SmartCOS®用户手册

Version 3.3

深圳市思创莱电子技术有限公司

2000 年 4 月

目　　录

（REV1-2001/11/08）

前　　言

随着电子技术的发展，集成电路（IC）卡的应用得到了社会各界的广泛重视。中国人民银行也于 1997 年 12 月 18 号版布了《中国金融集成电路（IC）卡规范》和《应用规范》，以促进集成电路（IC）卡在国内应用的规范化，保证国内的应用在国际上的兼容性、先进性、独立性。作为国内制卡行业的先锋，深圳市明华澳汉磁卡（IC 卡）系列有限公司开发出了符合《规范》及 ISO/IEC 7816 的、具有自主版权的 SmartCOS V3.3 以支持《规范》，提高集成电路（IC）卡在国内的应用和开发水平，为振兴民族产业作出一份贡献。

明华公司也希望国内外在芯卡操作系统领域有一定见解的专家、学者及同行和我们共同探讨、交流，从而提高国内芯卡操作系统的应用、开发水平。

1、SmartCOS V3.3 简介

1.1、 应用领域

SmartCOS V3.3 有如下特点：

1. 符合《中国金融集成电路（IC）卡规范》、《中国金融集成电路（IC）卡应用规范》。
2. 数据文件支持二进制文件、定长记录文件、变长记录文件、循环定长记录文件。
3. 支持符合银行规范的电子钱包、电子存折功能。
4. 支持 DES、Triple DES 等加密算法，并支持用户特有的安全加密算法的下载。
5. 支持线路加密、线路保密功能，防止通信数据被非法窃取或篡改。
6. 可用作安全保密模块，使用过程密钥实现加密、解密。
7. 支持符合 ISO-7816-3 标准的 T=0 通讯协议。
8. 卡片支持多种容量选择,可选择 2K、4K、8K、16K 字节的 EEPROM 空间。
9. 安全机制使用状态机，并支持 PIN 检验、KEY 认证、数据加密、解密、MAC 验证。
10. 满足个别需求，SmartCOS 可根据特殊行业的特殊用户的需求定制。
11. 支持防插拔功能。
12. 支持命令下载及用户自定义算法的下载。
13. 卡片支持休眠模式，降低功耗。

1.2、 内部结构

SmartCOS 的内部结构组成如下：CPU 及加密逻辑、RAM、ROM、EEPROM 及 I/O 五部分组成，是一个完整的计算机安全体系。用户数据放在被加密逻辑保护的 EEPROM 中，COS 掩膜在 ROM 中，保证代码安全。COS 将用户的过程密钥生成后放在 RAM 空间中，掉电后自动丢失，保证其安全性。

1.3、 功能模块化划分

SmartCOS V3.3 的基本操作方式为：从接口设备接收一条命令，然后经过处理返回应答信息给接口设备。其处理过程如下图所示：

命令处理过程：

传输管理器 ⇒ 加密运算器 ⇒ 命令解释器 ⇒ 文件管理器

命令应答过程：

传输管理器 ⇐ 加密运算器 ⇐ 命令解释器 ⇐ 文件管理器

每条命令的处理都要经过上述四个模块，如果其中的任意一个模块在处理中发现错误都将返回相应的出错信息。

1.3.1、 数据传输

传输管理器负责智能卡和接口设备之间的数据通信，接收过程中要处理对输入数据的缓冲，响应过程控制数据的发送。通信使用的协议是 ISO7816-3 所规定的 T=0 的异步半双工字符传输协议。

当接口设备给卡上电之后，首先由卡发送一个遵守《中国金融集成电路（IC）卡规范》的复位应答信息（ATR）给接口设备，然后接口设备发送命令头来启动命令处理过程。传输管理器在正确地接收到命令后交给下一个功能模块进行处

理，最后还要把该命令的执行结果返回给接口设备。

1.3.2、 保密通信

数据在传输方式上有三种类型：明文方式、明文校验方式和密文校验方式。对以明文方式进行传输的数据由传输管理器直接送给命令处理模块。当数据以校验或密文校验方式传输时需要加密运算器对数据做处理。

1.3.3、 命令解释

命令解释器对外部输入的每条命令做语法分析，分析和检查命令参数是否正确，然后根据命令参数的含义执行相应的功能模块。如果发现参数有错，将从该模块直接返回错误信息。

1.3.4、 文件管理器

文件管理控制对文件的操作和访问。在做数据操作前，文件管理器将根据文件的安全属性检查卡的安全状态，以确定操作的可行性。文件的安全属性和文件结构一旦产生便处于文件管理器的控制之下。

对文件数据的操作和管理将按照如下的规则：

1．对某个文件做操作之前，必须先选择该文件。

2．文件系统的三层结构，并且操作系统不支持以路径方式选择文件，所以在选择某个文件前必须先选择它的上一层文件，不允许跨层选择。卡片上电后自动选择主控文件。

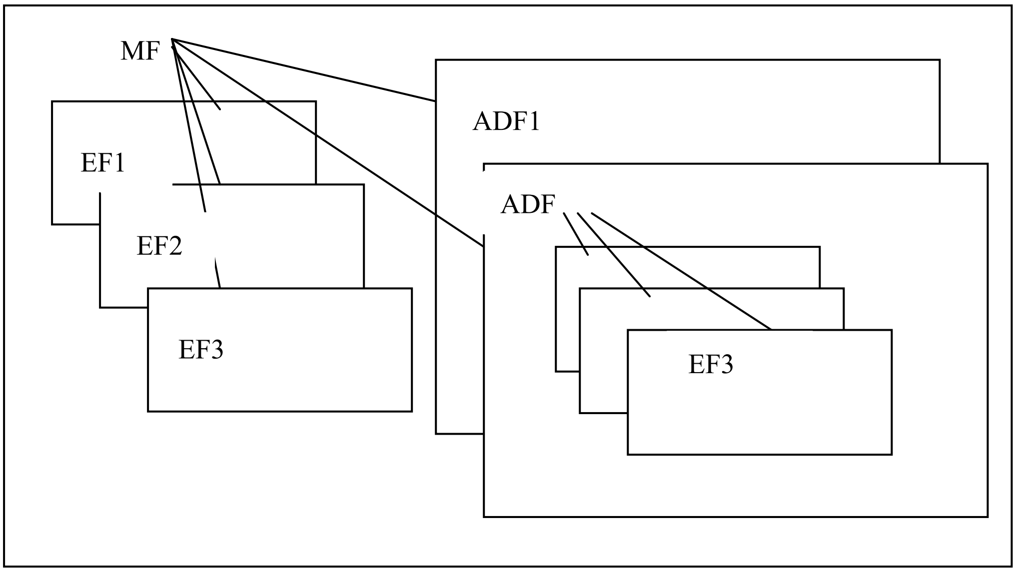
3．访问文件中的数据要受文件的安全属性的控制。

4．对文件的建立要受该文件所属的上层文件的安全属性的控制。

2、文件系统

2.1、 文件系统的组织结构

SmartCOS V3.3 的文件系统是完全遵照《中国金融集成电路 IC 卡规范及应用规范》和 ISO/IEC 7816-4 来组织的，具体的层次结构如下图所示：



1. 主控文件(Master File , MF)

主控文件是整个文件系统的根（可看做根目录），每张卡有且只有一个主控文件。它是在卡的个人化过程中首先被建立起来的，在卡的整个生命周期内一直存在并保持有效，可存储卡的公共数据信息并为各种应用服务。由个人化建立起来的主控文件包括文件控制参数以及文件安全属性等信息。在物理上，主控文件占有的存储空间包括 MF 文件头的大小以及 MF 所管理的 EF 和 DF 的存储空间。

2. 专用文件(Dedicated File，DF)

在 MF 下针对不同的应用建立起来的一种文件，是位于 MF 之下的含有 EF 的一种文件结构（可看做文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据。

DF 由创立文件命令建立。它的大小在建立后被确定，此后不能更改。对 DF 的建立操作由 MF 的安全属性控制。

在 DF 下面不可再建立子 DF，只能建立 EF

为了保证各个 DF 的相互独立，只能从文件系统的 MF 层次选择一个 DF，对 DF 下的数据进行的操作由各当前应用系统的状态机控制。

3. 基本文件(Elementary File，EF)

基本文件存储了各种应用的数据和管理信息，它存在于 MF 和 DF 下。EF 从存储内容上分为两类：安全基本文件和工作基本文件。

安全基本文件(Secret Elementary File，SEF)的内容包含用于用户识别和与加密有关的保密数据(个人识别码、密钥等)，卡将利用这些数据进行安全管理。SEF 要在 MF 或 DF 建立后，才能建立。建立后每个 KEY 都可以定义不同的修改权限和使用权限。安全基本文件的内容不可被读出，但可使用专门的指令来写入和修改。在 MF 和每个 DF 下只能建立 1 个安全基本文件，但每个文件中的 KEY 和 PIN 的类型由用户指定。

工作基本文件(Working Elementary File，WEF)包含了应用的实际数据，其内容不被卡解释。在符合 WEF 的读、修改安全属性时，可对其内容进行读取、修改。工作文件的个数和大小受到 MF 或 DF 所拥有空间的限制。

整个文件系统的空间在 MF、DF 和 EF 建立时被分配和确定，以后在物理上不会发生变化。当访问 EF 时，必须先选择相应的 MF 或 DF。

可以从文件系统的任何位置选择 MF。

2.2、 基本文件结构

根据 ISO/IEC 7816-4 和《中国金融集成电路 IC 卡规范及应用规范》有关基本文件结构的定义，SmartCOS V3.3 支持下列四种基本文件结构：

1. 二进制结构

二进制文件为一个数据单元序列，数据以字节为单位进行读写，其中的数据结构则由应用解释。

2. 线性定长记录文件结构

这种结构以固定的长度来处理每条记录。通过逻辑上连续的记录号，可访问这类记录，记录号的范围是 1 至 254，记录长度最长为 110 字节。每次访问只对一条记录进行操作，而且必须严格遵守记录长度的规定。

3. 线性变长记录文件结构

在这类结构中，每条记录的长度可以各不相同。仍然是以记录号来访问各条记录。在读取和修改记录时，操作与线性定长记录的相同。但是，添加记录时，记录的长度不能超过最大记录长度（110 字节）的规定。

4. 循环定长记录文件结构

这是一类特殊的定长记录文件结构。在逻辑上，这类文件可看作一个环形记录队列，记录按照先进先出的原则存储。添加记录时，最新一次写入的记录的记录号为 1，上一次写入的记录的记录号为 2，依次类推。记录的个数与预留的记录空间的大小以及记录的长度相关，记录个数=记录空间大小整除记录长度。

此外还有一些只能特殊使用的文件类型，如 ATR、钱包文件、存折文件、密钥文件等，但其文件结构也不超除以上四种文件的类型。

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 3F00 或其文件名来选择 MF

专用文件 DF

通过文件名或文件标识符来选择 DF，在 MF 下可以选择任意 DF。如果当前文件是一个 DF 下的一个 EF，同样可以通过选择 DF 的文件标识符或文件名来选择任意 DF。

二进制文件

在满足读条件时可使用 Read Binary 读取，在满足写条件时可用 Update Binary 来更改二进制文件的内容。

定长记录文件

在满足读条件时可使用 Read Record 读取，在满足写条件时，若记录未满则用 Append Record 增加新记录，若记录已满则用 Update Record 来更改指定记录的内容。

循环定长记录文件

在满足读条件时可使用 Read Record 读取，在满足追加条件时可使用 Append Record 在文件末尾追加一个记录，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。

变长记录文件

在满足读条件时可使用 Read Record 读出记录，在满足写条件时若记录未满则用 Append Record 增加新记录，若记录已满则用 Update Record 来更改指定记录的内容。变长记录文件的格式为 TLV 格式，Tag 为 1 字节的记录标识，L 为 1 字节的记录数据长度，V 为 L 字节的数据值。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不大于原来的整个记录长度相等，否则将返回错误码 67 00。

ATR 文件是存在于 MF 下的一个二进制文件，其内容是卡上电复位信息。如果不建立，则上电复位返回 SmartCOS 的缺省值。

KEY 文件及其文件中的密钥

每个 DF 或 MF 下有且只有一个 KEY 文件，在任何情况下密钥均无法读出。一旦离开该目录该目录下的所有权限将全部丢失。

在 KEY 文件中可存放多个密钥，每个密钥为一条定长记录，每条记录长度为 25 字节。记录中规定了其标识、版本、算法、属性及密钥本身等相关内容。

在满足 KEY 文件的增加权限时可用 Write KEY 命令增加一条记录；只有在

满足某个密钥的使用权限时才可以使用该密钥;在满足某个密钥的修改权限时才可以修改该密钥。

每种密钥具有其独立性,用于一种特定功能的密钥不可作为它用。SmartCOS V3.3 支持以下几种密钥:

个人密码(PIN)、外部认证密钥,内部认证密钥、Crypt 密钥、PIN 解锁密钥、PIN 重装密钥、应用维护密钥、消费取现密钥、圈存密钥、TAC 密钥、圈提密钥、更新透支限额密钥、及与以上各种密钥对应的 SAM 主密钥。

2.4、 文件的空间结构

SmartCOS V3.3 整个的文件空间划分如下:

当你建立完 MF 之后,SmartCOS 自动将整个 EEPROM 空间都分配给它。MF 的文件头长度为 10 个字节+文件名长度(5-16 个字节)。

每个 DF 所占空间=DF 文件头空间(等同于 MF)+DF 下所有的文件空间之和。

二进制结构文件的空间=文件头空间(10 个字节)+EF 所申请的空间。

定长记录和循环定长记录文件的空间=文件头空间(10 个字节)+记录数 X 记录长度。

变长记录结构文件的空间=文件头空间(10 个字节)+建立时申请的空间。

安全基本文件的空间=文件头空间(10 个字节)+密钥个数 X(25 个字节)

钱包文件的空间=文件头(10 个字节)+文件体(17 个字节)

存折文件的空间=文件头(10 个字节)+文件体(20 个字节)

2.5、 文件类型、密钥类型及相关命令

MF 在个人化的过程中首先被建立,且文件标识符固定为 3F 00,在其建立之后,如果要建立自己的复位信息文件(ATR 文件)则必须首先被建立,长度

最大为 10 个字节，其内容必须符合人行规范和 ISO/IEC 7816-4，否则某些终端可能不能识别，其后建立的必须是安全文件。在 DF 下首先被建立的是安全文件。

关于 **EF** 文件头中状态字节的定义

B7	B6	B5	B4	B3	B2	B1	B0	状态
				0	0	0	0	二进制
				0	0	0	1	定长记录
				0	0	1	0	循环定长
				0	0	1	1	变长记录
				0	1	0	0	ATR 文件
				0	1	0	1	密钥文件
				0	1	1	0	钱包文件
				0	1	1	1	存折文件
				1	0	0	0	特殊类型二进制文件
0	0							数据以明文
0	1							数据以明文+MAC 形式写入
1	0							数据以密文形式写入
1	1							数据以密文+MAC 形式写入

密钥类型如下：

KEY 类型	该类型 **KEY** 作用描述
00	消费取现密钥
01	圈存密钥
02	TAC 密钥
03	圈提密钥
04	修改透支限额密钥
05	应用维护密钥，用于产生应用锁定、应用解锁、卡片锁定、卡片锁定和读、更新二进制、记录命令的 MAC
06	PIN 解锁密钥，用于产生解锁 PIN 的 MAC
07	PIN 重装密钥，用于产生重装 PIN 的 MAC
08	外部认证密钥，用于外部认证过程
09	内部认证密钥，用于内部认证过程
0A	Crypt 密钥，应用于安全模块指令和增加修改密钥命令
0B	个人密码（PIN），用于个人密码校验
0C	超级 PIN，用于解锁、修改 PIN
40	SAM 密钥
80	用户自定义类型
其它	系统保留

对于 MF 下的个人 PIN 和外部认证 KEY，如果最高位置一，表示为全局 PIN

或全局外部认证 KEY，其后续状态与其它 KEY 的后续状态为或的关系，且全局 PIN 和全局外部认证 KEY 两者的后续状态互为或的关系。

全局 **PIN** 或全局外部认证 **KEY** 说明如下：

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
1				1	0	0	0	全局外部认证 KEY
1				1	0	1	1	全局 PIN
X				X	X	X	X	其余类型密钥保留

相关性参见下页表：

	主控文件MF	专用文件DF	二进制文件(00)	定长记录(01)	循环文件(03)	变长文件(02)	ATR文件(04)	钱包文件(06)	存折文件(07)	安全文件(05)
Create File	√	√	√	√	√	√	√	√	√	√
Write KEY										√
Read Binary			√				√			
Update Binary			√				√			
Read Record				√	√	√				
Append Record				√	√	√				
Update Record				√		√				
Select File	√	√	√	√	√	√	√			
Credit For Load								√	√	
Debit For Purchase/Case Withdraw								√	√	
Debit For Unload									√	
Get Balance								√	√	
Update Overdraw Limit									√	

2.6、 文件短标识符与文件名称

文件短标识符是文件的标识代码，用 1 个字节的低五位来表示，在使用短标识符选择文件时只要指出该文件的标识代码，同一个目录下的文件标识符必须是唯一的。MF 的文件标识符是 3F00，文件名自定义，符合银行规范名称应该是 1PAY.SYS.DDF01。

短文件标识符可以通过Read Binary、Update Binary命令的参数P1来实现文件的选择：若P1的高三位为100，则低5位为短文件标识符。例如：若P1为81H，即100<u>00001</u>，其中高三位为100，则所选的文件标识符为00001，十六进制文件标识表示为00 01。

短文件标识符选择还可以通过Read Record、Update Record命令参数P2来实现文件的选择，方法是若P2的高五位不全为0，低五位为100，则高五位为短文件标识符。对于命令Append Record低五位为000来表短文件标识符。

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为 31，若文件需要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之间。

3、SmartCOS的安全系统

SmartCOS 的安全体系有以下几个阶段：在芯片制造商完成芯片的制造后，SmartCOS 处于未初始化状态，卡片制造厂商封装完成后进行卡片初始化和检测，此时 SmartCOS 处于初始化阶段，初始化和检测完成后 SmartCOS 该卡处于未个人化阶段。将卡提交给发卡方后，发卡方需正确地使用个人化密钥后才能个人化，这样可保证卡在运输过程中的安全。个人化开始后 SmartCOS 处于个人化阶段，这个过程中发卡方设计自己应用的安全体系并下装到卡中，当个人化过程结束后，SmartCOS 将在发卡方规划的安全体系的保护下对《规范》和 ISO/IEC7816-3/4 中的指令进行解释和执行。

在进行安全体系的规划过程中须理解 SmartCOS V 安全体系的以下几个概念：状态机、安全属性和状态机的关系、状态机跳变机制、和密码算法。

3.1、 状态机

状态机又称安全状态，是指卡在当前所处的一种安全级别，卡的主控目录和当前应用目录分别具有 16 种不同的安全状态。在卡内部用一个寄存器的高四位表示主控目录的安全状态，其表示整个卡所处的安全级别。寄存器低四位表示当前应用的安全状态。安全状态共 16 种，即 0-F 种的一种。主控目录的安全状态复位后为 0，应用目录的改变不改变主控目录的安全状态，只有主控目录下的口令核对或外部认证才能改变主控目录的安全状态。

当前应用的安全状态在被成功地选择或复位后自动清为 0。只能用当前应用的口令核对或外部认证才能改变当前应用的状态。如当前的目录为 MF，则当前应用的安全状态等于主控目录的安全状态。

3.2、 安全属性和状态机的关系

安全属性是指对某个文件进行某种操作时必须达到的状态机，采用一字节

存储。其又称访问权限，一种访问权限是在建立该文件时指定的。SmartCOS 的访问权限具有其独特性，是一个状态机区间来描述一种权限的。比如描述一个文件的读权限的高 4 位为 X，低 4 位为 Y，则其访问权限为：当前应用的状态机 M 必须满足：X=<M=<Y。

因此，若要定义一种永远不能获得的权限的方法为，定义该安全属性为 XY(X>Y),即可。

如果定义一种权限可自动获得则定义该权限为 0X 即可。因为复位后的主控文件和成功选择后的应用的安全状态都为 0，0 是一种自动获得的状态机。

3.3、 状态机跳变机制

SmartCOS V3.3 通过核对口令和外部认证两种方法来实现状态机的转变，核对口令只在 DF 下有效。特别指出的是状态机不存在级别高低，同样的操作可定义为任意的状态机，即你可以用一种改变状态机的手段来实现从任一种状态机到另外任一种状态机的转变，即可以从 0 转变为 F，也可从 F 转变为 0。

3.4、 密码算法

SmartCOS V3.3 支持 Single DES、Triple DES 算法。算法完全遵照《中国金融集成电路(IC)卡规范及应用规范》，所以关于该算法的使用方法请参考《中国金融集成电路(IC)卡规范及应用规范》即可。

本手册第 7 部分也对密码算法作了陈述。

4、复位应答

对于 T=0 通讯协议的卡，在个人化时没有建立 ATR 文件，则缺省的复位应答信息如下表：

符号	字节内容	内容解释
TS	3B	正向约定
T0	6C	TB1 和 TC1 存在，历史字符为 12 个
TB1	00	无需额外的编程电压
TC1	02	需 2 个额外的保护时间
T1-TC	XX	历史字符

SmartCOS 历史字符的特定意义：

符号	字节内容	内容解释
T1	XX	SmartCOS 的版本号
T2	XX	卡状态字节
T3	86	明华公司 IC 卡制造机构标识号
T4	38	
T5-TC	XX	卡唯一序号

卡状态字节描述如下：

B7	**B6**	**B5**	**B4**	**B3**	**B2**	**B1**	**B0**	**状态**
0 1 1	X X X	X X X	0 0 1	X X X	X X X	X X X	X X X	该卡已初始化，并成功 该卡未被初始化 该卡初始化过程被锁
0	0	0	0	0	0	X	X	该卡未个人化
0	0	1	0	X	X	X	X	该卡个人化未结束
0	1	1	0	X	X	X	X	该卡个人化成功
0	0	0	1	X	X	X	X	该卡个人化没有成功，卡被锁
0	1	1	1	X	X	X	X	该卡个人化成功，卡被锁

T0 说明：

T0 字符的高半字节有效位 B8 B7 B6 B5，当相应的位为 1 时，分别表示后续接口字符 TD1、TC1、TB1、TA1 存在；字符的低半字节 B4B3B2B1 表示历史字符的个数 0-15。

例如：T0=6C

6（0110）：表示接口字符 TB1、TC1 存在；

C：表示后续有 12 个历史字符；

TD1 说明：

TD1 字符的高半字节有效位 B8B7B6B5,当相应的位为 1 时，分别表示后续接口字符 TDi、TCi、 TBi、TAi 存在；B4B3B2B1 表示后续发送的协议类型：0 为 T=0 协议；1 为 T=1 协议。

5、基本命令集

5.1、 命令与应答机制

智能卡与接口设备之间使用命令与应答的通信机制，即接口设备发送命令，智能卡接收并处理后发送响应给接口设备。这种机制包括两种数据单元——命令应用数据单元与响应应用数据单元。

命令应用数据单元包含两部分：固定的四个字节命令头和长度可变的命令体，其内容参见如下表格：

命 令 头				命 令 体		
CLA	INS	P1	P2	Lc	数据域	Le

CLA 字节指出命令的类型。如下表所述：

B7	B6	B5	B4	B3	B2	B1	B0	定 义
1 0								外部命令 内部命令
				1 0				安全报文传送 不附加安全报文件传送

INS 字节表示命令编码，P1 和 P2 为具体命令参数。

Lc 字节表示数据的长度，只有一个字节表示，取值范围为 1-110。如果 Lc 为 0 表示没有数据域。

Le 表示期望卡返回的数据长度，由单字节表示，取值范围 1-110。

响应应用数据单元也包括两部分：可能存在的响应数据体（应答体）和两个状态字节（应答尾部），如下表所示：

应答体	应答尾部	
响应数据体	SW1	SW2

5.2、 命令与应答编码

命令分为内部命令和外部命令两类，下面表格显示了命令的编码：

命令	指令类别	编码	用途	兼容性
Create File	80	E0	建立文件	Δ
Write KEY	80/84	D4	增加或修改密钥	Δ
Read Binary	00	B0	读二进制	√ *
Update Binary	04	D6	修改二进制	√ *
Read Record	00	B2	读记录	√ *
Append Record	00	E2	追加记录	*
Update Record	00	DC	修改记录	√ *
Select File	00	A4	选择文件	√ *
Credit For Load	80	52	圈存	√
Debit For Purchase/Case Withdraw	80	54	消费/取现	√
Debit For Unload	80	54	圈提	√
Get Balance	80	5C	读余额	√
Get Transaction Prove	80	5A	取交易认证	√
Initialize For Case Withdraw	80	50	取现初始化	√
Initialize For Load	80	50	圈存初始化	√
Initialize For Purchase	80	50	消费初始化	√
Initialize For Unload	80	50	圈提初始化	√
Initialize For Update	80	50	修改初始化	√
Update Overdraw Limit	80	58	修改透支限额	√
Application Block	84	1E	应用锁定	√
Application Unlock	84	18	应用解锁	√
Card Block	84	16	卡片锁定	√ *
External authentication	00	82	外部认证	√ *
Get Challenge	00	84	产生随机数	√ *
Get Response	00	C0	取响应	√ *
Internal Authentication	00	88	内部认证	√ *
Pin Change/Unblock	84	24	修改/解锁 PIN	√
Verify	00	20	校验 PIN	√ *
Change PIN	80	5E	修改 PIN	√
Reload PIN	80	5E	重装 PIN	√
Crypt	80	F6	安全模块指令	Δ
Generate KEY	80	FA	生成过程密钥	Δ

√ 表示遵照《中国金融集成电路（IC）卡规范》和《中国金融集成电路（IC）卡应用规范》。

* 表示遵照《规范》和 ISO/IEC 7816-3/4。

Δ 表示为自定义指令。

下表列出了一部分不针对具体命令的应答尾部状态字节（SW1、SW2）的编码定义，在以后对具体命令的描述中再列出与各个命令相关的状态字节。

正常返回码：

状态码	含义说明
90 00	正常结束
61 XX	正常结束，仍有 XX 个有效数据可取

错误或警告返回码

状态码	含义说明
63 CX	剩余尝试次数
65 81	写 EEPROM 失败
67 00	数据长度错误
69 01	无效的状态
69 81	文件类型不匹配
69 82	安全状态不满足
69 83	密钥已经被锁住
69 85	使用条件不满足
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
6A 82	没有找到文件
6A 83	没有找到记录
6A 84	没有足够的空间
6A 86	P1，P2 参数不正确
6B 00	参数错误（偏移地址超出了 EF 文件长度）
6D 00	不正确的 INS
6E 00	不正确的 CLA
6F 00	未定义的错误
93 02	MAC 无效
93 03	应用永久锁定
94 01	金额不足
94 03	密钥索引不支持
94 06	所需 MAC 不可用

6、命令描述

本章将对集中对每条命令的功能、使用条件、命令格式及其参数、响应格式及其参数做详细的描述，其中各命令参数及响应参数的编码均为十六进制。

6.1、 Create File 建立文件

1）.定义和范围

Create File 命令用于建立 MF 文件、DF 文件和 EF 文件。

当建立 MF 文件时，卡片必须为空，卡片首先验证制造商密钥，通过后把主控文件（MF）的数据写入 EEPROM。

建立 DF 文件时，只有 MF 存在且有足够的空间，并且满足当前建立文件的安全条件，MF 没有被锁住，才可建立 DF。

建立 EF 文件时，只有卡空间>EF 文件头+文件体，并且满足当前建立 EF 文件的安全条件才可建立 EF。

2）.命令报文

Create File 的命令报文如下：

代码	值
CLA	80
INS	E0
P1	00-- 建立 MF 01-- 建立 DF 02-- 建立 EF
P2	00-- 正在建立 01-- 建立结束（MF、DF）
Lc	文件信息长度
DATA	文件信息

3）.命令报文数据域

文件信息及其长度在建立不同类型的文件分别描述如下：

①建立 MF 文件时数据域的信息

Lc	有关文件信息			
0F/1A	传输代码 (8 字节)	建立文件权限(1 字节)	短文件标识符 (1 字节)	MF 的名称 (05-10）

8 个字节的传输代码是由工厂在卡片制造时设定的，如用户无特殊要求，则为：FF FF FF FF FF FF FF FF，在建立 MF 时，若传输代码错误，则内部错误计数器加一，超过 4 次卡片自动锁死不可再用。

短文件标识符指明 MF 下的应用列表文件，该文件是一个变长的记录文件，有效表示为该字节的高三位为 000，低 5 位为短文件的标识符。无列表文件填 00。

如果建立银行应用，则 MF 必须取名为：1PAY.SYS.DDF01。

②建立 DF 文件时数据域的信息

Lc	有关文件信息			
09/14	文件标识符(2 字节)	建立文件权限(1 字节)	00	DF 的名称 (05-10 字节)

③建立 EF 文件时数据域的信息

Lc	有关文件信息					
07	文件标识符 (2 字节)	文件类型 (1 字节)	权限 1 (1 字节)	权限 2 （1 字节）	Len1 (1 字节)	Len2 (1 字节)

文件类型说明见下表：

文件类型								类型描述
B7	B6	B5	B4	B3	B2	B1	B0	状态
				0	0	0	0	二进制
				0	0	0	1	定长记录
				0	0	1	0	循环定长
				0	0	1	1	变长记录
				0	1	0	0	ATR 文件
				0	1	0	1	密钥文件
				0	1	1	0	钱包文件
				0	1	1	1	存折文件
				1	0	0	0	特殊类型二进制文件
0	0							数据以明文或密文+MAC 形式写

文件类型								类型描述
B7	**B6**	**B5**	**B4**	**B3**	**B2**	**B1**	**B0**	**状态**
				0	0	0	0	二进制
				0	0	0	1	定长记录
				0	0	1	0	循环定长
				0	0	1	1	变长记录
				0	1	0	0	ATR 文件
				0	1	0	1	密钥文件
				0	1	1	0	钱包文件
				0	1	1	1	存折文件
				1	0	0	0	特殊类型二进制文件
								入
0	1							数据以明文+MAC 形式写入
1	0							数据以密文形式写入
1	1							数据以密文+MAC 形式写入

注：二进制文件类型为 00 时，数据也可以以密文+MAC 形式写入。类型为 08 时，表示为特殊类型二进制文件，数据可以明文+MAC 的形式写入。

权限 1、权限 2 说明如下：

①对于基本工作文件，权限 1 指明读权限，权限 2 指明更新权限；

②对于密钥文件，权限 1 指明增加新密钥的权限，权限 2 为 80H，则表示密钥需要以密文加上 MAC 码的形式写入（卡片内部将此字节清零，并将文件类型字节的第四位置 1）。

③对于钱包文件、存折文件的权限 1、权限 2 系统保留。

Len1 、Len2 说明如下：

①对于二进制文件、变长记录文件，Len1 和 Len2 两字节表示文件长度。文件长度应大于 00H,小于等于 7FFFH。

②对于 ATR 文件，Len1 和 Len2 两字节表示文件长度。文件长度应大于 00H,小于等于 000BH。

③对于定长记录文件、循环定长记录文件，Len1 指明记录数，Len2 指明记录长度。Len1 不能为零，Len2 不能超过 110 个字节。

④对于密钥文件，Len1 指明记录数，Len2 系统保留。Len1 不能为零，Len2 系统自动设为 18H。

⑤对于钱包文件、存折文件 Len1、Len2 均为系统保留

⑥需特殊指明，如果用户要建立 ATR 文件，则无法获得该卡的唯一序列号。

⑦对以上系统保留的字节，建议用户填写 00。

4）.特殊说明

建立 MF、DF 文件分别对应着 Create End 命令，当 Create End 成功执行之后，文件的安全条件才会有效。在执行此命令之前 SmartCOS 一直处在个人化状态，即使卡重新复位，SmartCOS 也能继续上次的个人化过程，直到收到 Create End 指令。其格式分别为：

CreateEnd DF

代码	值
CLA	80
INS	E0
P1	01
P2	01
Lc	02
DATA	FID

CreateEnd MF

代码	值
CLA	80
INS	E0
P1	00
P2	01
Lc	02
DATA	3F 00

5）.响应报文数据域

响应报文数据域不存在。

6）.响应报文状态码

响应报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	数据长度错误
63 CX	允许传输代码错误次数
69 01	创建状态不满足
69 82	安全条件不满足
6A 80	标识符已存在

6A 81	功能不支持（文件不可建立在 MF 或 DF）
6A 82	文件未找到
6A 84	没有足够的空间
6A 86	P1 或 P2 参数不正确
6D 00	不正确的 INS
6E 00	不正确的 CLA

关于 PBOC 应用中特殊文件标识符的说明：

1. 对于银行应用，**ADF** 下的 **00 18** 在 **SmartCOS** 中用作交易明细文件的标识符，该文件是一个循环定长记录文件，用来记录每一个交易的相关数据，每条记录的长度必须为 **17H**，记录个数不能少于 **10** 条。建立电子钱包文件和电子存折文件后必须建立一个交易明细文件用来记录每一笔交易，如果没有该文件则交易将无法完成。

00 01 在 **SmartCOS** 中用于钱包文件。

00 02 在 **SmartCOS** 中用于存折

对于非银行应用的卡片，上述文件标识符用户可自行使用。

2. 在 **SmartCOS** 中，如果发卡方需要建立发卡方专用数据文件，则文件标识符必须为 **00 15**，该文件是一个类型为 **00** 的二进制文件，其长度不能超过 **46H**。

3. 在 **SmartCOS** 中，如果发卡方需要建立持卡人专用数据文件，则文件标识符必须为 **00 16**，该文件是一个类型为 **00** 的二进制文件。

6.2、 Write KEY 增加或修改密钥

1）.定义和范围

WRITE KEY 命令可向卡中装载或更新卡中已经存在的密钥，本命令可支持 8 字节或 16 字节的密钥，密钥写入可以是明文或密文的方式。

当本命令用于增加密钥时必须满足密钥文件的增加权限。

在密钥以密文方式装载前必须用 GET CHANLLEGE 命令从 IC 卡取一个 4 字节的随机数。

2）.命令报文

明文安装或修改 KEY 的命令报文如下：

代码	值
CLA	80
INS	D4
P1	00—安装密钥 01—修改密钥
P2	00
Lc	密钥信息长度
DATA	密钥信息

密文安装或修改 KEY 的命令报文如下：

代码	值
CLA	84
INS	D4
P1	00— （用于安装密钥） XX— 密钥类型 （用于修改密钥）
P2	00— （用于安装密钥） XX— 密钥标识（用于修改密钥）
Lc	数据长度
DATA	加密后的密钥信息+4 字节 MAC 码

注：当密钥类型和标识都为 00 时，如果密钥文件为空，则表示安装卡片（或应用）主控密钥。

3）.命令报文数据域

关于 KEY 文件头中状态字节的定义

B7	B6	B5	B4	B3	B2	B1	B0	状态
				0	1	0	1	密钥文件
0	0							密钥以明文形式写入
0	1							密钥以明文+MAC 形式写入
1	0							密钥以密文形式写入
1	1							密钥以密文+MAC 形式写入

①．明文形式的数据域信息

其中密钥信息如下：

密钥信息（8 个字节密钥头+密钥值）									
密钥头									密钥值
密钥标识(1)	版本号(1)	算法标识(1)	密钥用途(1)	使用权限(1)	后续状态(1)	修改权限(1)	初始错误计数(1/2)	当前错误计数(1/2)	(02-10)

[注]：

密钥标识符（KID）： 不能等于 00h 和 FFh，同类型密钥的标识符必须唯一。

版本号： 同类密钥的版本。

算法标识： 算法标识确省为 00，算法是 Triple DES，如果是 Single DES 则算法标识为 01，算法标识对 PIN 没有意义。如果用户在 SmartCOS-PSAM 中定义了自己的算法，此处必须指明算法为 08。对于其它值系统保留。

使用权限： 指使用某一密钥时所需满足的安全条件。

修改权限： 指用 Write KEY 指令修改某一密钥时所需满足的安全条件。

后续状态： 只对 PIN、和外部认证 KEY 有效。当口令核对成功或外部认证成功后，置卡片状态机为后续状态的低半字节。

错误计数器： 错误计数器的高半字节为初始错误计数，指明密钥可以连续错误的最多次数；错误计数器的低半字节为当前错误计数，指明当前还可允许的错误次数。如果连续错误的次数超过初始错误计数的值，密钥自动锁死。

SmartCOS 支持的密钥类型如下表所列：

KEY 类型	该类型 KEY 作用描述
00	消费取现密钥
01	圈存密钥
02	TAC 密钥
03	圈提密钥
04	修改透支限额密钥
05	应用维护密钥，用于产生应用锁定、应用解锁、卡片锁定、卡片锁定和读、更新二进制、记录命令的 MAC
06	PIN 解锁密钥，用于产生解锁 PIN 的 MAC
07	PIN 重装密钥，用于产生重装 PIN 的 MAC
08	外部认证密钥，用于外部认证过程
09	内部认证密钥，用于内部认证过程
0A	Crypt 密钥，应用于安全模块指令和增加修改密钥命令
0B	个人密码（PIN），用于个人密码校验
0C	超级密码
40	SAM 密钥
80	用户自定义类型
其它	系统保留

对于 MF 下的个人 PIN 和外部认证 KEY，如果最高位置一，表示为全局 PIN 或全局外部认证 KEY，其后续状态与其它 KEY 的后续状态为或的关系，且全局 PIN 和全局外部认证 KEY 两者的后续状态互为或的关系。

全局 PIN 或全局外部认证 KEY 说明如下：

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
1				1	0	0	0	全局外部认证 KEY
1				1	0	1	1	全局 PIN
X				X	X	X	X	其余类型密钥保留

说明：

每一个应用下只能有一个个人密码（PIN），PIN 的长度为 2～6 个字节，内容必须为 0～9 的数字（每半字节）。超级 PIN 在每一个目录下也唯一，长度为 2-8 字节，其余密钥的长度为 8 或 16 个字节。

②. 明文+MAC 形式的数据域信息

明文密钥信息	4 字节 MAC

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

——密钥标识

——密钥版本号

——算法标识

——密钥类型

——使用权限

——后续状态

——修改权限

——错误计数器

——密钥值

加密和 MAC 计算的方法遵循《中国金融集成电路（IC）卡规范》。生成 MAC 码的初始值为：4 个字节的随机数+00 00 00 00。

③．密文形式的数据域信息

加密后的密钥信息	4 字节 MAC

密文安装密钥说明：

在使用密文形式进行安装密钥时，P1、P2 必须为零，命令报文数据域包括要装载的密钥密文信息和 MAC。

密文形式的数据域信息：

密钥密文信息使用主控密钥对以下数据加密（按所列顺序）产生的：

——数据长度

——密钥标识

——密钥版本号

——算法标识

——密钥类型

——使用权限

——后续状态

——修改权限

——错误计数器

——密钥值

在 MF 下装载密钥的控制过程为：

——卡片主控密钥在卡片传输密钥的控制下装载。

——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。

在 DF 下装载密钥的控制过程为：

——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。

SmartCOS 规定：密钥标识为 01 的外部认证密钥为主控密钥。应用下的其他密钥均由应用主控密钥加密安装。对密钥信息的加密方式按标准的 Triple DES 或 Single DES，请参考 7.4。

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》。生成 MAC 码的初始值为：4 个字节的随机数+00 00 00 00。

密文安装应用主控密钥时，所使用的密钥为上一层的卡片主控密钥。

密文安装 MF 下的卡片主控密钥时，则使用卡片的传输密钥进行安装。

密文修改密钥说明：

在使用密文形式进行修改密钥时，P1 为要修改密钥的类型，P2 为要修改密钥的标识，所使用的密钥为要修改的密钥本身。命令执行成功后，新的密钥值替换老的密钥值。修改密钥时，必须满足安全条件。对密钥信息的加密方式按标准的 Triple DES 或 Single DES，请参考 7.4。

密文形式的数据域信息：

密钥密文信息使用本密钥对以下数据加密（按所列顺序）产生的：

——数据长度

——密钥标识

——密钥版本号

——算法标识

——密钥类型

——使用权限

——后续状态

——修改权限

——错误计数器

——密钥值

MAC 是用本密钥对下数据进行 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》。生成 MAC

码的初始值为：4 个字节的随机数+00 00 00 00。

在使用密文形式进行修改个人 PIN 时，P1、P2 仍为密钥的类型和标识，但使用的密钥不为个人 PIN 本身，而是应用主控密钥。

[注]：无论明文密文，在修改密钥时，均不能改动密钥标识符和密钥类型。

3）.响应报文数据域

响应报文数据域不存在。

6）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	数据长度错误
69 01	功能不支持
69 81	命令与文件类型不相符
69 82	安全条件不满足
69 83	密钥锁定
69 84	取随机数无效
69 85	使用条件不满足（应用被锁定）
69 88	MAC 码不正确
6A 80	数据域不正确
6A 81	卡片锁定
6A 82	文件未找到
6A 84	文件空间不够
6A 86	P1、P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLA
93 03	应用永久锁定
94 03	没有找到 KEY

[例 1] 明文安装外部认证密钥

命令：

80 D4 00 00 18（5 个命令头）01（密钥标识符）01（密钥版本号）00（算法标识）08（密钥类型）0F（使用权限）02（后续状态）0F（修改权限） 33（错误计数器）11223344556677888877665544332211（密钥值）

[例 2] 密文+MAC 安装主控密钥

前提是卡中已建立 MF 文件和文件类型为 C5 的密钥文件。

这里假设：

卡片的传输代码为 8 字节 FFFFFFFFFFFFFFFF；

主控密钥信息 KeyInfo 为：

01（标识符）01（版本号）00（算法标识）08（密钥类型）0F（使用权限）02（后续状态）0F（修改权限）33（错误计数）11223344556677888877665544332211（密钥值）

1）计算密钥密文

Result=DES(TransKey,Data)

TransKey=FFFFFFFFFFFFFFFF

Data=18（数据长度）+KeyInfo(主控密钥信息)+80000000000000（补充值）

密钥密文：4cc2a6e5c865056638e80e804c21981b14fe76d36c4c4fadaf245faa4ee63711

2）从卡片取 4 字节随机数

命令：00 84 00 00 04

返回：b900cf0c

3）计算 MAC

Result =MAC(DES/3DES(Transcode,Data,INITIAL)

Transcode = FFFFFFFFFFFFFFFF

Data = 84D400024（命令头）+ 密钥密文

INITIAL = b900cf0c （随机数）00000000（补充值））

MAC：96eb7674

4）密文+MAC 安装主控密钥命令：

84D4000024（命令头）+

4cc2a6e5c865056638e80e804c21981b14fe76d36c4c4fadaf245faa4ee63711

（密钥密文）96eb7674（MAC）

6.3、 Generate KEY 生成子密钥或过程密钥

1）.定义和范围

Generate KEY 命令使用 SAM 卡上的 SAM 主密钥或外部认证主密钥生成子密钥或过程密钥存放在 RAM 中以供后续命令使用。该指令只用于 SAM 卡。

2）.命令报文

Generate KEY 的命令报文如下：

代码	值
CLA	80
INS	FA
P1	00- 生成子密钥 01- 生成过程密钥（长度必须为 10H） 02- 生成外部认证子密钥
P2	SAM 或外部认证主密钥标识符
Lc	08/10
DATA	用户数据

3）.命令报文数据域

用于生成子密钥的 SAM 主密钥必须是 SAM 主密钥或外部认证主密钥，否则将返回密钥不存在 9403。

过程密钥存在卡的 RAM 中，下电、复位或生成过程密钥后自动丢失。其生成过程如下：

首先将主 SAM 主密钥作为加密密钥，对输入数据的左 8 个字节进行加密生成子密钥的左半部分；

然后将主 SAM 主密钥作为加密密钥，对输入数据的左 8 个字节求反后进行加密生成子密钥的右半部分。

最后用刚生成的子密钥作为密钥对输入数据的右 8 个字节进行 Triple DES 加密，加密的结果即为过程密钥。

按银行规范，左 8 个字节为应用序列号，右 8 个字节是当次交易的部分数

据，由于每张卡的应用序列号唯一性和交易数据的随机性，所以生成的过程密钥也具有唯一性。生成过程密钥的过程完全在卡的内部完成，与外界无关，从而提高了系统的安全性。

子密钥的生成同过程密钥的前两步，因此输入的数据也只有 8 个字节。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
67 00	Lc 不是 16 个字节
69 83	密钥已经锁定
69 82	不满足安全状态
6A 81	功能不支持
6A 82	文件未找到
94 03	密钥未找到

6.4、 Crypt 安全模块命令

1）.定义和范围

该指令使用卡中已经存在的密钥对数据进行加密、解密或生成交易 MAC 码及应用 MAC 码。

2）.命令报文

Crypt 的命令报文如下：

代码	值
CLA	80
INS	F8
P1	00- 加密数据 01- 解密数据 02- 生成交易 MAC 码 03- 生成应用 MAC 码
P2	00 或指定密钥的标识符
Lc	Lc
DATA	用户数据
Le	期望返回数据长度

3）.命令报文数据域

P2≠00 且 P1=00、01、02、03 时，P2 指定的密钥如果不是加密类型的密钥，将返回 9403；如果 P2=00，则使用子密钥进行加、解密、MAC 码生成，该选项只能用于 SAM 卡。

DES 加、解密的输入数据长度不超过 48 个字节，方法同本手册的 7.4 节。生成交易 MAC 的数据可以不是 8 的倍数，方法同本手册的 7.3，只是生成 MAC 的初始值为 8 个 00。当生成应用 MAC 时，数据长度必须大于 8 且数据域前 8 个字节为初始值，之后的数据为生成 MAC 的数据。

DES 加、解密及生成 MAC 码的运算法方法请参见《中国金融集成电路（IC）卡规范》的运算方法。

4）.响应报文数据域

响应报文数据域为加密后的数据。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
61 XX	正常执行，但仍有 XX 个数据有效待取
67 00	错误的长度
69 81	P2 指定的密钥不是 Crypt 密钥
69 82	不满足安全状态
6A 81	功能不支持
94 03	密钥未找到

6.5、 Application Block 应用锁定

1）.定义和范围

Application Block 命令使当前选择的应用失效。

当 Application Block 成功完成后，用 Select File 命令选择已失效的应用，将回送状态“选择文件无效”（状态码 SW1 SW2=‘6A81’）。

对其它命令的影响根据不同的应用而定。

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- 临时锁定应用 01- 永久锁定应用
Lc	04
DATA	4 字节的报文鉴别代码(MAC)数据元，由应用维护密钥生成。
Le	不存在

3）.命令报文数据域

对于临时锁定的应用可以用 Application Unblock 命令解锁，可由 Select File 命令选择进入该目录，但对文件操作时返回‘6A81’。对于永久锁定的应用，SmartCOS V3.3 将不允许执行 Application Unblock 命令，可用 Select File 命令选择进入该目录，但对文件操作时返回‘6983’。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	内存失败
69 82	安全状态不满足
69 88	安全报文数据项不正确
6A 86	参数 P1 P2 不正确
94 03	未找到引用数据

6.6、 Application Unblock 应用解锁

1）.定义和范围

Application Unblock 命令用于恢复当前应用。如果对于某应用连续三次解锁失败，则 SmartCOS V3.3 将永久锁定此应用。

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	4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成。

3）.命令报文数据域

命令报文数据域为 4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成，初始值为 4 字节的随机数+00 00 00 00。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
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
69 88	安全报文数据项不正确
93 03	应用永久锁定

6.7、 Card Block 卡片锁定

1）.定义和范围

Card Block 命令使卡中所有应用久失效。

当 Card Block 命令成功完成后。所有后续的命令都将回送状态码‘6A81’（不支持此功能），且不执行任何其它操作。

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	4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成。

3）.命令报文数据域

命令报文数据域为 4 个字节的报文鉴别代码(MAC)数据元，使用应用维护密钥生成，初始值为 4 字节的随机数+00 00 00 00。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	内存失败
69 82	不满足安全状态
69 88	安全报文数据项不正确

6.8、 External Authentication 外部认证

1) 定义和范围

EXTERNAL AUTHENTICATION 命令用于卡片对外部的安全认证。计算的方法是利用卡片中的卡片主控密钥、应用主控密钥或外部认证密钥，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。

External Authentication 命令要求验证 IC 卡中的外部验证密钥，过程如下：首先执行产生随机数命令，直接获取 8 字节的随机数或 4 字节的随机数并补 00 00 00 00 后，用已知密钥加密后，放在外部认证命令的数据域内，执行外部认证执令。IC 卡将命令中的数据域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，错误允许计数器恢复成初始值；若比较不一致则认证失败，错误允许计数器值减 1，且不改变安全状态寄存器的值。

2）.命令报文

External Authentication 命令报文编码如下：

代码	值
CLA	00
INS	82
P1	00
P2	00 或密钥标识符
Lc	8
DATA	加密后的随机数

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（如果是 4 字节，则需后缀“00 00 00 00”之后）做 3DES 加密运算产生的。

- 若校验成功，则安全状态寄存器的值被置成该密钥的后续状态，同时错误允许计数器被置成初始值。若校验错误，则再试次数减 1。若外部认

证密钥已被锁死，则不能再执行该命令。被锁死后的外部认证密钥不能在恢复。

- 如果为全局 PIN，则 PIN 为全局后续状态且与其它非全局后续状态进行**或**操作；如果存在全局外部认证 KEY，则其后续状态与全局外部认证 KEY 进行**或**操作组成全局后续状态。
- 若校验失败时，IC 卡将回送 SW1 SW2＝63CX，X 表示允许重试的次数。当卡回送 63C0 时，表示不能重试，此时再使用校验命令时，将回送失败状态码‘6983’。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	校验失败，X 表示允许重试的次数
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
69 84	随机数无效
69 85	应用临时锁定
69 88	MAC 不正确
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	文件中存储空间不够
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.9、 Get Challenge 产生随机数

1）.定义和范围

Get Challenge 命令请求一个用于外部认证过程或其它过程的随机数。

在使用卡内随机数的前一条命令必须是 Get Challenge 命令。由卡产生 Le 字节随机数送给终端，若下一条指令为外部认证，则将终端传送的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。

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
Le	04/08

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

取长度为 4 的随机数后卡内随机数为 4 个随机数+00 00 00 00。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
67 00	长度错误
6A 86	参数 P1 P2 不正确

6.10、 Get Response 取响应

1）.定义和范围

Get Response 命令提供了一种从卡片向接口设备传送 APDU（或 APDU 的一部分）的传输方法。

2）.命令报文

Get Response 命令报文编码如下：

代码	值
CLA	00
INS	C0
P1	00
P2	00
Le	应答的期望数据长度

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

应答的期望数据长度。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
61 XX	还有 XX 数据可返回
67 00	长度错误(Lc 大于卡中应答数据长度)
6C XX	长度错误（Le 不正确，‘XX’表示实际长度）
6F 00	卡中无数据返回

6.11、 Internal Authentication 内部认证

1）.定义和范围

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。

2）.命令报文

Internal Authentication 命令报文编码如下：

代码	值
CLA	00
INS	88
P1	00
P2	00 或密钥标识符
Lc	08
DATA	认证数据

3）.命令报文数据域

命令报文数据域 DATA 的内容是应用专用的认证数据。

4）.响应报文数据域

应答报文数据域内容是相关认证数据 DES 运算的结果。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
67 00	长度 Lc 不正确
69 01	状态无效
69 82	不满足安全条件
69 85	使用条件不满足
6A 82	ISF 文件未找到
94 03	密钥未找到

6.12、 PIN Unblock 个人密码的解锁

1）.定义和范围

PIN Unblock 命令给发卡方提供了解锁人个密码的功能。

当 PIN Unblock 命令成功的完成后，卡将重置个人密码错误计数器；

2）.命令报文

PIN Unblock 命令报文编码如下：

代码	值
CLA	84
INS	24
P1	00
P2	01- 解锁个人密码
Lc	0C
DATA	加密的人个密码数据元+报文鉴别代码（MAC）数据元，使用 PIN 解锁密钥。
Le	不存在

3）.命令报文数据域

解锁个人密码应重置错误计数器，不改变个人密码。DATA 包括用 PIN 解锁密钥加密 PIN 后的密文+用 PIN 解锁密钥产生的 MAC。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	X 表示允许重试的次数
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足
69 88	安全报文数据项不正确

6A 80	数据不正确
6A 82	未找到 ISF 文件
6A 86	参数 P1 P2 不正确
94 03	密钥未找到
93 03	应用永久锁定

[例] 个人密码 PIN 解锁

前提条件是个人 PIN 已被锁，且密钥文件中已经安装了 PIN 解锁密钥 KEY。

假设 PIN 解锁密钥 KEY 为 11223344556677888877665544332211，被锁的个人 PIN 为 1234。

1）计算个人密码密文

Result = 3DES (KEY , Data)

KEY = 11223344556677888877665544332211

Data = 02（密码长度）1234（被锁的 PIN） 80000000 （补充值）

密码密文：08bb2cbec65bb695

2）从卡片取 4 字节随机数

命令：00 84 00 00 04

返回：23c47eca

3）计算 MAC

Result = MAC （DES/3DES（KEY，Data，INITIAL ））

KEY = 11223344556677888877665544332211

Data = 8424 00010C（命令头）08bb2cbec65bb695（密码密文）

INITIAL = 23c47eca（随机数） 00000000（补充值）

MAC ：d3d126d1

4）PIN 解锁命令:

842400010C（命令头）08bb2cbec65bb695（密码密文）d3d126d1（MAC）

6.13、 Read Binary 读二进制

1）.定义和范围

Read Binary 命令用于读取二进制文件的内容。

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
Le	XX

- 若 P1 的高三位为 100，则低五位为短的文件标识符，P2 为读的偏移量。
- Le 表示要读取的字节数，最大值为 110。若 Le 为 00 ，则送回警告状态 6C XX，请求 Le 置为 XX 并重发该命令。

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

应答报文数据域的内容为读出的二进制文件的内容。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
69 81	不是二进制文件
69 82	不满足安全条件
6A 81	不支持此功能
6A 82	未找到文件
6B 00	参数错误(偏移地址超出了 EF)
6C XX	长度错误（Le 不正确，‘XX’表示实际长度）

6.14、 Read Record 读记录

1）.定义和范围

Read Record 命令用于读取记录文件的内容。该命令适用于定长记录文件、循环定长记录文件、变长记录文件。

2）.命令报文

Read Record 命令报文编码如下：

代码	值
CLA	00
INS	B2
P1	记录号
P2	XX
Le	表示要读的字节数

- P1 为记录号，如果文件有 N 个记录，则 P1 可取为 1-N。
- P2 的低 3 位为 100，若高 5 位不为 00000 表示短文件标识符，否则表示当前文件。

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 命令的响应报文数据域由读取的记录组成。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
69 81	文件类型错误
69 82	读的条件不满足
69 86	不满足命令执行条件（无当前 EF）
6A 81	不支持此功能

6A 82	未找到文件
6A 83	未找到记录
6C XX	长度错误（Le 不正确，‘XX’表示实际长度）

6.15、 Select File 选择文件

1）.定义和范围

Select File 命令通过文件名来选择 IC 卡中的文件。

2）.命令报文

Select File 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 MF 或 DF 02- 选择 EF 04-按文件名选择应用
P2	00- 第一个或仅有的一个 02-下一个（按文件名选择）
Lc	XX
DATA	文件标识符或 DF（MF）名称

3）.命令报文数据域

命令报文数据域为文件标识符或文件名称。

4）.响应报文数据域

应答报文数据域包括所选择的 DDF 或 ADF 的文件控制信息 FCI。

DDF 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	文件控制信息专用模板	必备
88	目录基本文件的短文件标识符	必备

ADF 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

9F 0C	发卡方自定义数据的文件控制信息	可选

EF 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
A5	文件控制信息专用数据	必备
9F 0C	EF 文件控制信息（含文件标识符、类型、长度）	必备

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
61XX	命令正确执行
67 00	数据长度错误
6A 81	不支持此功能(无 MF 或应用已锁)
6A 82	未找到文件
6A 86	参数 P1 P2 不正确

[例] 选择主控文件 MF

假设建立 MF 的名称为 1PAY.SYS.DDF01，建立 MF 时指定 MF 下 DIR 文件的短文件标识符为 01。

1）按照文件名称选择

命令：00 A4 04 00 0E 315041592E5359532E4444463031（MF的名称）

返回：6F15840E315041592E5359532E4444463031（MF的名称）A503880101

说明：返回的数据信息为嵌套的 TLV 格式，以上为 4 层嵌套。

‘6F’为文件控制信息模板标识，‘15’为文件控制信息模板的数据长度，84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01 为15H 字节长度的数据。

‘84’为 DF 名称的记录标识，‘0E’为 DF 名称的数据长度，31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 为 0EH 字节长度的数据，即 1PAY.SYS.DDF01。

‘A5’为文件控制信息专用模板的数据标识，‘03’为文件控制信息专用模板的数据长度，88 01 01 为数据。

‘88’为 DIR 短文件标识符的记录标识，‘01’为长度，‘01’为 DIR 文件的短文件标识符。

2）按照文件标识符选择

命令：00 A4 00 00 02 3F00（MF 文件标识符）

返回：同 1)返回。

6.16、 Update Binary修改二进制

1）.定义和范围

Update Binary 命令根据文件属性，以密文、密文+MAC 或、明文、明文+MAC 的形式修改二进制文件。

2）.命令报文

Update Binary 命令报文编码如下：

代码	值
CLA	00/04
INS	D6
P1	XX
P2	XX
Lc	XX
DATA	写入的数据

P1 说明：若 P1 的高三位为 100，则低五位为二进制文件的短文件标识符，P2 为欲写文件的偏移量。

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
1								使用 SFI 方式
	0	0						RFU（如果 b8=1）
			X	X	X	X	X	SFI

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，命令中的数据域包明文+MAC 或者密文+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。

- 当文件类型最高位为 0，次高位为 0 时则采用明文形式，Lc 表示要写入的字节数，DATA 为要写入的数据。
- 当文件类型最高位为 1，次高位为 0 时则采用明文+MAC 安全报文形式，Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的明文数据 ＋4 字节安全报文。

- 当文件类型最高位为 1，次高位为 1 时则采用密文+MAC 安全报文形式，Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的密文数据 ＋4 字节安全报文。其中生成密文数据的明文形式为：明文数据长度（Len）+明文数据+补位（00）
- 文件类型的最高位为 0，次高位为 1 时则采用密文形式。写二进制文件时，若 CLA 与文件类型的第 4 位不匹配，如 CLA 为 04，而文件类型为 00 时，则返回“6A 81”。

注：二进制文件类型为 00 时，数据也可以以密文+MAC 形式写入。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 81	不是二进制文件
69 82	写的条件不满足
69 84	没有取随机数
69 88	安全报文数据项不正确
69 85	使用条件不满足（应用临时锁定）
6A 81	不支持此功能(无 MF、应用已锁或 CLA 与文件类型不符)
6A 82	未找到文件
6A 86	P1 或 P2 不正确
6B 00	P1 或 P2 超限
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

[例 1] 以密文+MAC 的方式写二进制数据

前提条件是卡中已建立类型为 C0 的二进制文件，且该二进制文件所在的应

用下已安装密钥类型为 05 的应用维护密钥 KEY。

这里假设 KEY 为 11223344556677888877665544332211，二进制文件标识为 06，欲写入数据为 1234。

1） 计算密文

Result = 3DES(KEY, DATA)

KEY= 11223344556677888877665544332211

DATA= 02（长度）1234（写入数据）8000000000（补充值）

密文： 08bb2cbec65bb695

3） 从卡片取 4 字节随机数 RND

命令：00 84 00 00 04

返回：c1bd4bd6

4） 计算 MAC

Result=MAC(3DES(KEY, DATA, INITIAL))

KEY=11223344556677888877665544332211

DATA=04D686000C(命令头)+08bb2cbec65bb695(密文)

INITIAL = c1bd4bd6（RND）00000000（补充值）

MAC：2364e470

5） 密文+MAC 写入数据命令：

04D686000C（命令头）08bb2cbec65bb695（密文）2364e470（MAC）

6.17、 Append Record 追加记录

1）.定义和范围

Append Record 命令用于追加记录文件。该命令适用于定长记录文件、变长记录文件和循环文件。

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	XX
Lc	后续数据域的长度
DATA	新记录数据

P2 说明：P2 的低 3 位为 000，如果高 5 位不为 00000 则表示短文件标识符，否则表示当前文件。

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
X	X	X	X	X				使用 SFI 方式
					0	0	0	第一个记录
其余值								保留

3）.命令报文数据域

命令报文数据域包括新数据，使用安全报文时，命令中的数据域包明文+MAC 或者密文+MAC。MAC 是由卡片维护密钥或应用维护密钥对更新的新数据计算而得到的。

- 命令报文数据域由写入的新记录组成。
- 当文件类型最高位为 0，次高位为 0 时则采用明文形式，Lc 表示要写入的字节数，DATA 为要写入的数据。
- 当文件类型最高位为 1，次高位为 0 时则采用明文+MAC 安全报文形式，Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的明文数据 ＋

4 字节安全报文。

- 当文件类型最高位为 1，次高位为 1 时则采用密文+MAC 安全报文形式，Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的密文数据 ＋4 字节安全报文。其中生成密文数据的明文形式为：明文数据长度（Len）+明文数据+补位（00）
- 文件类型的最高位为 0，次高位为 1 时则采用密文形式。写记录文件时，若 CLA 与文件类型的第 4 位不匹配，如 CLA 为 04，而文件类型为 00 时，则返回“6A 81”。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
69 84	随机数无效
69 85	应用临时锁定
69 88	MAC 不正确
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	文件中存储空间不够
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.18、 Update Record 修改记录

1）.定义和范围

Update Record 命令用于修改记录文件。该命令适用于定长记录文件和变长记录文件。

2）.命令报文

Update Record 命令报文编码如下：

代码	值
CLA	00
INS	DC
P1	= 00 当前记录 ≠00 指定的记录号
P2	XX
Lc	后续数据域的长度
DATA	更新原有记录的新记录

P2 说明：P2 的低 3 位为 100，如果高 5 位不为 00000 则表示短文件标识符。本命令可操作的三种记录文件被选择后当前记录都是第一条记录。

B7	B6	B5	B4	B3	B2	B1	B0	指令状态
X	X	X	X	X				使用 SFI 方式
					1	0	0	记录号在 P1 中给出
其余值								保留

3）.命令报文数据域

命令报文数据域包括由更新原有记录的新记录组成，使用安全报文时，命令中的数据域包明文+MAC 或者密文+MAC。MAC 是由卡片维护密钥对更新原有记录计算而得到的。

- 命令报文数据域由写入的新记录组成。
- 当文件类型最高位为 0，次高位为 0 时则采用明文形式，Lc 表示要写入的字节数，DATA 为要写入的数据。
- 当文件类型最高位为 1，次高位为 0 时则采用明文+MAC 安全报文形式，

Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的明文数据 ＋4 字节安全报文。

- 当文件类型最高位为 1，次高位为 1 时则采用密文+MAC 安全报文形式，Lc 为要写入的字节数 ＋4 字节安全报文，DATA 为要写入的密文数据 ＋4 字节安全报文。其中生成密文数据的明文形式为：明文数据长度（Len）+明文数据+补位（00）
- 文件类型的最高位为 0，次高位为 1 时则采用密文形式。写记录文件时，若 CLA 与文件类型的第 4 位不匹配，如 CLA 为 04，而文件类型为 00 时，则返回“6A 81”。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
69 84	随机数无效
69 85	应用临时锁定
69 88	MAC 不正确
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	文件中存储空间不够
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.19、 Verify 校验

1）.定义和范围

Verify 命令用于校验命令数据域的个人密码的正确性。

2）.命令报文

Verify 命令报文编码如下：

代码	值
CLA	00
INS	20
P1	00
P2	00
Lc	02－06
DATA	外部输入的人个密码

3）.命令报文数据域

命令报文数据域由持卡者输入的个人密码组成。

- 若校验成功，则安全状态寄存器的值被置成该密钥的后续状态，同时错误允许计数器被置成初始值。若校验错误，则再试次数减 1。若人个密码已被锁死，则不能再执行该命令。被锁死的人个密码可以用解锁、重装指令恢复。
- 如果为全局 PIN，则 PIN 为全局后续状态且与其它非全局后续状态进行或操作；如果存在全局外部认证 KEY，则其后续状态与全局外部认证 KEY 进行或操作组成全局后续状态。
- 命令数据域外部输入的人个密码与卡中存放的人个密码校验失败时，IC 卡将回送 SW1 SW2＝63CX，X 表示允许重试的次数。当卡回送 63C0 时，表示不能重试，此时再使用校验命令时，将回送失败状态码‘6983’。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	校验失败，X 表示允许重试的次数
65 81	写 EEPROM 失败
67 00	长度错误
69 81	当前文件不是线性定长文件或线性变长文件
69 82	写的条件不满足
69 84	随机数无效
69 85	应用临时锁定
69 88	MAC 不正确
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	文件中存储空间不够
6A 86	P1 或 P2 不正确
6D 00	不正确的 INS
6E 00	不正确的 CLASS
93 02	应用永久锁定
93 03	密钥索引不支持

6.20、 Change PIN 修改

1）.定义和范围

Change PIN 允许持卡人将当前个人密码修改为新的密码。当 Change PIN 命令成功完成后，卡片要进行以下操作：

①PIN 尝试计数器复位至尝试次数上限；

②将原个人密码置为新的个人密码。

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	00
Lc	05-0D
DATA	当前的 PIN || ‘FF’ || 新的 PIN

3）.命令报文数据域

命令报文数据域为当前的 PIN || ‘FF’ || 新的 PIN

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	X 表示允许重试的次数
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 83	验证方法锁定
6A 81	功能不支持(无 MF 或卡片已锁死)
6A 82	未找到文件
94 03	密钥未找到

6.21、 Reload PIN 重装个人密码

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个人密码(可以与原个人密码相同)。

Reload PIN 只能在拥有或能访问到 PIN 重装子密钥（DRPK）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：

①PIN 错误允许计数器复位；

②IC 卡的原 PIN 被设置为新的值。

2）.命令报文

Reload PIN 命令报文编码如下：

代码	值
CLA	84
INS	5E
P1	00
P2	00
Lc	06-0A
DATA	重装的 PIN（02-06）+报文鉴别码 MAC（4）

3）.命令报文数据域

命令报文数据域为重装的 PIN（02-06）+报文鉴别码 MAC（4），报文鉴别码是用类型为 PIN 重装子密钥的密钥来产生。

4）.响应报文数据域

响应报文数据域不存在。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
63 CX	X 表示允许重试的次数
65 81	写 EEPROM 失败
65 83	密钥被锁死
69 82	不满足安全状态
69 88	MAC 不正确
6A 81	功能不支持(无 MF 或卡片已锁死)
6A 82	未找到文件
94 03	密钥未找到
93 03	应用永久锁定

[例] 重装个人密码

前提条件是 KEY 文件中已经安装了个人密码 PIN 和 PIN 重装密钥 KEY。

假设 PIN 重装密钥 KEY 为 11223344556677888877665544332211，新安装的个人密码 PIN 为 1234。

1）计算过程密钥 SessionKey

SessionKey = Right (KEY) XOR Left (KEY)

KEY = 11223344556677888877665544332211

SessionKey： 9955551111555599

注：SessionKey 为重装密钥 KEY 左右 8 字节异或的结果。

2）计算 MAC

Result = MAC(DES (SessionKey , Data , INITIAL))

Data = 12 34 （重装的 PIN）80 00 00 00 00 00（补充值））

InitialData = 0000000000000000（8 字节初始值）

MAC ： d2affb82

3）重装 PIN 命令：

805E000006（命令头）1234（重装 PIN）d2affb82（MAC）

6.22、 解锁口令UNBLOCK

1）.定义和范围

UNBLOCK 命令用于解锁被锁定的个人密码。

2）.命令报文

UNBLOCK 的命令报文如下：

代码	值
CLA	80
INS	2C
P1	00
P2	00
Lc	PIN 长度
DATA	2—6 字节超级|| ’FF’ ||2—6 字节新 PIN

3）.命令报文数据域

数据域信息为 2—6 字节的超级 PIN 加上 2—6 字节的新 PIN，中间以‘||’的形式分隔。

在满足该解锁口令使用条件，并且该解锁口令未被锁死时才执行该命令，该命令不改变安全状态寄存器的值。

若解锁口令核对成功，则新口令值取代解锁口令指定的口令密钥原口令（不受更改权限的限制），且将口令错误计数器和解锁口令错误计数器恢复成原始值。

若解锁口令失败，则解锁口令可再试次数减一，如果超级 PIN 被锁住，则无法被解锁。

5）.响应报文数据域

响应报文数据域不存在。

6）.响应报文状态码

响应报文可能的状态码如下：

SW1 SW2	意义
90 00	命令正确执行
65 81	写 EEPROM 失败

67 00	数据长度错误
63 CX	允许传输代码错误次数
69 01	创建状态不满足
69 82	安全条件不满足
69 85	使用条件不满足（应用临时被锁定）
6A 80	标识符已存在
6A 81	功能不支持（文件不可建立在 MF 或 DF）
6A 82	文件未找到
6A 86	P1 或 P2 参数不正确
6D 00	不正确的 INS
6E 00	不正确的 CLA
93 03	应用永久锁定

6.23、 Initialize For Load 圈存初始化

1）.定义和范围

Initialize For Load 命令用于初始化圈存交易。通过圈存交易，持卡人可将其在银行相应帐户上的资金划入电子存折或电子钱包中。这种交易必须在金融终端上联机进行并要求验证口令。

在圈存交易之前必须先进行圈存初始化指令 Initialize For Load，在执行了 Initialize For Load 后便选择了圈存交易。

2）.命令报文

Initialize For Load 的命令报文编码如下：

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	见下表
Le	10

3）.命令报文数据域

命令报文数据域 Data 的内容：

Data 说明	长度(字节)
密钥标识符	1
交易金额	4
终端机编号	6

密钥标识符指定的密钥的类型必须为圈存子密钥。

4）.响应报文数据域

数据域内容：

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	1
算法标识	1
伪随机数	4
MAC1	4

过程密钥由密钥标识符指定的圈存子密钥对（4 字节随机数+2 字节电子存折或电子钱包联机交易序号+80 00）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 字节的交易金额+1 字节交易类型标识+6 字节终端机编号）加密生成。

交易类型标识如下表：

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

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
67 00	长度错误
69 85	使用条件不满足
6A 81	不支持此功能能(无 MF 或卡片已锁定)
6A 86	参数 P1，P2 错误
94 03	密钥索引不支持

如果圈存初始化不成功，则交易终止。

6.24、 Credit For Load 圈存

1）.定义和范围

当圈存初始化成功之后，继续进行圈存交易，通过圈存交易，持卡人可将其在银行相应帐户上的资金划入电子存折或电子钱包中。这种交易必须在金融终端上联机进行并要求验证口令。

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	见下表
Le	04

3）.命令报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
交易日期(主机)	4
交易时间(主机)	3
MAC2	4

MAC2 由过程密钥对（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。

4）.响应报文数据域

响应报文数据域不存在。

4 个字节的交易验证码 TAC	SW1	SW2

TAC 是用系统定义的 TAC 子密钥左右 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 字节的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。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
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	不支持此功能能(无 MF 或卡片已锁定)
93 02	MAC 无效

【注】 圈存交易完成后，电子存折或电子钱包文件的联机交易序号加 1，交易金额加在电子存折或电子钱包的余额上，并且在其交易明细文件中存有如下记录：

电子存折或电子钱包联机交易序号	2 字节
透支限额	3 字节
交易金额	4 字节
交易类型标识	1 字节
终端机编号	6 字节
主机交易日期	4 字节
主机交易时间	3 字节

[例] 圈存交易过程

此命令的执行必须在 ADF 下，且此 ADF 下必须包含以下文件和密钥：

<table>
<tr><td rowspan="6">ADF</td><td colspan="2">钱包文件 00 01</td></tr>
<tr><td colspan="2">存折文件 00 02</td></tr>
<tr><td colspan="2">交易明细文件 00 18</td></tr>
<tr><td rowspan="3">密钥文件</td><td>TAC 密钥</td></tr>
<tr><td>圈存密钥</td></tr>
<tr><td>个人密码 PIN</td></tr>
</table>

这里假设：

圈存密钥为 11223344556677888877665544332211；

个人密码 PIN 为 1234；

操作流程如下：

1）选择应用

命令：00A4000002（命令头）XX XX（ADF 标识符）

2）校验个人密码

命令：0020000002（命令头）1234（PIN）

3）圈存初始化

命令：

80 50 00 01 0B（命令头）01 （圈存密钥标识）00 00 10 00（交易金额）

00 00 00 00 00 01（终端机编号）

返回：

00000000（旧余额）0000（联机交易序号）01（密钥版本号）00（算法标识）

72d5a089（随机数）82dc9807（MAC1）

4）圈存

①计算过程密钥 SessionKey;

SessionKey = DES/3DES（KEY , Data1）

KEY = 11223344556677888877665544332211

Data1 = 72d5a089（随机数）0000（2 字节联机交易序号）8000（补充值）

SessionKey ： c40123a4297d7dba

②计算 MAC2

MAC2 = MAC（DES/3DES（SessionKey , Data2 , InitialData））

Data2 = 00001000（4 字节的交易金额）01（交易类型）000000000001（6 字节的终端编号） 20010910（4 字节的交易日期）130222（3 字节交易时间）

InitialData = 0000000000000000

计算结果：

MAC2= 4e8b20d4

③向卡片发送圈存指令：

805200000B（命令头）20010910（4 字节的交易日期）130222（3 字节交易

时间）4e8b20d4（MAC2）

6.25、 Initialize For Purchase 消费初始化

1）.定义和范围

Initialize For Purchase 命令用于初始化消费交易。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。

在消费交易前必须先执行消费初始化 Initialize For Purchase 命令，在执行 Initialize For Purchase 后即选择了消费交易。

2）.命令报文

Initialize For Purchase 的命令报文编码如下：

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	见下表
Le	10

3）.命令报文数据域

命令报文数据域 Data 内容：

Data 说明	**长度(字节)**
密钥标识符	1
交易金额	4
终端机编号	6

密钥标识符指明的密钥的类型必须为消费子密钥。

4）.响应报文数据域

响应报文数据域内容：

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	1
算法标识	1
伪随机数	4

过程密钥由密钥标识符指定的消费子密钥对（4 字节随机数+2 字节电子存折或电子钱包联机交易序号+终端交易序号的最后 2 个字节）加密生成。

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

交易类型标识如下表：

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

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
62 83	选择文件无效，文件或密钥校验错误
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	不支持此功能能(无 MF 或卡片已锁定)
6A 82	文件未找到
94 01	金额不足
94 03	密钥索引不支持

如果消费初始化不成功，则交易终止。

6.26、 Debit For Purchase 消费

1）.定义和范围

Debit For Purchase 命令用于消费交易。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。

2）.命令报文

如果消费初始化成功之后，继续进行消费交易，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	见下表
Le	08

3）.命令报文数据域

表定义了命令报文的数据域 DATA：

说明	长度(字节)
终端交易序号	4
终端交易日期	4
终端交易时间	3
MAC1	4

MAC1 由过程密钥对（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。

4）.响应报文数据域

响应报文数据域为：

4 字节交易验证码 TAC 和 4 字节的 MAC2	**SW1**	**SW2**

TAC 是用系统定义的 TAC 子密钥左右 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 字节主机交易时间）数据加密生成。MAC2 由卡中过程密钥对（4 字节交易金额）数据加密生成。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
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	不支持此功能(无 MF 或 MF 已锁定)
93 02	MAC 无效

【注】 消费取现交易完成后，电子存折或电子钱包的脱机交易序号加 1，电子存折或电子钱包的余额被减去交易金额。此外，若是对电子存折文件操作将在其交易明细文件中存有如下记录：

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

[例] 消费交易过程

此命令的执行必须在 ADF 下，且此 ADF 下必须包含以下文件和密钥：

<table>
<tr><td rowspan="6">ADF</td><td colspan="2">钱包文件 00 01</td></tr>
<tr><td colspan="2">存折文件 00 02</td></tr>
<tr><td colspan="2">交易明细文件 00 18</td></tr>
<tr><td rowspan="3">密钥文件</td><td>TAC 密钥</td></tr>
<tr><td>圈存密钥</td></tr>
<tr><td>个人密码 PIN</td></tr>
</table>

这里假设：

消费密钥为 11223344556677888877665544332211；

个人密码 PIN 为 1234；

操作流程：

1）选择应用

00A4000002（命令头）XXXX（ADF 标识符）

2）校验个人密码

0020000002（命令头）1234（PIN）

3）消费初始化

命令：

80 50 01 01 0B（命令头）01 （消费密钥标识）00 00 00 10（交易金额）00 00 00 00 00 01（终端机编号）

返回：

00001000（旧余额）0000（脱机交易序号）000000 （透支限额）01（密钥版本）00（算法标识）e398ed60（随机数）

4）消费

①计算过程密钥 SessionKey

SessionKey = DES/3DES（KEY , Data1）

KEY = 11223344556677888877665544332211

Data1 = e398ed60（随机数） 0000（2 字节脱机交易序号） 0001（终端交易序号的后 2 个字节）

计算结果：

SessionKey = e6874578af758168

②计算 MAC1

MAC1 = MAC（DES/3DES（Session Key , Data2 , InitialData））

Data2 = 00000010（交易金额）05（交易类型）000000000001（终端编号）20010910（交易日期）130222（交易时间））

InitialData = 0000000000000000

计算结果：

MAC1= c7d12550

③向卡片发送消费指令：

805400000F（命令头）00000001（终端交易序号）20010910（4 字节的交易日期）130222（3 字节交易时间）c7d12550（MAC1）

6.27、 Initialize For Cash Withdraw 取现

Initialize For Cash Withdraw 命令用于初始化取现交易。取现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。

在消费交易前必须先执行取现初始化 Initialize For Cash Withdraw 命令，在执行 Initialize For Cash Withdraw 后即选择了取现交易。

2）.命令报文

Initialize For Cash Withdraw 的命令报文编码如下：

代码	值
CLA	80
INS	50
P1	02
P2	01- 用于电子存折
Lc	0B
Data	见下表
Le	0F

3）.命令报文数据域

命令报文数据域 Data 内容：

Data 说明	长度(字节)
密钥标识符	1
交易金额	4
终端机编号	6

密钥标识符指明的密钥的类型必须为消费子密钥。

4）.响应报文数据域

响应报文数据域内容：

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
透支限额	3
密钥版本号	1

算法标识	1
伪随机数	4

过程密钥由密钥标识符指定的消费子密钥对（4 字节随机数+2 字节电子存折联机交易序号+终端交易序号的最后 2 个字节）加密生成。

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

交易类型标识如下表：

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

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	不支持此功能能(无 MF 或卡片已锁定)
6A 82	文件未找到
94 01	金额不足
94 03	密钥索引不支持

如果取现初始化不成功，则交易终止。

6.28、 Debit For Cash Withdraw 取现

1）.定义和范围

Debit For Cash Withdraw 命令用于取现交易。取现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。

2）.命令报文

如果取现初始化成功继续进行取现交易，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	见下表
Le	08

3）.命令报文数据域

下表定义了命令报文的数据域 Data：

说明	长度(字节)
终端交易序号	4
终端交易日期	4
终端交易时间	3
MAC1	4

MAC1 由过程密钥对（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。

4）.响应报文数据域

响应报文数据域为：

4 字节交易验证码 TAC 和 4 字节的 MAC2	SW1	SW2

TAC 是用系统定义的 TAC 子密钥左右 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 字节主机交易时间）数据加密生成。

MAC2 由卡中过程密钥对（4 字节交易金额）数据加密生成。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
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	不支持此功能(无 MF 或卡片已锁定)
93 02	MAC 无效

【注】 取现交易完成后，IC 卡将电子存折文件的脱机交易序号加 1，从电子存折的余额中减去交易金额。此外，若是对电子存折文件操作将在其交易明细文件中存有如下记录：

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

6.29、 Initialize For Unload 圈提

1）.定义和范围

Initialize For Unload 命令用于初始化电子存折的圈提交易。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。

在圈提交易前必须先执行圈提初始化 Initialize For Unload 命令，在执行 Initialize For Unload 后即选择了圈提交易。

2）.命令报文

Initialize For Unload 的命令报文编码如下：

代码	值
CLA	80
INS	50
P1	05
P2	01- 用于电子存折
Lc	0B
Data	见下表
Le	0F

3）.命令报文数据域

命令报文数据域 Data 内容：

Data 说明	长度(字节)
密钥标识符	1
交易金额	4
终端机编号	6

密钥标识符指明的密钥的类型为圈提子密钥。

4）.响应报文数据域

响应报文数据域内容为：

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	1
算法标识	1
伪随机数	4
MAC1	4

过程密钥由密钥标识符指定的圈提子密钥对（4 字节随机数+2 字节电子存折联机交易序号+80 00）加密生成。

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

交易类型标识如下表：

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

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
67 00	长度错误
69 85	使用条件不满足
6A 81	不支持此功能能(无 MF 或卡片已锁定)
6A 86	参数 P1，P2 错误
94 01	金额不足
94 03	密钥索引不支持

如果圈提初始化不成功，则交易终止。

6.30、 Debit For Unload 圈提

1）.定义和范围

Debit For Unload 命令用于电子存折的圈提交易。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。

2）.命令报文

如果圈提初始化成功继续进行圈提交易，Debit For Unload 命令报文编码如下：

代码	值
CLA	80
INS	54
P1	03
P2	00
Lc	0B
DATA	见下表
Le	04

2）.命令报文

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
主机交易日期	4
主机交易时间	3
MAC2	4

MAC2 由过程密钥对（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。

3）.命令报文数据域

执行成功则应答报文如下：

MAC3	90	00

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。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
67 00	长度错误
69 01	命令不接受(无效状态)
6A 81	不支持此功能(无 MF 或卡片已锁定)
93 02	MAC 无效

【注】 圈提交易完成后，电子存折文件的联机交易序号加 1，电子存折的余额被减去交易金额，并且在其交易明细文件中存有如下记录：

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

6.31、 Get Balance 读余额

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，读取电子存折余额应验证个人密码（PIN）。

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
Le	04

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

响应报文数据域为：

电子存折或电子钱包余额	90	00

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	不支持此功能(无 MF 或卡片已锁死)
6A 82	文件未找到

6.32、 Get Transaction Prove 取交易认证

1）.定义和范围

Get Transaction Prove 命令提供了一种在交易处理过程中卡拔出并重插后卡片的恢复机制。

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	要取 MAC 或 TAC 所对应的交易类型标识
Lc	02
DATA	要取 MAC 或交易认证码所对应的当前的电子存折或电子钱包联机或脱机交易序号
Le	08

3）.命令报文数据域

要取 MAC 或交易认证码所对应的当前的电子存折或电子钱包联机或脱机交易序号

4）.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，则应答报文的数据域如下表：

4 字节 MAC+4 字节交易验证码	SW1	SW2

5）.响应报文状态码

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 不可用，或命令由于其它原因执行不成功，则应答报文只返回 SW1 和 SW2。

SW1 SW2	意义
65 81	写 EEPROM 失败
69 82	不满足安全状态
69 85	使用条件不满足
6A 81	不支持此功能(无 MF 或 MF 已锁定)
6A 82	文件未找到
94 06	所需的 MAC 不可用

【注】 防拔功能解释如下：

此功能保证卡片在交易处理过程中的任何情况下，甚至是在更新 EEPROM 过程中掉电的情况下，都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余额或电子钱包余额时，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 Transaction Prove 命令获得此 MAC 或 TAC。

如果命令已执行结束，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 90 00，则表示卡片更新成功，交易完成。如果不返回 90 00，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。

6.33、 Initialize For Update修改透支限额初始化

1）.定义和范围

Initialize For Update 命令用于初始化修改透支限额。当电子存折中的实际金额不足时，该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，且必须校验个人密码。

在修改透支限额交易前必须先执行修改透支限额初始化 Initialize For Update 命令，在执行 Initialize For Update 后即选择了修改透支限额交易。

2）.命令报文

Initialize For Update 的命令报文编码如下：

代码	值
CLA	80
INS	50
P1	04
P2	01- 用于电子存折
Lc	07
Data	见下表
Le	13

3）.命令报文数据域

命令报文数据域 Data 内容：

Data 说明	长度(字节)
密钥标识符	1
终端机编号	6

密钥标识符指明的密钥的类型必须为修改透支限额子密钥。

4）.响应报文数据域

响应报文数据域内容为：

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	1
算法标识	1
伪随机数	4
MAC1	4

过程密钥由密钥标识符指定的修改透支限额子密钥对（4 字节随机数+2 字节电子存折联机交易序号+80 00）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）加密生成。

交易类型标识如下表：

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

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
62 83	选择文件无效,文件或密钥校验错误
65 81	写 EEPROM 失败
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	不支持此功能能(无 MF 或卡片已锁定)
6A 86	参数 P1，P2 错误
94 03	密钥索引不支持

如果修改透支限额初始化命令不成功，则交易终止。

6.34、 Update Overdraw Limit修改透支限额

1）.定义和范围

Update Overdraw Limit 命令用于修改透支限额。当电子存折中的实际金额不足时，该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，且必须校验个人密码。

2）.命令报文

如果初修改透支限额始化执行成功，继续进行修改透支限额交易，Update Overdraw Limit 命令报文编码如下：

代 码	值
CLA	80
INS	58
P1	00
P2	00
Lc	0E
DATA	见下表
Le	04

3）.命令报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
新透支现额	3
发卡方交易日期	4
发卡方交易时间	3
MAC2	4

MAC2 由过程密钥对（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 字节发卡方交易日期＋3 字节发卡方交易时间）数据加密生成。

4）.响应报文数据域

命令执行成功应答报文如下：

交易验证码 TAC	90	00

TAC 由系统定义的 TAC 子密钥对（4 个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 字节发卡方交易日期＋3 字节发卡方交易时间）数据加密生成。

5）.响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
65 81	写 EEPROM 失败
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	不支持此功能(无 MF 或 MF 已锁定)
93 02	MAC 无效
94 01	金额不足

【注】 修改透支限额交易完成后，电子存折文件的联机交易序号加 1，电子存折余额被置为新的电子存折余额，更新透支限额，并且在其交易明细文件中存有如下记录：

电子存折或电子钱包联机交易序号	2 字节
新透支限额	3 字节
交易金额	4 字节
交易类型标识	1 字节
终端机编号	6 字节
终端交易日期	4 字节
终端交易时间	3 字节

7、安全机制

7.1、 加密算法

SingleDES—密钥长度为 8 字节，数据为 8 字节

加密算法如下：

Y=DES(K)[X]

解密算法如下：

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

TripleDES—密钥长度为 16 字节（**K=**（**$K_L||K_R$**）)，数据为 8 字节

加密算法如下：

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

解密算法如下：

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

7.2、 密钥管理

7.2.1、 共存应用

为了独立地管理一张卡上不同应用的安全问题，每一个应用应该放在一个单独的 ADF 中。亦即在应用之间应该设计一道“防火墙”，以防止跨过应用进行非法访问。另外，每个应用也不应该与个人化要求和卡中共存的其它应用规则发生冲突。

7.2.2、 密钥的独立性

在 IC 卡中，用于特定功能（如：扣款）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。某些密钥也可以保存在 SAM 中，每一种密钥只能执行特定的功能。

7.2.3、 密钥的生成

密钥必须按照一定的算法在保密、安全的地方生成，例如首先生成主密钥或多级主密钥，然后将主密钥保存在绝对安全的地方（例如 IC 中或主机中）。密钥下装时，首先使用主密钥同 IC 卡的特征字节（如应用序号）做加密生成子密钥（临时存在），在进行密钥的分散时，将密钥以明文或密文的形式下装入 IC 卡中，之后临时子密钥消失，整个过程应在保密、安全可靠的方式下进行。

7.2.4、 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。

7.2.5、 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。

7.2.6、 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）.密钥类型：

密钥类型长度为 1 字节，约定如下：

——00，消费取现密钥

——01，圈存密钥

——02，TAC 密钥

——03，圈提密钥

——04，修改透支限额密钥

——05，应用维护密钥

——06，PIN 解锁密钥

——07，PIN 重装密钥

——08，外部认证（主控）密钥

——09，内部认证密钥

——0A，加密密钥

——0B，个人密码 PIN

——0C，超级 PIN

——40，SAM 密钥

——80，用户自定义密钥

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版本号，长度 1 字节。

4）.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。

7.2.7、 密钥的使用和存放

密钥在使用过程中，每一种密钥只能执行特定的功能，并且采用 Triple DES 使用 16 字节长度的密钥进行加密。在交易过程中，使用临时密钥进行安全交易。

密钥在 IC 卡中不应被泄露，也就是说，禁止对密钥进行读操作。

7.2.8、 密钥的终止

每种密钥都有其生命周期，如果卡片被永久锁住，密钥就被终止使用。

7.3、 安全报文

7.3.1、 报文完整性和验证（在非交易过程中的安全报文 MAC）

MAC 是使用命令中的所有的元素（包含命令头）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 的计算方法如下：

第一步：终端向 IC 卡发出一个 Get Challenge 命令，从 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。

第二步：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‘4’

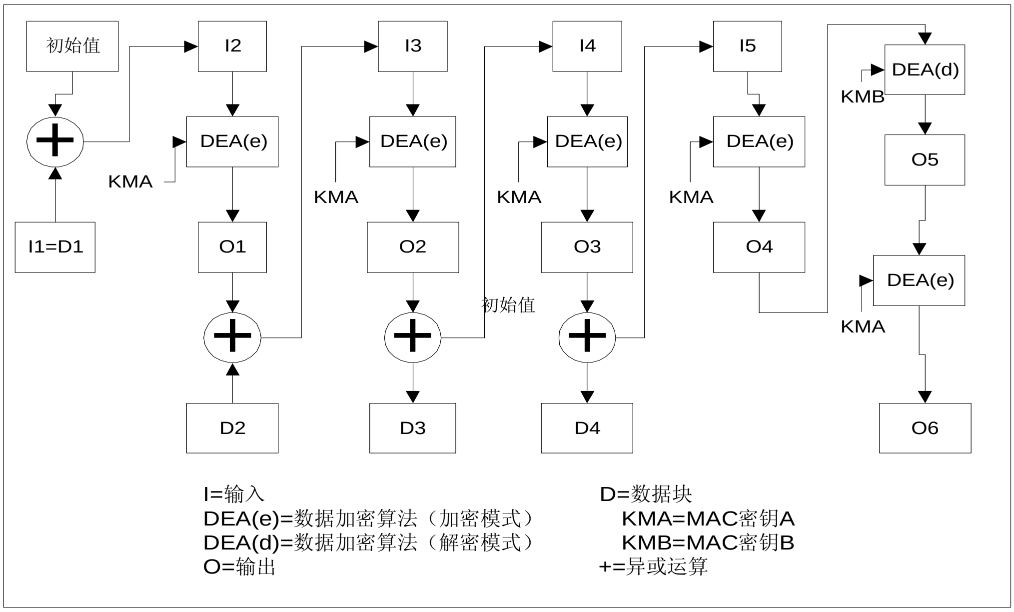
——在命令的数据域中（如果存在）包含明文或加密的数据

第三步：将该数据块分成 8 字节为单位的数据块，标号为 D1，D2，D3，D4 等，最后的数据块有可能是 1-8 个字节。

第四步：如果最后的数据块长度是 8 字节的话，则在其后加上 16 进制数字‘80 00 00 00 00 00 00 00’，转到第五步。如果最后的数据块长度不足 8 字节的话，则在其后加上 16 进制数字‘80’，如果达到 8 字节长度，则转入第五步；否则在其后加入 16 进制数字‘0’直到长度达到 8 字节。

第五步：对这些数据块使用相应的密钥进行加密。根据密钥的长度采用 Single DES 或 Triple DES。

Triple DES 的加密方法如下图所示：



第六步：最终得到是从计算结果左侧取得的 4 字节长度的 MAC。

7.3.2、 安全报文传送的命令情况

在 ISO/IEC7816-4 中定义了四种命令情况。

情况一：这种情况时，没有数据送到ICC（L_C）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	L_C	MAC

CLA的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C为MAC的长度。

情况二：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的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C为

MAC的长度。

情况三：这种情况时，命令中有数据送到卡中，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	L_C	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的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C为命令数据加上MAC的长度。

情况四：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	L_C	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的第二个半字节是‘4’表明支持第二种情况的安全报文传送。L_C为命令数据加上MAC的长度。

7.4、 数据的加、解密计算

7.4.1、 数据加密计算

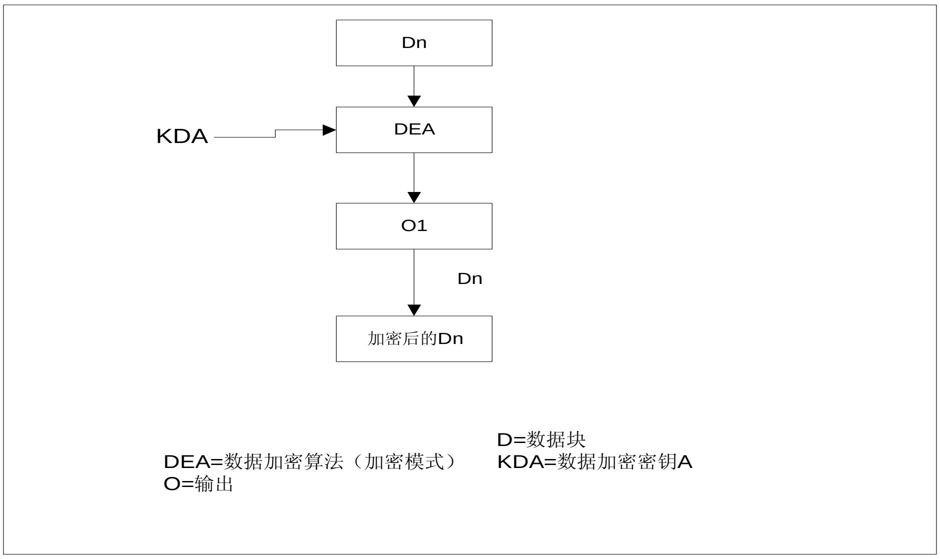
数据加密步骤如下：

第一步：用L_D表示明文数据的长度，在明文数据前加上L_D产生的新数据块。

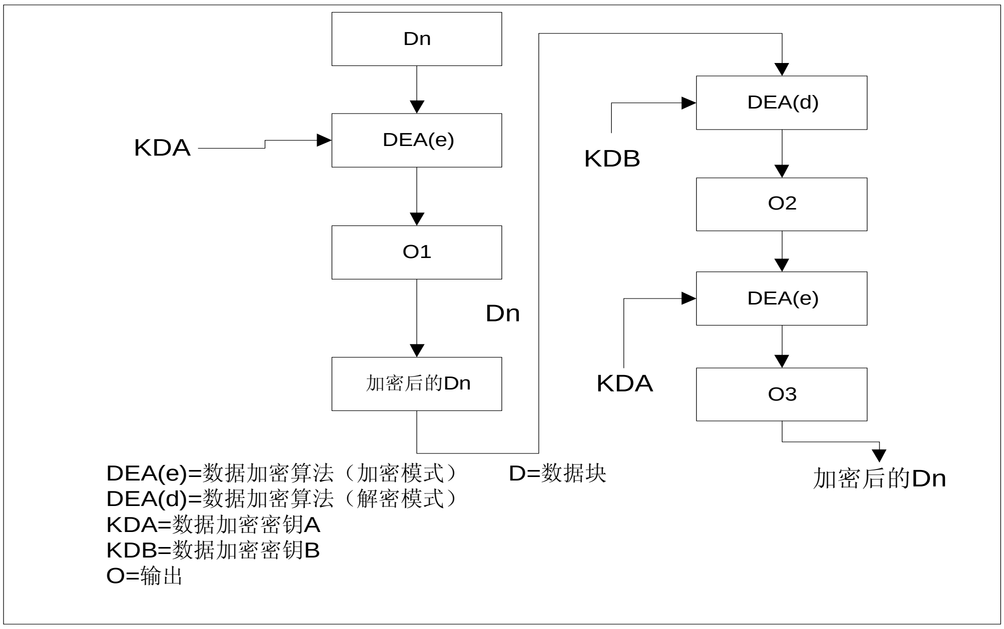
第二步：将第一步中生成的数据块分解成 8 字节数据块，标号为 D1，D2，D3，D4 等等。最后一个数据块的长度有可能不足 8 位。

第三步：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 1 字节 16 进制数字‘0’直到长度达到 8 字节。

第四步：对每个数据块用相应的密钥进行加密，根据密钥的长度可以使用 SingleDES 或 TripleDES。



使用 SingleDES 的数据加密



使用 TripleDES 的数据加密

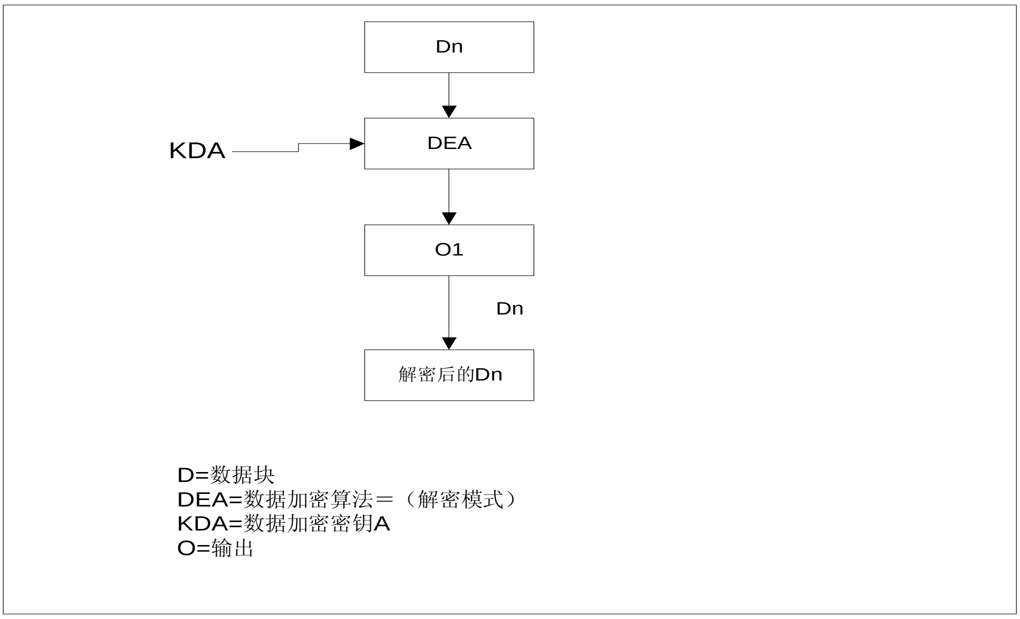
第五步：计算结束后，所有加密后的数据块依照原顺序连接在一起（加密后的 D1，加密后的 D2，等等）。并将结果数据块插入到命令数据域中。

7.4.2、 数据解密计算

数据解密步骤如下：

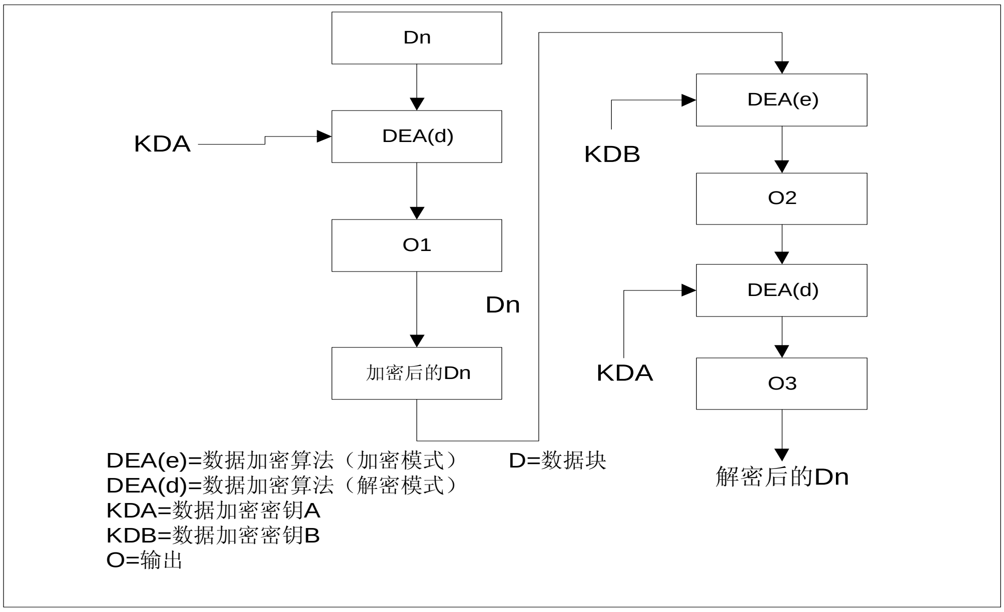
第一步：将命令数据域中的数据块分解成 8 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如下过程进行解密。

用与加密相同的密钥进行解密，SingleDES 和 TripleDES 的解密过程如下图：



使用 SingleDES 的数据解密

如果采用双长度数据加密的 DEA 密钥，则数据块的解密如图 16 所示（使用数据加密过程密钥 A 和 B 来进行解密）。



使用 Triple DES 的数据解密

第二步：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L_D，明文数据，填充字符组成。

第三步：因为L_D表示明文数据的长度，因此，它被用来恢复明文数据。

7.5、 ED/EP应用的密钥关系

7.5.1、 密钥关系表

密钥	发卡方	IC 卡	POS（PSAM）
用于消费/取现交易的密钥	消费主密钥（MPK）	消费子密钥（DPK），由 MPK 用应用序列号推导获得	消费主密钥（MPK）
用于圈存交易的密钥	圈存主密钥（MLK）	圈存子密钥（DLK），由 MLK 用应用序列号推导获得	N/A
消费/取现交易中用于产生 TAC 的密钥	TAC 主密钥（MTK）	TAC 子密钥（DTK），由 MTK 用应用序列号推导获得	N/A
用于解锁 PIN 的密钥	PIN 解锁主密钥（MPUK）	PIN 解锁子密钥（DPUK），由 MPUK 用应用序列号推导获得	由发卡方考虑决定
用于重装 PIN 的密钥	PIN 重装主密钥（MRPK）	PIN 重装子密钥（DRPK），由 MRPK 用应用序列号推导获得	N/A
用于应用维护功能的密钥	应用主控密钥（MAMK）	主控子密钥（DAMK）由 MAMK 用应用序列号推导获得	N/A

下表是 IC 卡中用于电子存折应用的密钥

密钥	发卡方	IC 卡	POS（PSAM）
用于圈提交易的密钥	圈提主密钥（MULK）	圈提子密钥（DULK），由 MULK 用应用序列号推导获得	N/A
用于修改透支限额交易的密钥	修改主密钥（MUK）	修改（透支限额）子密钥（DUK），由 MUK 用应用序列号推导获得	N/A

7.5.2、 子密钥推导方法

下面是 IC 卡中密钥的推导方法。图 B1 和图 B2 描述了 DPK 推导的过程。

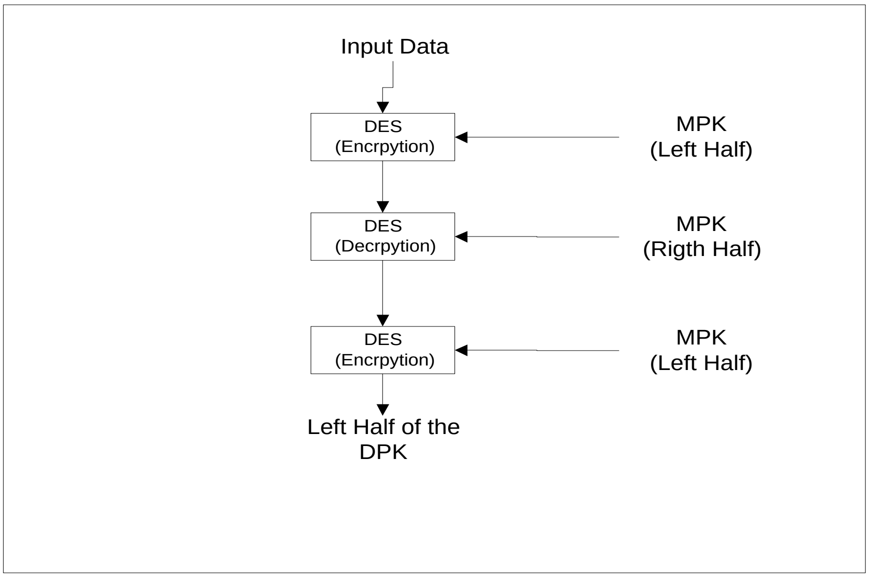
DPK 左半部分的推导方法

推导双倍长 DPK 左半部分的方法：

——将应用序列号的最右 16 个数字作为输入数据

——将 MPK 作为加密密钥

——用 MPK 对输入数据进行 Triple DES 运算



推导 DPK 左半部分

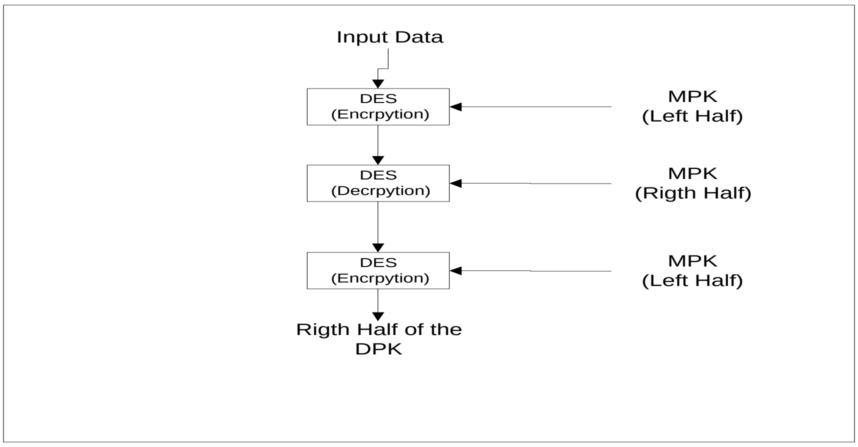
DPK 右半部分的推导方法

推导双倍长 DPK 右半部分的方法：

——将应用序列号的最右 16 个数字的求反作为输入数据

——将 MPK 作为加密密钥

——用 MPK 对输入数据进行 TripleDES 运算



推导 DPK 右半部分

图-B1 和图-B2 描述的方法同样适用于 ED 的消费/取现，圈存和圈提，修改

等子密钥的推导，及 EP 的消费和圈存子密钥的推导。

7.5.3、 过程密钥的产生

过程密钥是在交易过程中用可变数据产生的单倍长密钥。过程密钥产生后只能在某过程/交易中使用一次。

图 B3 描述了 EP 进行消费交易时产生过程密钥的机制。这方法也用于不同交易类型的过程密钥的产生，但输入的数据取决于不同的交易类型。

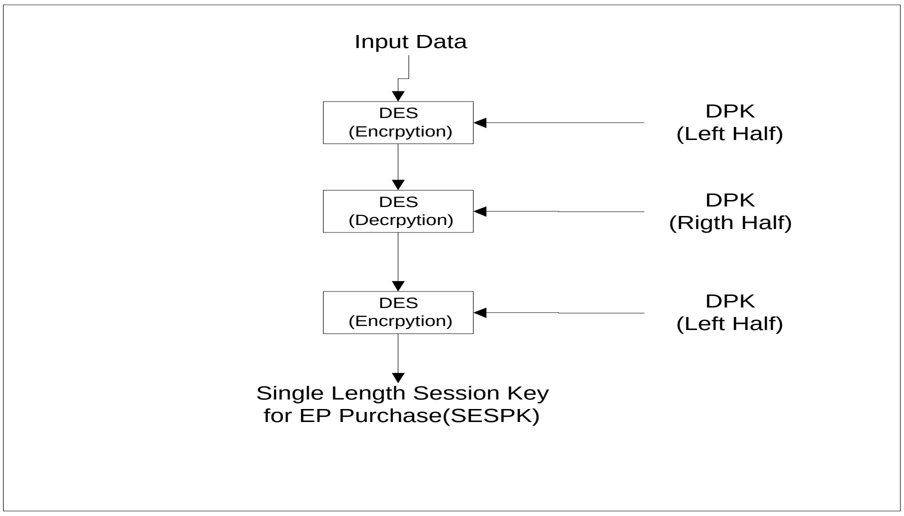


图-B3 过程密钥的产生

7.5.4、 交易 MAC/TAC的计算

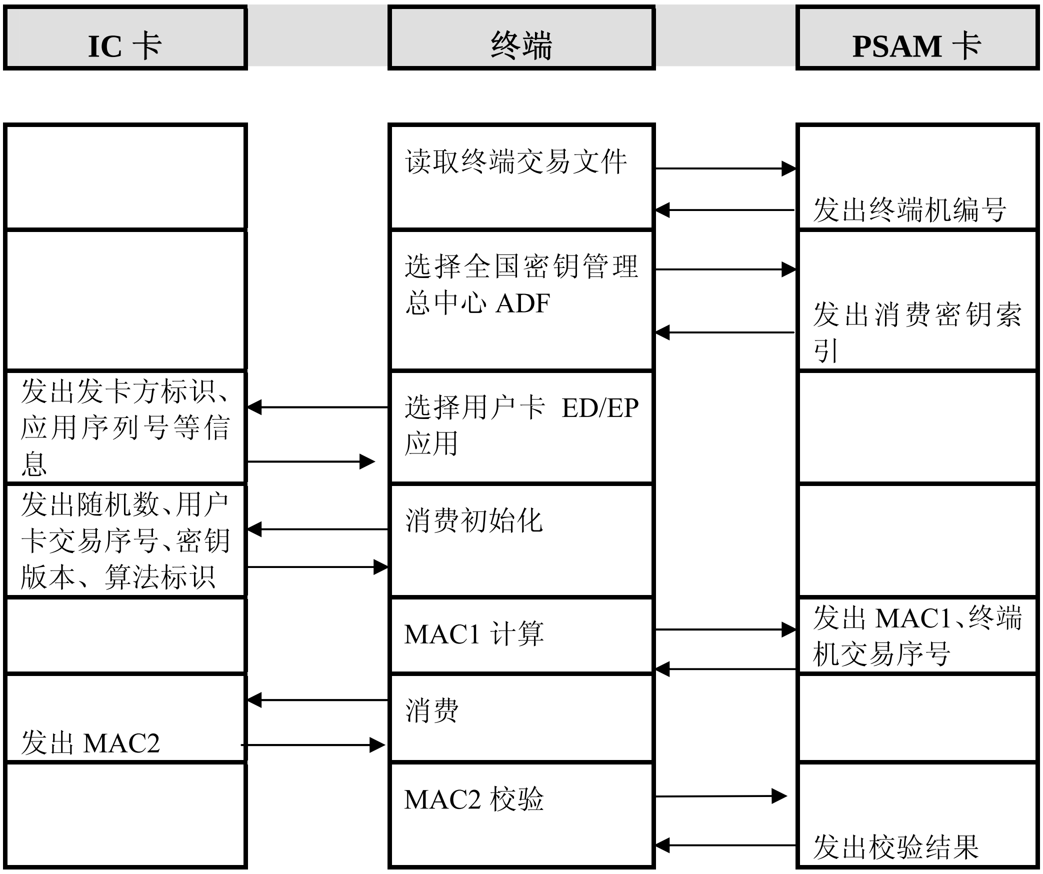
其计算方法如前所述的 MAC 的计算方法，只是其初始值为 8 个‘00’。

附录一、用户卡发卡流程

- 在 IC 卡生产过程中，IC 卡生产厂商在卡中设置生产商密钥（kMprd），控制 IC 卡的安全运输，以防止在 IC 卡生产商和发卡行机构间被人替换。在将 IC 卡交给发卡银行的同时，也将装有生产商密钥的母卡交给发卡银行。
- 发卡银行接到这一批 IC 卡后，首先按统一编号给每张 IC 卡分配母卡序列号（ASN）。每张 IC 卡具有唯一的 ASN，不同的 IC 卡具有不同的 ASN。
- PC 向高速发卡机发指令，送入一批卡片，利用生产商母卡上的 kMprd 来验证 IC 卡。
- 如验证通过，加载发卡银行的的主控密钥kIctlM，用kMprd将kIctlM加密，将密文 3DES（kMprd，kIctlM）载入IC卡，在IC卡内部使用kMprd解密密文，$3DES^{-1}$（kMprd，3DES（kMprd，kIctlM）），还原得到kIctlM。
- 在 kIctlM 的控制下，创建 MF 下的 EF 文件，并加载应用主控密钥 kActl，写入卡中。
- 在 kActl 的控制下，创建 ADF 下的文件，写入卡片子密钥。
- 在卡上打印应用序列号。
- 如果在写卡或打印卡号的过程中，出现错误，则将卡片作废，重新制作一张同样卡号的卡片。

附录二、消费交易流程

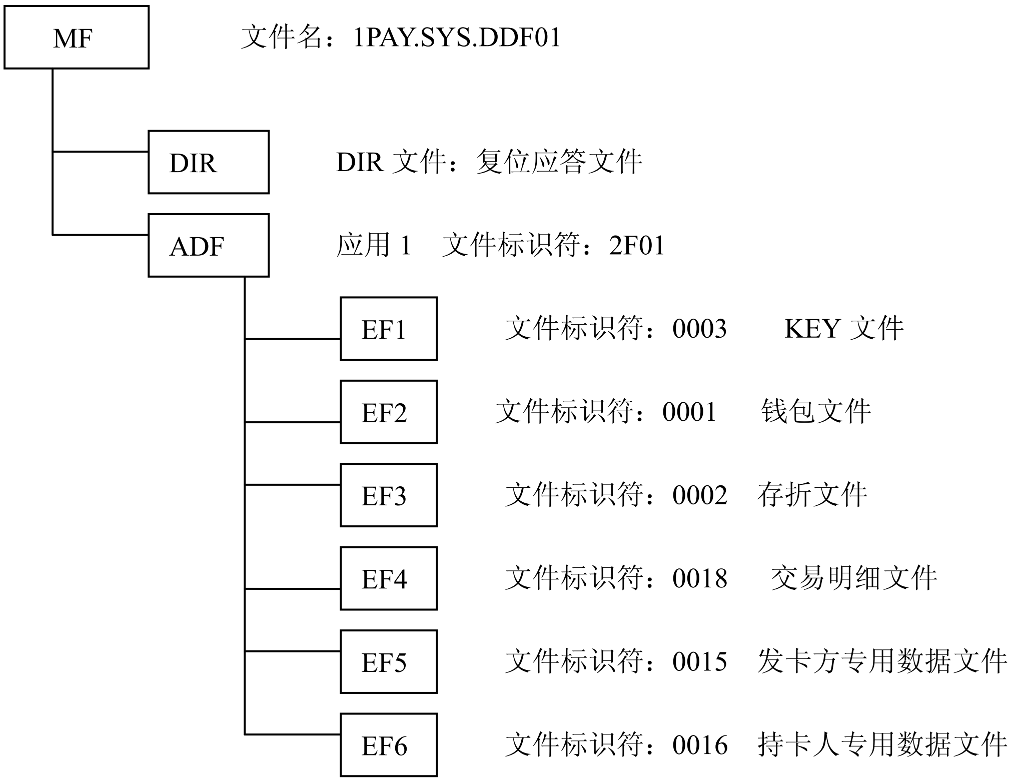
金融终端利用 PSAM 卡进行消费交易的处理流程如下图所示：



消费交易流程

附录三、SmartCOS金融应用举例

1．用户文件结构框图：



2．基本数据文件格式

在 PBOC 规范中定义了如下基本数据文件结构：

（1）电子存折 ED/电子钱包 EP 应用的公共应用基本数据文件

文件标识（SFI）			‘21’（十进制）
文件类型			透明
文件大小			30
文件存取控制		读=自由	改写=需要安全信息
字节	数据元		长度
1-8	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	应用启用日期		4
25-28	应用有效日期		4
29-30	发卡方自定义 FCI 数据		2

（2）电子存折 ED/电子钱包 EP 应用的持卡者基本数据文件

文件标识（SFI）		‘22’（十进制）
文件类型		透明
文件大小		39
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	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

（3）电子存折 ED/电子钱包 EP 交易明细文件

文件标识（SFI）		‘24’（十进制）
文件类型		循环
文件存取控制		读=PIN 保护 改写=不允许
记录大小		23
字节	数据元	长度
1-2	ED 或 EP 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（终端）	4
21-23	交易时间（终端）	3

（4）KEY 文件中必须安装如下密钥：

密钥类型	KEY 作用描述
0B	个人密码 PIN
00	消费/取现密钥
01	圈存密钥
02	TAC 密钥
03	圈提密钥
04	修改透支限额密钥
05	应用维护密钥
06	PIN 解锁密钥
07	PIN 重装密钥

3. 建立 PBOC 金融应用文件命令

建立 MF：
80 E0 00 00 18 (命令头) ff ff ff ff ff ff ff ff (8 字节传输代码) 0f (在 MF 下建立文件的权限) 01（DIR 文件的短文件标识符） 31 50 41 59 2e 53 59 53 2e 44 44 46 30 31(MF 的文件名称)

建立 DIR 文件：
80 E0 02 00 07 (命令头) 00 01（文件标识符）02（文件类型） 0F（读权限）0F（写权限）01（记录数）1E（记录长度）

写 DIR 文件：
00 E2 00 08 13 (命令头) 61 11 4F 09 A0 00 00 00 03 86 98 07 01 （ADF名称）50 04 50 42 4F 43

建立 ADF：
80 E0 01 00 0D (命令头) 2F 01（文件标识符）0f（建立文件权限） 00（保留） A0 00 00 00 03 86 98 07 01（ADF名称）

建立 DF 下密钥文件：
80 E0 02 00 07 (命令头) 6F 02（密钥文件标识 ）05（文件类型） 0F（增加新密钥的权限）00（保留） 0A（密钥个数） 00（保留，系统自动设置为 19）

安装个人密码 PIN ：
80 D4 00 00 0A (命令头) 01（密钥标识符）01（密钥版本号） 00（算法标识）0B（密钥类型）0F（使用权限） 01（后续状态）1F（修改权限）33 (错误计数器)12 34（个人密码）

安装外部认证密钥（DEAK） ：
80 D4 00 00 18 (命令头) 01（密钥标识符） 01（密钥版本号） 00（算法标识） 08（密钥类型） 0F（使用权限） 02（后续状态） 2F（修改权限） 33 （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装消费密钥 DPK ：
80 D4 00 00 18 (命令头) 02（密钥标识符） 01（密钥版本号） 00（算法标识） 00（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） 33 （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装圈存密钥 DLK ：
80 D4 00 00 18 (命令头) 01（密钥标识符） 01（密钥版本号） 00（算法标识） 01（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装圈提密钥 DULK ：

80 D4 00 00 18（命令头） 01（密钥标识符） 01（密钥版本号） 00（算法标识） 03（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装 TAC 的密钥 DTK ：
80 D4 00 00 18（命令头） 01（密钥标识符） 01（密钥版本号） 00（算法标识） 02（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装应用维护密钥 DAMK ：
80 D4 00 00 18（命令头） 01（密钥标识符） 01（密钥版本号） 00（算法标识） 05（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装 PIN 解锁密钥 DPUK ：
80 D4 00 00 18（命令头） 01（密钥标识符） 01（密钥版本号） 00（算法标识） 06（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装 PIN 重装密钥 DRPK ：
80 D4 00 00 18（命令头） 01（密钥标识符） 01（密钥版本号） 00（算法标识） 07（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

安装修改透支限额密钥 DUK ：
80 D4 00 00 18（命令头） 01（密钥标识符） 01（密钥版本号） 00（算法标识） 04（密钥类型） 0F（使用权限） 00（后续状态） F0（修改权限） FF （错误计数器）XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX（密钥内容）

建立公共应用基本文件 ：
80 E0 02 00 07（命令头） 00 15 （文件标识符）00（二进制文件类型)0F（读权限）0F(更新权限)00 1e（文件长度）

写公共应用基本数据文件:
00 D6 95 00 1E（命令头） A0 00 00 00 03 00 00 01（发卡方标识）03（应用类型标识）01（应用版本） 00 00 19 98 08 15 00 00 00 01（应用序列号） 20 00 10 01 （应用启用日期）20 02 12 31（应用有效日期）55 66 （发卡方自定义FCI数据）

建立持卡者基本数据文件 ：
80 E0 02 00 07（命令头） 00 16 （文件标识符）00（二进制文件类型)0F（读权限）0F（更新权限） 00 27（文件长度）

写卡持有者基本数据文件:
00 D6 96 00 27（命令头） 00（卡类型标识） 00（本行职工标识） 53 41 4d 50 00 00 00

00 00 00 00 00 00 00 00 00 00 00 00 00（持卡人姓名） 31 31 30 31 30 38 37 30 30 33 31 37 31 38 39 00（持卡人证件号码） 00 （持卡人证件类型）

建立交易明细文件 ：

80 E0 02 00 07（命令头） 00 18（文件标识符） 03（循环记录文件类型）0F（读权限）F0（更新权限）0a 17（文件长度）

建立电子钱包 EP 文件 ：

80 E0 02 00 07（命令头） 00 01（文件标识符）06（文件类型）00（保留）00（保留）00（保留）00（保留）

建立电子存折 ED 文件 ：

80 E0 02 00 07（命令头） 00 02（文件标识符）07（文件类型）00（保留）00（保留）00（保留）00（保留）

结束建立应用（DF） ：

80 E0 01 01 02（命令头） 2F 01（文件标识符）

结束建立 MF ：

80 E0 00 01 02（命令头） 3F 00（文件标识符）