--
CPU 卡消费密钥 2 PK2	42	02	10H	00	--
CPU 卡圈存密钥 LK	49	01	10H	00	--
CPU 卡 TAC 密钥 TK	4C	01	10H	00	--
OBU 认证主密钥 RK1	48	02	10H	00	--
OBU 加密主密钥 RK2	59	03	10H	00	--
OBU 应用维护密钥 AMK_OBU	46	01	10H	00	--

注：CPU 卡圈存密钥（LK）、OBU 应用维护密钥（AMK_OBU）仅为方便测试而设立，只存于测试阶段的 PSAM 卡中。

6 安全管理

6.1 安全计算方法

安全计算涉及用户卡中的所有计算类型。包括数据加密计算、普通MAC计算、消费MAC1计算和MAC2认证等。MAC总是命令或命令响应数据域中最后一个数据元素。

6.1.1 密钥分散计算方法

密钥分散通过分散因子产生子密钥。

分散因子为8字节，将一个双长度的主密钥MK，对分散数据进行处理，推导出一个双长度的子密钥DK，如图6-1和图6-2。

推导DK左半部分的方法是：

- 第一步：将分散因子作为输入数据；
- 第二步：将 MK 作为加密密钥；
- 第三步：用 MK 对输入数据进行 3DEA 运算。

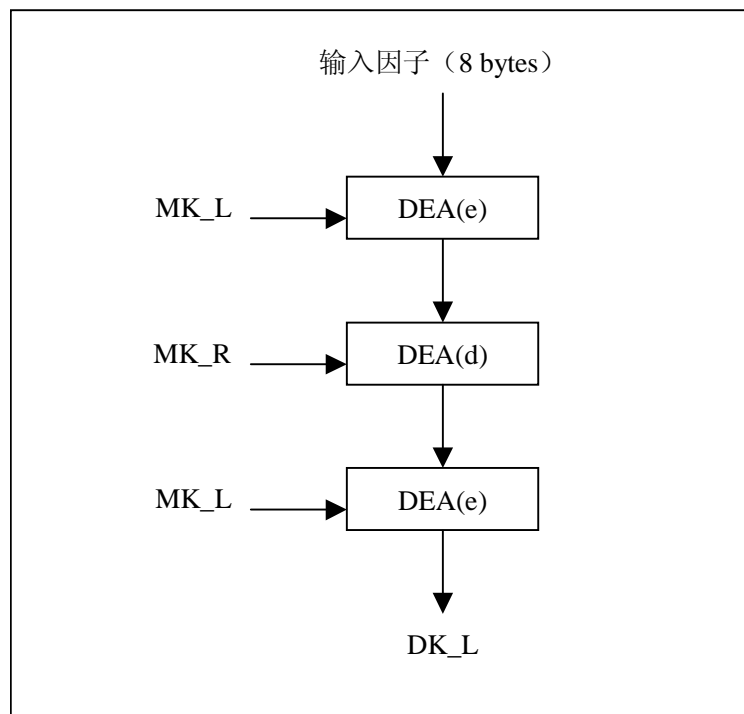


图 6-2: 推导 DK 左半部分

推导 DK 右半部分的方法是:

- 第一步: 将分散因子求反, 作为输入数据;
- 第二步: 将 MK 作为加密密钥;
- 第三步: 用 MK 对输入数据进行 3DEA 运算。

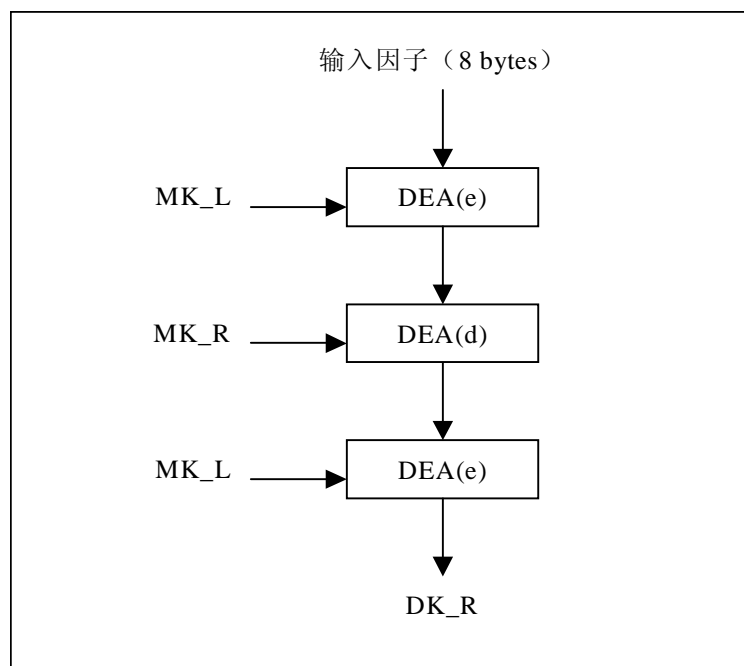


图6-3: 推导DK右半部分

6.1.2 数据加密的计算方法

按照如下方式对数据进行加密：

- 第一步： LD (1 字节) 表示明文数据的长度，在明文数据前加上 LD 产生新的数据块。
- 第二步： 将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1-8 个字节。
- 第三步： 如果最后（或唯一）的数据块的长度是 8 字节的话，转到第四步；如果不足 8 字节，则在其后加入 16 进制数‘80’，如果达到 8 字节长度，则转到第四步；否则在其后加入 16 进制数‘00’直到长度达到 8 字节。
- 第四步： 按照图 3-2 和图 3-3 所述的算法使用指定密钥对每一个数据块进行加密。
- 第五步： 计算结束后，所有加密后的数据块依照原顺序连接在一起。

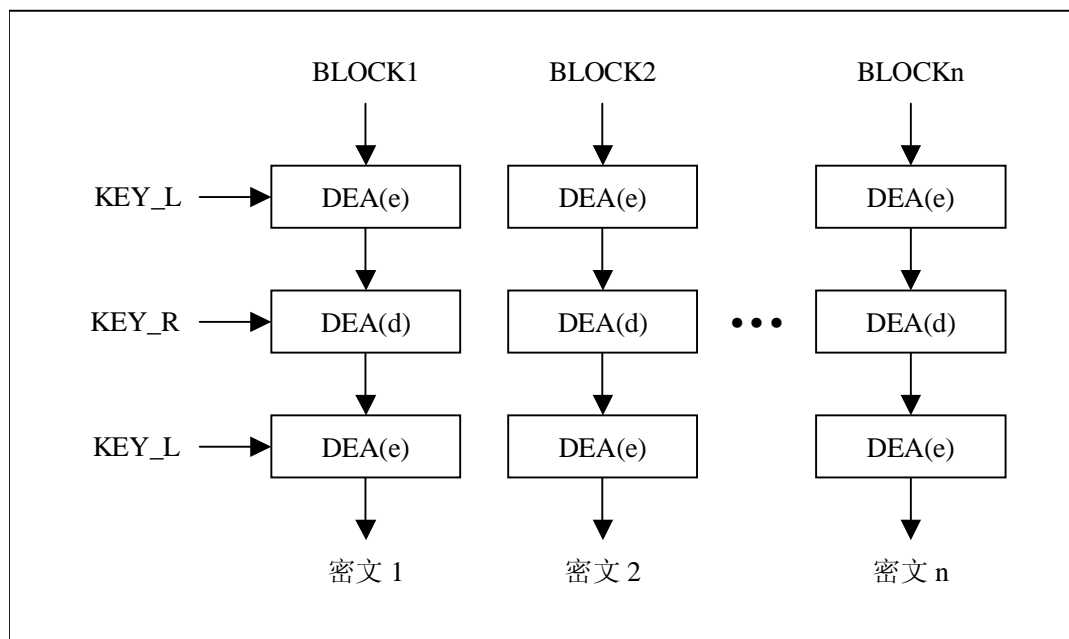


图 6-4：双倍长密钥 DEA 数据加密算法

6.1.3 安全报文的计算方法

(1) 命令安全报文中的MAC

命令安全报文中的 MAC 是使用命令的所有元素（包括命令头和命令数据域中的数据）来产生的。以保证命令连同数据能够正确完整地传送，并对发送方进行认证。此方法适用于 WRITE KEY 命令。

按照如下方式使用 DEA 加密方式产生 MAC：

- 第一步： 终端通过向 IC 卡发 GET CHALLENGE 命令获得一个 4 字节随机数，后补“00 00 00 00”作为初始值。
- 第二步： 将 5 字节命令头（CLA, INS, P1, P2, Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。注意，这里的 Lc 应是数据长度

加上将计算出的 MAC 的长度（4 字节）后得到的实际长度。

第三步：将该数据块分成 8 字节为单位的数据块， 表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。

第四步：如果最后的数据块的长度是 8 字节的话，则在该数据块之后再加一个完整的 8 字节数据块‘80 00 00 00 00 00 00 00’， 转到第五步。

第五步：如果最后的数据块的长度不足 8 字节，则在其后加入 16 进制数‘80’，如果达到 8 字节长度，则转到第五步；否则接着在其后加入 16 进制数‘00’直到长度达到 8 字节。

按图 3-6 所述的算法对这些数据块使用指定密钥进行加密来产生 MAC。

第六步：最终取计算结果（高 4 字节）作为 MAC。

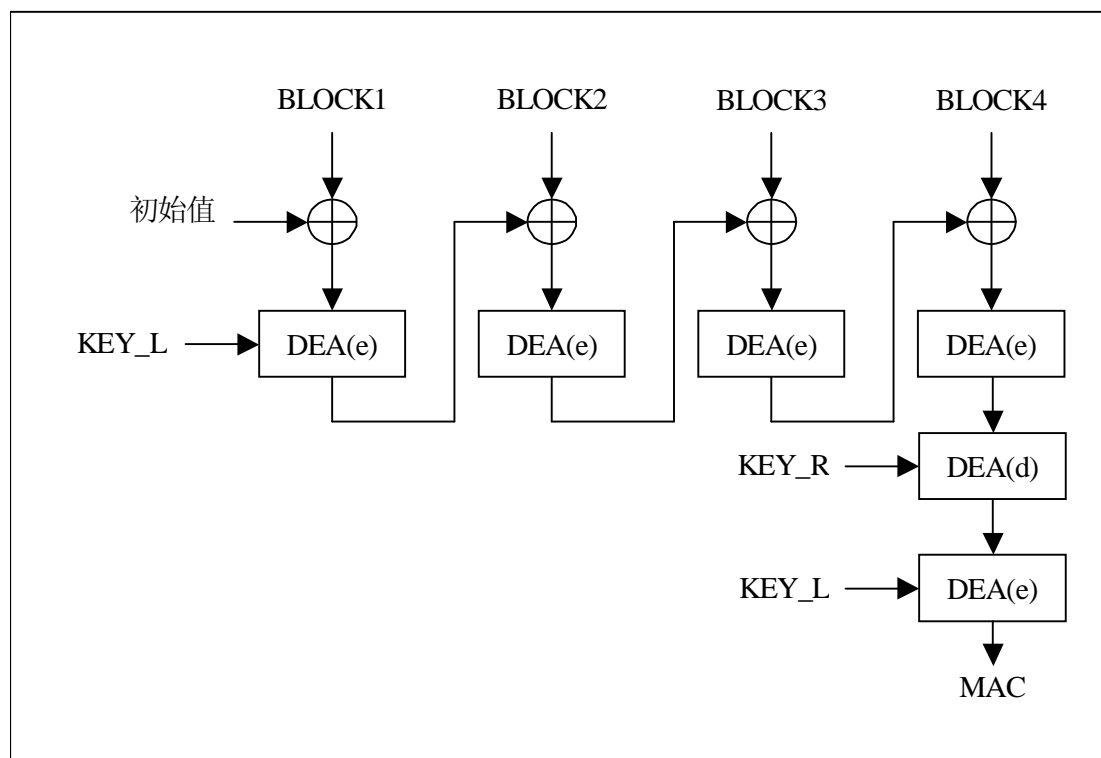


图6-5：安全报文中双倍长密钥MAC算法

（2）交易中的MAC

命令安全报文中的 MAC 是使用命令的所有元素（包括命令头和命令数据域中的数据）来产生的。以保证命令连同数据能够正确完整地传送，并对发送方进行认证。

此方法适用于所有命令，除 **WRITE KEY** 命令外。此方法分二步完成。先用指定密钥产生过程密钥；再用过程密钥计算 MAC。

按照如下方式使用 DEA 加密方式产生 MAC：

- 第一步： 将一个 8 字节长的初始值设定为 16 进制数‘00 00 00 00 00 00 00 00’
- 第二步： 将所有输入数据按指定顺序连接成一个数据块。
- 第三步： 将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。
- 第四步： 如果最后的数据块的长度是 8 字节的话，则在该数据块之后再加一个完整的 8 字节数据块‘80 00 00 00 00 00 00 00’，转到第五步。
- 如果最后的数据块的长度不足 8 字节，则在其后加入 16 进制数‘80’，如果达到 8 字节长度，则转到第五步；否则在其后加入 16 进制数‘00’直到长度达到 8 字节。
- 第五步： 按照图 3-7 所述的算法对这些数据块使用过程密钥（单倍长度）进行加密来产生 MAC。
- 第六步： 最终取计算结果（高 4 字节）作为 MAC。

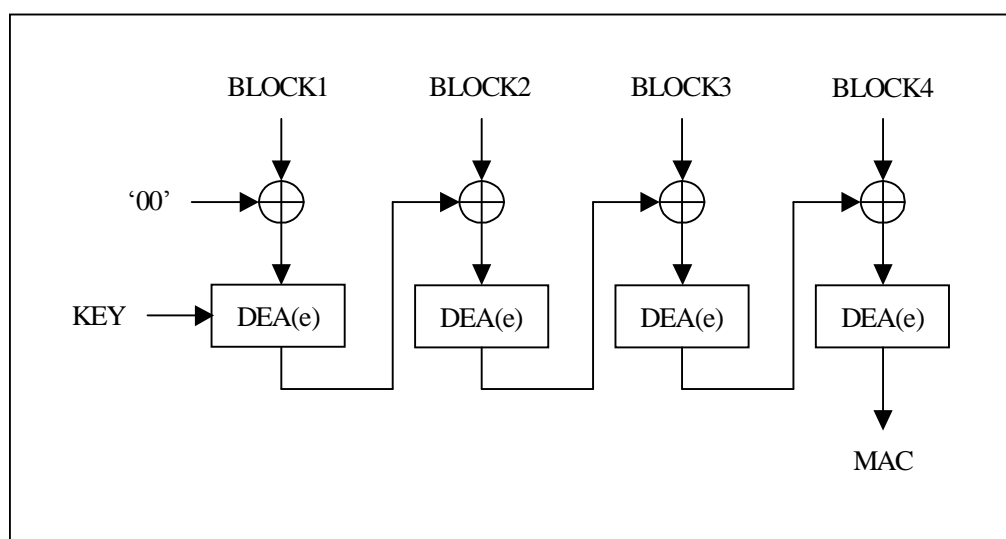


图6-6：交易中的MAC算法

（3）双向认证中的鉴别码

此方法为交通部联网电子收费专用，鉴别码的计算方法：

- 将文件数据进行 CRC 计算（多项式 $X^{16}+X^{12}+X^5+1$ ，起始 FFFFh），产生两字节 CRC0 和 CRC1。
- 将送入的随机数(8 bytes) 最低两字节（即最左边两个字节）分别更换为 CRC1、CRC0，形成 8 字节临时数据。
- 使用计算密钥对 8 字节数据进行加密计算：

$$\text{MAC} = \text{TDDES}(\text{KEY_MAC}, \text{CRC0} || \text{CRC1} || \text{Rand}(\text{高6字节}))$$

6.2 数据的安全计算步骤

数据的安全计算是指对外部提供的数据进行 DES 变换。主要计算有： Triple-DES 加密、Triple-DES MAC 计算。

PSAM 卡中完成数据的安全计算必须经过两个步骤：

1. 使用 DELIVERY KEY 命令，在卡内准备好参与计算的密钥；
2. 使用 CIPHER DATA 命令，用产生的临时密钥对外部提供的数据进行处理。

7 应用系统的兼容性

7.1 密钥分散

联网电子收费系统采用二级和三级密钥分散，应用程序在处理请求时，应该先判断用户终端（仅指用户卡）内密钥的分散级数。其中，用户卡 DF01 下，卡发行基本信息文件（“0015h”）的第 8 个字节为“密钥分散标识”，应用先根据此字节的数值来选择实际的应用。

- I 01：通过两级分散得到卡片密钥，第一级采用区域代码（复制一次变为 8 个字节）作为分散因子，第二级采用 CPU 卡内部编号作为分散因子。
- I 02：通过三级分散得到卡片密钥，第一级采用区域代码（复制一次变为 8 个字节）作为分散因子，第二级采用运营商标识（补“F”变为 8 个字节）作为分散因子，第三级采用 CPU 卡内部编号作为分散因子。
- I 03：通过三级分散得到卡片密钥，第一级采用运营商标识（补“F”变为 8 个字节）作为分散因子，第二级采用区域代码（复制一次变为 8 个字节）作为分散因子，第三级采用 CPU 卡内部编号作为分散因子。
- I 其它保留。

关于用户卡卡发行基本信息文件中，发卡方标识的数据构成，请参见《关键信息编码规则》。

7.2 扩展目录使用

联网电子收费的测试 PSAM 卡中，包括三个应用目录（ADF），其中基本应用目录（DF01h）为交通部发行的全国应用目录，其中装载全国电子收费应用的各种密钥。另外两个为扩展应用目录（DF02h、DF03h）为地方发行的区域应用目录，其文件结构和密钥装载由地方负责，仅在区域内部使用。

注：在测试 PSAM 卡中，DF02 目录的应用主控密钥为 16 个字节的“22h”；DF03 目录的应用主控密钥为 16 个字节的“33h”。

8 命令

8.1 基本命令

8.1.1 EXTERNAL AUTHENTICATE 命令

（1）命令描述

EXTERNAL AUTHENTICATE 命令的目的是 PSAM 卡验证外部接口设备的有效性，使接口设备对 PSAM 卡获得某种操作授权。

接口设备提供的认证数据应按以下规则产生：

- 1、Lc = '08'
- 2、用 GET CHALLENGE 命令向 IC 卡申请一组随机数。
- 3、用指定密钥对随机数作加密计算，产生认证数据。参见“安全计算”一节

(2) 使用条件和安全

EXTERNAL AUTHENTICATE 命令所使用的密钥（由 P2 参数指定）必须满足密钥的访问权限。密钥验证失败计数器减一。当计数器减为'0'值时，密钥被锁定。

(3) 命令格式

代码	数 值								
CLA	'00'								
INS	'82'								
P1	'00'								
P2	b8	B7	b6	b5	b4	b3	b2	b1	说 明
	0	X	x	x	x	x	x	x	全局密钥标识
	1	X	x	x	x	x	x	x	局部密钥标识
	0	0	0	0	0	0	0	0	当前 DF 下的 MK
Lc	'08'								
DATA	认证数据（8 字节）								
Le	不存在								

(4) 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
63	Cx	认证失败，还可认证 x 次
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.1.2 SELECT FILE 命令

(1) 命令描述

SELECT FILE 命令通过文件标识或应用名选择 PSAM 卡中的 MF、ADF 或 EF 文件。

成功执行该命令设定 MF 或 ADF 的路径，后续命令作用于与用 SFI 选定的 DDF 或 ADF 相联系的 AEF。

从 IC 卡返回的应答报文包含回送 FCI，FCI 数据从数据分组中获得。

(2) 使用条件和安全

SELECT FILE 命令无使用条件限制。该命令不能用于选择安全文件（SF）。

(3) 命令格式

代码	数 值
CLA	‘00’
INS	‘A4’
P1	‘00’通过 FID 选择 DF、EF，当 Lc=‘00’时，选 MF ‘04’通过 DF 名选择应用
P2	‘00’ ‘02’选择下一个文件（P1=04h 时）
Lc	P1=‘00’时，Lc=‘00’或‘02’ P1=‘04’时，Lc=‘01’~‘10’
DATA	文件标识符（FID—2 字节） 应用名（App-Name，P1=‘04’）
Le	FCI 文件的信息长度（选择 DF 时）

(4) 响应信息

响应信息的结构：

下表定义了成功选择 ADF 后回送的 FCI：

标签	值	存在性
‘6F’	FCI 模板	M
‘84’	DF 名	M

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
62	83	选择文件无效
62	84	FCI 格式与 P2 指定的不符
64	00	标志状态位没变
67	00	Lc 长度错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	87	Lc 与 P1-P2 不匹配
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.1.3 READ RECORD 命令

(1) 命令描述

READ RECORD命令读记录文件中指定的记录。

(2) 使用条件和安全

READ RECORD命令的执行必须满足相应文件的读条件和读属性。

(3) 命令格式

代码	值
CLA	00h
INS	B2h
P1	记录的序号
P2	引用控制参数（见下表）
Lc	不存在；
Data	不存在；
Le	00h

READ RECORD 命令报文

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SFI
					1	0	0	P1 为记录的序号

READ RECORD命令引用控制参数

(4) 响应信息

所有执行成功的READ RECORD命令响应报文数据域由读取的记录组成。

SW1	SW2	说 明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效(未申请随机数)
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6C	xx	Le 错误，‘xx’ 表示实际长度
6D	00	命令不存在

6E	00	CLA 错
93	03	应用永久锁定

8.1.4 UPDATE RECORD 命令

(1) 命令描述

UPDATE RECORD命令用给定的数据代替记录文件中指定的纪录。

对线性记录文件，可按记录号顺序添加记录。

(2) 使用条件和安全

UPDATE RECORD命令的执行必须满足相应文件的改写条件和改写属性。

(3) 命令格式

UPDATE RECORD命令报文见表下表。

代码	值
CLA	00h 或 04h
INS	DCh
P1	P1= 00h: 表示当前记录 P1≠ 00h: 指定的记录号
P2	见下表
Lc	后续数据域长度
Data	输入数据
Le	不存在

UPDATE RECORD 命令报文

b8	b7	b6	b5	b4	b3	b2	b1	含义
X	X	X	X	X				SFI
					0	0	0	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在 P1 中给出
其余值								RFU

UPDATE RECORD 命令引用控制参数

(4) 命令报文数据域

命令报文数据域由更新原有记录的新记录组成。使用安全报文时，命令报文的数据域中应包括MAC。MAC是由卡片维护密钥或应用维护密钥对更新原有记录的新记录计算而得到的。

(5) 响应信息

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态

69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.1.5 READ BINARY 命令

（1）命令描述

READ BINARY命令用于读出透明文件的内容。

（2）使用条件和安全

READ BINARY命令的执行必须满足访问文件的读权限和控制属性。

（3）命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘B0’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	1) 不存在——明文方式 2) ‘04’——校验方式								
DATA	1) 不存在 2) MAC								
Le	期望返回的数据长度								

可能的命令/响应有：

CER	CIPH	命令	响应
0	0	00 B0 P1 P2 Le	明文数据 SW1 SW2
0	1	04 B0 P1 P2 Le	密文数据 SW1 SW2
1	0	04 B0 P1 P2 Lc MAC Le	明文数据 SW1 SW2

1	1	04 B0 P1 P2 Lc MAC Le	密文数据 SW1 SW2
---	---	-----------------------	-----------------

(4) 响应信息

响应信息中的数据为明文或密文数据。

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
61	xx	还有 xx 字节要返回
62	81	部分回送的数据可能有错
62	82	文件长度<Le
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6C	xx	Le 长度错误。‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.1.6 UPDATE BINARY 命令

(1) 命令描述

UPDATE BINARY命令用于更新透明文件中的数据。

(2) 使用条件和安全

UPDATE BINARY命令的执行必须满足文件的访问权限和写控制属性。

(3) 命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘D6’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0, P2 为文件的低位地址 若 P1 的 b8=1, P2 为文件地址								

Lc	DATA 域的长度： 明文方式： '00' < Lc ≤ 'FF' 加密方式： '08' ≤ Lc ≤ '48'（模 8） 校验方式： '04' < Lc ≤ '44' 校验加密方式： '0C' ≤ Lc ≤ '4C'（模 8+4）
DATA	明文方式： 明文数据 加密方式： 密文数据 校验方式： 明文数据 校验码 校验加密方式： 密文数据 校验码
Le	不存在

（4）响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.1.7 GET CHALLENGE 命令

（1）命令描述

GET CHALLENGE 命令从 PSAM 卡中获取一组随机数，用于相关命令的安全认证。

（2）使用条件和安全

GET CHALLENGE 命令无使用条件限制。

（3）命令格式

代码	数 值
CLA	'00'
INS	'84'
P1	'00'

P2	‘00’
Lc	不存在
DATA	不存在
Le	‘04’、‘08’或‘10’随机数长度

(4) 响应信息

响应信息中的数据:

说 明	长度 (字节)
随机数	4 或 8 或 16

响应信息中可能返回的状态码有:

SW1	SW2	说 明
90	00	命令执行成功
67	00	Le 长度错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

8.1.8 GET RESPONSE 命令

(1) 命令描述

GET RESPONSE命令从PSAM卡中向接口设备传送APDU的数据。

(2) 使用条件和安全

GET RESPONSE命令无使用条件限制。

(3) 命令格式

代码	数 值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	响应的最大数据长度

(4) 响应信息

响应信息中的数据:

说 明	长度 (字节)
响应数据	X

响应信息中可能返回的状态码有:

SW1	SW2	说 明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	81	回送数据可能有错
67	00	Lc 或 Le 长度错误
6A	86	P1、P2 参数错
6C	xx	长度错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
6F	00	数据无效

8.2 扩展命令

8.2.1 APPLICATION UNBLOCK 命令

(1) 命令描述

APPLICATION UNBLOCK命令执行成功后，解锁当前锁定的应用。

(2) 使用条件和安全

此命令只能在金融应用环境下执行。

APPLICATION UNBLOCK命令的执行采用校验模式。计算校验码使用的KEY为ADF文件中的BLK-KID密钥。执行此命令必须满足BLK-KID密钥的访问权限。

(3) 命令格式

代码	数 值
CLA	‘84’
INS	‘18’
P1	‘00’
P2	‘00’
Lc	‘04’
DATA	信息认证码（MAC）
Le	不存在

(4) 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
62	81	回送数据可能出错
62	83	选择文件无效
64	00	状态标志位未变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	00	无信息提供
69	82	不满足安全状态
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足

69	88	安全信息（MAC）数据错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.2.2 CIPHER DATA 命令

(1) 命令描述

CIPHER DATA命令用于对输入数据进行安全计算，支持的安全计算包括：DES加密解密，DES计算MAC，3DES加密解密，3DES计算MAC。加解密采用ECB模式，计算MAC采用CBC模式。

(2) 使用条件和安全

CIPHER DATA命令的执行必须以DELIVERY KEY命令为前提条件，即该命令的上一条命令必须是DELIVERY KEY。该命令所使用的KEY，固定为临时密钥寄存器中的KEY。

本命令成功执行后，直到发下一个DELIVERY KEY命令，临时密钥寄存器中的KEY保持有效。

(3) 命令格式

代码	数 值
CLA	'80'
INS	'FA'
P1	'05'唯一一块 MAC 计算 '08'交通部 MAC 计算 '80'无后续块解密
P2	'00'
Lc	P1 = '08'时: Lc >= 9 P1 = 其他值: DES 算法: Lc 必须是 8 的模
DATA	安全计算数据。 若 P1='05'或'07'，则第一个数据块为 MAC 计算初始值（DES 算法的 MAC 计算初始值长度为 8 字节； 若 P1 = '08'时，随机数（8 字节）+文件数据。
Le	不存在

(4) 响应信息

响应信息中可能的状态码为：

SW1	SW2	说 明
90	00	命令执行成功
61	Xx	有 xx 字节要返回
67	00	Lc 长度错误
69	01	Delivery Key 命令没有执行或无效
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错

6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.2.3 CREDIT SAM FOR PURCHASE 命令（校验 MAC2）

（1）命令描述

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。MAC2校验失败，计算MAC2的KEY限制计数器减一，并回送状态码‘63Cx’。当KEY限制计数器减为0值时，锁定当前应用，可通过应用维护密钥解锁锁定应用。CREDIT SAM FOR PURCHASE命令成功后，SAM卡将应用中的消费交易序号加1。卡片的状态在命令执行后将复原为MAC1校验前的状态。用于MAC2计算的数据，请参照《中国金融集成电路（IC）卡规范》。

（2）使用条件和安全

CREDIT SAM FOR PURCHASE命令必须在INIT SAM FOR PURCHASE命令成功执行后才能进行。

（3）命令格式

代码	值
CLA	‘80’
INS	‘72’
P1	‘00’
P2	‘00’
Lc	‘04’
Data	MAC2
Le	不存在

（4）响应信息

响应信息中可能返回的状态码有：

SW1	SW2	含义
90	00	命令成功执行
67	00	Lc 长度错
69	01	命令不接受（无效状态）
69	85	使用条件不满足（应用非永久锁定）
6A	81	功能不支持（卡锁定）
6A	86	参数 P1, P2 不正确
6D	00	命令不存在
6E	00	CLA 错
93	02	MAC 无效
93	03	应用永久锁定

8.2.4 DELIVERY KEY 命令

（1）命令描述

DELIVERY KEY命令将指定的KEY分散至临时密钥寄存器中。该命令只支持分散KEY，不产生过程KEY。分散后的子KEY继承原始KEY的属性。

（2）使用条件和安全

DELIVERY KEY命令的执行必须满足KEY的访问属性。

(3) 命令格式

代码	数 值
CLA	'80'
INS	'1A'
P1	密钥用途
P2	密钥标识
Lc	分散数据长度 '00', 分散级数为 0 时 '08', 分散级数为 1 时 '10', 分散级数为 2 时 '18', 分散级数为 3 时 其它值保留
DATA	Lc='00'不存在 分散因子
Le	不存在

(4) 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.2.5 INIT SAM FOR PURCHASE 命令（计算 MAC1）

(1) 命令描述

INIT SAM FOR PURCHASE命令支持最多三级消费密钥分散机制，并产生MAC1。

在联网电子收费的应用中，使用了二级消费密钥分散机制，即使用地区分散因子和用户卡卡片序列号进行密钥分散。

PSAM卡产生脱机交易流程中MAC1的过程如下所示：

PSAM在其内部用GMPK（全国消费主密钥）对地区分散因子分散，得到二级消费主密钥BMPK；

I PSAM 在其内部用 BMPK 对卡片应用序列号分散，得到卡片消费子密钥 DPK；

I PSAM 在其内部用 DPK 对卡片传来的伪随机数、脱机交易序号、终端交易序号加密，得到过程密钥 SESPK，作为临时密钥存放在卡中；

I PSAM 在其内部用 SESPk 对交易金额、交易类型标识、终端机编号、交易日期（终端）和交易时间（终端）加密得到 MAC1，将 MAC1 传送出去。

（2）使用条件和安全

INIT SAM FOR PURCHASE命令支持三级消费密钥分散机制，消费密钥的分散过程由Lc和消费密钥共同确定，如果二者不一致，则返回错误信息。只有执行INIT SAM FOR PURCHASE命令后，才可执行MAC2校验命令。

（3）命令格式

代码	值
CLA	'80'
INS	'70'
P1	'00'
P2	'00'
Lc	金融应用环境中： 14h+8×N（N=1，2，3） 社保应用环境中： 1Ch+8×N（N=1，2，3）
Data	用户卡随机数，4 字节 用户卡交易序号，2 字节 交易金额，4 字节 交易类型标识，1 字节 交易日期（终端），4 字节 交易时间（终端），3 字节 消费密钥版本号，1 字节 消费密钥算法标识，1 字节 用户卡应用序列号，8 字节 成员银行标识，8 字节 试点城市标识，8 字节
Le	'08'（终端交易序号，4 字节；MAC1， 4 字节）

（4）响应信息

响应信息中可能返回的状态码有：

SW1	SW2	含义
90	00	命令执行成功
67	00	Lc 长度错
69	85	使用条件不满足（应用非永久锁定）
6A	81	功能不支持（卡锁定）
6A	86	参数 P1，P2 不正确
6A	88	未找到密钥参数
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

8.2.6 WRITE KEY 命令

（1）命令描述

WRITE KEY 命令装载或更新 PSAM 卡中的计算密钥。该命令格式符合《中国金融 IC 卡 PSAM 卡应用规范》。

(2) 使用条件和安全

执行 WRITE KEY 命令前，先要执行 GET CHANLLEGE 命令。WRITE KEY 命令数据域中的密钥信息内容：

- I 密钥用途 1 字节
- I 密钥版本 1 字节
- I 密钥算法标识 1 字节
- I 密钥值 8 字节或 16 字节

(3) 命令格式

代码	值
CLA	‘84’
INS	‘D4’
P1	‘00’
P2	‘00’
Lc	‘14’或‘1C’
Data	密文密钥信息 MAC
Le	不存在

(4) 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	含义
90	00	命令执行成功
65	81	内存失败
67	00	Lc 长度错
69	83	认证密钥锁定
69	84	引用数据无效（未取随机数）
69	85	使用条件不满足（应用非永久锁定）
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（卡锁定）
6A	86	参数 P1, P2 不正确
6A	88	未找到密钥参数
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

9 附录

PSAM 卡内密钥与 ESAM、用户卡内密钥对应关系：

PSAM 卡密钥	ESAM 密钥	用户卡密钥
CPU 卡外部认证密钥 UK _{DF01}		外部认证子密钥 UK _{DF01}
CPU 卡消费密钥 1 PK1		消费子密钥 1 DPK1
CPU 卡消费密钥 2 PK2		消费子密钥 2 DPK2
CPU 卡圈存密钥 LK		圈存子密钥 1 DLK1
CPU 卡 TAC 密钥 TK		TAC 子密钥 DTK
0BU 认证主密钥 RK1	DF01 应用认证密钥	
0BU 加密主密钥 RK2	DF01 应用加密密钥	
0BU 应用维护密钥 AMK _{0BU}	DF01 应用维护密钥	

注：CPU卡圈存密钥（LK）、0BU应用维护密钥（AMK_{0BU}）仅为方便测试而设立，只存于测试阶段的PSAM卡中