中国金融 IC 卡试点 PSAM 卡应用规范

（讨论修改稿）

中国金融 IC 卡试点工程实施小组

一 九 九 九 年 七 月

目 录

一. 文件结构

PSAM 卡用于商户 POS、网点终端、直联终端等端末设备上，负责机具的安全控管。PSAM 卡具有一定的通用性。经过个人化处理的 PSAM 卡能在不同的机具上使用。

PSAM 卡支持多级发卡的机制，各级发卡方在卡片主控密钥和应用主控密钥的控制下创建文件和装载密钥。

1. 文件结构

PSAM 卡文件结构符合 ISO/IEC7816－4。

本条款描述了符合本规范的应用文件结构，这些应用被定义为支付系统应用（PSA）。符合 ISO/IEC7816－4，但不符合本规范的其他应用也可出现在 PSA 上，并可以使用本规范中定义的命令进行操作。

PSAM 卡中 PSA 的路径可以通过明确选择支付系统环境（PSE）来激活。

PSAM 卡文件结构如下图所示：

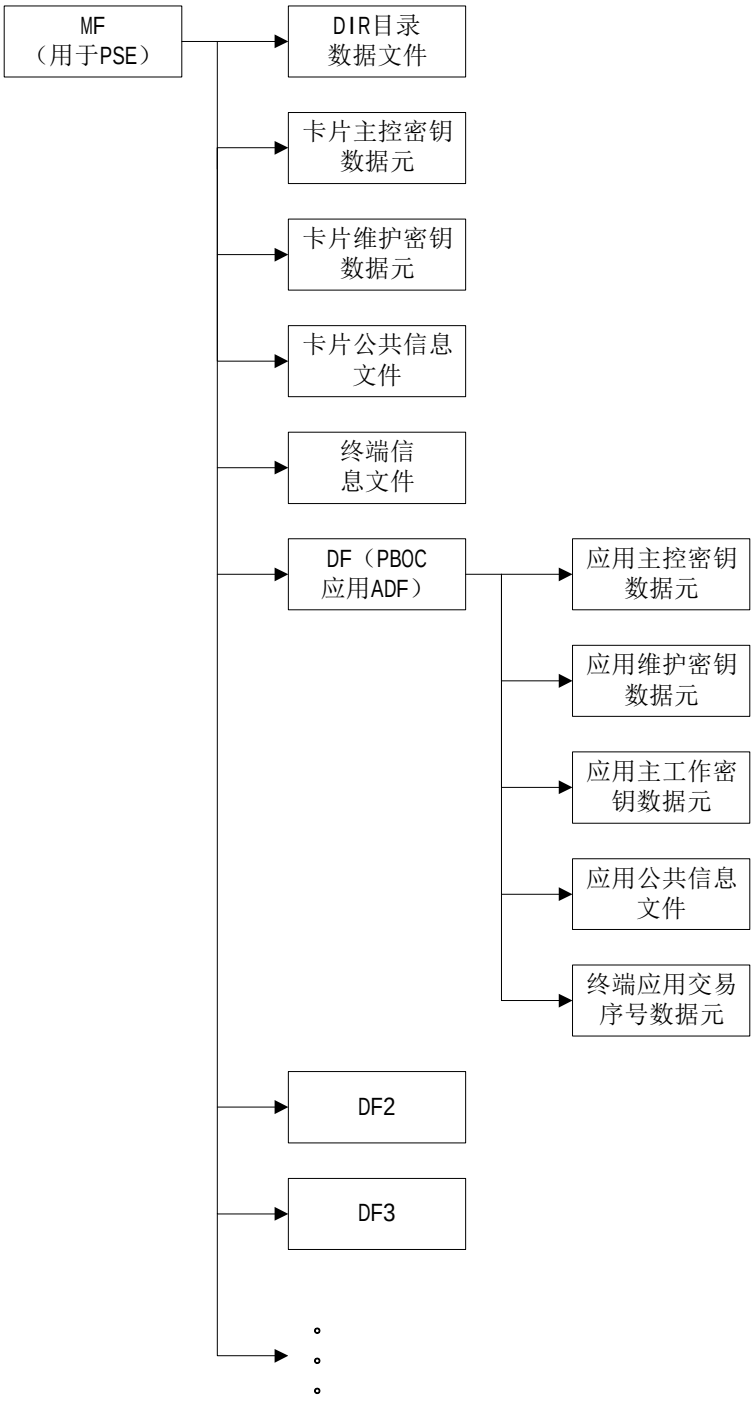

图 1　PSAM 卡文件结构

2. MF 区域说明

在 PSAM 卡的 MF 区域中，文件创建和密钥装载是在卡片主控密钥的控制

下进行。

1) DIR 目录数据文件

DIR 目录数据文件的说明参考《中国金融集成电路（IC）卡规范》，但 DIR 目录数据文件的入口地址必须包括全国密钥管理总中心应用 ADF。

2) 卡片主控密钥

卡片主控密钥是卡片的控制密钥，由卡片生产商写入，由发卡方替换为发卡方的卡片主控密钥。卡片主控密钥的更新在自身的控制下进行。发卡方必须在卡片主控密钥的控制下，

- 创建卡片 MF 区域的文件；
- 装载卡片维护密钥、应用主控密钥；
- 更新卡片主控密钥、卡片维护密钥。

卡片主控密钥的控制可通过外部认证操作实现，也可通过安全报文的方式实现。

3) 卡片维护密钥

卡片维护密钥用于卡片 MF 区域的应用维护，在卡片主控密钥的控制下装载和更新。卡片的管理者可在卡片维护密钥的控制下，

- 安全更新记录文件；
- 安全更新二进制文件。

卡片维护密钥的控制通过安全报文的形式实现。

4) 卡片公共信息文件

卡片公共信息文件存放卡片的公共信息，在卡片主控密钥的控制下创建，可自由读，可在卡片维护密钥的控制下改写。

5) 终端信息文件

终端信息文件存放终端的信息，在卡片主控密钥的控制下创建，可自由读，可在卡片维护密钥的控制下改写。

3. ADF 区域说明

在 PSAM 卡的 ADF（Application Data File）区域中，文件创建和密钥装载是在应用主控密钥的控制下进行。ADF 下的文件结构可由应用发行者自行确定。全国密钥管理中心应用 ADF 的文件结构必须包括应用主控密钥、应用维护密钥、应用主工作密钥数据元、应用公共数据文件和终端应用交易序号数据元。

1) 应用主控密钥

应用主控密钥是应用的控制密钥，在卡片主控密钥控制下写入。发卡方必须在应用主控密钥的控制下，

- 装载应用维护密钥、应用主工作密钥；
- 更新应用主控密钥、应用维护密钥。

应用主控密钥的控制可通过外部认证操作实现，也可通过安全报文的方式实现。

2) 应用维护密钥

应用维护密钥用于卡片 ADF 区域的应用维护，在应用主控密钥的控制下装载和更新。卡片的管理者可在应用维护密钥的控制下，

- 安全更新记录文件；
- 安全更新二进制文件；
- 进行应用解锁。

卡片维护密钥的控制通过安全报文的形式实现。

3) 应用主工作密钥

应用主工作密钥用于卡片的交易，在应用主控密钥的控制下装载。

4) 应用公共信息文件

应用公共信息文件存放应用的公共信息，在应用主控密钥的控制下创建，可自由读，可在卡片维护密钥的控制下改写。

5) 终端应用交易序号数据元

终端应用交易序号长度 4 字节，用于终端的脱机交易，在消费交易 MAC2 验证通过的情况下由卡片操作系统改写。

终端应用交易序号只对本应用有效。

二. 基本命令

1. 选择文件（Select）

1) 定义和范围

SELECT 命令通过文件名或 AID 来选择 IC 卡中的 PSE、DDF 或 ADF。

命令执行成功后，PSE、DDF 或 ADF 的路径被设定。

应用到 AEF 的后续命令将采用 SFI 方式联系到所选定的 PSE、DDF 或 ADF。

从 IC 卡的响应报文应由回送的 FCI 组成。

2) 命令报文

SELECT FILE 命令报文见表 2 - 1。

代码	值
CLA	00h
INS	A4h
P1	引用控制参数（见表 2 - 2）
P2	00h：第一个或仅有一个 02h：下一个
Lc	05h ~ 10h
Data	文件名
Le	00h

表 2 - 1 SELECT 命令报文表

b8	b7	b6	b5	b4	b3	b2	b1	含义

0	0	0	0	0				
					1			通过文件名选择
						0	0	

表 2 - 2 SELECT 命令引用控制参数

3) 命令报文数据域

命令报文数据域应包括所选择的 PSE 名、DF 名或 AID。

4) 响应报文数据域

响应报文中数据域应包括所选择的 PSE、DDF 或 ADF 的 FCI。表 2 - 3 到表 2 - 5 规定了此定义所用的标志。本规范不规定 FCI 中回送的附加附加标志。

表 2 - 3 定义了成功选择 PSE 后回送的 FCI：

标志	值	存在方式
'6F'	FCI 模板	M
'84'	DF 名	M
'A5'	FCI 专用数据	M
'88'	目录基本文件的 SFI	M

表 2 - 3 SELECT PSE 的响应报文（FCI）

表 2 - 4 定义了成功选择 DDF 后回送的 FCI：

标志	值	存在方式
'6F'	FCI 模板	M
'84'	DF 名	M
'A5'	FCI 专用数据	M
'88'	目录基本文件的 SFI	M

表 2－4　SELECT DDF 的响应报文（FCI）

表 2－5 定义了成功选择 ADF 后回送的 FCI：

标志	值	存在方式
'6F'	FCI 模板	M
'84'	DF 名	M
'A5'	FCI 专用数据	M
'9F0C'	发卡方自定义数据的 FCI	O

表 2－5　SELECT ADF 的响应报文（FCI）

2. 读记录文件（Read Record）

1) 定义和范围

READ RECORD 命令用于读取记录文件中内容。

IC 卡的响应由回送的记录数据组成。

2) 命令报文

READ RECORD 命令报文见表 2－6。

代码	值
CLA	00h
INS	B2h
P1	记录的序号
P2	引用控制参数（见表 2－7）
Lc	不存在；
Data	不存在；
Le	00h

表 2－6 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

表 2－7 READ RECORD 命令引用控制参数

3) 命令报文数据域

命令报文数据域不存在。

4) 响应报文数据域

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。

3. 写记录文件（Update Record）

1) 定义和范围

UPDATE RECORD 命令用命令 APDU 中给定的数据更改指定的记录。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

在安全更新记录时，若安全报文连续三次出错，则永久锁定应用。

2) 命令报文

UPDATE RECORD 命令报文见表 2 - 8。

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	见表 2 - 8
Lc	后续数据域长度
Data	输入数据
Le	不存在

表 2 - 8 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

表 2 - 9 UPDATE RECORD 命令引用控制参数

3) 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。

4) 响应报文数据域

响应报文数据域不存在。

4. 读二进制文件（Read Binary）

1) 定义和范围

READ BINARY 命令用于读取二进制文件的内容（或部分内容）。

2) 命令报文

READ BINARY 命令报文见表 2 - 10。

代码	值
CLA	00h
INS	B0h
P1	见表 2 - 11
P2	从文件中读取的第一个字节的偏移地址
Lc	不存在
Data	不存在
Le	00

表 2 - 10 READ BINARY 命令报文

b8	b7	b6	b5	b4	b3	b2	b1	含义
X 1								读取模式： - 用 SFI 方式
	0	0						RFU（如果 b8 = 1）
			X	X	X	X	X	SFI（取值范围 21 - 30）

表 2 - 11 READ BINARY 命令引用控制参数

3) 命令报文数据域

命令报文数据域不存在。

4) 响应报文数据域

当 Le 的值为 0 时，只要文件的最大长度在 256（短长度）或 65536（扩展长度）之内，则其全部字节将被读出。

5. 写二进制文件（Update Binary）

1) 定义和范围

UPDATE BINARY 命令用命令 APDU 中给定的数据修改 EF 文件中已有的数据。

2) 命令报文

UPDATE BINARY 命令报文见表 2 - 12。

代码	值
CLA	00h 或 04h
INS	D6h
P1	见表 2 - 13
P2	要修改的第一个字节的偏移地址
Lc	后续数据域的长度
Data	修改用的数据
Le	不存在

表 2 - 12 UPDATE BINARY 命令报文

b8	b7	b6	b5	b4	b3	b2	b1	含义
X 1								读取模式： - 用 SFI 方式
	0	0						RFU（如果 b8 = 1）
			X	X	X	X	X	SFI（取值范围 21 - 30）

表 2 - 13 UPDATE BINARY 命令引用控制参数

3) 命令报文数据域

命令报文数据域包括更新原有数据的新数据。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数据的新数据计算而得到的。

4) 响应报文数据域

响应报文数据域不存在。

6. 外部认证（External Authentication）

1) 定义和范围

EXTERNAL AUTHENTICATION 命令用于对卡片外部的安全认证。计算的方法是利用卡片中的卡片主控密钥或应用主控密钥，对卡片产生的随机数（使用 GET CHALLENGE 命令）和接口设备传输进来的认证数据进行验证。

2) 命令报文

EXTERNAL AUTHENTICATION 命令报文见表 2－14。

代码	值
CLA	00h
INS	82h
P1	00h
P2	00h
Lc	08h
Data	发卡方认证数据
Le	不存在

表 2－14 EXTERNAL AUTHENTICATION 命令报文

3) 命令报文数据域

命令报文数据域中包含 8 字节的加密数据，该数据是用主控密钥对此命令前一条命令“GET CHALLENGE”命令获得的随机数后缀“00 00 00 00”之后做 3DES 加密运算产生的。

4) 响应报文数据域

响应报文数据域不存在。

7. 取响应数据（Get Response）

1) 定义和范围

当 APDU 不能用现有协议传输时，GET RESPONSE 命令提供了一种从 IC 卡向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

2) 命令报文

GET RESPONSE 命令报文见表 2 - 15。

代码	值
CLA	00h
INS	C0h
P1	00h
P2	00h
Lc	不存在
Data	不存在
Le	期望数据的最大长度

表 2 - 15 GET RESPONSE 命令报文

3) 命令报文数据域

命令报文数据域不存在。

4) 响应报文数据域

响应报文数据域的长度由 Le 的值决定。如果 Le 的值为 0，在后续数据有效时，IC 卡必须回送状态码‘6Cxx’，否则‘6F00’。

8. 取随机数（Get Challenge）

1) 定义和范围

GET CHALLENGE 命令用于从 IC 卡中获得一个 4 个字节的随机数。该随机数服务于安全过程（如安全报文），在使用随机数的命令执行后失效。

2) 命令报文

GET CHALLENGE 命令报文见表 2 - 16。

代码	值
CLA	00h
INS	84h
P1	00h
P2	00h
Lc	不存在
Data	不存在
Le	04h

表 2 - 16 GET CHALLENGE 命令报文

3) 命令报文数据域

命令报文数据域不存在。

4) 响应报文数据域

IC 卡产生的随机数，长度为 4 字节。

三. 扩展命令

为符合《中国金融集成电路（IC）卡规范（V1.0）》和《银行 IC 卡联合试点技术方案》的安全控管要求，PSAM 卡必须支持以下专用命令。

1. 写入密钥（Write Key）

1) 定义和范围

WRITE KEY 命令可向卡中装载密钥或更新卡中已存在的密钥。本命令可支持 8 字节或 16 字节的密钥，密钥写入必须采用加密的方式，在主控密钥的控制下进行。

在密钥装载前必须用 GET CHANLLEGE 命令从 PSAM 卡取一个 4 字节的随机数。

2) 命令报文

WRITE KEY 命令报文见表 3 - 1。

代码	值
CLA	84h
INS	D4h
P1	00h
P2	00h
Lc	14h 或 1Ch
Data	加密后的密钥信息、MAC
Le	不存在

表 3 - 1 WRITE KEY 命令报文

3) 命令报文数据域

命令报文数据域包括要装载的密钥密文信息和 MAC。

密钥密文信息是用主控密钥对以下数据加密（按所列顺序）产生的：

——密钥用途

——密钥版本

——密钥算法标识

——密钥值

MAC 是用主控密钥对下数据进行 MAC 计算（按所列顺序）产生的：

——CLA

——INS

——P1

——P2

——Lc

——密钥密文信息

加密和 MAC 计算的方法遵循《中国金融集成电路（IC）卡规范》。

装载 8 字节的单长度密钥时，数据长度为 14h；装载 16 字节的双长度密钥时，数据长度为 1Ch。

4) 响应报文数据域

响应报文数据域不存在。

2. 通用 DES 计算初始化（INIT_FOR_ DESCRYPT）

1) 定义和范围

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。

不支持计算临时密钥计算的密钥类型有：

——主控密钥

——维护密钥

——消费密钥

双长度密钥产生双长度临时密钥的密钥类型有：

——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

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

指定密钥经过几级处理由密钥分散级数和 Lc 确定，若二者不一致，则返回错误信息。

临时密钥在 PSAM 卡下电后自动消失，不允许读。

临时密钥产生后，与原密钥的属性一致。

2) 命令报文

INIT_FOR_ DESCRYPT 命令报文见表 3 - 2。

代码	值
CLA	80h
INS	1Ah
P1	密钥用途
P2	密钥版本
Lc	待处理数据的长度
Data	待处理的数据
Le	无

表 3 - 3 INIT_FOR_ DESCRYPT 命令报文

3) 命令报文数据域

命令报文数据域包括待处理的输入数据。数据长度为 8 的整数倍，长度也可以为 0。密钥类型取密钥用途的低 5 位，密钥分散级数取密钥用途的高 3 位。

如待处理的输入数据包括多级的分散因子，按最后一次分散因子在前、最先一次分散因子在后的顺序输入。

4) 响应报文数据域

响应报文数据域不存在。

3. 通用 DES 计算（DES Crypt）

1) 定义和范围

DES CRYPT 命令利用指定的密钥来进行运算。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，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的加密。

MAC 计算遵循《中国金融集成电路（IC）卡规范》，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的 MAC 计算。

DES CRYPT 命令必须在 INIT_FOR_ DESCRYPT 命令成功执行后才能进行。卡片状态在执行无后续块计算后，复原为通用 DES 计算初始化执行前的状态。

2) 命令报文

DES CRYPT 命令报文见表 3 - 3。

代码	值
CLA	80h
INS	Fah
P1	见表 3 - 4
P2	00h
Lc	要加密的数据长度
Data	要加密的数据
Le	不存在

表 3 - 3 DES CRYPT 命令报文

b8	b7	b6	b5	b4	b3	b2	b1	含义
							X	计算模式 ——0，加密 ——1，MAC 计算
						X		后续块 ——0，无后续块 ——1，有后续块
					X			初始值（仅对 MAC 计算有效） ——0，无初始值 ——1，有初始值

表 3 - 4　DES CRYPT 命令引用控制参数

P1 值计算模式如下：

——0，无后续块加密

——1，下一块 MAC 计算

——2，有后续块加密

——3，最后一块 MAC 计算

——5，唯一一块 MAC 计算

——7，第一块 MAC 计算

——其他，保留

3)　命令报文数据域

命令报文数据域包括要加密的数据。加密数据的长度为 8 的整数倍。在 P1

的 b3 位为 1 时，待处理数据的前 8 个字节为 MAC 计算的初始值。

4) 响应报文数据域

在 P1 的 b1 位为 0 时，响应报文数据域包括加密结果，数据长度是 8 的整数倍。

在 P1 的 b1 位为 1，且 P1 的 b2 位为 0 时，响应报文数据域包括 4 字节的 MAC。

4. 应用解锁（Application Unblock）

1) 定义和范围

APPLICATION UNBLOCK 命令用于恢复当前应用。当命令成功完成后，对应用访问的限制将被取消，利用消费密钥校验 MAC2 的错误计数器将被重置。

如果应用解锁连续失败三次，卡将永久锁定此应用。

在 APPLICATION UNBLOCK 命令执行前必须执行 GET CHANLLENGE 命令取得 4 字节的随机数。

2) 命令报文

APPLICATION UNBLOCK 命令报文见表 3 - 5。

代码	值
CLA	84h
INS	18h
P1	00
P2	00
Lc	数据字节数
Data	报文鉴别代码数据元
Le	不存在

表 3 - 5 APPLICATION UNBLOCK 命令报文

3) 命令报文数据域

命令报文数据域包括报文鉴别代码，由应用维护密钥对以下数据（按所列顺序）进行 MAC 计算而得到的：

——CLA

——INS

——P1

——P2

——Lc

MAC 计算的方式参见《中国金融集成电路（IC）卡规范。》

4) 响应报文数据域

响应报文数据域不存在。

5. MAC1 计算（INIT_SAM_FOR_PURCHASE）

1) 定义和范围

INIT_SAM_FOR_PURCHASE 命令可支持多级消费密钥分散机制，产生《中国金融集成电路（IC）卡规范》中定义的 MAC1。根据银行 IC 卡试点技术方案，可以利用试点城市标识、成员行标识、卡片应用序列号、随机数和交易信息得到过程密钥，进而加密得到 MAC。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）对试点城市标识分散，得到二级消费主密钥 BMPK；
- PSAM 在其内部用 BMPK 对成员行标识分散，得到成员行消费主密钥 MPK；
- PSAM 在其内部用 MPK 对卡片应用序列号分散，得到卡片消费子密钥 DPK；
- 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；
- 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。

在此过程中，所有的中间结果只保留在卡片内部，外界无法得到。只有进行本命令后，才允许进行 MAC2 校验的命令。

参与处理的终端机编号和终端交易序号由卡片操作系统从卡片中取得。

INIT_SAM_FOR_PURCHASE 命令可支持多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。

2) 命令报文

INIT_SAM_FOR_PURCHASE 命令报文见表 3 - 6。

代码	值
CLA	80h
INS	70h
P1	00h
P2	00h
Lc	14h + 8×N（N = 1，2，3）
Data	要处理的数据
Le	08

表 3 - 6 INIT_SAM_FOR_PURCHASE 命令报文

3) 命令报文数据域

命令报文数据域包括的数据以下列顺序排列：

- 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

4) 响应报文数据域

响应报文数据域包括以下数据（按顺序返回）：

——4 字节的终端脱机交易序号

——4 字节的 MAC1

6. 校验 MAC2（CREDIT_SAM_FOR_PURCHASE）

1) 定义和范围

CREDIT_SAM_FOR_PURCHASE 命令利用 INIT_SAM_FOR_PURCHASE 命令产生的过程密钥 SESPKP 校验 MAC2，过程如下所示：

- 检查 MAC2 尝试计数器 ,如 MAC2 未被锁定 ,PSAM 在其内部用 SESPK 对交易金额加密得到 MAC2，与命令报文中的数据进行比较；
- 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；
- 如命令执行不成功，PSAM 卡将 MAC2 尝试计数器减 1，并回送状态码’63Cx’，这里’x’是 MAC2 尝试计数器的新值；
- 如果’x’为零，PSAM 卡将锁定消费密钥所在的 ADF。

在此过程中，所有的中间结果只保留在卡片内部，外界无法得到。

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

若 MAC2 尝试计数器为 0 的话，消费密钥所在的应用将被锁定，只能在应用维护密钥的控制下应用解锁后使用。

应用下的 MAC2 错误计数器在应用下所有消费密钥 MAC2 校验错误的情况下都要被减 1。

卡片的状态在命令执行后将复原为 MAC1 校验前的状态。

2) 命令报文

CREDIT_SAM_FOR_PURCHASE 命令报文见表 3 - 7。

代码	值

CLA	80h
INS	72h
P1	00h
P2	00h
Lc	04h
Data	MAC2
Le	不存在

表 3 - 7 CREDIT_SAM_FOR_PURCHASE 命令报文

3) 命令报文数据域

命令报文数据域包括 4 字节的 MAC2。

4) 响应报文数据域

响应报文数据域不存在。

四. 应用流程

1. 全国密钥管理中心洗卡

GMPK 是整个系统的根密钥，如果一旦被盗取或被非法使用，就可能会伪造出大量的假卡，所有的银行 IC 卡将不得不停止使用，从而带来政治、经济上的重大损失。所以，从安全的角度来说，全国所有的 PSAM 卡必须在全国密钥管理总中心统一安全装载 GMPK。除了全国密钥管理总中心外，任何其他个人和组织无法得到 GMPK 的明文 ,也无法通过 PSAM 卡来利用 GMPK 进行非法的密钥运算。各个成员行可以向通过二级密钥管理中心申报所需 PSAM 卡的数量，由全国密钥管理总中心按需求量统一洗卡。

全国密钥管理总中心从生产商处得到一批 PSAM 卡，卡片已经过预个人化处理，卡片 MF 区域和全国密钥管理总中心 ADF 区域下的文件已由厂商建好，生产商密钥 (卡片主控密钥) 也已装载。在 IC 卡生产商将这一批 IC 卡交给全国密钥管理总中心的同时 ,存放生产商密钥的生产商母卡也要交给全国密钥管理总中心。

全国密钥管理总中心在接到这批卡之后，用生产商母卡中的生产商密钥 kMprd 来鉴别每一张 IC 卡。鉴别通过后，全国密钥管理总中心将用自己产生的密钥 kIctlR，来替换卡上的生产商密钥 kMprd，成为卡上的卡片主控密钥。

kIctlR 是全国密钥管理总中心随机产生或采用其他方法产生的，被加密导入后作为这一批 PSAM 卡的主控密钥，控制 MF 区域下文件创建和密钥更新。

全国密钥管理总中心必须在卡片主控密钥的控制下装载和更新密钥。具体的

过程如下所示：

——在生产商密钥（卡片主控密钥）的控制下，更新卡片主控密钥

——在卡片主控密钥的控制下，装载卡片维护密钥

——在卡片维护密钥的控制，安全更新卡片 MF 区域的文件

——在卡片主控密钥的控制下，装载应用主控密钥

——在应用主控密钥的控制下，装载应用维护密钥

——在应用主控密钥的控制下，装载应用主工作密钥

——在应用维护密钥的控制下，安全更新卡片 ADF 区域的文件

2. 消费交易流程

金融终端利用 PSAM 卡进行消费交易的处理流程如下图所示：

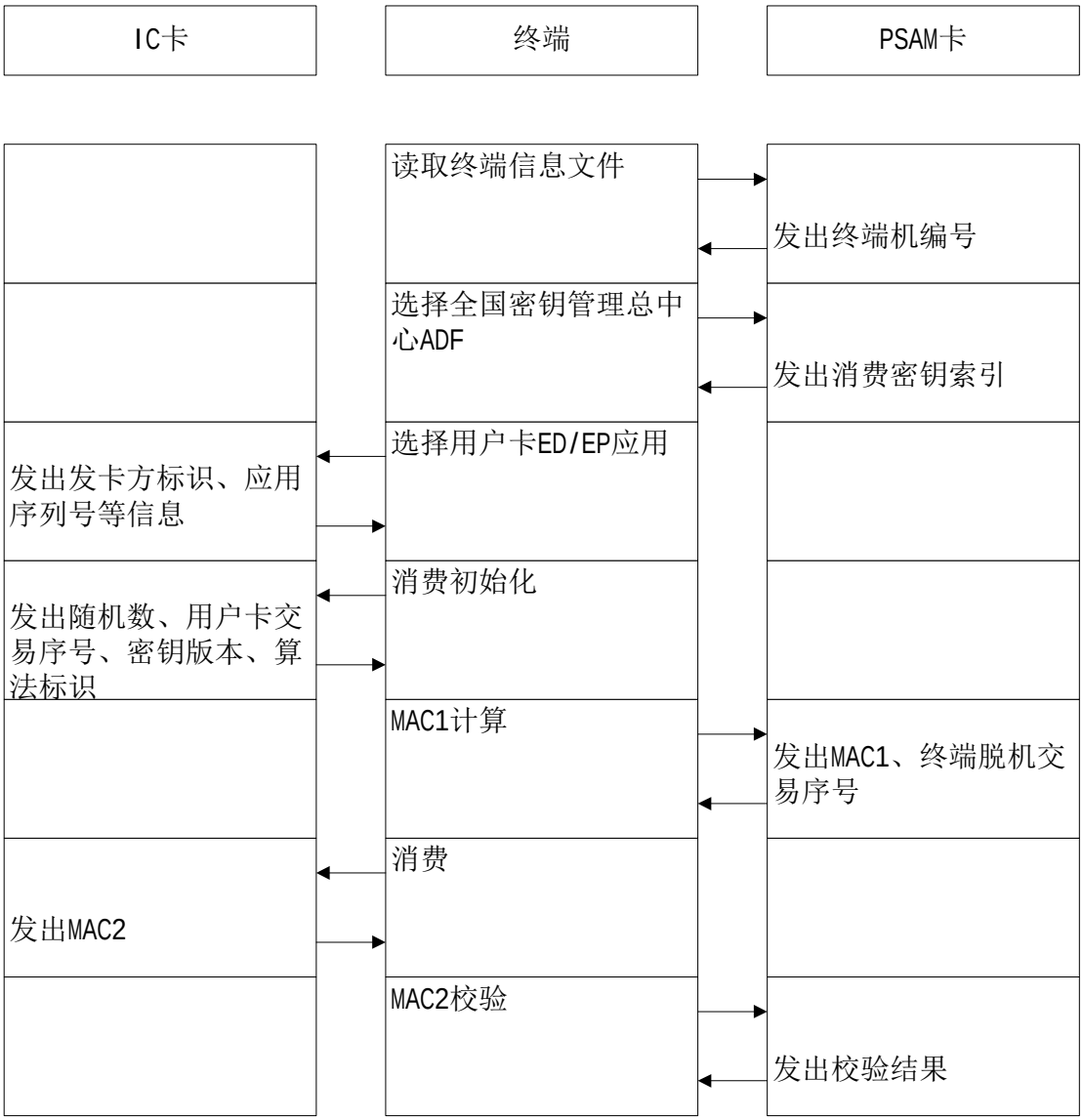
IC卡
终端
PSAM卡
读取终端信息文件
发出终端机编号
选择全国密钥管理总中心ADF
发出消费密钥索引
选择用户卡ED/EP应用
发出发卡方标识、应用序列号等信息
消费初始化
发出随机数、用户卡交易序号、密钥版本、算法标识
MAC1计算
发出MAC1、终端脱机交易序号
消费
发出MAC2
MAC2校验
发出校验结果

图 2　消费交易流程图

五. 安全特性

1. 密钥装载

密钥装载采用安全报文的方式，利用 WRITE KEY 命令来进行。安全报文产生的方式参见命令的说明。

密钥装载的控制过程如下：

- 卡片主控密钥在卡片主控密钥的控制下更新；
- 卡片维护密钥在卡片主控密钥的控制下装载和更新；
- 应用主控密钥在卡片主控密钥的控制下装载；
- 应用主控密钥在应用主控密钥的控制下更新；
- 应用维护密钥在应用主控密钥的控制下装载和更新；
- 应用主工作密钥在应用主控密钥的控制下装载和更新。

2. 密钥访问

- 密钥不允许直接读；
- 密钥必须在主控密钥的控制下更新；
- 消费密钥不能被外界直接访问 ,只能接受内部操作系统发来的进行 MAC 计算的指令，按照指定的流程计算出 MAC；
- 计算临时密钥产生的结果只保留在卡片内部，不能被外界直接访问。

3. 密钥属性

密钥的使用都有一定的限制，必须满足密钥属性的要求。

密钥属性应包括以下几项：

1) 密钥用途：

密钥用途长度为 1 字节，低 5 位为密钥类型，高 3 位为密钥分散级数。密钥类型约定如下：

——0，主控密钥

——1，维护密钥

——2，消费密钥

——3，PIN 解锁密钥

——4，重装 PIN 密钥

——5，用户卡应用维护密钥

——6，MAC 密钥

——7，加密密钥

——8，MAC、加密密钥

——9 - 31，保留

2) 密钥算法标识

密钥算法标识指定了密钥所支持加密算法，长度 1 字节。密钥算法标识约定如下：

——0，3DES

——1，DES

——2 - 255，保留

3) 密钥版本

密钥版本指定某种类型密钥的标识，长度 1 字节。对消费密钥来说，密钥版本是用于消费交易密钥选择过程中的密钥版本号，而对于其他密钥来说，密钥版本是密钥标识。

4. 加密算法描述

1) DES 算法

DES 算法遵循国际标准，加密模式采用 ECB 模式。

利用加密密钥对 8 字节块的输入数据 X_1，X_2，X_3... 加密，得到 8 字节块的输出数据 Y_1，Y_2，Y_3... 。

其中，

Y_I = DES（加密密钥）[X_I]

2) 3DES 算法

3DES 算法是指使用双长度（16 字节）密钥 K =（$K_L||K_R$）将 8 字节明文数据块加密成密文数据块，如下所示：

$$Y = DES(K_L)[DES^{-1}(K_R)[DES(K_L[X])]]$$

解密的方式如下：

$$X = DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L[Y])]]$$

3) 密钥分散算法

简称 Diversify，是指将一个双长度的密钥 MK，对分散数据进行处理，推导出一个双长度的密钥 DK。

推导 DK 左半部分的方法是：

- 将分散数据的最右 16 个数字作为输入数据；
- 将 MK 作为加密密钥；
- 用 MK 对输入数据进行 3DEA 运算。

推导 DK 右半部分的方法是：

- 将分散数据的最右 16 个数字求反，作为输入数据；
- 将 MK 作为加密密钥；
- 用 MK 对输入数据进行 3DEA 运算。

六. 状态码

命令返回的状态码如下所示：

状态号	返回状态码	性质	错误解释
00h	9000	正常	成功执行
01h	6200	警告	信息未提供
02h	6281	警告	回送数据可能出错
03h	6282	警告	文件长度小于 Le
04h	6283	警告	选中的文件无效
05h	6284	警告	FCI 格式与 P2 指定的不符
06h	6300	警告	鉴别失败
07h	63Cx	警告	校验失败（x - 允许重试次数）
08h	6400	出错	状态标志位没有变
09h	6581	出错	内存失败
0Ah	6700	出错	长度错误
0Bh	6882	出错	不支持安全报文
0Ch	6981	出错	命令与文件结构不相容，当前文件非所需文件
0Dh	6982	出错	操作条件（AC）不满足，没有校验 PIN
0Eh	6983	出错	认证方法锁定，PIN 被锁定
0Fh	6984	出错	随机数无效，引用的数据无效
10h	6985	出错	使用条件不满足

11h	6986	出错	不满足命令执行条件（不允许的命令，INS 有错）
12h	6987	出错	MAC 丢失
13h	6988	出错	MAC 不正确
14h	698D	保留	
15h	6A80	出错	数据域参数不正确
16h	6A81	出错	功能不支持；创建不允许；目录无效；应用锁定
17h	6A82	出错	该文件未找到
18h	6A83	出错	该记录未找到
19h	6A84	出错	文件预留空间不足
1Ah	6A86	出错	P1 或 P2 不正确
1Bh	6A88	出错	引用数据未找到
1Ch	6B00	出错	参数错误
1Dh	6Cxx	出错	Le 长度错误，实际长度是 xx
1Eh	6E00	出错	不支持的类：CLA 有错
1Fh	6F00	出错	数据无效
20h	6D00	出错	不支持的指令代码
21h	9301	出错	资金不足
22h	9302	出错	MAC 无效
23h	9303	出错	应用被永久锁定
24h	9401	出错	交易金额不足
25h	9402	出错	交易计数器达到最大值
26h	9403	出错	密钥索引不支持

27h	9406	出错	所需 MAC 不可用
28h	6900	出错	不能处理
29h	6901	出错	命令不接受（无效状态）
2Ah	61xx	正常	需发 GET RESPONSE 命令
2Bh	6600	出错	接收通讯超时
2Ch	6601	出错	接收字符奇偶错
2Dh	6602	出错	校验和不对
2Eh	6603	警告	当前 DF 文件无 FCI
2Fh	6604	警告	当前 DF 下无 SF 或 KF
30h		出错	密钥属性和命令参数不一致

附录 A 命令清单

附录 B 卡片中的基本数据文件

表 B1 MF 的卡片公共信息文件

文件标识（SFI）		'21'（十进制）
文件类型		透明
文件大小		14
文件存取控制	读 = 自由	改写 = 需要 安全信息
字节	数据元	长度
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

表 B2 MF 的终端信息文件

文件标识（SFI）		'22'（十进制）
文件类型		透明
文件大小		6
文件存取控制	读 = 自由	改写 = 需要 安全信息
字节	数据元	长度

1 - 6	终端机编号	6

表 B3 全国密钥管理总中心应用的应用公共信息文件

文件标识（SFI）		'23'（十进制）
文件类型		透明
文件大小		25
文件存取控制	读 = 自由	改写 = 需要 安全信息
字节	数据元	长度
1	全国消费密钥索引号	1
2 - 9	应用发行者标识	8
10 - 17	应用接收者标识	8
18 - 21	应用启用日期	4
22 - 25	应用有效日期	4