SmartCOS®用户手册

Version 4.5

深圳市明华澳汉科技股份有限公司

2009 年 5 月

目　　录

1. SMARTCOS 简介

由于 CPU 卡具有很高的安全性及一张卡支持多种应用的特点，所以 IC 卡家族中的 CPU 卡的使用范围正日益扩大。类似一台计算机，CPU 卡内也有 CPU、存储器和输入、输出接口，所以在应用中 CPU 卡也必然需要操作系统。深圳市明华澳汉科技股份有限公司成功地开发了自主版权的 CPU 卡操作系统--SMARTCOS（Smart Card Operating System），该操作系统符合 ISO 7816 系列标准及《中国金融集成电路（IC）卡规范》，适用于保险、医疗保健、社会保障、公共事业收费、安全控制、证件、交通运输等诸多应用领域,特别是在金融领域。SMARTCOS 详细规定了电子钱包、电子存折和磁条卡功能（Easy Entry）三种基本应用。

1.1. SMARTCOS 特点

- 支持 Single DES、Triple DES 算法：可自动根据密钥的长度选择 Single DES、Triple DES 算法
- 支持线路加密、线路保护功能：防止通信数据被非法窃取或篡改
- 支持在一张卡上实现多个不同的应用：可建立三级目录
- 支持电子钱包功能：钱包大小可由用户自行设定
- 支持多种文件类型：包括二进制文件、定长记录文件、变长记录文件、循环文件、钱包文件
- 支持 ISO14443-4：T=CL 通讯协议
- 满足银行标准：符合《中国金融集成电路（IC）卡规范》电子钱包/存折规范。
- 防插拔功能：交易处理过程中非正常拔出的卡片自动恢复

1.2. SMARTCOS V4.5 内部结构

CPU	RAM
加密逻辑	ROM
RF 接口	EEPROM

1.2.1. CPU 及加密逻辑

保证 EEPROM 中数据安全，使外界不能用任何非法手段获取 EEPROM 中的数据。

1.2.2. RAM

SMARTCOS 工作时存放命令参数、返回结果、安全状态及临时工作密钥的区域。

1.2.3. ROM

存放 SMARTCOS 程序的区域。

1.2.4. EEPROM

存放用户应用数据区域，SMARTCOS 将用户数据以文件形式保存在 EEPROM 中，在满足用互规定的安全条件时，可进行读或写。

1.3. 功能模块

SMARTCOS 由传输管理、文件管理、安全体系、命令解释四个功能模块组成。

- 传输管理：按 ISO7816-3、ISO14443-4 标准监督卡与终端之间的通信，保证数据正确地传输，防止卡与终端之间通讯数据被非法窃取和篡改。
- 文件管理：将用户数据以文件形式存储在 EEPROM 中，保证访问文件时快速性和数据安全性。
- 安全体系：安全体系是 SMARTCOS 的核心部分，它涉及到卡的鉴别与核实，对文件访问时的权限控制机制。
- 命令解释：根据接收到的命令检查各项参数是否正确，执行相应的操作。

1.4. 命令列表

表 1.1 SmartCOS 4.5 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

2. SMARTCOS 文件结构

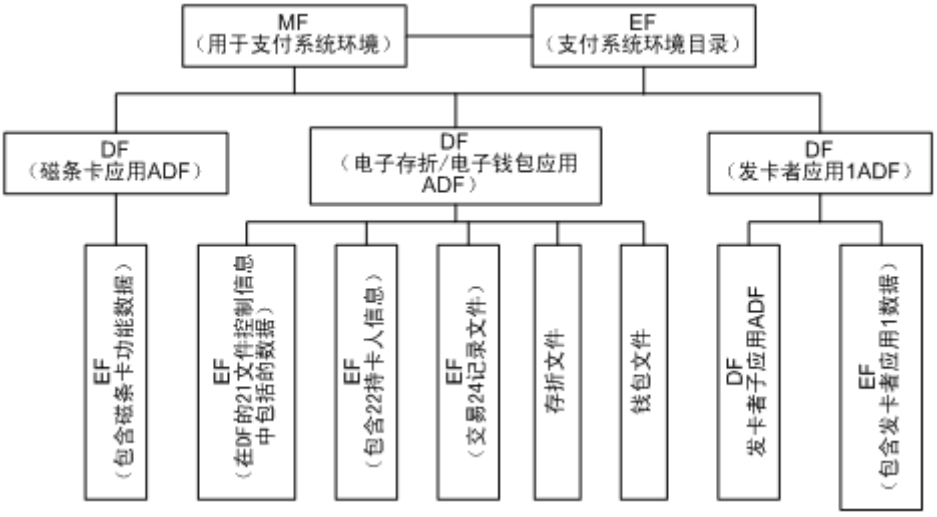
2.1. 文件结构

SMARTCOS IC 卡的基本文件系统是由主文件 MF（Master File）、目录文件 DF（Directory File）和基本文件 EF（Element File）组成。主文件 MF 在 IC 卡中唯一存在，在 MF 下可以有多个目录文件 DF 和基本文件 EF，每一个 MF 目录下的 DF 可以存放多个基本文件 EF 和多个下级目录文件 DF，在这里我们称包含下级目录的目录文件为 DDF，不含下级目录的目录文件为 ADF。

SMARTCOS 描述了符合<<中国金融集成电路（IC）卡规范>>的应用文件结构，这些应用被定义为支付系统应用。IC 卡中支付系统应用可以通过明确选择支付系统环境来激活，一个成功的支付系统环境选择能够对目录结构进行访问。

从终端角度来看，与支付系统应用相关的支付系统环境文件呈一种可通过目录结构访问的树形结构。树的每一分支是一个应用数据文件 ADF。一个 ADF 是一个或多个应用基本文件 EF 的入口点。一个 ADF 及其相关数据文件处于树的同一分支上。

下图给出了一个卡片内部结构示例，该卡片支持电子存折、电子钱包、磁条卡功能应用（Easy entry）以及一个没有定义的发卡方应用。



2.1.1. MF 文件

在 SMARTCOS 卡中，MF 文件唯一存在，是卡片文件系统的根。它相当于 DOS 的根目录。IC 卡复位后，卡片自动选择 MF 文件为当前文件。SMARTCOS 卡支持用于支付系统环境应用列表的目录结构，支付系统环境由发卡方通过目录选择。目录结构包括一个必备的支付系统目录文件和一些可选的由 DDF 引用的附加记录。 目录文件 DF 的个数仅受 EEPROM 空间的限制。

2.1.2. DF 文件

目录文件 DF 相当于 DOS 的目录，每个 DDF 下可建立一个目录文件，但不是强制的。任何一个 DF 在物理上和逻辑上都保持独立，都有自己的安全机制和应用数据，可以通过应用选择实现对其逻辑结构的访问。可以将单个 DF 文件以及其中一个或多个 EF 文件当作

一个应用，也可以将多个 DF 以及其中多个 EF 文件当作一个应用，在使用 IC 卡时，用户可以根据不同的应用环境自行定义。

2.1.3. EF 文件

基本文件 EF 用于存放用户数据或密钥，存放用户数据的文件称为工作基本文件，在满足一定的安全条件下用户可对文件进行相应的操作。存放密钥的文件称为内部基本文件，不可由外界读出，但当获得许可的权限时可在卡内进行相应的密码运算，在满足写的权限时可以修改密钥。

KEY 文件为内部基本文件。

KEY 文件必须在 MF/DF 下最先被建立，且一个目录只能有一个 KEY 文件，KEY 文件可存多个口令密钥、外部认证密钥、DES 运算密钥，每个密钥为一条 TLV 格式的记录。

- 二进制文件：二进制文件为一个数据单元序列，数据以二进制为单位进行读写，其中的数据结构由应用者解释。
- 定长记录文件：定长记录文件每条记录长度都相同，数据以记录为单位进行存储，记录长度最大为 248 个字节。
- 循环文件：循环文件为具有固定长度记录的环行文件，每条记录都只有一个数据域，记录长度最大为 248 个字节。应用时只能顺序增加记录，当写记录时，当前写入的为第一条记录，则上一次写入的记录为第二条，依此类推，滚动写入。记录只能在文件头中所规定的范围内滚动写入，当写完最后一条记录时将覆盖最先写入的记录。
- 钱包文件：钱包文件内部采用专用的结构，由 COS 维护，保存电子钱包、存折的余额、透支限额等信息。
- 变长记录文件： 变长记录文件的每条记录长度在写记录时是可变的，数据以记录为单位进行存储。更新记录时，新的记录长度必须与卡中的原有记录长度相同，否则本次更新无效。 记录最大长度不能超过 248 字节。变长记录格式 TLV 如下：

TAG：标识	Length：数据长度	Val：L 字节数据

2.2. 文件空间结构

每个文件在 EEPROM 中存放的格式如下：

11 字节文件头 （文件类型，文件标识符，文件主体空间大小，权限，校验等）
文件主体

每个基本文件所占的 EEPROM 空间=文件头 11 字节+文件主体空间。

定长和循环文件的主体空间=记录个数×(记录长度+1)。

电子钱包和电子存折文件主体空间=22 字节。

每个 DF 所占的 EEPROM 空间=DF 头 11 字节+DF 下所有文件的空间和+DF 名称长度。

MF 的空间=MF 头 11 字节+MF 下所有文件空间之和+ MF 名称长度（若不使用默认名称）。

MF 空间不能超过卡 EEPROM 空间容量，若建 MF 空间小于 EEPROM 空间，则剩余空间不可用。

2.3. 文件访问方式

- 主文件 MF：复位后自动被选择，在任何一级子目录下可通过文件标识 3F 00 或 MF 名称来选择 MF。创建时默认名称为 1PAY.SYS.DDF01。
- 目录文件 DF：通过文件标识符或目录名称选择目录文件 DF。
- 二进制文件：在满足读条件时可使用 READ BINARY 读取，在满足写条件时 UPDATE BINARY 更改二进制文件内容。
- 定长记录文件：在满足读条件时可使用 READ RECORD 读指定记录，在满足写条件时使用 UPDATE RECORD 更改指定记录。在满足追加条件时可使用 APPEND RECORD 在文件末尾追加一条记录。
- 循环文件：在满足读条件时可使用 READ RECORD 读指定记录，在满足追加条件时可使用 APPEND RECORD 在文件开头追加一条记录，当记录写满后自动覆盖最早写的记录，最后一次写入的记录，其记录号总是 1，上次写入的记录号是 2，依次类推。
- 钱包文件：在满足使用条件时可用 GET BALANCE 读余额或在规定的密钥控制下完成圈存、圈提、消费、取现、修改透支限额。
- 变长记录文件：在满足读条件时可使用 READ RECORD 读出指定记录，在满足写条件时可以使用 UPDATE RECORD 写一条新记录或更改已存在的记录，或用 APPEND RECORD 在文件末尾追加一条新记录。变长记录文件的格式为 TLV 格式，Tag 为 1 字节记录标识，L 为一字节记录数据域长度。V 为 L 字节数据值。在执行 UPDATE RECORD 更改已存在的记录时，新写的整条记录长度必须和原来的整个记录长度相等，否则该命令不能成功执行。
- KEY 文件及其文件中的密钥：每个 DF 或 MF 下只能有一个 KEY 文件，且必须最先被建立，在任何情况下密钥数据均无法读出。当进入 DF 或 MF 时，若该目录下无 KEY 文件和其它文件，则在该目录下可任意建立文件和读写文件而不受文件访问权限的限制。一旦离开该目录再进入此目录时，将遵循文件的访问权限。
- 在 KEY 文件中可以存放多个密钥，每个密钥为一条可变长的记录，记录的长度为密钥数据长度加 8。如 Triple DES 密钥记录的长度为 24 字节，Single DES 密钥记录的长度为 16 字节。
- 在满足 KEY 文件增加密钥的权限时可用 WRITE KEY 增加一条密钥记录，在满足某个密钥规定的更改权限时可使用 WRITE KEY 更改密钥数据，在满足使用权限时才可使用相应的密钥进行认证或密码运算。
- 密钥具有独立性，用于一种特定功能的加密/解密密钥不能被任何其它功能所使用，包括保存在 IC 卡中的密钥和用来产生、派生、传输这些密钥的密钥。
- 口令密钥：在满足口令密钥的使用权限时，可用 VERIFY 核对口令，或 PIN CHANGE/UNBLOCK 更改并解锁口令.在核对口令通过之后，设置安全状态寄存器的值为该口令密钥规定的后续状态值。口令密钥中提供错误次数计数器，每次核对口令失败时错误次数计数器自动减一，当错误次数达到 0 时，口令密钥被自动锁住。
- 解锁口令密钥：在满足使用权限时，可通过 UNBLOCK 核对解锁口令而达到解锁因连续核对口令错误被封锁的口令密钥，同时修改新的口令。解锁口令锁死后无法再被解锁。
- 外部认证密钥：在满足使用权限时可执行 EXTERNAL AUTHENTICATE 命令进行外部

认证，在满足更改权限时可使用 WRITE KEY 更改密钥。外部认证密钥锁死后无法被解锁。

2.4. 文件类型及命令集

下表为 SMARTCOS 命令适用的文件类型及命令集，水平方向表示 SMARTCOS 的文件类型， 垂直方向表示 SMARTCOS 命令集：

文件类型 命令	MF38	DF38	二进制 28	定长记录 2A	循环 2E	钱包 2F	变长记录 2C	KEY 文件 3F
CREATE	V	V	V	V	V	V	V	V
SELECT	V	V	V	V	V	V	V	V
READ BINARY			V					
UPDATE BINARY			V					
READ RECORD				V	V		V	
UPDATE RECORD				V	V		V	
PULL						V		
CHARGE						V		
WRITE KEY								V
ERASE DF	V	V						
CREDIT FOR LOAD						V		
DEBIT FOR PURCHASE/ CASE WITHDRAW						V		
DEBIT FOR UNLOAD						V		
GET BALANCE						V		
GET TRANSCATION PROVE						V		
INITIALIZE FOR CASE WITHDRAW						V		
INITIALIZE FOR LOAD						V		
INITIALIZE FOR PURCHASE						V		
INITIALIZE FOR UNLOAD						V		
INITIALIZE FOR UPDATE						V		
UPDATE OVERDRAW LIMIT						V		

说明：

表格中 V 表示命令可用于对应的文件类型，如第三行第三列为 V 表示用 READ BINARY 命令可读二进制文件，第三行第四列无 V 标识，表示定长记录文件不可用 READ BINARY 命令读取。

文件类型表示文件内部结构组织形式，用一个字节来表示，如某个文件类型为 28H 则表示该文件为二进制文件。文件类型在建立文件时规定。

2.5. 文件标识符与文件名称

文件标识符是文件的标识代码，用 2 个字节来表示，在选择文件时只要指出该文件的标识代码，SMARTCOS 就可以找到相应文件，同一目录下的文件标识符必须是唯一的。MF 的文件标识符是 3F00，默认文件名为 1PAY.SYS.DDF01。

所有文件都可以通过文件标识符用 SELECT 命令进行选择，目录文件 DF 还可以通过目录名称进行选择。

短文件标识符选择可以通过 READ BINARY、UPDATE BINARY 命令的参数 P1 来实现文件的选择：若参数 P1 的高三位为 100，则低 5 位为短的文件标识符。eg. 若 P1 为 81H 即 10000001，其中高三位为 100，则所选的文件标识符为 0001。

短文件标识符选择还可以通过 READ RECORD、UPDATE RECORD、APPEND RECORD、DECREASE、INCREASE 命令的参数 P2 来实现文件的选择：若 P2 的高五位不全为 0，低三位为 100，则高五位为短的文件标识符。eg. 若 P2 为 0CH 即 00001100，其中低三位为 100，所选的文件标识符为 0001。

短文件标识符选择只能用五位来决定文件标识符，所以可选择的最大文件标识符为 31。若文件需要用短文件标识符进行选择，则建立文件时就需将文件标识符取在 1-31（00001-11111）之间。

选择文件后，只要文件存在，该文件就被置为当前文件，以后可以不用选择而直接对该当前文件进行操作。

3. SMARTCOS 独特的安全体系

SMARTCOS 的安全体系从概念上可以分为安全状态、安全属性、安全机制和密码算法。

3.1. 安全状态

安全状态是指卡在当前所处的一种安全级别。SMARTCOS 的根目录和应用目录分别具有 16 种不同的安全状态。SMARTCOS 在卡内部用安全状态寄存器来表示安全级别；寄存器的值可以是 0 至 F 之间的某一值。

当前目录的安全状态寄存器的值在复位后或选择目录文件命令成功地被执行时被置为 0，如选择下级子目录时被置为 0，在当前目录下的口令核对或外部认证通过后该状态寄存器值发生变化。

3.2. 安全属性

安全属性是指对某个文件进行某种操作时所必须满足的条件，也就是在进行某种操作时要求安全状态寄存器的值是什么。

安全属性又称访问权限，一种访问权限在建立该文件时用一个字节指定。SMARTCOS 的访问权限有别于其它任何操作系统的访问权限，它用一个区间来严格限制其他非法访问者。

访问权限为 0Y 时表示要求 MF 的安全状态寄存器的值大于等于 Y。如某文件读的权限为 05 表示在对该文件进行读之前必须使 MF 的安全状态寄存器的值大于等于 5。

访问权限为 XY 时（X 不为 0）表示要求当前目录的安全状态寄存器的值大于等于 Y 且小于等于 X。若 X=Y 表示要求当前目录的安全状态寄存器的值等于 X，若 X<Y 表示不允许该操作。 如某文件写的权限为 53 表示对该文件进行写之前必须使当前目录的安全状态寄存器的值为 3、4 或 5。

例：某文件读的权限为 F0，写的权限为 F1，代表可任意读取，写时必须满足当前目录的安全状态寄存器的值大于等于 1。

3.3. 安全机制

安全机制是指某种安全状态转移为另一种安全状态所采用的方法和手段。SMARTCOS 通过核对口令和外部认证来改变安全状态寄存器的值。当在 MF 下时，认证通过之后同时改变 MF 和当前目录的安全状态寄存器的值，若不在 MF 下则认证通过之后只改变当前目录的安全状态寄存器值。

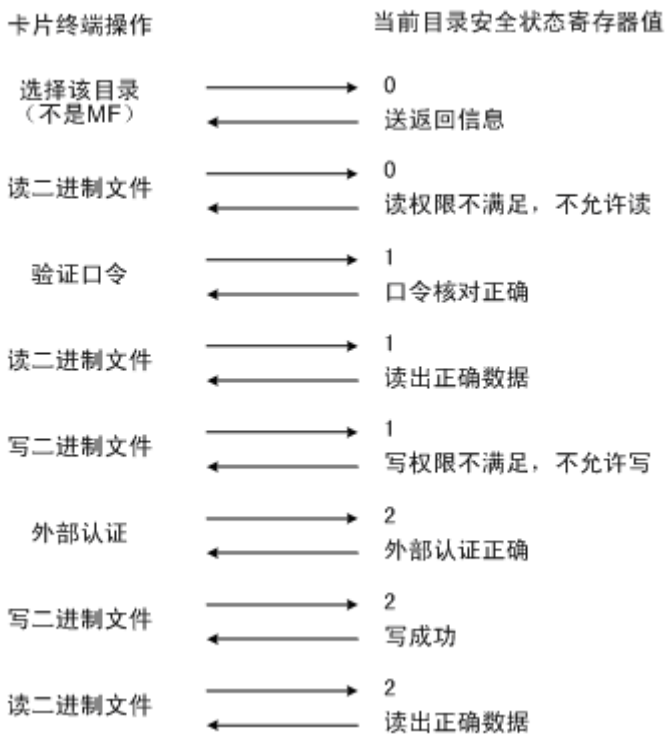
当建立口令或外部认证密钥时，参数的后续状态表示该口令核对成功或外部认证成功后，置当前目录的安全状态寄存器的值为后续状态。如某口令密钥的后续状态为 01 表示对口令核对成功后，当前目录的安全状态寄存器的值为 1。当上电复位后或从父目录进入子目录或退回上级目录时，当前目录的安全状态寄存器的值均自动被置为 0。

为更好的理解 SMARTCOS 的安全机制，下面举一例说明：

设卡中某目录下有一个二进制文件，定义读二进制文件的权限为 F1,写二进制文件权

限为 F2。该目录下有一个口令密钥，口令核对通过之后的后续状态为 1，卡中有一外部认证密钥，使用权限为 11，外部认证通过之后后续状态为 2。

请看下面的操作及当前目录的状态寄存器的变化情况：



3.4. 密码算法

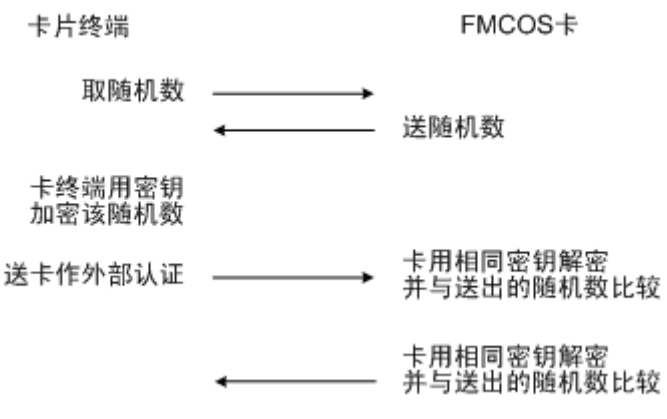
SMARTCOS 支持 Single DES、Triple DES。

在建立 DES 密钥时，若密钥长度为 8 字节则运算时使用 Single DES 算法，若密钥长度为 16 字节则运算时使用 Triple DES 算法（MAC 只能用 Single DES 算法）。

运算时使用加密还是解密算法完全由密钥类型决定，如：用于加密的密钥不可用于解密或 MAC 运算，用于外部认证的密钥也不可用于内部认证。

SMARTCOS 在使用 DES 算法时，若数据长度大于 8 字节时使用 ECB 模式，若数据长度不是 8 的倍数时在计算过程中自动在数据后补 80 00...00 使其长度为 8 的倍数。如果数据为 12 23 34 56 78 89 90 A1 B1，由于数据长度不是 8 的倍数，所以在计算过程中自动将数据改写为 12 23 34 56 78 89 90 A1 B1 80 00 00 00 00 00 00 后再进行计算。

用 DES 算法作外部认证的过程如下：



4. 命令与应答

4.1. 命令与应答结构

情形一：

命令：	CLA	INS	P1	P2	00
应答：	SW1	SW2			

情形二：

命令：	CLA	INS	P1	P2	Le
应答：	Le 字节 DATA		SW1	SW2	

情形三：

命令：	CLA	INS	P1	P2	Lc	DATA
应答：	SW1	SW2				

情形四：

命令：	CLA	INS	P1	P2	Lc	DATA	Le
应答：	Le 字节 DATA		SW1	SW2			

CLA：指令类别

INS：指令类型的指令码，见 1.SMARTCOS 简介

P1 P2：命令参数

Lc：数据域 DATA 长度，该长度不可超过 239 字节

DATA：数据域或应答数据域

Le：要求返回数据长度，Le 为 00 表示返回卡中最大数据长度，该长度不可超过 239 字节

SW1 SW2：卡执行命令的返回代码（状态字）

4.2. 状态字 SW1、SW2 的意义

任意一条命令的应答至少由一个状态字（2 个字节）组成。状态字说明了命令处理的情况，即命令是否被正确执行，如果未被正确执行，原因是什么。

SW1 SW2	意　义
90 00	正确执行
62 81	回送的数据可能错误
62 83	选择文件无效，文件或密钥校验错误
63 CX	X 表示还可再试次数
64 00	状态标志未改变
65 81	写 EEPROM 不成功
67 00	错误的长度
69 00	CLA 与线路保护要求不匹配
69 01	无效的状态

SW1 SW2	意　义
69 81	命令与文件结构不相容
69 82	不满足安全状态
69 83	密钥被锁死
69 85	使用条件不满足
69 87	无安全报文
69 88	安全报文数据项不正确
6A 80	数据域参数错误
6A 81	功能不支持或卡中无 MF 或卡片已锁定
6A 82	文件未找到
6A 83	记录未找到
6A 84	文件无足够空间
6A 86	参数 P1 P2 错误
6A 88	密钥未找到
6B 00	在达到 Le/Lc 字节之前文件结束，偏移量错误
6C xx	Le 错误
6E 00	无效的 CLA
6F 00	数据无效
93 02	MAC 错误
93 03	应用已被锁定
94 01	金额不足
94 03	密钥未找到
94 06	所需的 MAC 不可用

注意：

当 SW1 的高半字节为’9’，且低半字节不为’0’时，其含义依赖于相关应用。

当 SW1 的高半字节为’6’，且低半字节不为’0’时，其含义与应用无关。

5. SMARTCOS 命令

5.1. 外部认证 EXTERNAL AUTHENTICATE

5.1.1. 定义和范围

EXTERNAL AUTHENTICION 命令要求 IC 卡中存在用于外部认证的密钥。

在满足该密钥的使用条件且该密钥未被锁死时才能执行此命令。

将命令中的数据用指定外部认证密钥解密，然后与先前产生的随机数进行比较，若一致则表示认证通过，置安全状态寄存器为该密钥规定的后续状态值，错误计数器恢复成初始值；若比较不一致则认证失败，可再试错误数减一，且不改变安全状态寄存器的值。

5.1.2. 命令报文

EXTERNAL AUTHENTICATE 命令报文编码如下：

代码	值
CLA	00
INS	82
P1	00
P2	外部认证密钥标识号
Lc	08
Data	8 字节加密后的随机数
Le	不存在

5.1.3. 命令报文数据域

命令报文数据域中包括 8 字节加密后的随机数。

5.1.4. 响应报文数据域

响应报文数据域不存在。

5.1.5. 响应报文状态码

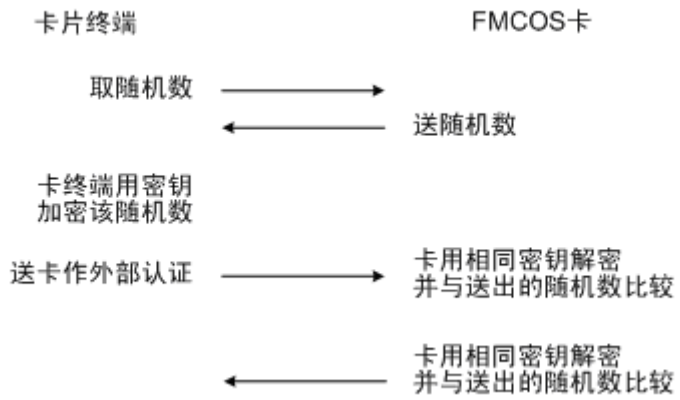
此命令执行成功的状态码是’9000’。

IC 卡可能回送的错误状态码如下所示：

SW1 SW2	意　义
62 83	密钥校验错误
65 81	写 EEPROM 不成功
67 00	错误的长度
69 81	不是外部认证密钥
69 82	密钥使用条件不满足
69 83	认证方法（外部认证密钥）锁死
6A 82	KEY 文件未找到

SW1 SW2	意　义
6A 88	密钥未找到
63 CX	认证失败，可再试 X 次
93 02	安全信息不正确

[例]：密钥标识号为 01 的外部认证密钥，使用权 F0，更改权 EF，错误计数器 33，后续状态 11，8 字节的密钥为 01 02 03 04 05 06 07 08，则外部认证的过程如下：



- 卡终端从 SMARTCOS 卡取随机数，则命令为：
  00 84 00 00 04
  由卡片返回的响应数据为：
  BB 83 BF F3 9000
- 说明：BB 83 BF F3 为卡片返回的 4 字节的随机数。
  卡终端用与外部认证密钥相同的密钥 01 02 03 04 05 06 07 08 对 8 字节随机数（4 字节的随机数+4 字节 00） 进行加密，加密后的结果为：
  74 B0 04 7D D6 81 D9 6C
- 卡终端将加密后的随机数送到卡中作外部认证，如果成功则置安全状态寄存器值为该外部认证密钥的后续状态 11，命令为：
  00 82 00 01 08 74 B0 04 7D D6 81 D9 6C

5.2. 取随机数 GET CHALLENGE

5.2.1. 定义和范围

GET CHALLENGE 命令请求一个用于线路保护过程的随机数。

除非掉电、选择了其它应用或又发出一个 GET CHALLENGE 命令，该随机数仅在下一条指令时有效。

由卡产生 Le 字节随机数送给终端，若下条指令为外部认证，则外部认证数据用指定的外部认证密钥解密后与该随机数进行比较。

5.2.2. 命令报文

GET CHALLENGE 命令报文编码如下：

代码	值
CLA	00
INS	84
P1	00
P2	00
Lc	不存在
Data	不存在
Le	04/08

5.2.3. 命令报文数据域

命令报文数据域不存在

5.2.4. 响应报文数据域

响应报文数据域包括随机数，长度为 Le 个字节。

5.2.5. 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	含　义
6A 81	不支持此功能(无 MF 或卡片已锁定)
67 00	长度错误

5.3. 内部认证 INTERNAL AUTHENTICATE

5.3.1. 定义和范围

在满足该密钥的使用条件时才能执行此命令。

INTERNAL AUTHENTICATION 命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据认证的功能。

5.3.2. 命令报文

INTERNAL AUTHENTICATE 命令报文编码如下：

代码	值
CLA	00
INS	88
P1	00：加密计算
	01：解密计算
	02：MAC 计算
P2	DES 密钥标识号
Lc	认证数据的长度
Data	认证数据
Le	不存在

DES 密钥标识：SMARTCOS 用密钥本身规定的算法进行相应的 DES 运算。例如密钥类型为 30（或 31 或 32）则 SMARTCOS 用密钥文件中的密钥对数据进行加密（或解密或生成 MAC）。

5.3.3. 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

5.3.4. 响应报文数据域

响应报文数据域的内容是相关认证数据，即 DES 或 MAC 运算的结果。

5.3.5. 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
62 83	密钥校验错误
67 00	错误的长度
69 81	密钥与运算方法不匹配
69 82	不满足安全状态
69 85	不满足使用条件
6A 82	KEY 文件不存在
6A 88	密钥未找到

[说明]：如果 KEY 文件中没有相应类型的密钥，卡片将返回’6A 88’即密钥未找到。

[例 1]：密钥标识号为 01 的 DES 加密密钥，使用权 F0，更改权 EF，算法标识 98，密钥版本号 05，8 字节的密钥为 11 22 33 44 55 66 77 88，则内部认证即 DES 加密过程如下：

对数据 01 02 03 04 05 06 07 08 进行 DES 加密，则命令为：

00 88 00 01 08 01 02 03 04 05 06 07 08

由卡片返回的响应数据为：

17 8F 59 F8 57 8E 0D 3F 9000

说明：17 8F 59 F8 57 8E 0D 3F 为内部认证即 DES 加密的结果。

[例 2]：密钥标识号为 02 的 DES 解密密钥，使用权 F0，更改权 EF，算法标识 98，密钥版本号 05，8 字节的密钥为 11 22 33 44 55 66 77 88，则内部认证即 DES 解密过程如下：

对数据 17 8F 59 F8 57 8E 0D 3F 进行 DES 解密，则命令为：

00 88 01 02 08 17 8F 59 F8 57 8E 0D 3F

由卡片返回的响应数据为：

01 02 03 04 05 06 07 08 9000

说明：01 02 03 04 05 06 07 08 为内部认证即 DES 解密的结果。由此可以看出，相同密钥的 DES 加密过程和 DES 解密过程互为逆过程。

[例 3]：密钥标识号为 03 的 DES MAC 密钥，使用权 F0，更改权 EF，算法标识 98，密钥版本号 05，8 字节的密钥为 11 22 33 44 55 66 77 88，则内部认证即生成 MAC 过程如下：

对数据 01 02 03 04 05 06 07 08 进行加密生成 MAC，则命令为：

00 88 02 03 08 01 02 03 04 05 06 07 08

由卡片返回的响应数据为：

A8 2A 8C EB 9000

说明：A8 2A 8C EB 为通过内部认证生成的 4 字节的 MAC 码。

[注]：内部认证实际上就是 DES 运算，无论内部认证成功与否均不能改变安全状态寄存器的值。

5.4. 选择文件 SELECT

5.4.1. 定义和范围

SELECT 命令通过文件名、文件标识符或选择下一个应用来选择 IC 卡中 MF、DDF 或 ADF。

从 IC 卡的响应报文应由回送文件控制信息 FCI 组成。

5.4.2. 命令报文

SELECT 命令报文编码如下：

代码	值
CLA	00
INS	A4
P1	00：按文件标识符选择，选择当前目录下基本文件或子目录文件。
	04：用目录名称选择，选择与当前目录平级的目录、当前目录的下级子目录。
P2	00
Lc	XX
Data	空或文件标识符或 DF 名称
Le	00

P1=00：按文件标识符选择，选择当前目录下基本文件或子目录文件。

P1=04：用目录名称选择，选择 MF，或当前目录本身，或与当前目录平级的目录,或当前目录的下级子目录。

在任何情况下均可通过标识符 3F 00 或目录名称选择 MF。

5.4.3. 命令报文数据域

命令报文数据域可为空或包含文件标识符或 DF 名称。

5.4.4. 响应报文数据域

响应报文数据域应包括所选择的 DDF 或 ADF 的文件控制信息（FCI）。见下表：

表 7.1 定义了成功选择了 DDF 后回送的文件控制信息 FCI：

表 7.1 成功选择了 DDF 后回送的文件控制信息 FCI

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF 名	必备
A5	文件控制信息专用数据	必备
88	目录基本文件的短文件标识符	必备

表 7.2 定义了成功选择了 ADF 后回送的文件控制信息 FCI：

表 7.2 成功选择了 ADF 后回送的文件控制信息 FCI

标志	值	存在方式
6F	文件控制信息模板	必备
84	DF 名	必备
A5	文件控制信息专用数据	必备
9F0C	发卡方自定数据的文件控制信息	可选

5.4.5. 响应报文状态码

此命令执行成功的状态码为’9000’。

IC 卡可能回送的警告状态码如下所示：

SW1 SW2	含　义
62 83	选择的文件无效

IC 卡可能回送的错误状态码如下所示：

SW1 SW2	含　义
67 00	错误的长度
6A 81	不支持此功能(无 MF 或卡片已锁定)
6A 82	未找到文件
6A 86	参数 P1 P2 不正确

范例：

符合银行标准的应用目录的选择

建立 MF 时指定 MF 下指示目录结构的基本文件（DIR）的短文件标识符为 01，对主文件 MF 进行选择即对 DDF 进行选择，则命令为：

00 A4 00 00 02 3F 00

由卡片返回的响应数据为：

6F 15 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01 9000

说明：返回的信息为嵌套的 TLV 格式的变长记录。’6F’为文件控制信息模板的记录标识，’15’为文件控制信息模板的记录数据长度（不包括 Tag、Length），84 0E 31 50 41 59 2E 53 59 2E 44 44 46 30 31 A5 03 88 01 01 为 21 字节的记录数据。’84’为 DF 名称的记录标识，’0E’为 DF 名称的记录数据长度（不包括 Tag、Length），31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 为 14 字节的记录数据，即 MF 的名称 1PAY.SYS.DDF01。’A5’为文件控制信息专用模板的记录标识，’03’ 为文件控制信息专用模板的记录数据长度（不包括 Tag、Length），88 01 01 为 3 字节的记录数据。’88’为 DIR 短文件标识符的记录标识，’01’为 DIR 短文件标识符的记录数据长度（不包括 Tag、Length），’01’为 1 字节的记录数据，即目录基本文件（DIR）的短文件标识符。

- DIR 为变长记录文件，读目录基本文件（DIR）的第一条记录，则命令为：
  00 B2 01 0C 00

  由卡片返回的响应数据为：

61 11 4F 09 A0 00 00 00 03 86 98 07 01 50 04 50 42 4F 43 9000

说明：返回的信息为嵌套的 TLV 格式的变长记录。’4F’为银行应用目录文件 ADF 名称的记录标识，’09’为银行应用目录文件 ADF 名称的记录数据长度（不包括 Tag、Length），’A0 00 00 00 03 86 98 07 01’为 9 字节的记录数据，即银行应用目录文件 ADF 的名称。

- 建立银行应用目录文件 ADF 时指定 ADF 下发卡方专用数据文件的短文件标识符为

95，ADF 的名称为‘A0 00 00 00 03 86 98 07 01’，对 ADF 进行选择，则命令为：

00 A4 04 00 09 A0 00 00 00 03 86 98 07 01

由卡片返回的响应数据为：

6F 2E 84 09 A0 00 00 00 03 86 98 07 01 A5 21 9F 0C 1E 11 11 22 22 33 33 00 06 03 01 00 06 19 98 08 17 00 00 00 30 19 98 08 15 19 98 12 15 55 66 90 00

说明：返回的信息为嵌套的 TLV 格式的变长记录。’6F’为文件控制信息模板的记录标识，’2E’为文件控制信息模板的记录数据长度（不包括 Tag、Length），其后为 2E（HEX）字节的记录数据。’84’为 DF 名称的记录标识，’09’为 DF 名称的记录数据长度（不包括 Tag、Length），A0 00 00 00 03 86 98 07 01 为 9 字节的记录数据，即 ADF 的名称。’A5’为文件控制信息专用数据的记录标识，’21’ 为文件控制信息专用数据的记录数据长度（不包括 Tag、Length），其后为 21（HEX）字节的记录数据．’9F0C’为发卡方定义的基本数据文件的文件控制信息的记录标识，’1E’ 为发卡方定义的文件控制信息专用数据的记录数据长度（不包括 Tag、Length），即标识符为 0015 的二进制文件的内容（见附录中的应用举例）。’55 66’为 2 字节的发卡方自定义 FCI 数据。

- 在任何目录下选择主文件 MF

CLA	INS	P1	P2	Lc	DATA
00	A4	00	00	02	3F 00

MF 将成为当前目录，且当前目录安全状态寄存器的值自动等于 MF 的安全状态寄存器的值。当然，也可用 SELECT 命令对文件’1PAY.SYS.DDF01’直接选择。

- 按文件标识符选择当前目录下的文件或下级子目录

CLA	INS	P1	P2	Lc	DATA
00	A4	00	00	02	文件标识符

若选择的文件为子目录时，该目录成为当前目录，且当前目录安全状态寄存器的值变为 0。

若选择的文件为 EF 时，该文件成为当前文件。

- 通过目录名称选择 DF

CLA	INS	P1	P2	Lc	DATA
00	A4	04	00	XX	DF 文件名

Lc 定义了 DF 文件名的长度。

当前目录安全状态寄存器的值变为 0。

5.5. 读二进制文件 READ BINARY

5.5.1. 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）。

5.5.2. 命令报文

READ BINARY 命令报文编码如下：

代码	值
CLA	00
INS	B0
P1	XX
P2	XX
Lc	不存在；（CLA=04 时除外）
Data	不存在；（CLA=04 时，应包括 MAC）
Le	XX

若 P1 的高三位为 100，则低 5 位为短的文件标识符，P2 为读的偏移量。

若 P1 的最高位不为 1，则 P1 P2 为欲读文件的偏移量(P1 为偏移量高字节，P2 为低字节)，所读的文件为当前文件。

5.5.3. 命令报文数据域

一般情况下，命令报文数据域不存在。当使用安全报文时，命令报文数据域中应包含 MAC。

5.5.4. 响应报文数据域

该文件被置成线路保护时，若 CLA 置为 00 时响应报文不含 MAC，CLA 置为 04 时响应报文包含 MAC。

5.5.5. 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
62 81	部分回送的数据可能有错
67 00	错误的长度
69 81	不是二进制文件
69 82	读的条件不满足
6A 81	不支持此功能（无 MF 或 MF 已锁定）
6A 82	未找到文件
6B 00	参数错误（偏移地址超出了 EF）

[注]：若文件校验不正确，卡将送出所读的数据，并给出警告状态 SW1 SW2=6281。若下次重写该文件，卡将重新计算校验。读一个未曾写过数据的二进制文件也将返回’6281’。

[例 1]：文件标识符为 0005 的二进制文件，文件主体空间的大小为 8 个字节，建立时不采用线路保护。

读出自偏移量 01 开始到文件结束的所有数据，不进行线路保护，则命令为：

00 B0 85 01 00

由卡片返回的响应数据为：

11 22 33 44 55 66 77 9000

[例 2]：文件标识符为 0001 的二进制文件，文件主体空间的大小为 8 个字节，建立时采用线路保护。

读出自偏移量 00 开始到文件结束的所有数据，使用线路保护密钥进行线路保护，则命令为：

04 B0 00 00 04 82 26 99 9B

说明：由于 P1 的最高位不为 1，则欲写文件的偏移量为 00 00，所读的文件为当前文件，82 26 99 9B 为使用线路保护密钥生成的 4 字节 MAC 码。

由卡片返回的响应数据为：

01 02 03 04 05 FF FF FF 38 F4 EA 15 9000

[例 3]：文件标识符为 0005 的二进制文件，文件主体空间的大小为 8 个字节，建立时采用线路加密保护。

读出自偏移量 02 开始 10 字节数据，使用线路保护密钥进行线路加密保护，1C BD 1F 23 F5 4F 8C 9A 为 10 80 00 00 00 00 00 00 的加密数据,则命令为：

04 B0 85 02 0C 1C BD 1F 23 F5 4F 8C 9A DC 8B 2D 0F

由卡片返回的响应数据为：

6E 68 85 9B 17 04 7E D9 8A 75 BA 0B 9000

说明：6E 68 85 9B 17 04 7E D9 为使用线路保护密钥对数据 66 77 88 FF FF FF 加密后的结果，8A 75 BA 0B 为使用线路保护密钥生成的 4 字节 MAC 码。

[注]：此处使用到的线路保护密钥为文件线路保护密钥（36 密钥）。

5.6. 读记录文件 READ RECORD

5.6.1. 定义和范围

READ RECORD 命令用于读取定长记录文件、循环文件、钱包文件和变长记录文件的内容。IC 卡的响应由回送记录组成。

5.6.2. 命令报文

READ RECORD 命令报文编码如下：

代码	值
CLA	00/04
INS	B2
P1	见表 7.3
P2	见表 7.4
Lc	不存在（CLA=04 时除外）
Data	不存在（CLA=04 时除外）
Le	00：表示读取整条记录 XX：表示要读取的字节数

表 7.3 READ RECORD 命令中 P1 的含义

类型	P1 的含义
定长记录文件	记录号，若该文件有 N 条记录，则记录号可以是 1~N。
变长记录文件	记录号，若该文件有 N 条记录，则记录号可以是 1~N。（参数 P2 含义如下） 记录标识，如按记录标识来读，则 P2 的低 3 位必须为’000’。
循环文件	记录号，最新写入的记录号为 01，上 1 条记录的记录号为 02, 依次类推...

表 7.4 READ RECORD 命令中 P2 的含义

b8	b7	b6	b5	b4	b3	b2	b1	P2 的含义
X	X	X	X	X	1	0	0	b4-b8 为短文件标识符
0	0	0	0	0	1	0	0	当前文件

5.6.3. 命令报文数据域

当无安全报文使用时，命令报文数据域不存在。使用安全报文时，命令报文的数据域中应包含 MAC。

5.6.4. 响应报文数据域

所有执行成功的 READ RECORD 命令的响应报文数据域由读取的记录组成。

若该记录文件为线路保护文件且 CLA 为 04 则回送的数据还包括 4 字节的 MAC。

5.6.5. 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
62 81	回送的数据可能有错
67 00	错误的长度
69 81	命令与文件结构不相容
69 82	读的条件不满足
6A 81	不支持此功能（无 MF 或 MF 已锁定）
6A 82	未找到文件
6A 83	未找到记录
6C XX	记录实际长度为 XX 字节

[例 1]：文件标识符为 0001 的定长记录文件，它有 3 条记录，每条记录长度为 12 个字节。

读出定长记录文件中记录号为 02 的记录，不进行线路保护，则命令为：

00 B2 02 0C 00，由卡片返回的响应数据为：

01 02 03 04 05 06 07 08 09 0A 0B 0C 9000

说明：01 02 03 04 05 06 07 08 09 0A 0B 0C 为读出的记录号为 02 的记录的内容。

[例 2]：文件标识符为 0003 的循环文件，它有 3 条记录，每条记录长度为 12 个字节。

读出循环文件中记录号为 01 的记录，即最新写入的记录，不进行线路保护，则命令为：

00 B2 01 1C 00

由卡片返回的响应数据为：

11 22 33 44 55 66 77 88 99 AA BB CC 9000

说明：11 22 33 44 55 66 77 88 99 AA BB CC 为读出的记录号为 01 的记录的内容。

[例 3]：文件标识符为 0007 的变长记录文件。

- 按记录标识来读，读出变长记录文件中记录标识为 AA 的记录，不进行线路保护，则命令为：

  00 B2 AA 38 00

  说明：由于按记录标识来读，则 P2 的低 3 位必须为’000’。

  由卡片返回的响应数据为：

AA 01 11 9000

说明：读出的是 TLV 格式的记录，AA 为记录标识，01 表示记录数据的长度，11 为 1 个字节的记录数据。

- 按记录号来读，读出变长记录文件中的第 1 条记录，不进行线路保护，则命令为：

  00 B2 01 3C 00

  说明：由于按记录号来读，则 P2 的低 3 位必须为’100’。

  由卡片返回的响应数据为：

AA 01 11 9000

说明：读出的是 TLV 格式的记录，AA 为记录标识，01 表示记录数据的长度，11 为 1 个字节的记录数据。

[注]：READ RECORD 命令使用文件线路保护密钥进行线路保护。

5.7. 写二进制文件 UPDATE BINARY

5.7.1. 定义和范围

UPDATE BINARY 命令用于写二进制文件、FAC 秘密钥文件、FAC 公开钥文件。

5.7.2. 命令报文

UPDATE BINARY 命令报文编码如下：

代码	值
CLA	00/04
INS	D6/D0
P1	XX
P2	XX
Lc	XX
Data	写入文件的数据
Le	不存在

若 P1 的高三位为 100，则低 5 位为短的二进制文件标识符，P2 为欲写文件的偏移量。

若 P1 的最高位不为 1，则 P1 P2 为欲写文件的偏移量，所写的文件为当前文件。

Lc 表示要写入的字节数。

- 若为线路保护，Lc 为写入数据的长度+4 字节 MAC。
- 若为加密线路保护，Lc 为加密后数据的长度+4 字节 MAC。

5.7.3. 命令报文数据域

报文数据包括要写入的新数据。

若为线路保护文件数据域应包含 4 字节 MAC 码

若为线路加密保护文件数据域应包含加密后的数据及 4 字节 MAC 码

5.7.4. 响应报文数据域

响应报文数据域不存在。

5.7.5. 响应报文状态码

此命令执行成功的状态码是’9000’。

IC 可能回送的错误如下所示：

SW1 SW2	意　义
65 81	写 EEPROM 失败
67 00	长度错误（Lc 域为空）
69 81	不是二进制或 FAC 密钥文件不可写
69 82	写的条件不满足
69 87	无安全报文
6A 81	不支持此功能（无 MF 或 MF 已锁定）

SW1 SW2	意　义
6A 82	未找到文件
6B 00	参数错误（偏移地址超出了 EF）

[例 1]：文件标识符为 0001 的二进制文件，文件主体空间的大小为 8 个字节，建立时不采用线路保护。

- 选择二进制文件，则命令为：
  00 A4 00 00 02 00 01
- 写二进制文件，不进行线路保护，则命令为：
  00 D6 00 00 02 01 02

说明：由于 P1 的最高位不为 1，则欲写文件的偏移量为 00 00，所写的文件为当前文件。

[例 2]：文件标识符为 0005 的二进制文件，文件主体空间的大小为 8 个字节，建立时采用线路保护。

写二进制文件，必须使用线路保护密钥进行线路保护，则命令为：
04 D6 85 01 06 11 22 16 0A C8 C5

说明：由于 P1 的最 3 位为 100，则低 5 位表示短文件标识符 05，欲写文件的偏移量 P2 为 01，16 0A C8 C5 为使用线路保护密钥生成的 4 字节 MAC 码。

[例 3]：文件标识符为 0005 的二进制文件，文件主体空间的大小为 8 个字节，建立时采用线路加密保护。

写二进制文件，必须使用线路保护密钥进行线路加密保护，则命令为：
04 D6 85 00 0C 19 47 93 07 DF 79 1D 7F 24 1E D0 03

说明：19 47 93 07 DF 79 1D 7F 为使用线路保护密钥对数据 01 02 03 04 05 06 07 加密后的结果，24 1E D0 03 为使用线路保护密钥生成的 4 字节 MAC 码。

[注]：此处使用到的线路保护密钥为文件线路保护密钥（36 密钥）。

5.8. 写记录文件 UPDATE RECORD

5.8.1. 定义和范围

UPDATE RECORD 命令用于更新定长、变长或循环记录文件。

5.8.2. 命令报文

UPDATE RECORD 命令报文编码如下：

代码	值
CLA	00/04
INS	DC
P1	P1＝‘00’指明当前记录 P≠‘00’是所规定记录的号
P2	见表 7.5
Lc	XX
Data	写入的数据
Le	不存在

[注]：P1 为记录号，若该文件有 N 条记录，则记录号可以是 1-N。

Lc 表示要写入的字节数，若为线路保护，Lc 为写入数据的长度+4 字节 MAC；若为加密线路保护，Lc 为加密后数据的长度+4 字节 MAC。

表 7.5 UPDATE RECORD 命令中 P2 的含义

b8	b7	b6	b5	b4	b3	b2	b1	含　义
X	X	X	X	X	-	-	-	b4-b8 为短文件标识符
0	0	0	0	0	-	-	-	当前文件
1	1	1	1	1	-	-	-	保留
-	-	-	-	-	1	0	0	使用 P1 中的记录号
-	-	-	-	-	0	0	0	P1 指定标示的第一个记录
-	-	-	-	-	0	0	1	P1 指定标示的最后一个记录
-	-	-	-	-	0	1	0	P1 指定标示的下一个记录
-	-	-	-	-	0	1	1	P1 指定标示的上一个记录

[注]：循环记录文件只能用 P1=’00’，P2=’03’来添加。

5.8.3. 命令报文数据域

命令报文数据域由写入的记录数据组成。如果更新的文件为变长记录文件，则数据域需要按照 TLV 格式填写

若为线路保护则由写入的记录数据附上 4 字节 MAC 组成。

若为线路加密保护则由被加过密的记录数据附上 4 字节 MAC 码组成。

5.8.4. 响应报文数据域

响应报文数据域不存在。

5.8.5. 响应报文状态码

此命令执行成功的状态码是’9000’。

IC 可能回送的错误如下所示：

SW1 SW2	意　义
62 83	选择文件无效
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是定长或变长记录文件
69 82	写的条件不满足
6A 81	不支持此功能（无 MF 或 MF 已锁定）
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件无足够空间

[例 1]：文件标识符为 0002 的定长记录文件，它有 3 条记录，每条记录长度为 12 个字节，建立时不采用线路保护。

写定长记录文件，不进行线路保护，则命令为：

00 DC 01 14 0C 01 02 03 04 05 06 07 08 09 0A 0B 0C

说明：01 02 03 04 05 06 07 08 09 0A 0B 0C 为写入的数据。

[例 2]：文件标识符为 0001 的定长记录文件，它有 3 条记录，每条记录长度为 12 个字节，且建立时采用了线路保护。

写定长记录文件，必须使用线路保护密钥进行线路保护，则命令为：

04 DC 01 0C 10 01 02 03 04 05 06 07 08 09 0A 0B 0C 15 BD 23 3C

说明：01 02 03 04 05 06 07 08 0A 0B 0C 为写入的数据，15 BD 23 3C 为使用线路保护密钥生成的 4 字节 MAC。

[例 3]：文件标识符为 0001 的定长记录文件，它有 3 条记录，每条记录长度为 12 个字节，且建立时采用了加密线路保护。

写定长记录文件，必须使用线路保护密钥进行线路加密保护，则命令为：04 DC 01 0C 14 A5 DF E4 94 0B 63 DC 35 47 1E D8 A8 CD 09 88 43 C9 52 13 A6

说明：A5 DF E4 94 0B 63 DC 35 47 1E D8 A8 CD 09 88 43 为使用线路保护密钥对数据 01 02 03 04 05 06 07 08 09 0A 0B 0C 加密后的结果，C9 52 13 A6 为使用线路保护密钥生成的 4 字节 MAC。

[例 4]：文件标识符为 0001 的变长记录文件，建立时不采用线路保护。

在变长记录文件中建立 1 条记录标识为 AA 的新记录，不进行线路保护，则命令为：

00 DC 00 0A 04 AA 02 11 22

修改记录标识为 AA 的记录，同时将记录标识改为 CC，不进行线路保护，则命令为：

00 DC AA 08 04 CC 02 33 44

[例 5]：文件标识符为 0003 的循环文件，它有 2 条记录，每条记录长度为 12 个字节，建立时不采用线路保护。
往循环文件中追加 1 条记录，不进行线路保护，则命令为：
00 DC 01 1A 0C 11 22 33 44 55 66 77 88 99 AA BB CC

[注]：UPDATE RECORD 命令使用文件线路保护密钥进行线路保护

5.9. 添加记录文件 APPEND RECORD

5.9.1. 定义和范围

APPEND RECORD 命令用于在定长、变长或循环记录文件结尾添加记录。

命令在成功执行后，设置记录指针到所更新记录。

5.9.2. 命令报文

APPEND RECORD 命令报文编码如下：

代码	值
CLA	00/04
INS	E2
P1	00
P2	见表 7.6
Lc	XX
Data	写入的数据
Le	不存在

表 7.6 APPEND RECORD 命令中 P2 的含义

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X	X	X	X	X	1	0	0	b4-b8 为短文件标识符
0	0	0	0	0	1	0	0	当前文件

5.9.3. 命令报文数据域

命令报文数据域由写入的记录数据组成。如果更新的文件为变长记录文件，则数据域需要按照 TLV 格式填写

若为线路保护则由写入的记录数据附上 4 字节 MAC 组成。

若为线路加密保护则由被加过密的记录数据附上 4 字节 MAC 码组成。

5.9.4. 响应报文数据域

响应报文数据域不存在。

5.9.5. 响应报文状态码

此命令执行成功的状态码是’9000’。

IC 可能回送的错误如下所示：

SW1 SW2	意 义
62 83	选择文件无效
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是定长或变长记录文件
69 82	写的条件不满足

6A 81	不支持此功能（无 MF 或 MF 已锁定）
6A 82	未找到文件
6A 84	文件无足够空间

5.10.验证口令 VERIFY PIN

5.10.1. 定义和范围

VERIFY PIN 命令用于校验命令数据域的口令密钥的正确性。

5.10.2. 命令报文

VERIFY PIN 命令的编码如下：

代码	值
CLA	00
INS	20
P1	00
P2	口令密钥标识符
Lc	02-06
Data	外部输入的口令密钥
Le	不存在

在满足该口令密钥文件使用权限时才可执行该命令。

若口令验证成功，则安全状态寄存器的值被置成该密钥的后续状态，同时口令错误计数器被置成初始值。

若验证错误，则口令可试次数减一，若口令已被锁死，则不能再执行该命令，可以用 PBOC_IC 命令对其进行解锁，重装等操作，并可能成功地返回 9000。

[说明]：若 PIN 值的后面字节为连续的 FF，校验时可以忽略该段字节，但若 PIN 值为全 FF，则最少应输入一个 FF 值。

5.10.3. 命令报文数据域

命令报文数据域由持卡者输入的口令密钥组成。若为线路保护则由口令密钥附上 4 字节 MAC 码组成。若为线路加密保护则由被加过密的口令密钥附上 4 字节 MAC 码组成。

5.10.4. 响应报文数据域

响应报文数据域不存在。

5.10.5. 响应报文状态码

此命令执行成功的状态码是’9000’。

当前的应用选择中，命令数据域中外部输入的口令密钥与卡中存放的口令密钥校验失败时，IC 卡将回送 SW2=CX，X 表示个人密码允许重试的次数：当卡回送 C0 时，表示不能重试口令密钥。此时再使用 VERIFY PIN 命令时，将回送失败状态码 SW1 SW2= ‘6983’。

IC 卡可能回送的错误状态码如下所示：

SW1 SW2	意　义
62 83	口令密钥校验错误
65 81	写 EEPROM 错误
67 00	错误的长度

69 81	不是口令密钥
69 82	密钥使用条件不满足
69 83	认证方法（口令密钥）锁死
6A 82	KEY 文件未找到
63 CX	校验失败，X 表示允许重试的次数
93 02	密钥线路保护错误
94 03	密钥未找到

[例 1]：如密钥标识号为 00 的 5 位字节口令密钥，值为 12345，则 Verify PIN 的命令为：

00 20 00 00 03 12 34 5F31 32 33 34 35 36

5.11.擦除目录文件 ERASE DF

5.11.1. 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）。

5.11.2. 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

5.11.3. 命令报文数据域

命令报文数据域不存在。

5.11.4. 响应报文数据域

响应报文数据域不存在。

5.11.5. 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。

5.12.增加或修改密钥 WRITE KEY

5.12.1. 定义和范围

WRITE KEY 命令用于在密钥文件中增加或修改密钥

5.12.2. 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

5.12.3. 命令报文数据域

- CASE1：增加 DES 加密、DES 解密、DESMAC、内部密钥、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	30/31/32/34/35/3C/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
34：	内部密钥
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
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）。
- 内部密钥是用于产生内部临时密钥的密钥。
- 添加新密钥时只支持明文和明文 MAC 两种方式，不支持密文加密方式
- 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。

5.12.4. 响应报文数据域

响应报文数据域不存在。

5.12.5. 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）

5.13.建立文件 CREATE FILE

5.13.1. 定义和范围

CREATE FILE 命令用于建立文件系统，包括 MF、DF 和 EF。

5.13.2. 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

5.13.3. 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	
-	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。

5.13.4. 响应报文数据域

响应报文数据域不存在。

5.13.5. 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

6. 中国金融 IC 卡专用命令

6.1. 卡片锁定 CARD BLOCK

6.1.1. 定义和范围

CARD BLOCK 命令使卡中所有应用永久失效。

当 CARD BLOCK 命令成功地完成后，所有后续的命令都将回送状态码“不支持此功能”（SW1 SW2='6A81'），且不执行任何其它操作。

6.1.2. 命令报文

CARD BLOCK 命令报文编码如下：

代码	值
CLA	84
INS	16
P1	00
P2	00
Lc	04
Data	MAC（由线路保护密钥生成）
Le	不存在

6.1.3. 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。

6.1.4. 响应报文数据域

响应报文数据域不存在。

6.1.5. 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
64 00	状态标志未改变
65 81	写 EEPROM 不成功
69 87	安全报文数据项丢失
69 88	安全报文数据项不正确

6.2. 应用解锁 APPLICATION UNBLOCK

6.2.1. 定义和范围

APPLICATION UNBLOCK 命令用于恢复当前的应用。

当 APPLICATION UNBLOCK 命令成功地完成后，用 APPLICATION BLOCK 命令产生的对应用命令响应的限制将被取消。

如果对某应用连续三次解锁失败，则 IC 卡将永久锁定此应用。

6.2.2. 命令报文

APPLICATION UNBLOCK 命令报文编码如下：

代码	值
CLA	84
INS	18
P1	00
P2	00
Lc	04
Data	MAC（由文件线路保护密钥生成）
Le	不存在

6.2.3. 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。

6.2.4. 响应报文数据域

响应报文数据域不存在。

6.2.5. 响应报文状态码

无论应用是否已经失效，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	不满足安全状态
69 83	认证方式锁定
69 88	安全报文数据项不正确
93 03	应用永久锁定

[注]：此命令的执行并不改变电子存折或电子钱包联机交易序号的值。

6.3. 应用锁定 APPLICATION BLOCK

6.3.1. 定义和范围

APPLICATION BLOCK 命令使当前选择的应用失效。

当 APPLICATION BLOCK 命令成功地完成后，用 SELECT 命令选择已失效的应用，将回送状态码“选择文件无效”（SW1 SW2=‘6A81’）。

对其它命令的影响跟据不同应用而定。

6.3.2. 命令报文

APPLICATION BLOCK 命令报文编码如下：

代码	值
CLA	84
INS	1E
P1	00
P2	00：临时锁定
	01：永久锁定
Lc	04
Data	MAC（由文件线路保护密钥生成）
Le	不存在

P2=00：此命令执行成功后可锁定应用，但该应用可以用 APPLICATION UNBLOCK 命令解锁，可由 SELECT 命令选择进入该目录，但对文件操作时返回 6A81。

P2=01：此命令执行成功后将永久锁定应用，IC 卡将设置一个内部标志以表明不允许执行 APPLICATION UNBLOCK 命令，可由 SELECT 命令选择进入该目录，但对文件操作时返回 6A81。

6.3.3. 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。

6.3.4. 响应报文数据域

响应报文数据域不存在。

6.3.5. 响应报文状态码

无论应用是否已经失效，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
64 00	状态标志未改变
65 81	写 EEPROM 不成功
69 82	不满足安全状态
6A 86	参数 P1 P2 不正确
69 88	安全报文数据项不正确

[例 1]：文件标识符为 3F01 的目录文件，目录名称为 A00000000386980701，进行应用暂时性锁定及解锁。

- 选择该目录文件，则命令为：
  00 A4 04 00 09 A0 00 00 00 03 86 98 07 01
  返回的数据为：
  6F 2E 84 09 A0 00 00 00 03 86 98 07 01 A5 21 9F 0C 1E 11 11 22 22 33 33 00 06 03 01 00 06 19 98 08 17 00 00 00 30 19 98 08 15 19 99 12 31 55 66 9000

- 暂时性锁定该应用，则命令为：
  84 1E 00 00 04 3D E8 17 09
  返回的状态为：
  9000

- 卡片复位后再次选择该目录文件，则命令为：
  00 A4 00 00 02 3F 01
  返回的状态为：
  6A81

说明：状态码 6A81 表明命令不支持。

- 对该应用进行解锁，则命令为：
  84 18 00 00 04 A3 2F 38 1D
  返回的状态为：
  9000

[例 2]：文件标识符为 3F01 的目录文件，目录名称为 A00000000386980701，进行应用永久性锁定。

首先也必须对目录进行选择，然后用 APPLICATION BLOCK 命令永久性锁定该目录，则命令为：

84 1E 00 01 04 84 7D BB AE

返回的数据为：

9000

说明：卡片永久性锁定后将不能被解锁，复位后再次选择该目录文件将返回 6A81。

[注]：此命令的执行并不改变电子存折或电子钱包联机交易序号的值。

6.4. 口令密钥解锁 PIN UNBLOCK

6.4.1. 定义和范围

PIN UNBLOCK 命令发卡方提供了解锁口令密钥的功能。

当 PIN UNBLOCK 命令成功完成后，卡片将重置个人密码错误计数器的值。

命令中口令密钥的传递采用加密方式。

6.4.2. 命令报文

PIN UNBLOCK 命令报文编码如下：

代码	值	
CLA	84	
INS	24	
P1	口令密钥标识符	
P2	00	
Lc	0C 或 14	
Data	加密的口令密钥	08 或 10 字节
	MAC	4 字节
Le	不存在	

6.4.3. 命令报文数据域

命令报文数据域由口令密钥数据元（如果存在）和其后的报文鉴别代码（MAC）数据元组成。

[注]：此处的 Data 为密钥线路保护密钥对原口令值进行加密和计算 MAC.

6.4.4. 响应报文数据域

响应报文数据域不存在。

6.4.5. 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 失败
69 82	不满足安全状态
6A 82	KEY 文件未找到
6A 86	参数 P1 P2 不正确
69 88	安全报文数据项不正确
93 03	应用永久锁定
94 03	密钥未找到

[例 1]：密钥标识符为 00 的口令密钥被锁死，对该口令密钥进行解锁，必须使用密钥线路

保护密钥进行线路保护，则命令为：

84 24 00 01 0C F3 97 B1 FD 0C D1 74 7A 8E 0C B9 3B

由卡片返回的响应数据为：

9000

说明：在解锁口令密钥命令报文中并不能指定口令密钥的密钥标识符，系统将自动对密钥文件中标识为 00 的口令密钥进行解锁。

6.5. 重装/修改口令密钥 RELOAD/CHANGE PIN

6.5.1. 定义和范围

RELOAD PIN 命令用于发卡方重新给持卡人产生一个新的 PIN（可以与原 PIN 不同）。

RELOAD PIN 只能在拥有或能访问到重装口令密钥的密钥的发卡方终端（例如发卡方银行终端）上执行。

在成功执行 RELOAD PIN 命令后，IC 卡必须完成以下操作：

- 密钥错误尝试计数器复位。
- IC 卡的原密钥必须设置为新的值。

命令中的密钥数据以明文传送。

6.5.2. 命令报文

RELOAD PIN 命令报文编码如下：

代码	值	
CLA	80	
INS	5E	
P1	00	
P2	口令密钥标识符	
Lc	06-0A	
Data	重装的 PIN	2~6 字节
	报文鉴别代码 MAC	4 字节
Le	不存在	

6.5.3. 命令报文数据域

命令报文数据域由重装的 PIN 和报文鉴别码（MAC）组成。

[注]：此处的 MAC 是由重装口令密钥前后 8 字节异或后对 2-6 字节新口令值计算的 MAC，并非是使用线路保护密钥对整个命令报文作线路保护的结果。

6.5.4. 响应报文数据域

响应报文数据域不存在。

6.5.5. 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
67 00	长度错误
69 82	不满足安全状态
69 83	认证方式锁定
69 85	使用条件不满足

93 02	MAC 错误
93 03	应用永久锁定
94 03	密钥未找到

[例]：密钥文件中有一个密钥标识符为 00，长度为 6 字节的口令密钥，发卡方重新给持卡人产生一个新的口令密钥，不进行线路保护，则命令为：

80 5E 00 00 0A 22 33 44 55 66 77 1C E6 AA 60

说明：22 33 44 55 66 77 为重装的 6 字节新口令，1C E6 AA 60 为 4 字节的 MAC 码，但应特别注意的是此处的 MAC 并非是使用线路保护密钥作线路保护生成的，而是由重装口令密钥前后 8 字节相异或后对 6 字节新口令值计算的 MAC。

由卡片返回的响应数据为：9000

说明：在重装口令密钥命令报文中并不能指定口令密钥的密钥标识符，系统将自动对密钥文件中标识为 00 的口令密钥进行重装。

6.6. 修改口令密钥命令 CHANGE PIN

6.6.1. 修改口令密钥命令定义和范围

CHANGE PIN 允许持卡人将当前长度为 2~6 字节的口令密钥修改为新的密钥，且新密钥的长度可以与原口令密钥的长度不同。

当 CHANGE PIN 命令成功完成后，卡片要进行以下操作：

- 密码尝试计数器复位至密码尝试次数的上限。
- 将原个人密码置为新的口令密钥。

此命令中的口令密钥值以明文传送。

6.6.2. 命令报文

CHANGE PIN 命令报文编码如下：

代码	值
CLA	80
INS	5E
P1	01
P2	口令密钥标识符
Lc	05~0D
Data	旧的口令密钥 ‖ ‘FF’ ‖ 新的口令密钥
Le	不用

6.6.3. 命令报文数据域

命令报文数据域由旧的口令密钥、填充的 1 字节的’FF’及新的口令密钥三部分组成 。

6.6.4. 响应报文数据域

响应报文数据域不存在。

6.6.5. 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
63 CX	X 表示还可再试次数
65 81	写 EEPROM 不成功
69 82	不满足安全状态
69 83	认证方法锁定
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到
94 03	密钥未找到

[例]：密钥文件中有一个密钥标识符为 00，长度为 2 字节的口令密钥，修改该口令密钥进

行解锁，不进行线路保护，则命令为：

84 5E 01 00 05 00 00 FF 31 32

说明：00 00 为旧的口令密钥，31 32 为新的口令密钥。

由卡片返回的响应数据为：9000

说明：在修改口令密钥命令报文中并不能指定口令密钥的密钥标识符，系统将自动对密钥文件中标识为 00 的口令密钥进行修改。

6.7. 圈存命令

6.7.1. 圈存初始化 INITIALIZE FOR LOAD

6.7.1.1. 圈存初始化命令定义和范围

INITIALIZE FOR LOAD 命令用于初始化圈存交易。

6.7.1.2. 命令报文

INITIALIZE FOR LOAD 命令报文编码如下：

代码	值	
CLA	80	
INS	50	
P1	00	
P2	01：用于电子存折	
	02：用于电子钱包	
Lc	0B	
Data	密钥标识符	1 字节
	交易金额	4 字节
	终端机编号	6 字节
Le	10	

6.7.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

交易金额：此次圈存交易待处理的金额

终端机编号：6 字节终端机编号，由终端给出

6.7.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 8.3 INITIALIZE FOR LOAD 命令执行成功的响应报文数据域

说明	长度（字节）
电子存折或电子钱包旧余额	4
电子存折或电子钱包联机交易序号	2
密钥版本号（DATA 中第一字节指定的圈存密钥）	1
算法标识（DATA 中第一字节指定的圈存密钥）	1
伪随机数（IC 卡）	4
MAC1	4

过程密钥由 DATA 中第一字节即密钥标识符指定的圈存密钥对（4 字节随机数+2 字节电子存折或电子钱包联机交易序号+8000）数据加密生成。

MAC1 由卡中过程密钥对（4 字节电子存折或电子钱包旧余额+4 字节交易金额+1 字节交易类型标识+6 字节终端机编号）数据加密生成。

交易类型标识：

值	含义
01	电子存折圈存
02	电子钱包圈存

6.7.1.5. 响应报文的状态码

圈存初始化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
67 00	长度错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 03	密钥索引不支持

[注 1]：要想进行圈存交易首先必须进行圈存初始化，IC 卡将 INITIALIZE FOR LOAD 响应报文回送给终端处理。如果 IC 卡回送的状态码不是’9000’，则交易中止。

[注 2]：在银行的应用目录下，当符合中国金融 IC 卡应用规范的专用钱包文件用作电子存折时，文件标识符固定为 0001；用作电子钱包时，文件标识符固定为 0002。

6.7.2. 圈存命令 CREDIT FOR LOAD

6.7.2.1. 圈存命令定义和范围

CREDIT FOR LOAD 命令用于圈存交易。

6.7.2.2. 命令报文

CREDIT FOR LOAD 命令报文编码如下：

代码	值	
CLA	80	
INS	52	
P1	00	
P2	00	
Lc	0B	
Data	交易日期（主机）	4 字节
	交易时间（主机）	3 字节
	MAC2	4 字节
Le	04	

6.7.2.3. 命令报文数据域

过程密钥由与圈存初始化相同的内部密钥对（4 字节随机数+2 字节电子存折或电子钱包联机交易序号+8000）数据加密生成。

MAC2 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节主机交易日期+3 字节主机交易时间）数据加密生成。

交易类型标识见圈存初始化命令。

6.7.2.4. 响应报文数据域

此命令执行成功的响应报文数据域如下表：

表 8.5 CREDIT FOR LOAD 命令响应报文数据域

说明	长度（字节）
交易验证码 TAC	4

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节电子存折或电子钱包新余额+2 字节电子存折或电子钱包联机交易序号（加 1 前）+4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节主机交易日期+3 字节主机交易时间）数据加密生成。

6.7.2.5. 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	含义
65 81	写 EEPROM 不成功
67 00	长度错误
69 01	命令不接受（无效状态）

SW1 SW2	含义
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
93 02	MAC 无效

[注]：完成圈存交易后，IC 卡把交易金额加在电子存折或电子钱包的余额上，将电子存折或电子钱包联机交易序号加 1，并用下表的数据组成一个记录，保存在电子存折或电子钱包所指定的记录长度为 23 个字节的交易明细文件中。

表 8.6 23 字节交易明细文件内容

说　明	长度（字节）
电子存折、钱包联机交易序号（加 1 前）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

6.7.3. 圈存交易流程图


IC卡
POS机
主机
取应用序列号SELECT
送应用序列号
主机依据应用序列号分散出圈存子密钥
返回9000
初始化圈存交易INITIALIZE FOR LOAD
80 50 01 01/02 0B 密钥标识符 金额 终端号
生成过程密钥：随机数+联机交易序号+8000
生成MAC1：旧余额+金额+类型标识+终端号
旧余额 联机序号 密钥版本号 算法标识 随机数 MAC1
旧余额 联机序号 版本号 算法标识 随机数 MAC1
由主机验证MAC1的有效性，如有效则产生MAC2
生成MAC2的数据：金额+类型标识+终端号+日期+时间
主机将联机交易序号加1
主机交易日期 主机交易时间MAC2
圈存交易 CREDIT FOR LOAD
80 52 00 00 0B 交易日期 交易时间 MAC2
由IC卡验证MAC2的有效性，如有效则：
1.将联机交易序号加1
2.将交易金额加到余额上
3.组成一条记录更新交易明细文件
4.用以下数据生成TAC
新余额+联机交易序号（加1前）+交易金额+交易类型标识+终端编机号+主机交易日期+主机交易时间
4字节TAC

6.8. 消费交易（存折或钱包）

消费交易允许持卡人使用电子存折或电子钱包的余额进行购物或获取服务。此交易可以在销售点终端（POS）上脱机进行。使用电子存折进行的消费交易必须验证口令，使用电子钱包则不需要。

6.8.1. 消费初始化 INITIALIZE FOR PURCHASE

6.8.1.1. 命令定义和范围

INITIALIZE FOR PURCHASE 命令用于初始化消费交易。

6.8.1.2. 命令报文

INITIALIZE FOR PURCHASE 命令报文编码如下：

代码	值	
CLA	80	
INS	50	
P1	01	
P2	01：用于电子存折	
	02：用于电子钱包	
Lc	0B	
Data	密钥标识符	1 字节
	交易金额	4 字节
	终端机编号	6 字节
Le	0F	

6.8.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

交易金额：此次消费交易待处理的金额

终端机编号：6 字节终端机编号，由终端给出

6.8.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 8.8 INITIALIZE FOR PURCHASE 命令响应报文数据域

说明	长度（字节）
电子存折或电子钱包旧余额	4
电子存折或电子钱包脱机交易序号	2
透支限额	3
密钥版本号（DATA 中第一字节指定的消费密钥）	1
算法标识（DATA 中第一字节指定的消费密钥）	1
伪随机数（IC 卡）	4

过程密钥由 DATA 中第一字节即密钥标识符指定的消费密钥对（4 字节随机数+2 字节

电子存折或电子钱包脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

MAC1 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

交易类型标识：

值	含义
05	电子存折消费
06	电子钱包消费

6.8.1.5. 响应报文的状态码

消费初始化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
62 83	选择文件无效，文件或密钥校验错误
65 81	写 EEPROM 不成功
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到
94 01	金额不足
94 03	密钥索引不支持

[注 1]：要想进行消费交易首先必须进行消费初始化，IC 将 INITIALIZE FOR PURCHASE 响应报文回送给终端处理。如果 IC 卡回送的状态码不是’9000’，则交易中止。

[注 2]：在银行的应用目录下，当符合中国金融 IC 卡应用规范的专用钱包文件用作电子存折时，文件标识符固定为 0001；用作电子钱包时，文件标识符固定为 0002。

6.8.2. 消费命令 DEBIT FOR CAPP PURCHASE

6.8.2.1. 定义和范围

DEBIT FOR PURCHASE 命令用于消费交易。

6.8.2.2. 命令报文

DEBIT FOR PURCHASE 命令报文编码如下：

代码	值	
CLA	80	
INS	54	
P1	01	
P2	00	
Lc	0F	
Data	终端交易序号	4 字节
	交易日期（终端）	4 字节
	交易时间（终端）	3 字节
	MAC1	4 字节
Le	08	

执行 INITIALIZE FOR PURCHASE 后即选择了消费交易。

6.8.2.3. 命令报文数据域

过程密钥由与消费初始化相同的消费密钥对（4 字节随机数+2 字节电子存折或电子钱包脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

MAC1 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

交易类型标识见消费初始化命令。

6.8.2.4. 响应报文数据域

此命令执行成功的响应报文数据域如下表：

表 8.11 INITIALIZE FOR PURCHASE 命令响应报文数据域

说明	长度（字节）
交易验证码 TAC	4
MAC2	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

MAC2 由卡中过程密钥对（4 字节交易金额）数据加密生成。

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易序号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

6.8.2.5. 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：

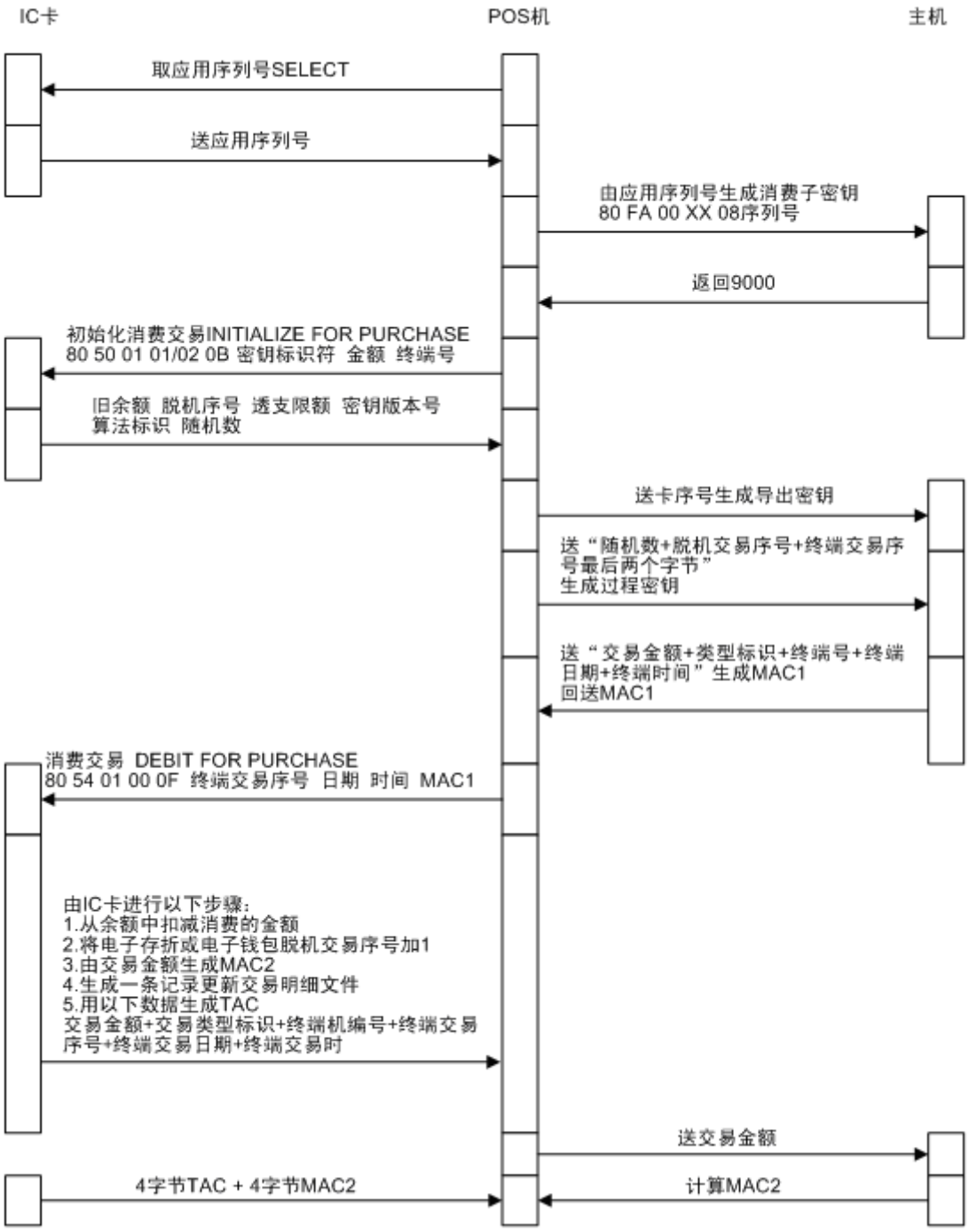
SW1 SW2	含义
65 81	写 EEPROM 不成功
67 00	长度错误
69 01	命令不接受（无效状态）
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
93 02	MAC 无效
94 01	金额不足

[注]：完成消费交易后，IC 卡从电子存折或电子钱包余额中扣减消费的金额，将电子存折或电子钱包脱机交易序号加 1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。

表 8.12 23 字节交易明细文件内容

说明	长度（字节）
电子存折脱机交易序号（加 1 前）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
终端交易日期	4
终端交易时间	3

6.8.3. 消费交易流程图


IC卡
POS机
主机
取应用序列号SELECT
送应用序列号
由应用序列号生成消费子密钥
80 FA 00 XX 08序列号
返回9000
初始化消费交易INITIALIZE FOR PURCHASE
80 50 01 01/02 0B 密钥标识符 金额 终端号
旧余额 脱机序号 透支限额 密钥版本号
算法标识 随机数
送卡序号生成导出密钥
送“随机数+脱机交易序号+终端交易序号最后两个字节”
生成过程密钥
送“交易金额+类型标识+终端号+终端日期+终端时间”生成MAC1
回送MAC1
消费交易 DEBIT FOR PURCHASE
80 54 01 00 0F 终端交易序号 日期 时间 MAC1
由IC卡进行以下步骤：
1.从余额中扣减消费的金额
2.将电子存折或电子钱包脱机交易序号加1
3.由交易金额生成MAC2
4.生成一条记录更新交易明细文件
5.用以下数据生成TAC
交易金额+交易类型标识+终端机编号+终端交易序号+终端交易日期+终端交易时
送交易金额
4字节TAC + 4字节MAC2
计算MAC2

6.9. 复合应用消费交易（钱包）

复合应用消费交易允许持卡人使用电子钱包的余额进行购物或获取服务。此交易可以在销售点终端（POS）上脱机进行。此交易无需提交个人密码（PIN）。

6.9.1. 消费初始化 INITIALIZE FOR CAPP PURCHASE

6.9.1.1. 命令定义和范围

INITIALIZE FOR CAPP PURCHASE 命令用于初始化消费交易。

6.9.1.2. 命令报文

INITIALIZE FOR CAPP PURCHASE 命令报文编码如下：

代码	值	
CLA	80	
INS	50	
P1	03	
P2	02	
Lc	0B	
Data	密钥标识符	1 字节
	交易金额	4 字节
	终端机编号	6 字节
Le	0F	

6.9.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

交易金额：此次复合消费交易待处理的金额

终端机编号：6 字节终端机编号，由终端给出

6.9.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 8.14 INITIALIZE FOR PURCHASE 命令响应报文数据域

说明	长度（字节）
电子存折或电子钱包旧余额	4
电子存折或电子钱包脱机交易序号	2
透支限额	3
密钥版本号（DATA 中第一字节指定的消费密钥）	1
算法标识（DATA 中第一字节指定的消费密钥）	1
伪随机数（IC 卡）	4

过程密钥由 DATA 中第一字节即密钥标识符指定的消费密钥对（4 字节随机数+2 字节电子存折或电子钱包脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

MAC1 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4

字节终端交易日期+3 字节终端交易时间）数据加密生成。

复合消费交易的交易类型标识为 09。

6.9.1.5. 响应报文的状态码

消费初始化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
62 83	选择文件无效，文件或密钥校验错误
65 81	写 EEPROM 不成功
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到
94 01	金额不足
94 03	密钥索引不支持

[注 1]：要想进行消费交易首先必须进行消费初始化，IC 将 INITIALIZE FOR PURCHASE 响应报文回送给终端处理。如果 IC 卡回送的状态码不是’9000’，则交易中止。

[注 2]：在银行的应用目录下，当符合中国金融 IC 卡应用规范的专用钱包文件用作电子存折时，文件标识符固定为 0001；用作电子钱包时，文件标识符固定为 0002。

6.9.2. 更新复合应用数据缓存 UPDATE CAPP DATA CACHE

6.9.2.1. 定义和范围

UPDATE CAPP DATA CHACHE 命令用于复合应用消费交易中更新复合应用数据缓存，缓存数据将被 DEBIT FOR CAPP PURCHASE 命令用于改写复合应用专用文件中相关记录。

6.9.2.2. 命令报文

UPDATE CAPP DATA CACHE 命令报文编码如下：

代码	值
CLA	80
INS	DC
P1	复合应用类型标识符
	记录号
P2	见下表
Lc	XX
Data	更新原有记录的新数据
Le	不存在

[注]：Lc 表示要写入的字节数，若为线路保护，Lc 为写入数据的长度+4 字节 MAC；若为加密线路保护，Lc 为加密后数据的长度+4 字节 MAC。

表 8.9 UPDATE CAPP DATA CACHE 命令中 P2 的含义

b8	b7	b6	b5	b4	b3	b2	b1	含 义
X	X	X	X	X	-	-	-	b4-b8 为短文件标识符
0	0	0	0	0	-	-	-	当前文件
1	1	1	1	1	-	-	-	保留
-	-	-	-	-	0	0	0	第一个标识符出现的记录
-	-	-	-	-	1	0	0	P1 表示的为记录号
-	-	-	-	-	X	X	X	RFU

6.9.2.3. 命令报文数据域

此命令报文数据域由更新原有记录的新记录组成。

6.9.2.4. 响应报文数据域

响应报文数据域不存在。

6.9.2.5. 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
62 83	选择文件无效

SW1 SW2	意　义
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是定长或变长记录文件
69 82	写的条件不满足
6A 81	不支持此功能（无 MF 或 MF 已锁定）
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件无足够空间

6.9.3. 复合应用消费命令 DEBIT FOR CAPP PURCHASE

6.9.3.1. 定义和范围

DEBIT FOR CAPP PURCHASE 命令用于消费交易。

6.9.3.2. 命令报文

DEBIT FOR CAPP PURCHASE 命令报文编码如下：

代码	值	
CLA	80	
INS	54	
P1	01	
P2	00	
Lc	0F	
Data	终端交易序号	4 字节
	交易日期（终端）	4 字节
	交易时间（终端）	3 字节
	MAC1	4 字节
Le	08	

执行 INITIALIZE FOR CAPP PURCHASE 后即选择了复合应用消费交易。

6.9.3.3. 命令报文数据域

过程密钥由与消费初始化相同的消费密钥对（4 字节随机数+2 字节电子存折或电子钱包脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

MAC1 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

交易类型标识见消费初始化命令。

6.9.3.4. 响应报文数据域

此命令执行成功的响应报文数据域如下表：

表 8.15 INITIALIZE FOR CAPP PURCHASE 命令响应报文数据域

说明	长度（字节）
交易验证码 TAC	4
MAC2	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

MAC2 由卡中过程密钥对（4 字节交易金额）数据加密生成。

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易序号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

6.9.3.5. 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：

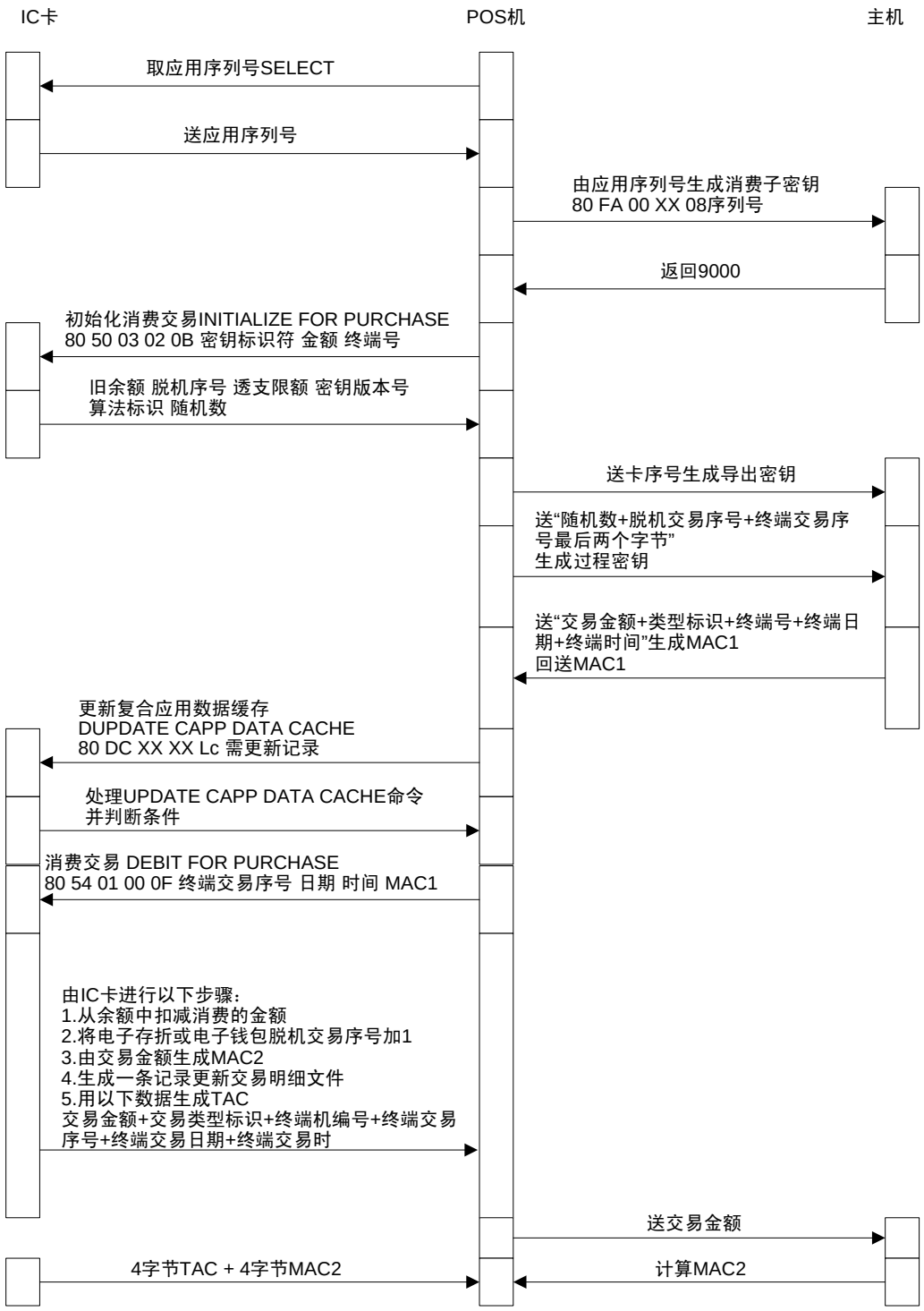
SW1 SW2	含义
65 81	写 EEPROM 不成功
67 00	长度错误
69 01	命令不接受（无效状态）
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
93 02	MAC 无效
94 01	金额不足

[注]：完成消费交易后，IC 卡从电子存折或电子钱包余额中扣减消费的金额，将电子存折或电子钱包脱机交易序号加 1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。

表 8.16 23 字节交易明细文件内容

说明	长度（字节）
电子存折脱机交易序号（加 1 前）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
终端交易日期	4
终端交易时间	3

6.9.4. 复合应用消费交易流程图



6.10.圈提交易（存折）

通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回到其在银行的相应帐户上。这种交易必须在金融终端上联机进行并要求验证口令。只有电子存折应用支持圈提交易。

6.10.1. 圈提初始化 INITIALIZE FOR UNLOAD

6.10.1.1. 命令定义和范围

INITIALIZE FOR UNLOAD 命令用于初始化圈提交易。

6.10.1.2. 命令报文

INITIALIZE FOR UNLOAD 命令报文编码如下：

代码	值	
CLA	80	
INS	50	
P1	05	
P2	01：用于电子存折	
Lc	0B	
Data	密钥标识符	1 字节
	交易金额	4 字节
	终端机编号	6 字节
Le	10	

6.10.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

交易金额：此次圈提交易待处理的金额

终端机编号：6 字节终端机编号，由终端给出

6.10.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 8.18 INITIALIZE FOR UNLOAD 命令响应报文数据域

说明	长度（字节）
电子存折旧余额	4
电子存折联机交易序号	2
密钥版本号（DATA 中第一字节指定的圈提密钥）	1
算法标识（DATA 中第一字节指定的圈提密钥）	1
伪随机数（IC 卡）	4
MAC1	4

过程密钥由 DATA 中第一字节即密钥标识符指定的圈提密钥对（4 字节随机数+2 字节电子存折联机交易序号+8000）数据加密生成。

MAC1 由卡中过程密钥对（4 字节电子存折旧余额+4 字节交易金额+1 字节交易类型标识+6 字节终端机编号）数据加密生成。

圈提的交易类型标识为 03。

6.10.1.5. 响应报文的状态码

圈提初始化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
67 00	长度错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 01	金额不足
94 03	密钥索引不支持

[注 1]：要想进行圈提交易首先必须进行圈提初始化，IC 将 INITIALIZE FOR UNLOAD 响应报文回送给终端处理。如果 IC 卡回送的状态码不是’9000’，则交易中止。

[注 2]：在银行的应用目录下，当符合中国金融 IC 卡应用规范的专用钱包文件用作电子存折时，文件标识符固定为 0001。

6.10.2. 圈提命令 CREDIT FOR UNLOAD

6.10.2.1. 定义和范围

CREDIT FOR UNLOAD 命令用于圈提交易。

6.10.2.2. 命令报文

CREDIT FOR UNLOAD 命令报文编码如下：

代码	值	
CLA	80	
INS	54	
P1	03	
P2	00	
Lc	0B	
Data	主机交易日期	4 字节
	主机交易时间	3 字节
	MAC2	4 字节
Le	04	

6.10.2.3. 命令报文数据域

过程密钥由与圈提初始化相同的圈提密钥对（4 字节随机数+2 字节电子存折联机交易序号+8000）数据加密生成。

MAC2 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节主机交易日期+3 字节主机交易时间）数据加密生成。

交易类型标识见圈提初始化命令。

6.10.2.4. 响应报文数据域

此命令执行成功的响应报文数据域如下表：

表 8.20 CREDIT FOR UNLOAD 命令响应报文数据域

说明	长度（字节）
MAC3	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

MAC3 由卡中过程密钥对（4 字节电子存折新余额+2 字节电子存折联机交易序号（加 1 前）+4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节主机交易日期+3 字节主机交易时间）数据加密生成。

6.10.2.5. 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	含义
65 81	写 EEPROM 不成功
67 00	长度错误

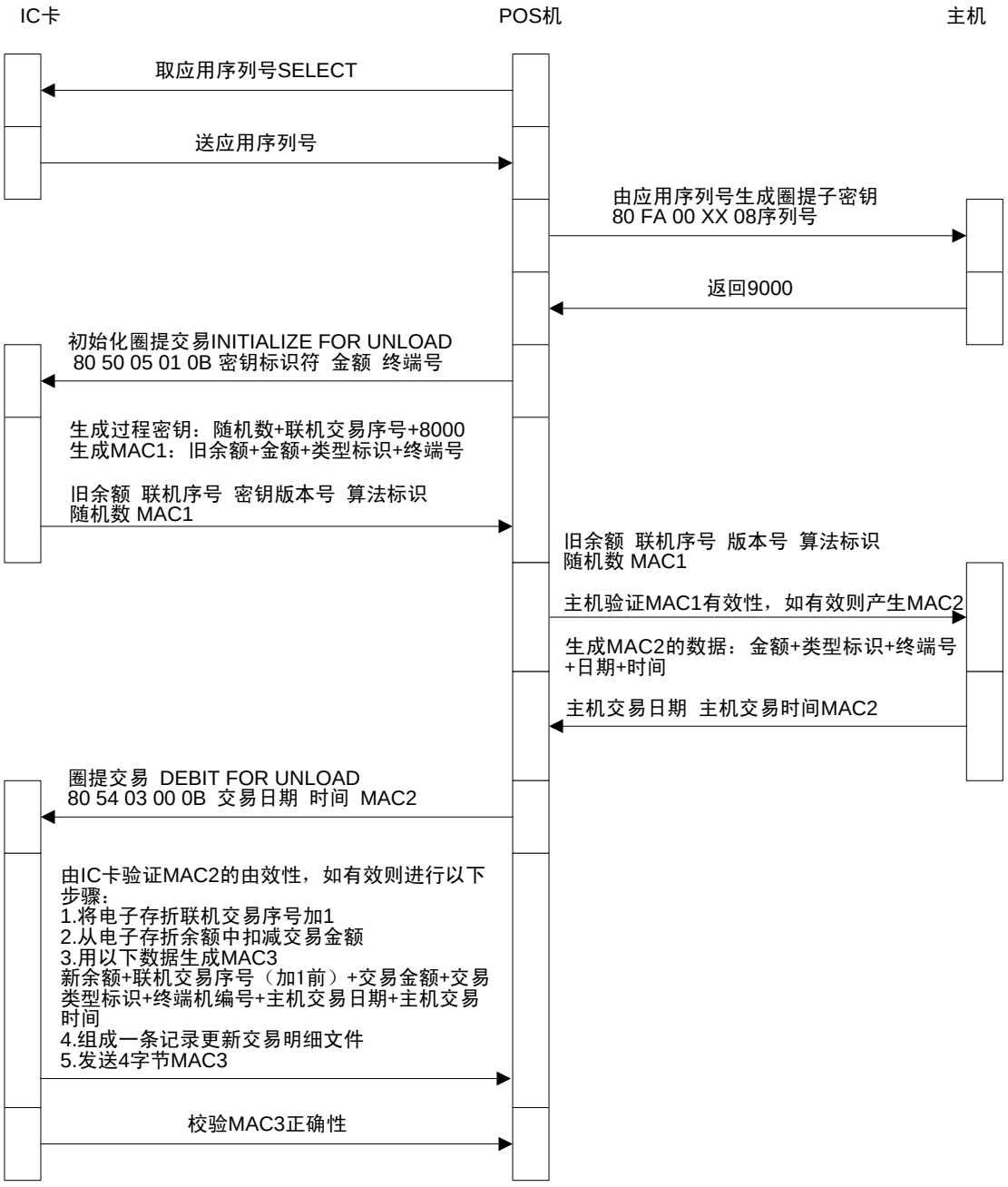
69 01	命令不接受（无效状态）
6A 81	功能不支持(无 MF 或卡片已锁死)
93 02	MAC 无效

[注]：完成消费交易后，IC 卡从电子存折或电子钱包余额中扣减消费的金额，将电子存折或电子钱包脱机交易序号加 1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。

表 8.20 23 字节交易明细文件内容

说明	长度（字节）
电子存折联机交易序号（加 1 前）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

6.10.3. 圈提交易流程图



6.11.取现交易（存折）

取现交易允许持卡人从电子存折中提取现金。此交易必须在金融终端上进行，但可以脱机处理。只有电子存折应用支持此交易，且必须验证口令。

6.11.1. 取现初始化 INITIALIZE FOR CASH WITHDRAW

6.11.1.1. 命令定义和范围

INITIALIZE FOR CASH WITHDRAW 命令用于初始化取现交易。

6.11.1.2. 命令报文

INITIALIZE FOR CASH WITHDRAW 命令报文编码如下：

代码	值	
CLA	80	
INS	50	
P1	02	
P2	01：用于电子存折	
Lc	0B	
Data	密钥标识符	1 字节
	交易金额	4 字节
	终端机编号	6 字节
Le	0F	

6.11.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

交易金额：此次取现交易待处理的金额

终端机编号：6 字节终端机编号，由终端给出

6.11.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 8.22 INITIALIZE FOR CASH WITHDRAW 命令响应报文数据域

说明	长度（字节）
电子存折旧余额	4
电子存折脱机交易序号	2
透支限额	3
密钥版本号（DATA 中第一字节指定的消费密钥）	1
算法标识（DATA 中第一字节指定的消费密钥）	1
伪随机数（IC 卡）	4

过程密钥由 DATA 中第一字节即密钥标识符指定的消费密钥对（4 字节随机数+2 字节电子存折脱机交易序号+2 字节终端交易序号的最右两个字节）数据加密生成。

MAC1 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4

字节终端交易日期+3 字节终端交易时间）数据加密生成。

取现的交易类型标识为 04。

6.11.1.5. 响应报文的状态码

取现初始化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
62 83	选择文件无效，文件或密钥校验错误
65 81	写 EEPROM 不成功
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到
94 01	金额不足
94 03	密钥索引不支持

[注 1]：要想进行取现交易首先必须进行取现初始化，IC 将 INITIALIZE FOR CASH WITHDRAW 响应报文回送给终端处理。如果 IC 卡回送的状态码不是’9000’，则交易中止。

[注 2]：在银行的应用目录下，当符合中国金融 IC 卡应用规范的专用钱包文件用作电子存折时，文件标识符固定为 0001；用作电子钱包时，文件标识符固定为 0002。

6.11.2. 取现命令 DEBIT FOR CASH WITHDRAW

6.11.2.1. 定义和范围

DEBIT FOR CASH WITHDRAW 命令用于取现交易。

6.11.2.2. 命令报文

DEBIT FOR CASH WITHDRAW 命令报文编码如下：

代码	值	
CLA	80	
INS	54	
P1	01	
P2	00	
Lc	0F	
Data	终端交易序号	4 字节
	终端交易日期	4 字节
	终端交易时间	3 字节
	MAC1	4 字节
Le	08	

执行 INITIALIZE FOR CASH WITHDRAW 后即选择了取现交易。

6.11.2.3. 命令报文数据域

过程密钥由与取现初始化相同的消费密钥对（4 字节随机数+2 字节电子存折脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

MAC1 由卡中过程密钥对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

交易类型标识见取现初始化命令。

6.11.2.4. 响应报文数据域

此命令执行成功的响应报文数据域如下表：

表 8.24 DEBIT FOR CASH WITHDRAW 命令响应报文数据域

说明	长度（字节）
交易验证码 TAC	4
MAC2	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

MAC2 由卡中过程密钥对（4 字节交易金额）数据加密生成。

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易序号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

6.11.2.5. 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：

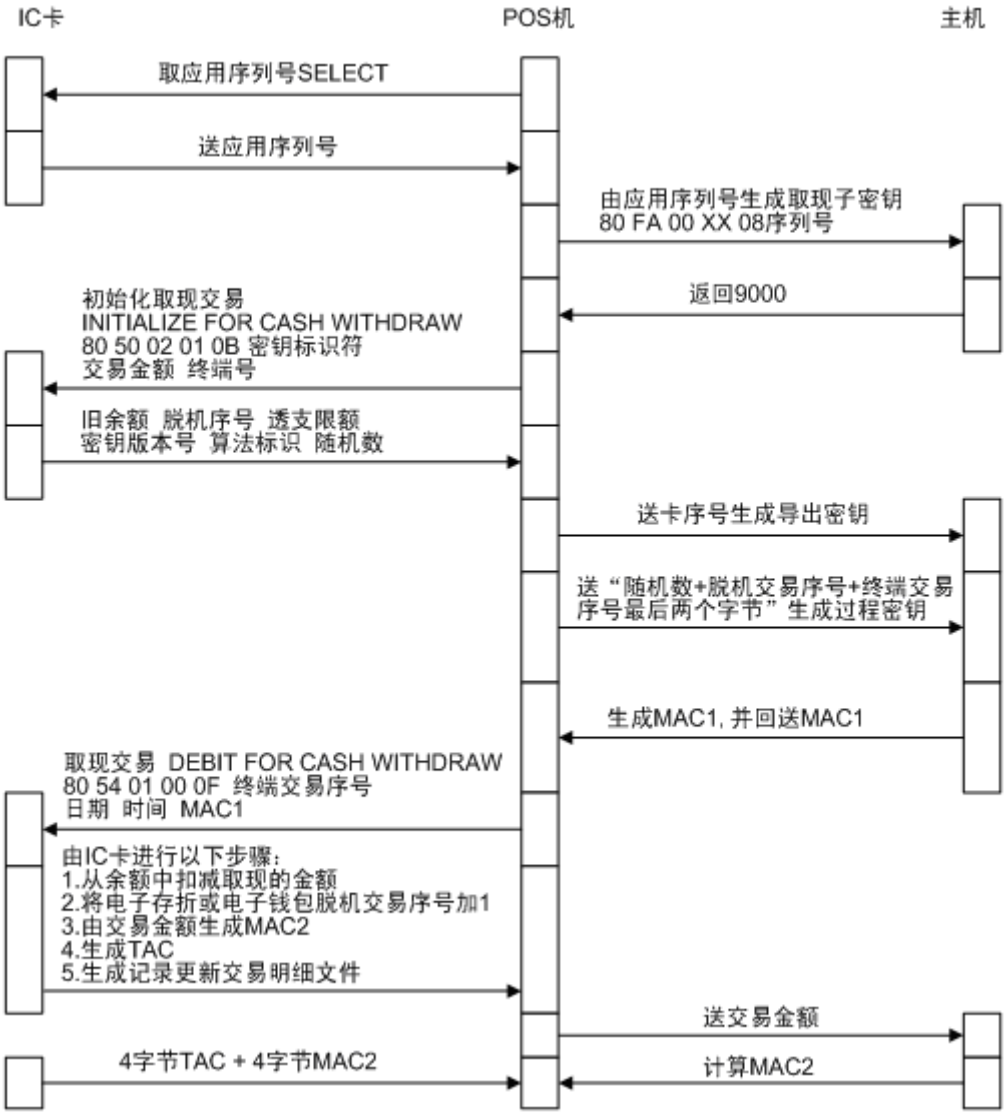
SW1 SW2	含义
65 81	写 EEPROM 不成功
69 01	命令不接受（无效状态）
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
93 02	MAC 无效
94 01	金额不足

[注]：完成取现交易后，IC 卡从电子存折余额中扣减取现交易的金额，将电子存折脱机交易序号加 1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。

表 8.25 23 字节交易明细文件内容

说明	长度（字节）
电子存折脱机交易序号（加 1 前）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
终端交易日期	4
终端交易时间	3

6.11.3. 取现交易流程图



6.12.修改透支限额交易（存折）

当电子存折中的实际金额不足时，“透支功能”为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。修改透支限额交易必须在金融终端上联机进行，且必须验证口令。

6.12.1. 初始化修改透支限额命令 INITIALIZE FOR UPDATE

6.12.1.1. 定义和范围

INITIALIZE FOR UPDATE 命令用于初始化修改透支限额交易。

6.12.1.2. 命令报文

INITIALIZE FOR UPDATE 命令报文编码如下：

代码	值	
CLA	80	
INS	50	
P1	04	
P2	01：仅用于电子存折	
Lc	07	
Data	密钥标识符	1 字节
	终端机编号	6 字节
Le	13	

6.12.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

终端机编号：6 字节终端机编号，由终端给出

6.12.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 8.27 INITIALIZE FOR UPDATE 命令响应报文数据域

说明	长度（字节）
电子存折旧余额	4
电子存折联机交易序号	2
旧透支限额	3
密钥版本号（DATA 中第一字节指定的修改透支密钥）	1
算法标识（DATA 中第一字节指定的修改透支密钥）	1
伪随机数（IC 卡）	4
MAC1	4

过程密钥由 DATA 中第一字节指定的修改透支限额密钥对（4 字节随机数+2 字节电子存折联机交易序号+8000）数据加密生成。

MAC1 由卡中过程密钥对（4 字节电子存折余额+3 字节旧透支限额+1 字节交易类型标

识+6 字节终端机编号）数据加密生成。

修改透支限额交易类型标识为 07。

6.12.1.5. 响应报文的状态码

取现初始化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
62 83	选择文件无效，文件或密钥校验错误
65 81	写 EEPROM 不成功
67 00	长度错误
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到
6A 86	参数 P1 P2 错误
94 03	密钥标识不支持

[注 1]：要想进行修改透支限额交易首先必须进行修改透支限额初始化，IC 将 INITIALIZE FOR UPDATE 响应报文回送给终端处理。如果 IC 卡回送的状态码不是’9000’，则交易中止。

[注 2]：在银行的应用目录下，当符合中国金融 IC 卡应用规范的专用钱包文件用作电子存折时，文件标识符固定为 0001；用作电子钱包时，文件标识符固定为 0002。

6.12.2. 修改透支限额命令 UPDATE OVERDRAW LIMIT

6.12.2.1. 定义和范围

UPDATE OVERDRAW LIMIT 命令用于修改透支限额交易。

6.12.2.2. 命令报文

UNDATE OVERDRAW LIMIT 命令报文编码如下：

代码	值	
CLA	80	
INS	58	
P1	00	
P2	00	
Lc	0E	
Data	新透支限额	3 字节
	发卡方交易日期	4 字节
	发卡方交易时间	3 字节
	MAC2	4 字节
Le	04	

6.12.2.3. 命令报文数据域

过程密钥由与修改透支限额初始化相同的修改透支限额密钥对（4 字节随机数+2 字节电子存折联机交易序号+8000）数据加密生成。

MAC2 由卡中过程密钥对（3 字节新透支限额+1 字节交易类型标识+6 字节终端机编号+4 字节主机交易日期+3 字节主机交易时间）数据加密生成。

交易类型标识见修改透支限额初始化。

6.12.2.4. 响应报文数据域

此命令执行成功的响应报文数据域如下表：

表 8.29 UPDATE FOR UPDATE 命令响应报文数据域

说明	长度（字节）
交易验证码 TAC	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

TAC 用内部密钥 DTK 直接对（4 字节电子存折新余额+2 字节电子存折联机交易序号（加 1 前）+3 字节电子存折新透支限额+1 字节交易类型标识+6 字节终端机编号+4 字节主机交易日期+3 字节主机交易时间）数据加密生成。

6.12.2.5. 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	含义
65 81	写 EEPROM 不成功

SW1 SW2	含义
69 01	命令不接受（无效状态）
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
93 02	MAC 无效
94 01	金额不足

[注]：完成修改透支限额交易后，IC 卡将当前电子存折余额置为新的电子存折余额，更新透支限额，使电子存折联机交易序号加 1，并用下表的数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。

表 8.30 23 字节交易明细文件内容

说明	长度（字节）
电子存折脱机交易序号（加 1 前）	2
新透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
终端交易日期	4
终端交易时间	3

6.12.3. 修改透支限额交易流程图

6.13.取交易认证 GET TRANSACTION PROVE

6.13.1. 定义和范围

GET TRANSACTION PROVE 命令提供了一种在交易处理过程中拔出并重插卡后卡片的恢复机制。

6.13.2. 命令报文

GET TRANSACTION PROVE 命令报文编码如下：

代码	值
CLA	80
INS	5A
P1	00
P2	待取认证码的交易类型标识
Lc	02
Data	待取认证码的交易序号
Le	08

各交易交易类型标识符见下表：

值	含义
01	电子存折圈存
02	电子钱包圈存
03	圈提
04	电子存折取款
05	电子存折消费
06	电子钱包消费
07	电子存折修改透支限额
09	复合消费

6.13.3. 响应报文数据域

如果命令中指定的交易类型标识和电子存折、电子钱包联机或脱机交易序号对应的报文鉴别代码 MAC 或交易验证码 TAC 可用，则响应报文数据域如下表：

表 8.32 GET TRANSCTION PROVE 命令响应报文数据域

说明	长度（字节）
报文鉴别代码 MAC	4
交易验证码 TAC	4

6.13.4. 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	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到
93 02	MAC 无效
94 06	所需 MAC 不可用

6.13.5. 防拔功能

此功能保证卡片在交易处理中的任何情况下，甚至是在更新 EEPROM 过程中掉电的情况下，仍能保持数据的完整性。

在终端发给 IC 卡一个命令以更新电子存折或电子钱包余额时，卡片总会回送一个报文鉴别代码（MAC）或交易验证码（TAC），以证明更新已经发生。一旦余额更新成功，可以通过 GET TRANSCATION PROVE 命令获得此 MAC 或 TAC。

如果在命令已执行结束，而终端还未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否更新的不定状态。在这种情况下，终端可以用 GET TRANSACTION PROVE 命令取回 MAC 或 TAC，如果返回’9000’则表示卡片更新成功，交易完成。如果不返回’9000’则表示卡片更新失败，要想完成该交易必须从交易初始化开始重新进行。

6.14.读余额 GET BALANCE

6.14.1. 定义和范围

GET BALANCE 命令用于读取电子钱包或电子存折余额，实现查询余额交易。

读取电子存折余额需验证口令密钥（PIN）。

6.14.2. 命令报文

GET BALANCE 命令报文编码如下：

代码	值
CLA	80
INS	5C
P1	00
P2	01：用于电子存折
	02：用于电子钱包
Lc	不存在
Data	不存在
Le	04

6.14.3. 响应报文数据域

命令执行成功的响应报文数据域如下所示：

表 8.33 GET BALANCE 命令响应报文数据域

说明	长度（字节）
电子存折或电子钱包余额	4

如果命令执行不成功，则在响应报文中回送 SW1 和 SW2。

6.14.4. 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
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 82	文件未找到

7. 加油卡交易命令

加油卡命令用于加油卡灰锁、解扣等命令

SMARTCOS21、SMARTCOS-ROM 支持此部分命令

7.1. 灰锁初始化 INITIALIZE FOR GREY LOCK

7.1.1. 灰锁初始化命令定义和范围

INITIALIZE FOR GREY LOCK 命令用于初始化灰锁命令。

7.1.2. 命令报文

INITIALIZE FOR GREY LOCK 命令报文编码如下：

代码	值	
CLA	E0	
INS	7A	
P1	08	
P2	01：用于电子存折	
	02：用于电子钱包	
Lc	07	
Data	密钥标识符	1 字节
	终端机编号	6 字节
Le	0F	

7.1.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

终端机编号：6 字节终端机编号，由终端给出

7.1.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 9.1 INITIALIZE FOR GREY LOCK 命令执行成功的响应报文数据域

说明	长度（字节）
电子存折或电子钱包旧余额	4
电子存折或电子钱包联机交易序号	2
透支限额	3
密钥版本号（DATA 中第一字节指定的圈存密钥）	1
算法标识（DATA 中第一字节指定的圈存密钥）	1
伪随机数（IC 卡）	4

7.1.4.1. 响应报文的状态码

圈存初始化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
6E 00	CLA 参数错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 03	密钥索引不支持

7.2. 灰锁命令 GREY LOCK

7.2.1. 灰锁命令定义和范围

GREY LOCK 用于灰锁指定的 ED 或 EP。该命令只有在成功执行 INITIALIZE FOR GREY LOCK 之后才能执行。

7.2.2. 命令报文

GREY LOCK 命令报文编码如下：

代码	值	
CLA	E0	
INS	7C	
P1	08	
P2	00	
Lc	0B	
Data	终端交易序号	4 字节
	终端随机数	4 字节
	交易日期	4 字节
	交易时间	3 字节
	MAC1	4 字节
Le	10	

7.2.3. 命令报文数据域

首先使用灰锁密钥对（4 字节随机数+2 字节脱机交易序号+终端交易序号最右两字节）数据加密生成临时密钥。

使用临时密钥对（4 字节终端随机数+80000000）加密生成过程密钥。

MAC1 由过程密钥对（交易类型（91：电子存折、92：电子钱包）+6 字节终端机编号+4 字节交易日期+3 字节交易时间）数据加密生成。

灰锁命令交易类型标识为：

值	含义
91	电子存折灰锁
92	电子钱包灰锁

7.2.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 9.2 GREY LOCK 命令响应报文数据域

说明	长度（字节）
GTAC	4
MAC2	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

MAC2 由卡中过程密钥对（4 字节电子钱包余额+1 字节脱机交易序号）数据加密生成。

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易序号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

7.2.4.1. 响应报文的状态码

圈提初始化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
67 00	长度错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 01	金额不足
94 03	密钥索引不支持

7.3. 解扣命令 DEBIT FOR UNLOCK

7.3.1. 灰锁命令定义和范围

DEBIT FOR UNLOCK 用于灰锁指定的 ED 或 EP。该命令只有在 ED/EP 处于灰锁状态下才能成功执行。

7.3.2. 命令报文

DEBIT FOR UNLOCK 命令报文编码如下：

代码	值	
CLA	E0	
INS	7E	
P1	08	
P2	01：用于电子存折	
	02：用于电子钱包	
Lc	1B	
Data	交易金额	4 字节
	ED/EP 脱机交易序号	2 字节
	终端机编号	6 字节
	终端交易序号	4 字节
	交易日期	4 字节
	交易时间	3 字节
	GMAC	4 字节
Le	04	

DEBIT FOR UNLOCK 命令前允许终端对 IC 卡下电，COS 会自动记录过程密钥。重新上电进行交易预处理后可以继续执行 DEBIT FOR UNLOCK 不受影响。

7.3.3. 命令报文数据域

GMAC 是使用灰锁命令相同的过程密钥对（4 字交易金额）按 PBOC MAC 方式计算生成的。

7.3.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 9.2 INITIALIZE FOR UNLOAD 命令响应报文数据域

说明	长度（字节）
TAC	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易序号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

解扣命令交易类型标识为：

值	含义
93	电子存折解扣
94	电子钱包解扣

7.3.4.1. 响应报文的状态码

圈提初始化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
67 00	长度错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 01	金额不足
94 06	脱机交易金额不符
93 02	GMAC 错误

7.4. 灰锁初始化 INITIALIZE FOR GREY UNLOCK

7.4.1. 灰锁初始化命令定义和范围

INITIALIZE FOR GREY UNLOCK 命令用于初始化灰锁命令。

7.4.2. 命令报文

INITIALIZE FOR GREY UNLOCK 命令报文编码如下：

代码	值	
CLA	E0	
INS	7A	
P1	09	
P2	01：用于电子存折	
	02：用于电子钱包	
Lc	07	
Data	密钥标识符	1 字节
	终端机编号	6 字节
Le	12	

7.4.3. 命令报文数据域

密钥标识符：IC 卡内的密钥标识符

终端机编号：6 字节终端机编号，由终端给出

7.4.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 9.1 INITIALIZE FOR GREY UNLOCK 命令执行成功的响应报文数据域

说明	长度（字节）
ED/EP 余额	4
脱机交易序号	2
联机交易序号	2
密钥版本号	1
密钥算法标识	1
伪随机数（ICC）	4
MAC1	4

过程密钥由 DATA 中第一字节即密钥标识符指定的圈提密钥对（4 字节随机数+2 字节电子存折联机交易序号+8000）数据加密生成。

MAC1 由卡中过程密钥对（4 字节电子存折旧余额+4 字节交易金额+1 字节交易类型标识+6 字节终端机编号）数据加密生成。

联机解扣交易类型标识为：

值	含义

95	电子存折联机解扣
96	电子钱包联机解扣

7.4.4.1. 响应报文的状态码

圈存初始化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
6E 00	CLA 参数错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 03	密钥索引不支持

7.5. 灰锁命令 GREY UNLOCK

7.5.1. 灰锁命令定义和范围

GREY LOCK 用于灰锁指定的 ED 或 EP。该命令只有在成功执行 INITIALIZE FOR GREY LOCK 之后才能执行。

7.5.2. 命令报文

GREY LOCK 命令报文编码如下：

代码	值	
CLA	E0	
INS	7C	
P1	09	
P2	00	
Lc	0F	
Data	交易金额	4 字节
	交易日期	4 字节
	交易时间	3 字节
	MAC2	4 字节
Le	04	

7.5.3. 命令报文数据域

首先使用灰锁密钥对（4 字节随机数+2 字节脱机交易序号+终端交易序号最右两字节）数据加密生成临时密钥。

使用临时密钥对（4 字节终端随机数+80000000）加密生成过程密钥。

MAC2 由过程密钥对（交易类型（91：电子存折、92：电子钱包）+6 字节终端机编号+4 字节交易日期+3 字节交易时间）数据加密生成。

7.5.4. 响应报文数据域

此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

此命令执行成功的响应报文数据域如下表：

表 9.2 GREY LOCK 命令响应报文数据域

说明	长度（字节）
GTAC	4
MAC2	4

如果此命令执行不成功，则只在响应报文中回送 SW1 和 SW2。

MAC2 由卡中过程密钥对（4 字节电子钱包余额+1 字节脱机交易序号）数据加密生成。

TAC 用内部密钥 DTK 左右 8 位字节异或运算的结果对（4 字节交易金额+1 字节交易类型标识+6 字节终端机编号+4 字节终端交易序号+4 字节终端交易日期+3 字节终端交易时间）数据加密生成。

7.5.4.1. 响应报文的状态码

圈提初始化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
67 00	长度错误
69 85	使用条件不满足
6A 81	功能不支持（无 MF 或卡片已锁死）
6A 86	参数 P1 P2 错误
94 01	金额不足
94 03	密钥索引不支持

8. 安全报文传送

8.1. 安全报文传送

卡与外界进行数据传输（卡接收命令，发送应答）时，若以明文方式传输，攻击者通过劫获这些数据，可以分析出卡的结构，掌握卡中的数据。同时，也可以对传输的数据进行篡改。

如何避免这个问题呢？方法就是采用安全报文传送。

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。安全报文传送有三种情况：

- 线路保护：对传输的数据附加 4 字节 MAC 码，接收方收到后首先进行校验，只有校验正确的数据才予以接受，这样就防止了对传输数据的篡改。
  数据完整性和对发送方的认证通过使用 MAC 来实现。
- 线路加密：对传输的数据进行 DES 加密，这样传输的就是密文，攻击者即使获得的数据没有意义，分析后也只能得到错误的结果。
  数据的可靠性通过对数据域的加密来得到保证。
- 线路加密保护：对传输的数据进行 DES 加密后再附加 4 字节 MAC 码。

[注]：至于采取哪种方法进行安全报文传送由用户根据实际情况来决定。应该指出，高安全性是以降低速度，增加实现难度来换取的，所以并不是安全性越高越好，而一定要根据具体的要求来确定。

8.2. 如何实现安全报文传送

二进制文件、定长记录文件、变长记录文件、循环文件、钱包文件都可以采用安全报文传送。如对上述文件进行安全报文传送，只需在建立文件时改变文件类型字节高两位即可：

最高位置 1 表示数据域附加 4 字节 MAC，次高位置 1 表示对数据加密。

对于密钥也可以采用安全报文传送。如进行安全报文传送，只需在安装密钥时改变密钥类型字节高两位即可：

最高位置 1 表示数据域附加 4 字节 MAC，次高位置 1 表示对数据加密。

例：建立文件时若需进行线路保护则将文件类型最高位置 1，如二进制类型由 28 变为 A8。若需对密钥进行线路加密保护则将密钥类型的最高位及次高位均置 1，如 PIN 类型由 3A 变为 FA。

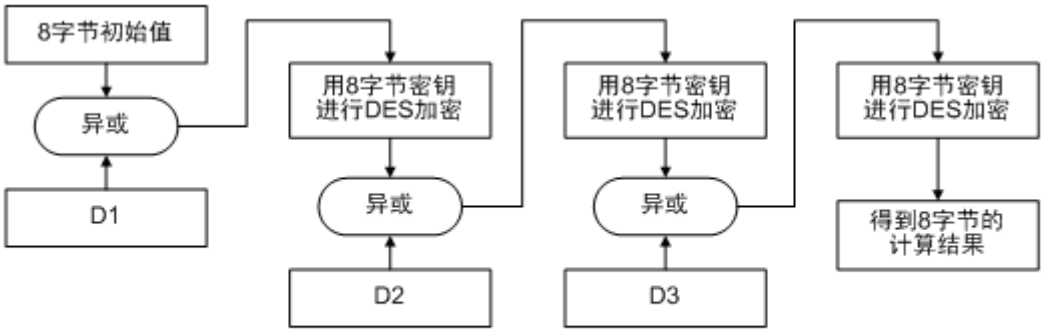
[注]：在对文件进行读写，或使用密钥（如核对、解锁、认证或更改密钥）时，若需采用安全报文传送，必须置 CLA 的后半字节为十六进制'4'。

8.3. MAC 的计算

MAC 是使用命令的所有元素（包括命令头）产生的。MAC 是命令数据域中最后一个数据元，它的长度为 4 个字节。

MAC 的计算步骤如下：

- 终端向 IC 卡发出一个 GET CHALLENGE 命令，从 IC 卡取回 4 字节随机数。
- 将 IC 卡回送的 4 字节随机数后缀以’00 00 00 00’，所得到的结果作为初始值。
- 按照顺序将以下数据连接在一起形成数据块：
  CLA，INS，P1，P2，Lc+4，DATA
  必须置 CLA 的后半字节为十六进制’4’。
  在命令的数据域中（如果存在）包含明文或加密的数据。
  （例: 如果要进行线路加密保护，加密后的数据块放在命令数据域中传输）
- 将该数据块分成 8 字节为单位的数据块，标号为 D1，D2，D3 等。最后的数据块有可能是 1-8 个字节。
- 如果最后的数据块长度是 8 字节的话，也必须在其后加上 16 进制数字’80 00 00 00 00 00 00 00’，转到第六步。
  如果最后的数据块长度不足 8 字节，则在其后加上 16 进制数字’80’，如果达到 8 字节长度，则转入第六步；否则在其后加上 16 进制数字’00’直到长度达到 8 字节为止。
- 对这些数据块使用相应密钥进行加密。（密钥由 SMARTCOS 命令或中国金融 IC 卡专用命令所指定）
  如果该密钥长度为 8 字节，则依照图 1 的方式来产生 MAC（根据在第三步中产生的数据块长度的不同，有可能在计算中会多于或少于三步）。
  如果该密钥长度为 16 字节，则依照图 2 的方式来产生 MAC（根据在第三步中产生的数据块长度的不同，有可能在计算中会多于或少于三步）。
- 最终得到是从计算结果左侧取得的 4 字节长度的 MAC。



［注］：图中的8字节密钥均相同，由FMCOS命令或中国金融IC卡专用命令所指定。

图 9-1 用长度为 8 字节的密钥产生 MAC 的算法

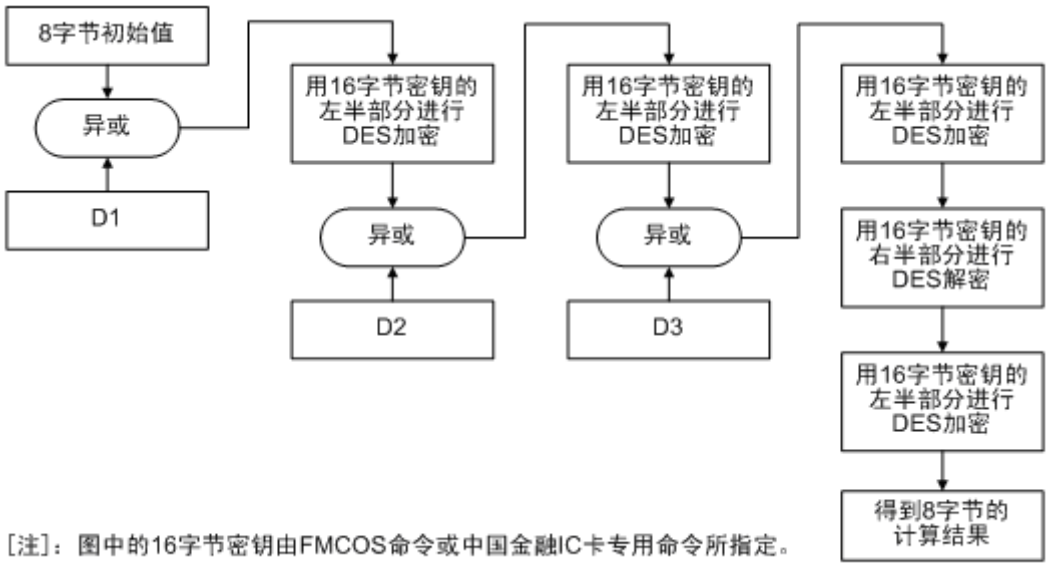


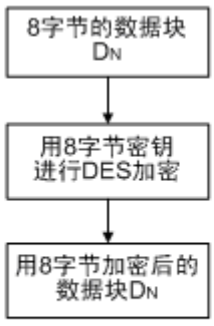
图 9-2 用长度为 16 字节的密钥产生 MAC 的算法

8.4. 数据加密/解密的计算

8.4.1. 数据加密计算

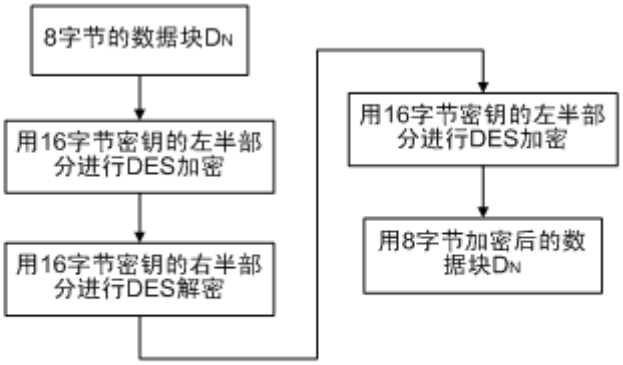
数据加密计算步骤如下：

- 用 LD 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。
- 将第一步中生成的数据块分解成 8 字节数据块，标号为 D1，D2，D3，D4 等等。最后一个数据块长度有可能不足 8 位。
- 如果最后（或唯一）的数据块长度等于 8 字节，转入第四步；如果不足 8 字节，在右边添加 16 进制数字’80’。如果长度已达 8 字节，转入第四步；否则，在其右边添加 16 进制数字’00’直到长度达到 8 字节。
- 对每一个数据块使用相应密钥进行加密。（密钥由 SMARTCOS 命令或中国金融 IC 卡专用命令所指定）
  如果该密钥长度为 8 字节，则依照图 9-1 的方式来加密数据块；
  如果该密钥长度为 16 字节，则依照图 9-2 的方式来加密数据块。
- 计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的 D1，加密后的 D2，等等）。并将结果数据块插入到命令数据域。



[注]：图中的8字节密钥均由FMCOS命令或中国金融IC卡专用命令所指定。

图 9-3 用长度为 8 字节的密钥进行数据加密的算法



[注]：图中的16字节密钥由FMCOS命令或中国金融IC卡专用命令所指定。

图 9-4 用长度为 16 字节的密钥进行数据加密的算法

8.4.2. 数据解密计算

数据解密计算步骤如下：

- 将命令数据域块分解成 8 字节长的数据块，标号为 D1，D2，D3，D4 等等。
- 对每一个数据块使用与数据加密相同的密钥进行解密。（密钥由 SMARTCOS 命令或中国金融 IC 卡专用命令所指定）
  如果该密钥长度为 8 字节，则依照图 3 的方式来解密数据块。
  如果该密钥长度为 16 字节，则依照图 4 的方式来解密数据块。
- 计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2，等等）链接在一起。数据块由 LD、明文数据、填充字符组成。
- 因为 LD 表示明文数据长度，因此，它被用来恢复明文数据。

图 9-5 用长度为 8 字节的密钥进行数据加密的算法

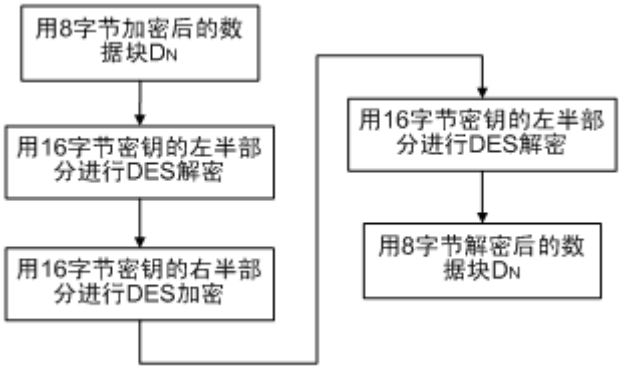


图 9-6 用长度为 16 字节的密钥进行数据加密的算法

8.5. 安全报文传送的命令情况

- CASE1：这种情况时，没有数据送到卡（Lc）中，也没有数据从卡中返回（Le）。

  没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2

  有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC

  CLA 的低半字节是’4’表明支持第二种情况的安全报文传送技术。Lc 为 MAC 的长度。

- CASE2：这种情况时，命令中没有数据送到卡中，但有数据从卡中返回。

  没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Le

  有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	MAC	Le

  CLA 的低半字节是’4’表明支持第二种情况的安全报文传送技术。Lc 为 MAC 的长度。

- CASE3: 这种情况时，命令中有数据传送到卡中，但没有数据从卡中返回。

  没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据

  有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC

  CLA 的低半字节是’4’表明支持第二种情况的安全报文传送技术。Lc 为 MAC 的长度。

- CASE4: 这种情况时，在命令中有数据送到卡中，也有数据从卡中返回。

  没有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	Le

  有安全报文传送要求的命令情况如下：

CLA	INS	P1	P2	Lc	命令数据	MAC	Le

  CLA 的低半字节是’4’表明支持第二种情况的安全报文传送技术。Lc 为 MAC 的长度。

附录A. 电子存折/电子钱包应用的基本数据文件

表 A-1 电子存折和电子钱包应用的公共应用基本数据文件

文件标识符	‘0015’	
文件类型	‘A8’（线路保护的二进制文件）	
文件主体空间	‘1E’	
读权限	‘F0’（自由读取）	
写权限	‘F0’（写二进制时必须使用 DAMK 进行线路保护，如连续三次执行此命令失败，IC 卡回送‘9303’即应用永久锁定）	
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	发卡方自定义文件控制信息数据	2

表 A-2 电子存折和电子钱包应用的持卡人基本数据文件

文件标识符	‘0016’	
文件类型	‘A8’（线路保护的二进制文件）	
文件主体空间	‘27’	
读权限	‘F0’（自由读取）	
写权限	‘F0’（写二进制时必须使用 DAMK 进行线路保护，如连续三次执行此命令失败，IC 卡回送‘9303’即应用永久锁定）	
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
23-38	持卡人证件号码	16
39	持卡人证件类型	1

表 A-3 电子存折和电子钱包应用的交易明细文件

文件标识符	‘0018’	
文件类型	‘2E’（循环文件）	
记录个数	‘0A’（该循环文件必须能够容纳至少十条消费、取现、圈存、圈提交易 记录）	
记录长度	‘17’	
读权限	‘F1’（必须先验证口令）	
写权限	‘EF’（交易明细由 IC 卡维护，不允许外部对其修改）	
字节	数据元	长度
1-2	电子存折/电子钱包联机或脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标识	1
11-16	终端机编号	6
17-20	交易日期	4
21-23	交易时间	3

附录B. 术语和定义

- 终端 Terminal
  为完成卡片操作而安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。
- 命令 Command
  终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。
- 触点 Contact
  在集成电路卡和外部接口设备之间保持电流连续性的导电元件。
- 响应 Response
  IC 卡处理完成收到的命令报文后，返回给终端的报文。
- 集成电路 Integrated Circuit（IC）
  设计用于完成处理和/或存储功能的电子器件。
- 集成电路（IC 卡）Integrated Circuit（s） Card
  内部封装一个或多个集成电路的 ID - 1 型卡。
- 报文 Message
  由终端向卡或卡向终端发出的，不含传输控制字符的字节串。
- 报文鉴别代码 Message Authentiction Code
  对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。
- 半字节 Nibble
  一个字节的高四位或低四位。
- 明文 Plaintext
  没有加密的信息。
- 密文 Ciphertext
  通过密码系统产生的不可理解的文字或信号。
  密钥 Key
  控制加密转换操作的符号序列。
- 加密算法 Cryptographic Algorithm
  为了隐藏或揭露信息内容而变换数据的算法。
- 安全状态及安全状态寄存器
  安全状态是指卡在当前所处的一种安全级别。SMARTCOS 的根目录和应用目录分别具有 16 种不同的安全状态。SMARTCOS 在卡内部用两个 4 位寄存器来表示安全状态：一个寄存器称为 MF 的安全状态寄存器，它表示整个卡所处的安全级别；另一个寄存器为当前目录的安全状态寄存器，每个寄存器的值可以是 0 至 F 之间的某一值。
- 安全属性
  安全属性是指对某个文件进行某种操作时所必须满足的条件，也就是在进行某种操作时要求安全状态寄存器的值是什么。
- 数据完整性 Data Integrity
  数据不受未经许可的方法变更或破坏的属性。
- 密钥文件 Key File
  密钥文件必须在 MF/DF 下最先被建立，且一个目录只能有一个密钥文件，密钥文件可存多个口令密钥、外部认证密钥、DES 运算密钥，每个密钥为一条 TLV 格式的记录。
- 文件标识符 File Identifier
  文件标识符是文件的标识代码，用 2 个字节来表示，在选择文件时只要指出该文件的

标识代码，SMARTCOS 就可以找到相应文件，同一目录下的文件标识符必须是唯一的。MF 的文件标识符是 3F00，文件名为 1PAY.SYS.DDF01。

- 电子存折 Electronic Deposit
  一种为持卡人进行消费、取现等交易而设计的使用口令密钥（PIN）保护的金融 IC 卡应用。它支持圈存、圈提、消费、取现等交易。
- 电子钱包 Electronic Purse
  一种为方便持卡人小额消费而设计的金融 IC 卡应用。它支持圈存、消费以及查询余额交易。除圈存交易外，使用电子钱包进行的任何交易均不记录交易明细，且无需验证口令（PIN）。
- 圈存 Load
  持卡人将其在银行相应帐户上的资金划转到电子存折或电子钱包中。圈存交易必须在金融终端上联机进行。
  一般情况下，圈存到电子存折中的资金计付活期利息，圈存到电子钱包中的资金不计付利息。但具体作法由发卡方自行决定。
- 圈提 Unload
  持卡人将电子存折中的部分或全部资金划回到其在银行的相应帐户上。圈提交易必须在金融终端上联机进行。
- 消费 Purchase
  消费交易允许持卡人使用电子存折或电子钱包的余额进行购物或获取服务。此交易可以在销售点终端（POS）上脱机进行。使用电子存折进行的消费交易必须提交个人密码（PIN），使用电子钱包则不需要。
- 取现 Cash Withdraw
  取现交易允许持卡人从电子存折中提取现金。此交易必须在金融终端上进行，但可以脱机处理。只有电子存折应用支持此交易，且必须提交个人密码 PIN。
- 透支限额 Overdraw Limit
  “透支功能”是一种基于电子存折应用的有限信用功能。当电子存折中的实际金额不足时，它为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。修改透支限额交易必须在金融终端上联机进行，且必须提交个人密码 PIN。