TimeCOS/PSAM 通用技术

参考手册

(V1.0)

握奇数据系统有限公司

二零零二年九月

重要声明：

随着 TimeCOS/PSAM 卡片产品的升级，本手册内容将会做相应的修改。握奇数据系统有限公司保留对本手册内容进行修改的权利。

手册变化动态

修改日期	新版本序号	主要变化内容描述
2001 年 5 月	1.0	初稿
2002 年 9 月	1.0	修改稿

目 录

图形目录

表格目录

1. 关于本手册

1.1 内容概述

本手册各部分内容概述如下：

- TimeCOS/PSAM 简介
  本章介绍了 TimeCOS/PSAM 特点和 TimeCOS/PSAM 体系结构，使您对 TimeCOS/PSAM 卡片有一个初步的了解。

- PSAM 卡标准文件结构

- 安全报文传送
  本章描述了安全报文基本概念、安全报文传送实现方法、MAC 计算、DES 加密/解密计算及安全报文传送的命令情况。

- 基于 DES 的加密算法
  本章描述了 DES 算法、密钥分散算法、Double-One-Way 算法和安全计算。

- 命令与应答
  本章描述了命令与应答结构及命令返回状态码 SW1SW2 的意义。

- TimeCOS/PSAM 基本命令

- TimeCOS/PSAM 扩展命令

- 附录一 TimeCOS/PSAM 的复位应答

注：有关“TimeCOS/PSAM 文件管理”、“TimeCOS/PSAM 的安全体系”、“卡片初始化设置”和“TimeCOS/PSAM 发卡命令”见《TimeCOS/PSAM 专用技术参考手册》。

1.2 参考文献

[1] 《中国金融 IC 卡试点 PSAM 应用规范》

[2] ISO/IEC 7816 PART 3：识别卡，带触点的集成电路卡：电气特性和传输协议。

[3] ISO/IEC 7816 PART 4：识别卡，带触点的集成电路卡：行业间交换用命令。

1.3 定义

- 接口设备
  终端上插入 IC 卡的部分，包括其中的机械和电气部分。

- 终端 Terminal
  为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。包括接口设备，也可包括其他部件和接口，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。

- 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。

- 功能 Function
  由一个或多个命令实现的处理过程，其操作结果用于完成全部或部分交易。

- 集成电路
  设计用于完成处理和/或存储功能的电子器件。

- 集成电路卡(IC 卡)Integrated Circuit(s) Card
  内部封装一个或多个集成电路的 ID-1 型卡（如 ISO 7810、ISO 7811 第 1 至 5 部分、ISO 7812 和 ISO 7813 中描述的）。

- 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 Authentication 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。

- 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。

- 保密密钥 Secret Key
  对称加密技术中仅供指定实体所用的密钥。

- 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。

- 对称加密技术 Symmetric Cryptographic Technique
  发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

- 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。

- T=0
  面向字符的异步半双工传输协议。

- T=1
  面向块的异步半双工传输协议。

- 金融交易
  持卡者、商户和收单行之间基于收、付款方式的商品或服务交换行为。

- 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个人密码（PIN）保护的金融 IC 卡应用。它支持圈存、圈提、消费、取现、修改透支限额及查询余额交易。

- 电子钱包 Electronic Purse
  一种为持卡人小额消费而设计的金融 IC 卡应用。它支持圈存、消费和查询余额交易。除圈存交易外，使用电子钱包进行的其他交易均不记录明细，且均无需提交个人密码（PIN）。

- 消费 Puchase
  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。

1.4 缩略语和符号表示

以下缩略语和符号表示适用于本手册：

AID	：	应用标识符（Application Identifier）
APDU	：	应用协议数据单元（Application Protocol Data Unit）
ATR	：	复位应答（Answer to Reset）
b	：	二进制（Binary）
BER	：	基本编码规则（Basic Encoding Rules）
BWI	：	块等待时间整数（Block Waiting Time Integer）
CLA	：	命令报文的类别字节（Class Byte of the Command Message）
CWI	：	字符等待时间整数（Character Waiting Time Integer）
DEA	：	数据加密算法（Data Encryption Algorithm）

DES : 数据加密标准（Data Encryption Satandard）
DF : 专用文件（Dedicated File）
DIR : 目录（Directory）
ED : 电子存折（Electronic Deposit）
EDC : 错误检测代码（Error Detection Code）
EF : 基本文件（Elementary File）
EMV : Europay、Mastercard、VISA
EP : 电子钱包（Electronic Purse）
Etu : 基本时间单元（Elementary Time Unit）
FCI : 文件控制信息（File Control Information）
FID : 文件标识（File Identifier）
GND : 地（Ground）
Hex. : 十六进制数（Hexadecimal）
IC : 集成电路（Integrated Circuit）
ICC : 集成电路卡（Integrated Circuit Card）
IEC : 国际电工委员会（International Electrotechnical Commission）
INS : 命令的指令字节（Instruction Byte of Command Message）
ISO : 国际标准化组织（International Standardization Organization）
Lc : 终端发出的命令数据域的实际长度
Le : 响应数据的最大期望长度
LEN : 长度（Length）
MAC : 报文鉴别代码（Message Authentication Code）
MF : 主控文件（Master File）
P1 : 参数 1（Parameter 1）
P2 : 参数 2（Parameter 2）
PBOC : 中国人民银行
PIN : 个人密码（Personal Identification Number）
PIX : 专用应用标识符扩展码（Proprietary Application Identifier Extension）
PSA : 支付系统应用（Payment System Application）
PSAM : 消费安全存取模块（Purchase Secure Access Module）
PSE : 支付系统环境（Payment System Environment）
RFU : 保留为将来使用（Reserved for Future Use）
RID : 已注册的应用提供者标识（Registered Application Provider Identify）
RST : 复位（Reset）
SAM : 安全存取模块（Secure Access Module）
SFI : 短文件标识符（Short File Identifier）
SW1 : 状态码 1（Status Word One）
SW2 : 状态码 2（Status Word Two）
TAC : 交易认证码（Transaction Authorization Crypogram）
TCK : 校验字符（Check Character）
TLV : 标签、长度、值（Tag Length Value）
VCC : 电源电压（Supply Voltage）
VPP : 编程电压（Programming Voltage）

‘0’～‘9’和‘A’ ～‘F’ ： 十六进制数
0x00～0x0F ：十六进制数
XX ： 1 个字节 16 进制数
XXXX ： 2 个字节 16 进制数
XX…XX ：未知个字节 16 进制数

2. TimeCOS/PSAM 简介

2.1 关于 TimeCOS/PSAM

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

TimeCOS/PSAM(Time Card Operating System)是由握奇数据系统有限公司自行开发的智能卡（SmartCard）操作系统，完全符合以下国际、国内标准：

- 识别卡，带触点的集成电路卡标准 《ISO7816-1/2/3/4》
- 《中国金融IC卡试点PSAM应用规范》

TimeCOS/PSAM具有以下主要特征：

- 支持一卡多应用，各应用之间相互独立（多应用、防火墙功能）。
- 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。
- 在通讯过程中支持多种安全保护机制（信息的机密性和完整性保护）。
- 支持多种安全访问方式和权限（认证功能和口令保护）。
- 支持中国人民银行认可的Single DES、Triple DES算法。
- 支持中国人民银行规定的PSAM卡消费交易流程。
- 支持多级密钥分散机制，用分散后的密钥作为临时密钥对数据进行加密、解密、MAC等运算，以完成终端与卡片之间的合法性认证等功能。
- 支持多种速率选择 可支持9600bps、38400bps、56K bps等不同的通讯速率。

2.2 TimeCOS 体系结构

2.2.1 卡片逻辑内部结构

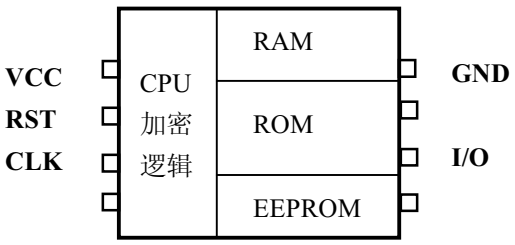


图 2-1 卡片内部逻辑结构

TimeCOS 卡片芯片由以下四部分硬件模块组成：（见图 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。

- RAM
  TimeCOS 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。
- ROM
  存放 TimeCOS 程序的区域。
- EEPROM
  存放用户应用数据区域，TimeCOS 将用户数据以文件形式保存在 EEPROM 中，在满足用户规定的安全条件时，可进行读或写。

2.2.2 TimeCOS 功能模块划分

TimeCOS 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 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 TimeCOS 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。

2.2.3 TimeCOS/PSAM 命令集

表 2.1 TimeCOS/PSAM 命令集

编号	命令名称	CLA	INS	功能描述	兼容性
1	Verify PIN	00	20	验证口令	ISO&PBOC
2	External Authentication	00	82	外部认证	ISO&PBOC
3	Get Challenge	00	84	取随机数	ISO&PBOC
4	Internal Authentication	00	88	内部认证	ISO&PBOC
5	Select File	00	A4	选择文件	ISO&PBOC
6	Read Binary	00	B0	读二进制文件	ISO&PBOC
7	Read Record	00	B2	读记录文件	ISO&PBOC
8	Get Response	00	C0	取响应数据	ISO&PBOC
9	Update Binary	00/04	D6	写二进制文件	ISO&PBOC
10	Update Record	00/04	DC	写记录文件	ISO&PBOC
11	Application Unblock	84	18	应用解锁	PBOC
12	Init_For_Descrypt	80	1A	通用 DES 计算初始化	PBOC
13	Application Block	84	1E	应用锁定	PBOC
14	Reload/Change PIN	80	5E	重装/修改 PIN	PBOC
15	Init_SAM_For_Purchase	80	70	MAC1 计算	PBOC
16	Credit_SAM_For_Purchase	80	72	校验 MAC2	PBOC
17	DES Crypte	80	FA	通用 DES 计算	PBOC
18	Erase DF	80	0E	擦除 DF	专有
19	Secure Calculation	80	1C	安全计算	专有
20	Write Key	80/84	D4	增加或修改密钥	专有
21	Create File	80	E0	建立文件	专有

3. PSAM 卡文件结构

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

PSAM 卡文件结构如下图所示：

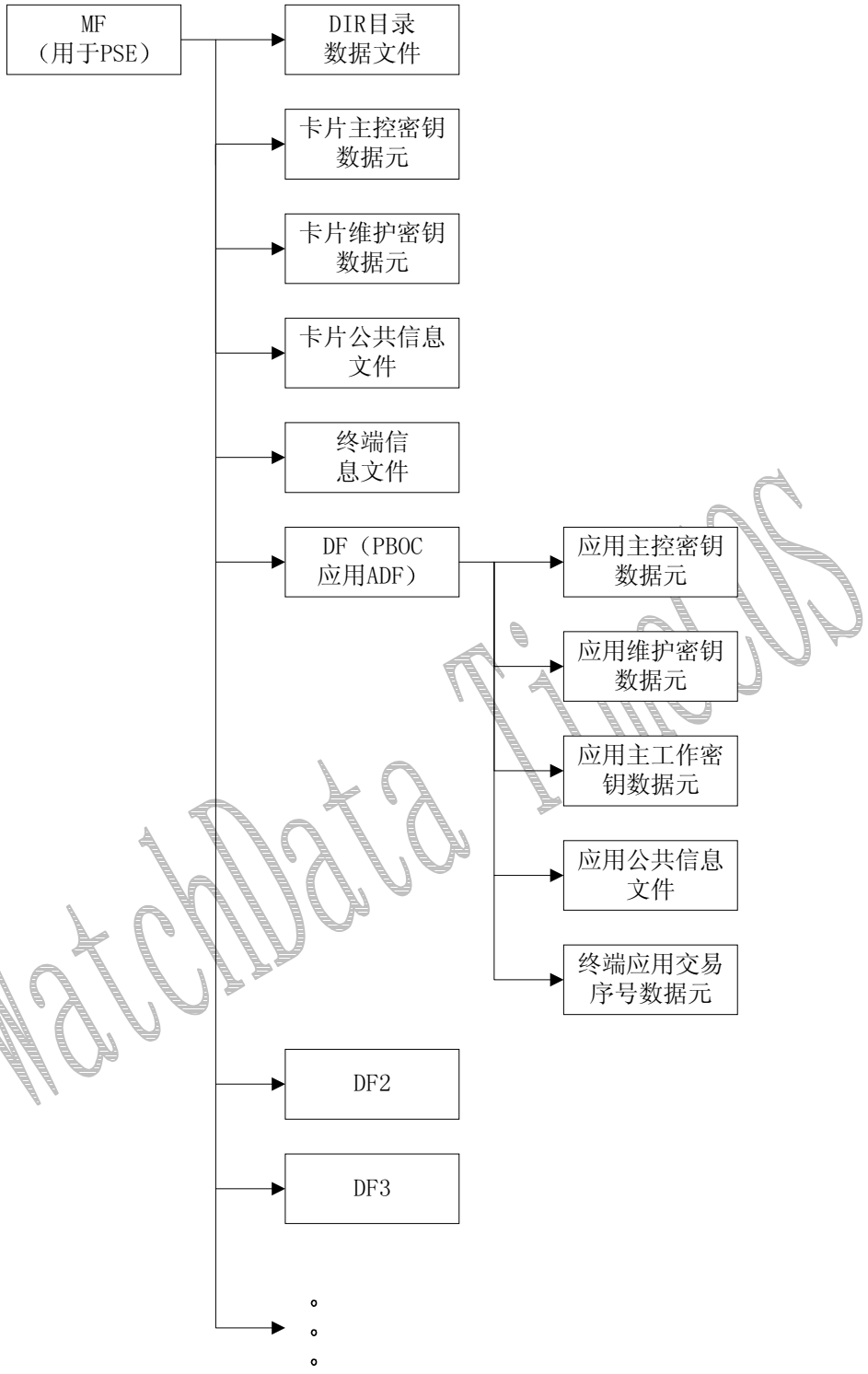


图 3-1 PSAM 卡文件结构

4. 安全报文传送

4.1 安全报文传送概念

安全报文传送的目的是保证数据的机密性、完整性和对发送方的认证。数据的机密性通过对数据域的加密来得到保证。数据完整性和对发送方的认证通过使用报文鉴别代码MAC来实现。

1. 完整性保护（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。

2. 机密性保护（加密保护）

对传输的数据进行DES加密，这样传输的就是密文，攻击者即使获得数据也没有意义，分析后只能得到错误的结果。

数据的机密性通过对数据域的加密来得到保证。

3. 机密性和完整性保护（线路加密保护）

此种方式最安全。 对传输的数据进行DES加密，后对传输的数据附加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。

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。

4.2 如何实现安全报文传送

4.2.1 文件

二进制文件、定长记录文件、变长记录文件、循环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。

文件类型定义如下：

b7	b6	b5	b4	b3	b2	b1	b0	线路保护方式
0	0	文件类型						无
1	0	文件类型						MAC
1	1	文件类型						DES&MAC

图 4-1 文件类型设置

[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。

- 卡片可以在建立文件时分别设置读/写文件所使用的维护密钥标识（详细设置见“《TimeCOS/PSAM专用技术参考手册》之7.1 Create File”）。

4.2.2 密钥

密钥的安装与更新必须采用加密带MAC方式。

4.3 MAC 计算

MAC 总是命令或命令响应数据域中最后一个数据元素。在 TimeCOS/PSAM 中规定 MAC 的长度皆为 4 个字节。

MAC 的计算步骤如下：

第一步： 终端向 IC 卡发出一个 Get Challenge 命令，从 IC 卡取回 4 字节随机数。
然后在该随机数后补‘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：
——命令报文：CLA，INS，P1，P2，Lc+4，DATA。
必须置CLA的后半字节为十六进制‘4’。
在命令报文数据域中（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)
——命令响应报文：DATA（包含明文或密文）。
——TimeCOS/PSAM命令中定义的数据。

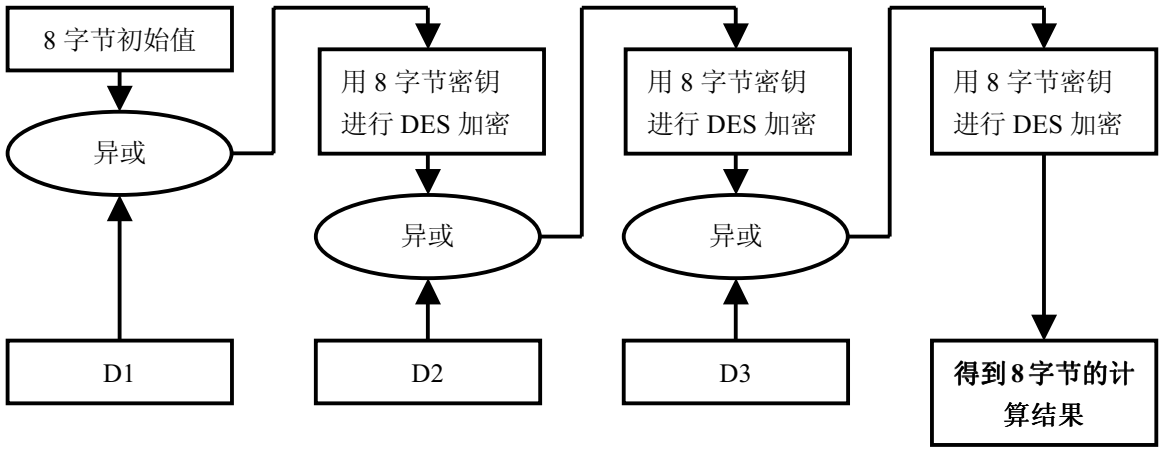
第三步： 将该数据块分成 8 字节为单位的数据块，标号为 D1，D2，D3 等。最后的数据块有可能是 1-8 个字节。

第四步： 如果最后的数据块长度是 8 字节的话，也必须在其后加上 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，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；否则在其后加上 16 进制数字‘00’直到长度达到 8 字节为止。

第五步： 对这些数据块使用相应密钥进行加密。(有关密钥由 TimeCOS/PSAM 命令或中国金融 PSAM 卡专用命令所指定)

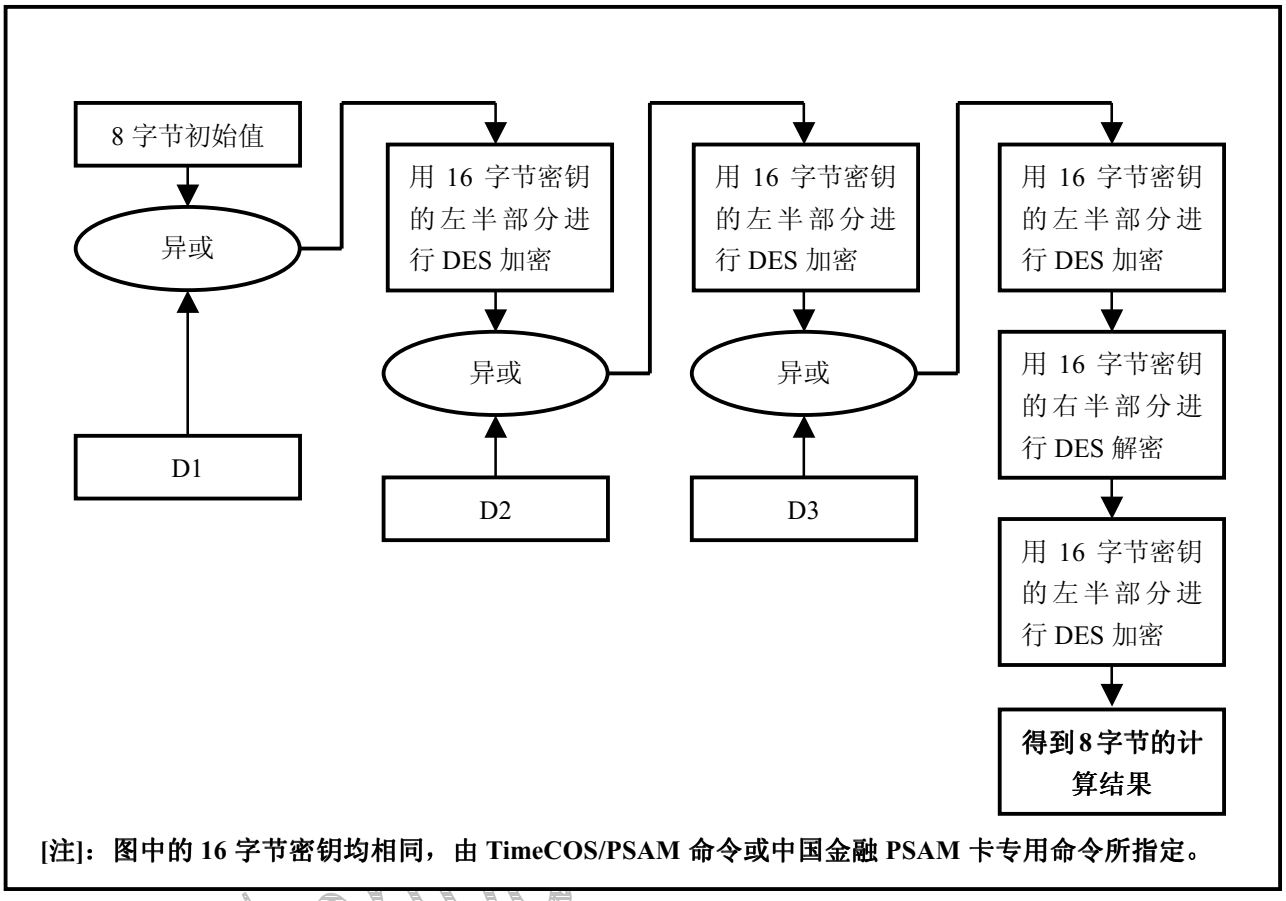
- 如果该密钥长度为8字节，则依照图4-2的方式来产生MAC（根据在第三步中产生的数据块长度的不同，有可能在计算中会多于或少于三步）。
- 如果该密钥长度为16字节，则依照图4-3的方式来产生MAC（根据在第三步中产生的数据块长度的不同，有可能在计算中会多于或少于三步）。

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。



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

图 4-2 用 Single DES 密钥产生 MAC 的算法



[注]：图中的 16 字节密钥均相同，由 TimeCOS/PSAM 命令或中国金融 PSAM 卡专用命令所指定。

图 4-3 用 Triple DES 密钥产生 MAC 的算法

4.4 数据加密和解密

4.4.1 数据加密

按照如下方式对数据进行加密：

第一步： 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。

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 16 进制数字‘00’直到长度达到 8 字节。

第四步： 对每一个数据块使用相应密钥进行加密。（密钥由 TimeCOS/PSAM 命令或中国金融 PSAM 卡专用命令所指定）。

- 如果该密钥长度为 8 字节，则依照图 4-4 的方式来加密数据块。
- 如果该密钥长度为 16 字节，则依照图 4-5 的方式来加密数据块。

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。

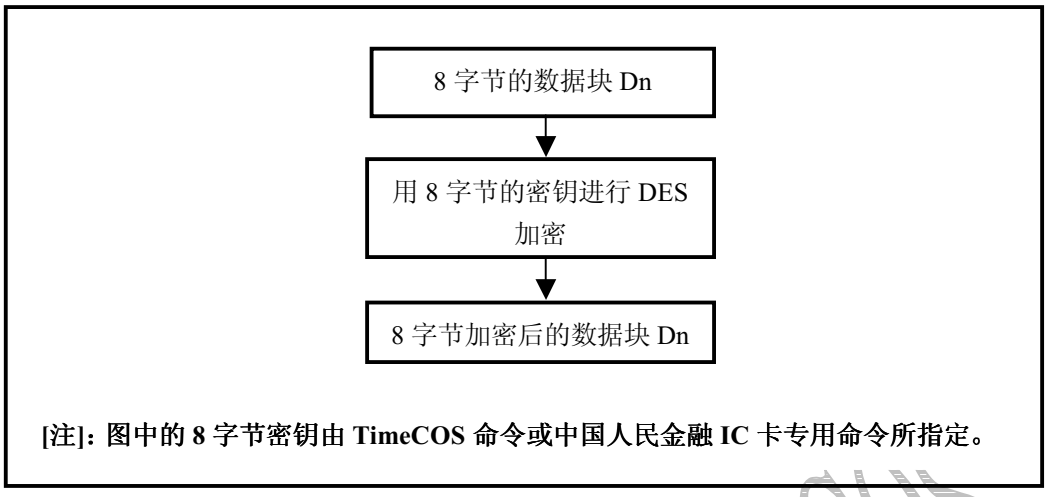


图 4-4 用 Single DES 密钥进行数据加密的算法

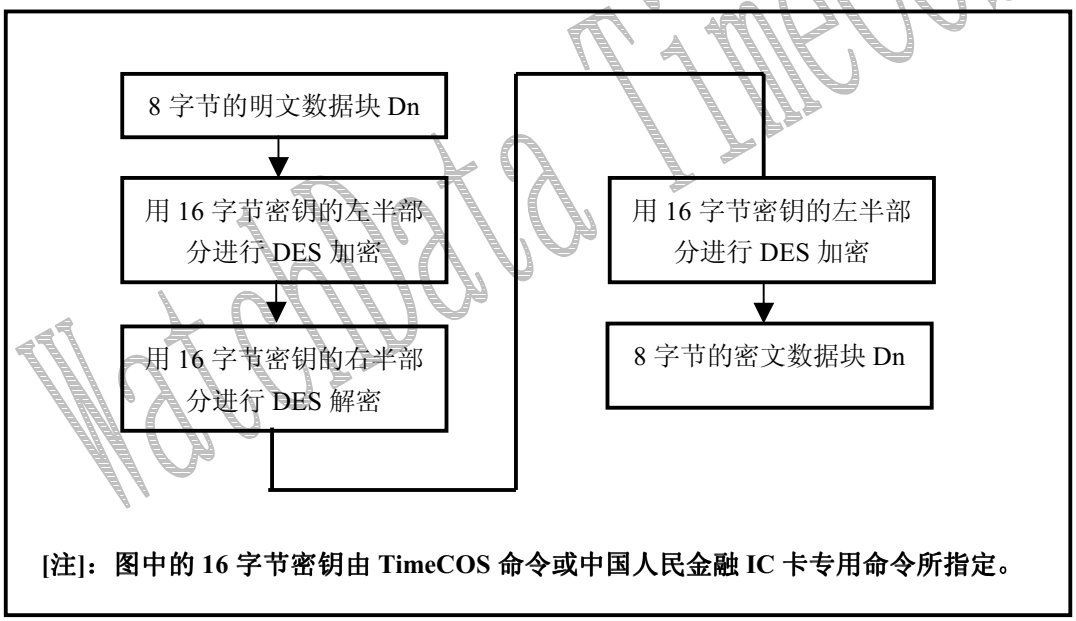


图 4-5 用 Triple DES 密钥进行数据加密的算法

4.4.2 数据解密

按照如下方式对数据进行解密：

第一步： 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。

第二步： 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 TimeCOS/PSAM 命令或中国金融 PSAM 卡专用命令所指定）

- 如果该密钥长度为 8 字节，则依照图 4-6 的方式来解密数据块。
- 如果该密钥长度为 16 字节，则依照图 4-7 的方式来解密数据块。

第三步： 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 LD、明文数据、填充字符组成。

第四步：因为 LD 表示明文数据长度，因此，它被用来恢复明文数据。

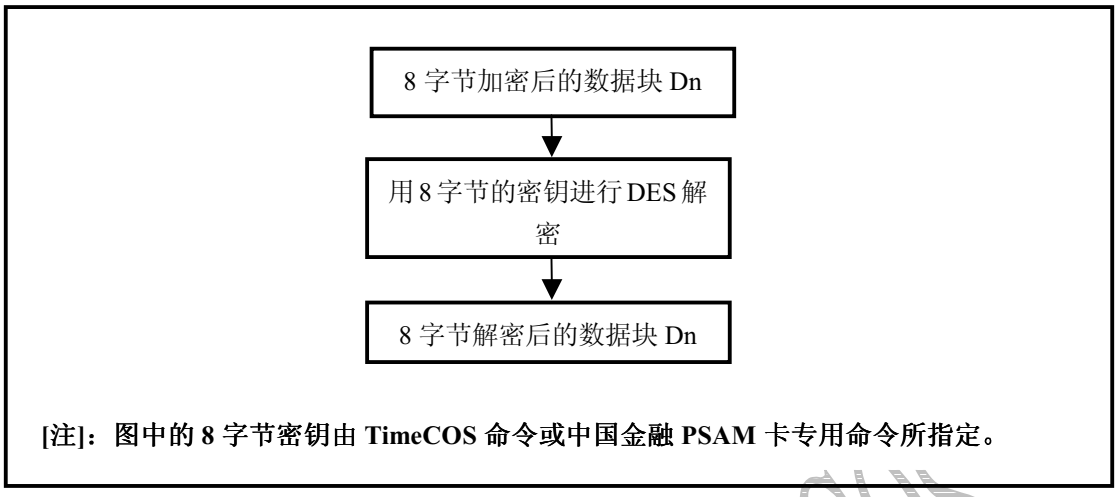


图 4-6 用 Single DES 密钥进行数据解密的算法

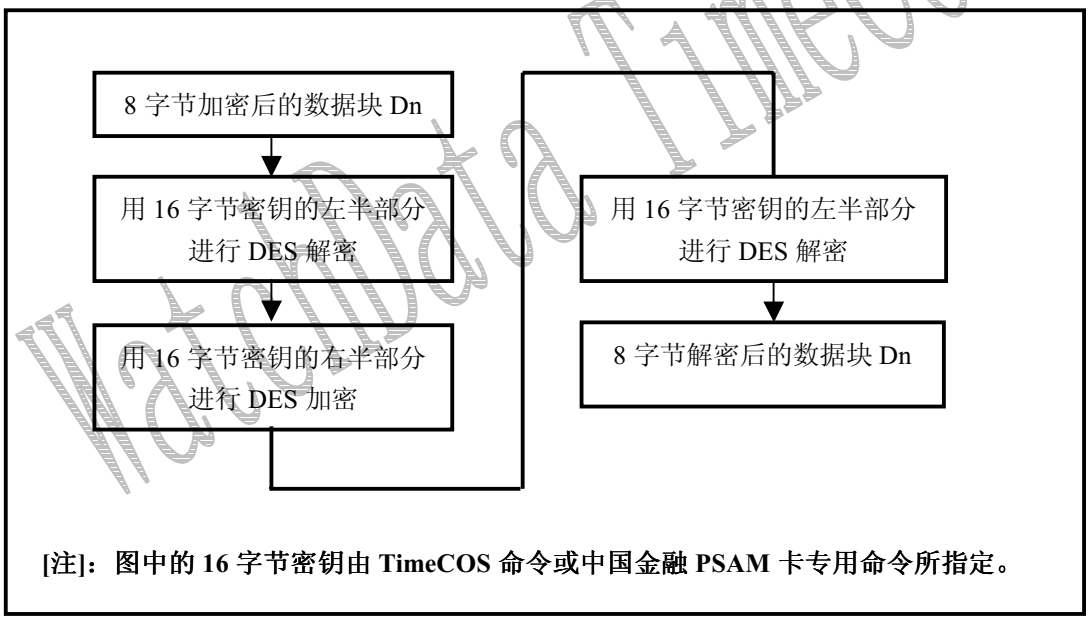


图 4-7 用 Triple DES 密钥进行数据解密的算法

4.4.3 过程密钥

过程密钥是由指定密钥对可变数据加密产生的单倍长密钥。过程密钥产生后只能在某一（消费、取现等）过程中有效。

图 4-8 描述了产生过程密钥的机制。输入数据是 8 字节，输入数据的定义见相关命令描述。

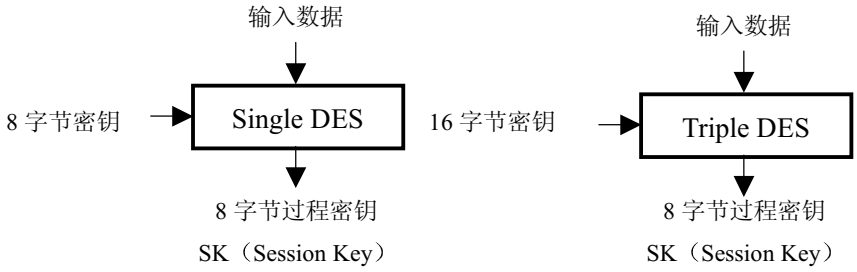


图 4-8 过程密钥的产生

4.5 安全报文传送的命令情况

- 情形 1

  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）。

不含安全报文的命令：	**CLA**	**INS**	**P1**	**P2**		
含安全报文的命令：	**CLA**	**INS**	**P1**	**P2**	**Lc**	**MAC**

  安全报文传送： **CLA** 字节的低 4 位必须是 04.
  Lc 是 MAC 的长度（4 字节）.

- 情形 2

  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。

不含安全报文的命令：	**CLA**	**INS**	**P1**	**P2**	**Le**		
含安全报文的命令：	**CLA**	**INS**	**P1**	**P2**	**Lc**	**MAC**	**Le**

  安全报文传送： **CLA** 字节的低 4 位必须是 04.
  Lc 是 MAC 的长度（4 字节）.

- 情形 3

  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。

不含安全报文的命令：	**CLA**	**INS**	**P1**	**P2**	**Lc**	**DATA**	
含安全报文的命令：	**CLA**	**INS**	**P1**	**P2**	**Lc**	**DATA**	**MAC**

  安全报文传送： **CLA** 字节的低 4 位必须是 04.
  Lc =数据长度+MAC 的长度（4 字节）.

- 情形 4

  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。

不含安全报文的命令：	CLA	INS	P1	P2	Lc	DATA	Le

含安全报文的命令：	CLA	INS	P1	P2	Lc	DATA	MAC	Le

安全报文传送： **CLA** 字节的低 4 位必须是 04.
Lc =数据长度+MAC 的长度（4 字节）.

4.6 应用举例

[1] 命令：写二进制文件（Update Binary）

- 线路保护模式： DES&MAC（线路加密保护）
- 维护密钥值：5741544348444154415469 6D65434F53
- 条件：文件标识符=03；

  文件主体空间=8 字节；

  文件建立时采用线路加密保护。
- 操作：写二进制文件，写入数据：1122334455667788

[步骤 1] 取 4 字节随机数，计算 MAC 用。

命令：00 84 00 00 04

响应：46 4E 84 AF 9000

[步骤 2] 写二进制文件，写入数据：1122334455667788

命令：04 D6 83 00 14 68 7E 0F 83 F6 A9 85 80 C4 01 5C EB 8D 00 F3 8B 1C AB E2 B9

说明：68 7E 0F 83 F6 A9 85 80 C4 01 5C EB 8D 00 F3 8B 为使用维护密钥对数据 08 11 22 33 44 55 66 77 88 80 00 00 00 00 00 00 加密后的结果，加密方法见“4.4.1 数据加密”。 1C AB E2 B9 为使用维护密钥对命令报文生成的 4 字节 MAC 码，计算方法见“4.3 MAC 计算”。

响应：9000

5. 基于 DES 的加密算法

5.1 DES 加密算法

TimeCOS/PSAM支持Single DES、Triple DES密码算法，密钥长度分别是8和16个字节。DES属于对称算法，加密和解密密钥相同。

Single DES算法

Single DES 算法是指使用单长度（8 字节）密钥 K 对 8 字节块的输入数据 X_1，X_2，X_3…加密，得到 8 字节块的输出数据 Y_1，Y_2，Y_3…。其中，

$$Y_I = DES\ (K)\ [\ X_I\ ]$$

解密方式如下：

$$X_I = DES^{-1}\ (K)\ [\ Y_I\ ]$$

3DES 算法（Triple DES 算法）

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

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

解密的方式如下：

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

5.2 密钥分散算法

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 8 个字节作为输入数据；
- 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 8 个字节求反，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。

5.3 Double-One-Way 算法

Double One Way 方式是用双长度的密钥 MK 对 8 字节的输入数据按下列方式进行运算。具体运算的过程如下（MK 的左半部为 LK，右半部为 RK）：

- 用 LK 对输入数据进行解密运算；

- 用 RK 对第一步结果进行加密运算；
- 用 LK 对第二步结果进行解密运算；
- 输入数据与第三步结果进行异或。

5.4 安全计算（Secure Calculation）

安全计算(Secure Calculation)用 KeyID 指定的密钥对输入数据进行运算，具体过程如下：

方式 0:

首先用卡内密钥对最后 8 字节序列号加密.

用加密的结果作为临时密钥对 inputdata1 进行解密运算,解密的结果与 inputdata2 异或后再用临时密钥解密,依此类推.

解密运算的结果与 inputdata N-1 异或,用临时密钥解密,将最后的解密运算的 8 字节结果送出.

方式 1:

首先用卡内密钥对最后 8 字节序列号解密.解密的结果与输入异或后作临时密钥。

用临时密钥对 inputdata1 进行加密运算,加密的结果与 inputdata2 异或后再用临时密钥加密,依此类推.

加密运算的结果与 input N-1 异或,用临时密钥加密,将最后的加密运算的 8 字节结果送出.

6. 命令与应答

6.1 命令与响应格式

从终端发出的命令和卡片响应的信息必须遵从以下 4 种格式。

情形 1:

命令：	**CLA**	**INS**	**P1**	**P2**	**00**
响应：	**SW1**	**SW2**			

情形 2:

命令:	**CLA**	**INS**	**P1**	**P2**	**Le**
响应:	**Le 字节的 DATA**			**SW1**	**SW2**

情形 3:

命令:	**CLA**	**INS**	**P1**	**P2**	**Lc**	**DATA**
响应：	**SW1**	**SW2**				

情形 4:

命令:	**CLA**	**INS**	**P1**	**P2**	**Lc**	**DATA**	**Le**
响应:	**Le 字节的 DATA**				**SW1**	**SW2**	

6.2 命令格式

TimeCOS 命令由 4 字节的命令头和命令体组成，见图 6-1。

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

图 6-1 命令格式

6.2.1 命令头域

命令头定义板报文的内容如下表所示：

表 6.1 命令头域

代码	长度 (byte)	值 (Hex)	描述
CLA	1	X0	不带安全报文的命令
		X4	带安全报文的命令
INS	1	XX	指令代码
P1	1	XX	参数 1
P2	1	XX	参数 2

6.2.2 命令体

命令体中各项是可选的。

Lc 命令数据域中 DATA 的长度，该长度不可超过 178 字节。
Data 命令和响应中的数据域
Le 响应数据域中期望数据的长度。
Le=00，表示需要最大字节数， 该长度不可超过 178 字节。

XX ⇒ 1 个字节 16 进制数
XXXX ⇒ 2 个字节 16 进制数
XX...XX ⇒ 未知个字节 16 进制数

6.3 响应数据格式

TimeCOS 命令的应答由数据和状态字组成，见图 6-2。

数据	状态字	
响应中接收的数据位串	SW1	SW2

图 6-2 响应数据格式

6.3.1 返回数据

返回数据域是可选项。

6.3.2 返回状态字（SW1SW2）

SW1 SW2 是卡片执行命令的返回代码，任何命令的返回信息都至少由一个状态字组成。

6.4 状态字 SW1SW2 意义

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。

状态字由2部分组成：

- SW1（status word1）：表示命令处理状态；
- SW2（status word1）：表示命令处理限定。

表 6.2 状态字 SW1SW2

SW1	SW2	Description
90	**00**	正确执行
61	**XX**	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
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
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
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。

7. TimeCOS/PSAM 基本命令

- 有关安全报文的操作见“4.安全报文传送”。

表 7.1 列出了 TimeCOS/PSAM 基本命令。

表 7.1 TimeCOS/PSAM 基本命令列表

序号	命令	CLA	INS	功能描述	兼容性
1	**External Authentication**	00	82	外部认证	ISO&PBOC
2	**Get Chanllenge**	00	84	取随机数	ISO&PBOC
3	**Get Response**	00	C0	取响应数据	ISO&PBOC
4	**Internal Authentication**	00	88	内部认证	ISO&PBOC
5	**Read Binary**	00	B0	读二进制文件	ISO&PBOC
6	**Read Record**	00	B2	读记录文件	ISO&PBOC
7	**Select File**	00	A4	选择文件	ISO&PBOC
8	**Update Binary**	00/04	D6	写二进制文件	ISO&PBOC
9	**Update Record**	00/04	DC	写记录文件	ISO&PBOC
10	**Verify PIN**	00	20	验证口令	ISO&PBOC

7.1 External Authentication（外部认证）

7.1.1 定义与范围

External Authentication命令要求IC卡中的应用验证密码。

7.1.2 命令报文

表 7.2 External Authentication 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	00	-
INS	1	82	-
P1	1	00	-
P2	1	XX	外部认证密钥标识号
Lc	1	8	-
DATA	8	XX...XX	8 字节加密后的随机数
Le	-	-	-

说明：

将命令中的数据用指定主控密钥或外部认证密钥解密，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。

7.1.3 命令报文数据域

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

7.1.4 响应报文数据域

响应报文数据不存在。

7.1.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.3 External Authentication 命令响应状态码

SW1	SW2	意义
90	00	正确执行
63	CX	还剩 x 次可试机会
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
93	02	安全信息不正确
94	03	密钥未找到

7.1.6 外部认证过程

外部认证是卡片对机具的认证，认证过程如下图所示：

终端	方向	PSAM 卡片
取 4 字节随机数	⇒	卡片内部产生随机数 RND_{ICC}
	⇐	送随机数 RND_{ICC}
用与卡片认证密钥相同的密钥 Cardkey 对 RND_{ICC}+4 字节‘00’进行加密得鉴别数据 D1。即：D1=DES(Cardkey, RND_{ICC}+‘00000000’)；		
送鉴别数据 D1 作外部认证。	⇒	卡片用指定的外部认证密钥对 D1 进行解密运算，产生鉴别数据 D2，后比较 D2 和 RND_{ICC}+‘00000000’。即：1)D2=DES^{-1}(KID,D1) 2)D2?=RND_{ICC}+‘00000000’
	⇐	送比较结果(即 SW1SW2)，若比较正确，则置安全状态寄存器值为该密钥后续状态。

图 7-1 外部认证过程

说明：

1．终端从卡片取随机数 RND_{ICC}；

2．终端用相应的密钥对 RND_{ICC} 和‘00000000’进行 DES 加密运算，产生鉴别数据 D1；

4．终端向卡片发出外部认证命令，送入 D1 到卡片内；

00 82 00 kid 08 D1

5．卡片收到 D1 后，用卡内的相应密钥对 D1 进行 DES 解密运算，产生 8 字节鉴别数据 D2；
卡片比较RND_{ICC}+‘00000000’和D2，

- 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。

7.1.7 应用举例

[1] 条件：外部密钥标识号=01；

使用权限=0xF0；

更改权限=0xEF；

错误计数器=0x33；

后续状态=01；

16 字节的密钥=‘574154434844415441546 96D65434F53’。

操作：外部认证。

[步骤 1] 取 8 字节随机数。

命令：00 84 00 00 04

响应：D3 89 BF 67 9000

[步骤 2] 卡终端用与外部认证密钥相同的密钥‘574154434844415441546 96D65434F53’对随机数+’00000000’进行加密，加密后的结果为 CA 19 81 F5 70 7F 35 BC.

[步骤 3] 卡终端将加密后的随机数送到卡中作外部认证。

命令：00 82 00 00 08 CA 19 81 F5 70 7F 35 BC

说明：其中 C1 8A 5B 4B 13 40 25 21 是[步骤 2]中加密后的数据。

响应：9000

说明：成功执行后置安全状态寄存器值为该外部认证密钥的后续状态 01.

7.2 Get Response（取响应数据）

7.2.1 定义与范围

当 APDU 不能用现有协议传输时，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。

7.2.2 注意事项

- 此命令只用于T=0通讯协议。

7.2.3 命令报文

表 7.4 Get Response 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	00	-
INS	1	C0	-
P1	1	00	-
P2	1	00	-
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	XX	期望响应数据的长度

7.2.4 命令报文数据域

命令报文数据不存在。

7.2.5 响应报文数据域

响应报文数据的长度由 Le 的值决定。

7.2.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.5 Get Response 命令响应状态码

SW1	SW2	意义
90	00	正确执行
67	00	长度错误（Le 大于卡中响应数据长度）
6F	00	卡中无数据可返回

7.2.7 应用举例

[1] 操作：选择 MF.

命令：00 A4 00 00 02 3F 00

响应：6117

说明：对于 T=0 的卡片，6117 表示卡片要回送的数据长度，可以通过 Get Response 命令取返回数据。对于握奇读写机具，产品默认设置为可自动读取卡片响应数据，所以无需通过 Get Response 命令取返回数据。

命令：00 C0 00 00 17

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

7.3 Get Challenge（取随机数）

7.3.1 定义与范围

Get Challenge命令请求一个用于安全相关过程（如安全报文）的随机数。

7.3.2 命令报文

表 7.6 Get Challenge 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	00	-
INS	1	84	-
P1	1	00	-
P2	1	00	-
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	04-10	要求卡片返回的随机数长度

7.3.3 命令报文数据域

命令报文数据不存在。

7.3.4 响应报文数据域

响应报文数据包括随机数，长度为 Le 个字节。

7.3.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.7 Get Challenge 命令响应状态码

SW1	SW2	意义
90	00	正确执行
67	00	长度错误
6A	81	不支持此功能（无 MF 或卡片已锁定）

7.4 Internal Authentication（内部认证）

7.4.1 定义与范围

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。

7.4.2 注意事项

- 在满足该密钥的使用条件时才能执行此命令。

7.4.3 命令报文

表 7.8 Inernal Authentication 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	00	-
INS	1	88	-
P1	1	00	加密
P2	1	XX	内部认证密钥标识号
Le	1	XX	-
DATA	XX	XX...XX	认证数据
Le	1	00	-

7.4.4 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。

7.4.5 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运算的结果。

7.4.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.9 Internal Authentication 命令响应状态码

SW1	SW2	意义
90	00	正确执行
61	XX	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
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
94	03	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‘9403’即密钥未找到。

7.4.7 内部认证过程

内部认证是机具对卡片的认证，认证过程如下图所示：

终端	方向	PSAM 卡
产生两个 8 字节随机数 RND_{IFD}		
送 RND_{IFD} 作内部认证	⇒	卡片用指定的 DES 加密钥对随机数 RND_{IFD} 进行 DES 加密运算，产生鉴别数据 D1。即： D1=DES（KID，RND_{IFD}） 送 D1
	⇐	
用与卡片内部认证密钥相同的密钥 Cardkey 对 RND_{IFD} 进行 DES 加密运算，产生产生鉴别数据 D2，后比较 D1 和 D2。即： 1）D2=DES(CardKey，RND_{IFD}) 2）D1？=D2		

图 7-2 内部认证过程

说明：

1．终端自己产生 1 个 8 字节随机数 RND_{IFD}；

2．终端向卡片发出内部认证命令，送入 RND_{IFD} 到卡片内；

00 88 00 KID 08 RND_{IFD}

3．卡片收到 RND_{IFD} 后，用卡内的相应密钥对随机数 RND_{IFD} 进行 DES 加密运算，产生 8 字节鉴别数据 D1；

4．卡片送鉴别数据 D1 到卡外；

5．终端接收到卡片送出的鉴别数据D1后，用相应密钥对随机数RND_{IFD}进行DES加密运算，产生8字节鉴别数据D2；

终端比较D1和D2，若一致则认证通过，不一致认证失败。

7.4.8 应用举例

[1] 条件：密钥标识号=01；

密钥类型是内部认证密钥；

使用权限=0xF0；

更改权限=0xEF；

算法标识=01；

密钥版本号=01；

16 字节的密钥=‘574154434844415441546 96D65434F53’；

待加密数据=‘1122334455667788’。

操作：内部认证即 DES 加密。

命令：00 88 00 01 08 11 22 33 44 55 66 77 88

响应；6108

说明：对于 T=0 的卡片，6108 表示卡片要回送的数据长度，可以通过 Get Response 命令取返回数据。对于握奇读写机具，产品默认设置为可自动读取卡片响应数据，所以无需通过 Get Response 命令取返回数据。

命令：00 C0 00 00 08

响应：07 CB F6 15 E7 D7 2F 96 9000

说明：07 CB F6 15 E7 D7 2F 96 是内部认证即 DES 加密的结果。

7.5 Read Binary（读二进制文件）

7.5.1 定义与范围

Read Binary命令用于读取二进制文件的内容（或部分内容）。

7.5.2 注意事项

- Read Binary命令只适用于二进制文件。
- 访问二进制文件的命令如下：
  - 建立文件（Create File）
  - 选择文件（Select File）
  - 读二进制文件（Read Binary）/写二进制文件（Update Binary）
- 只有满足二进制文件读权限时才能执行此命令。

7.5.3 命令报文

表 7.10 Read Binary 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	00	-
INS	1	B0	-
P1	1	XX	见说明
P2	1	XX	见说明
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	XX	要读取的数据长度

说明：

- 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。

P1								P2
b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
1	0	0	短文件标识符					文件的偏移量

- 若 P1 的最高位不为 1，则 P1 P2 为欲读文件的偏移量，所读的文件为当前文件。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件的偏移量							

7.5.4 命令报文数据域

命令报文数据域不存在。

7.5.5 响应报文数据域

响应报文数据域由读取的数据组成。

7.5.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.11 Read Binary 命令响应状态码

SW1	SW2	意义
90	00	正确执行
61	XX	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
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）
6C	XX	Le 错误

说明：

- 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’。
- 当 Le=00 或大于文件实际长度时，则送回警告状态 6Cxx 请求将 Le 置为 xx 并重发该命令。

7.5.7 应用举例

[1] 条件：文件类型：二进制文件；
文件标识符=0005；

文件主体空间的大小=8 个字节。

操作：读出自偏移量 00 开始到文件结束的所有数据，不进行线路保护。

命令：00 B0 85 00 00

响应：6C08

说明：对于 T=0 的卡片，6C08 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=0x08.

命令：00 B0 85 00 08

响应：11 22 33 44 55 66 77 88 9000

7.6 Read Record（读记录文件）

7.6.1 定义与范围

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

7.6.2 注意事项

- Read Record命令适用于定长记录文件、循环文件和变长记录文件。
- 访问记录文件的命令如下：
  - 建立文件（Create File）
  - 选择文件（Select File）
  - 读记录文件（Read Record）
  - 写记录文件（Update Record）
- 只有满足记录文件读权限时才能执行此命令。

7.6.3 命令报文

表 7.12 Read Record 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	00	-
INS	1	B2	-
P1	1	XX	记录号或记录标识符，见说明
P2	1	XX	见说明
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	XX	‘00’或要读取的数据长度

说明：

- 参数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。 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...

- 参数 P2 的含义

b7	b6	b5	b4	b3	b2	b1	b0	描述
0	0	0	0	0	-	-	-	对当前文件进行操作
x	x	x	x	x	-	-	-	基本文件标识符
-	-	-	-	-	1	0	0	按记录号，读 P1 指定的记录
-	-	-	-	-	1	0	1	按记录号，从 P1 指定的记录读到最后一条记录
-	-	-	-	-	1	1	0	按记录号，从最后一条记录读到 P1 指定的记录
-	-	-	-	-	0	0	0	读 P1 指定记录标识符的第一个记录
-	-	-	-	-	0	0	1	读 P1 指定记录标识符的最后一个记录
-	-	-	-	-	0	1	0	读 P1 指定记录标识符的下一个记录
-	-	-	-	-	0	1	1	读 P1 指定记录标识符的上一个记录

注：X X X X X 代表短文件标识符（SFI）；- - - - - 代表全 0 或短文件标识符

7.6.4 命令报文数据域

命令报文数据域不存在。

7.6.5 响应报文数据域

响应报文数据域由读取的记录组成。

7.6.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.13 Read Record 命令响应状态码

SW1	SW2	意义
90	00	正确执行
61	XX	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
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	Le 错误

说明：当 Le 不等于该记录的实际长度时,则送回警告状态 6Cxx 请求将 Le 置为 xx 并重发该命令。

7.6.7 应用举例

[1] 条件：文件类型：定长记录文件；
文件标识符=0001；
记录数=3 条；
记录长度=12 个字节。
建立时不采用线路保护。
操作：读出定长记录文件中记录号为 02 的记录。
命令：00 B2 02 0C 00 返回状态 6C 0C
响应：6C0C
说明：对于 T=0 的卡片，6C0C 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=12。
命令：00 B2 02 0C 0C
响应：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。

[2] 条件：文件类型：循环文件
文件标识符=0003；
记录数=3 条；
记录长度=12 个字节。
建立时不采用线路保护。
操作：读出循环文件中记录号为 01 的记录，即最新写入的记录。
命令：00 B2 01 1C 00
响应：6C0C
说明：对于 T=0 的卡片，6C0C 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=12.
命令：00 B2 01 1C 0C
响应：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。

[3] 条件：文件类型：变长记录文件
文件标识符=0007；
建立时不采用线路保护。

[操作 1]：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。

命令：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’。

响应：6C03

说明：对于 T=0 的卡片，6C03 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=3.

命令：00 B2 AA 38 03

响应：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 个字的记录数据。

[操作 2]：按记录号来读，读出变长记录文件中的第 1 条记录。

命令：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’。

响应：6C03

说明：对于 T=0 的卡片，6C0C 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=3.

命令：00 B2 01 3C 03

响应：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。

[4] 条件：文件类型：钱包文件
文件标识符=0004；
记录数=2 条；
记录长度=4 个字节。
建立时不采用线路保护。

操作：读出钱包文件中记录号为 01 的记录，即最新写入的记录。

命令：00 B2 01 24 00

响应：6C04

说明：对于 T=0 的卡片，6C04 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=4.

命令：00 B2 01 24 04

响应：00 00 00 01 9000

说明：00 00 00 01 为钱包的新余额。

7.7 Select File（选择文件）

7.7.1 定义与范围

Select File命令通过文件名、文件标识符或选择下一个应用来选择IC卡中能够选择到父DF，同级DF和下级DF、EF以及MF。IC卡的响应报文应由回送文件控制信息FCI组成。

7.7.2 注意事项

- 正确选择 MF 后，MF 安全寄存器将被复位为 0.
- 正确选择 MF 下各个 DF 后，DF 安全寄存器将被复位为 0，MF 安全寄存器的值不变。

7.7.3 命令报文

表 7.14 Select File 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	00	-
INS	1	A4	-
P1	1	00/04	见说明
P2	1	00/02	见说明
Lc	1	XX	-
DATA	XX	XX...XX	文件标识符或 DF 名称
Le	1	00	对于 DF 而言为卡片自动返回的 FCI 的最大长度

说明：

- P1=00，表示按文件标识符选择（P2 必须等于 0），可选择
  - 当前目录（DF）下基本文件或子目录文件。
  - 同级目录文件（DF）。
- P1=04，表示用 DF 名称选择，分如下两种情况：
  - P2=00，表示第一个或仅有一个；
  - P2=02，表示下一个。

  用此方法可以选择DF。

在任何情况下均可通过标识符‘3F00’或目录名称1PAY.SYS.DDF01选择MF。

7.7.4 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。

7.7.5 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)，如表7.21和表7.22所示。

表 7.15 成功选择 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 名称	必备
A5	文件控制信息专用数据	可选
88	目录基本文件的短文件标识符	可选

表 7.16 成功选择 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 名称	必备
A5	文件控制信息专用数据	可选
9F0C	发卡方自定数据的文件控制信息	可选

7.7.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.17 Select File 命令响应状态码

SW1	SW2	意义
90	00	正确执行
61	XX	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
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

7.7.7 应用举例

- 符合银行标准的应用目录的选择

[1] 条件：MF 下目录基本文件的短文件标识符=01；

操作：对主文件 MF 进行选择即对 DDF 进行选择。

命令：00 A4 00 00 02 3F 00

响应：6117

说明：对于 T=0 的卡片，6117 表示卡片要回送的数据长度，可以通过 Get Response 命令取返回数据。对于握奇读写机具，产品默认设置为可自动读取卡片响应数据，所以无需通过 Get Response 命令取返回数据。

命令：00 C0 00 00 17

响应：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'为目录短文件标识符的记录标识。
    - '01'为目录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。

[2] 条件：目录基本文件是一个变长记录文件。

操作：读目录基本文件（DIR）的第一条记录。

命令：00 B2 01 0C 00

响应：6C15

说明：对于 T=0 的卡片，6C15 表示要求终端向 IC 卡重发前一个命令的命令头，其中 Le=0x15.

命令：00 B2 01 0C 15

响应：70 13 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。

- '70' 是变长记录的标识。
- '13' 是变长记录数据长度。
- '61' 是 ADF 应用目录入口封装标志。
- '15' 是 ADF 应用目录入口封装数据长度。
- '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。
- ‘50’为应用标签。
- ‘04’为应用标签长度。
- ‘50 42 4F 43’是‘PBOC’的 ASC 码。

[3] 条件：ADF 下发卡方专用数据文件的短文件标认识符=0x95(在建立银行应用目录文件 ADF 下的 KEY 文件时指定）

ADF 的名称:；‘A0 00 00 00 03 86 98 07 01’.

操作：对 ADF 进行选择。

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

响应：6130

说明：对于 T=0 的卡片，6130 表示卡片要回送的数据长度，可以通过 Get Response 命令取返回数据。对于握奇读写机具，产品默认设置为可自动读取卡片响应数据，所以无需通过 Get Response 命令取返回数据。

命令：00 C0 00 00 30

响应：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）
- 后续为‘2E’个字节的记录数据。
- ‘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)。
- ‘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 2 的应用举例)。

7.7.8 在任何目录下选择 MF

命令格式：

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

说明：成功选择 MF 后，MF 将成为当前目录，且 DF 安全状态寄存器的值自动等于 MF 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。

7.7.9 按文件标识符选择当前目录下的文件或下级目录

命令格式：

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

说明：成功选择文件后，若选择的文件为子目录时，该目录成为当前目录，且 DF 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。

7.7.10 通过文件名称选择 DF

命令格式：

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

说明：Lc 定义了 DF 文件名的长度。
成功选择 DF 后，该目录成为当前目录，DF 安全状态寄存器的值变为 0。

7.8 Update Binary（写二进制文件）

7.8.1 定义与范围

Update Binary 命令用于写二进制文件。

7.8.2 注意事项

- Update Binary命令只适用于二进制文件。
- 访问二进制文件的命令：
  - 建立文件（Create File）
  - 选择文件（Select File）
  - 读二进制文件（Read Binary）/写二进制文件（Update Binary）
- 只有满足二进制文件写权限时才能执行此命令。
- 若采用安全报文更新文件时，若安全报文连续三次出错，则永久锁定应用。

7.8.3 命令报文

表 7.18 Update Binary 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	00/04	-
INS	1	D6	-
P1	1	XX	见说明
P2	1	XX	见说明
Lc	1	XX	-
DATA	XX	XX...XX	写入文件的数据
Le	-	-	不存在

说明：

- 若 P1 的高三位为 100，则低 5 位为短的文件标识符，P2 为欲读文件的偏移量。

P1								P2
b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
1	0	0	短文件标识符					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。

P1								P2
b7	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**	
0	文件的偏移量							

- 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。

7.8.4 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。
用维护密钥加密数据和计算MAC，方法见“4.安全报文传送”。

7.8.5 响应报文数据域

响应报文数据域不存在。

7.8.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.19 Update Binary 命令响应状态码

SW1	SW2	意义
90	00	正确执行
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）
6A	82	未找到文件
6B	00	参数错误（偏移地址超出了 EF）

7.8.7 应用举例

[1] 条件：文件类型：二进制文件；
文件标识符=0005；

文件主体空间的大小=8 个字节；
建立时不采用线路保护。

操作：写二进制文件

命令：00 D6 85 00 08 11 22 33 44 55 66 77 88

响应：9000

7.9 Update Record（写记录文件）

7.9.1 定义与范围

Update Record命令用于添加记录或更改指定的记录。

对线性结构文件来说，当指定的记录号不存在时，可按记录号顺序添加记录。按记录标识符访问的记录不存在时，也应视为添加新的记录。

对循环结构文件来说，当使用“上一个记录”命令选项时应视为添加新的记录。

7.9.2 注意事项

Update Record命令适用于定长记录文件、变长记录文件和循环记录文件。

访问记录文件的命令如下所示：

建立文件（Create File）

选择文件（Select File）

读记录文件（Read Record）

写记录文件（Update Record）

只有满足记录文件写权限时才能执行此命令。

7.9.3 命令报文

表 7.20 Update Record 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	00/04	-
INS	1	DC	-
P1	1	XX	记录号或记录标识符（‘00’，表示当前记录）
P2	1	XX	见说明
Lc	1	XX	数据长度
DATA	XX	XXXX	添加的或更新原有记录的新记录
Le	-	-	不存在

说明：

参数 P2 的含义

b7	b6	b5	b4	b3	b2	b1	b0	描述
0	0	0	0	0	–	–	–	当前的 EF 文件
x	x	x	x	x	–	–	–	SFI
1	1	1	1	1	–	–	–	保留
–	–	–	–	–	1	x	x	利用 P1 中的记录号
–	–	–	–	–	1	0	0	P1 记录号
–	–	–	–	–	0	x	x	利用 P1 中的记录标识符
–	–	–	–	–	0	0	0	P1 指定标识的第一个记录
–	–	–	–	–	0	0	1	P1 指定标识的最后一个记录
–	–	–	–	–	0	1	0	P1 指定标识的下一个记录
–	–	–	–	–	0	1	1	P1 指定标识的上一个记录

注：X X X X X 代表短文件标识符（SFI）；- - - - - 代表全 0 或短文件标识符

注：1、循环记录文件只能用 P1=‘00’，P2=‘03’来添加。

2、当 P1≠‘00’，P2=‘04’， 若 P1 等于已有记录的最大记录号+1，则添加。

7.9.4 命令报文数据域

命令报文数据域由添加的或更新原有记录的新记录组成。

7.9.5 响应报文数据域

响应报文数据域不存在。

7.9.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.21 Update Record 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
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

7.9.7 应用举例

条件：文件类型：定长记录文件；

文件标识符=0002；

记录数=3 条；
记录长度=12 个字节；
建立时不采用线路保护。
操作：写定长记录文件，不进行线路保护。
命令：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。

条件：文件类型：变长记录文件；
文件标识符=0001；
建立时不采用线路保护。
[操作 1]：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。
命令：00 DC 00 0A 04 AA 02 11 22
响应：9000
[操作 2]：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。
命令：00 DC AA 08 04 CC 02 33 44
响应：9000

条件：文件类型：循环文件
文件标识符=0003；
记录数=3 条；
记录长度=12 个字节；
建立时不采用线路保护。
操作：往循环文件中追加 1 条记录，不进行线路保护。
命令：00 DC 00 03 0C 11 22 33 44 55 66 77 88 99 AA BB CC
响应：9000

7.10 Verify PIN（验证口令）

7.10.1 定义与范围

Verify PIN命令用于校验命令数据域的口令密钥正确性。

7.10.2 注意事项

- 在满足该口令密钥的使用权限时才可执行该命令。
- 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。

7.10.3 命令报文

表 7.22 Verify PIN 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	00	-
INS	1	20	-
P1	1	00	-
P2	1	00	-
Lc	1	02-06	-
DATA	02-06	XX...XX	外部输入的口令密钥
Le	-	-	不存在

说明：

- 在验证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的口令密钥进行验证。
- 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Reload PIN进行口令重装操作。

7.10.4 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。

7.10.5 响应报文数据域

响应报文数据不存在。

7.10.6 响应报文状态码

当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；
- 当卡片回送SW2=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 卡可能回送的状态码如下所示：

表 7.23 Verify PIN 命令响应状态码

SW1	SW2	意义
90	00	正确执行
63	CX	还剩 x 次可试机会
62	83	口令密钥校验错误
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
93	02	密钥线路保护错误
94	03	密钥未找到

8. TimeCOS/PSAM 扩展命令

表 8.1 列出了 TimeCOS/PSAM 扩展命令。

表 8.1 TimeCOS/PSAM 扩展命令列表

序号	命令	CLA	INS	功能描述	兼容性
1	**Application Block**	84	1E	应用锁定	PBOC
2	**Application Unblock**	84	18	应用解锁	PBOC
3	**Init_For_Descrypt**	80	1A	通用 DES 计算初始化	PBOC
4	**DES crypt**	80	FA	通用 DES 计算	PBOC
5	**Init_SAM_For_Purchase**	80	70	MAC1 计算	PBOC
6	**Credit_SAM_For_Purchase**	80	72	校验 MAC2	PBOC
7	**Reload/Change PIN**	80	5E	重装/修改个人密码	PBOC
8	**Secure Calculation**	80	1C	安全计算	专有

8.1 Application Block（应用锁定）

8.1.1 定义与范围

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’）。

8.1.2 命令报文

表 8.2 Application Block 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	84	-
INS	1	1E	-
P1	1	00	-
P2	1	00/01	见说明
Lc	1	04	MAC 码长度
DATA	4	XX...XX	MAC
Le	-	-	不存在

说明：

- 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 File 命令选择进入该目录，但对文件操作时返回 6A81。

8.1.3 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。

用密钥版本为00的16字节维护密钥计算MAC，方法见“4.安全报文传送”。

8.1.4 响应报文数据域

响应报文数据域不存在。

8.1.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 8.3 Application Block 命令响应状态码

SW1	SW2	意义
90	00	正确执行
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

8.2 Application Unblock（应用解锁）

8.2.1 定义与范围

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 Unblock命令产生的对应用命令响应的限制将被取消。

8.2.2 注意事项

- 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。

8.2.3 命令报文

表 8.4 Application Unblock 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	84	-
INS	1	18	-
P1	1	00	-
P2	1	00	-
Lc	1	04	MAC 码长度
DATA	4	XX...XX	MAC
Le	-	-	不存在

8.2.4 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。

用密钥版本为00的16字节维护密钥计算MAC，方法见“4.安全报文传送”。

8.2.5 响应报文数据域

响应报文数据域不存在。

8.2.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 8.5 Application Unblock 命令响应状态码

SW1	SW2	意义
90	00	正确执行
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

8.3 Init_ For_Descrypt（通用 DES 计算初始化）

8.3.1 定义与范围

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

不支持计算临时密钥计算的密钥类型有：

——主控密钥

——维护密钥

——消费密钥

双长度密钥产生双长度临时密钥的密钥类型有：

——PIN 解锁密钥

——用户卡应用维护密钥

双长度密钥左右异或产生单长度临时密钥的密钥类型有：

——重装 PIN 密钥

双长度密钥产生双长度临时密钥，单长度密钥产生单长度临时密钥的密钥类型有：

——MAC 密钥

——加密密钥

——MAC、加密密钥

——解密密钥

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

临时密钥在 PSAM 卡下电后自动消失，不允许读。

临时密钥产生后，与原密钥的属性一致。

8.3.2 命令报文

表 8.6 Init_For_ Descrypt 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	80	-
INS	1	1A	-
P1	1	XX	密钥用途
P2	1	XX	密钥版本
Lc	1	XX	-
DATA	XX	XX...XX	待处理数据
Le	-	-	不存在

8.3.3 命令报文数据域

命令报文数据域包括待处理的输入数据。数据长度为 8 的整数倍，长度也可以为 0。密钥类型取

密钥用途的低 5 位，密钥分散级数取密钥用途的高 3 位。

如待处理的输入数据包括多级的分散因子，按最后一次分散因子在前、最先一次分散因子在后的顺序输入。密钥分散方法见“5. 基于 DES 的加密算法”。

8.3.4 响应报文数据域

响应报文数据域不存在。

8.3.5 响应报文状态码

见“6.4 状态字 SW1SW2 意义”。

8.3.6 应用举例

例如：假设某应用下有一 TYPE = 63、Kv = 00、Algorithm ID = 00 的密钥，则使用该密钥产生临时密钥的命令报文如下：

80 1A 63 00 18 11 22 33 44 55 66 77 88 99 00 AA BB CC DD EE FF 11 22 33 44 55 66 77 88

响应状态为： 9000

8.4 DES crypt(通用 DES 计算)

8.4.1 定义与范围

DES Crypt 命令利用指定的密钥来进行运算。若一条命令无法传输所有的待处理数据，可分几条命令输入。

加密计算采用 ECB 模式，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的加密。

MAC 计算方法见“4.安全报文传送”，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的 MAC 计算。

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

8.4.2 命令报文

表 8.7 DES Crypt 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	80	-
INS	1	FA	-
P1	1	XX	见下表
P2	1	00	-
Lc	1	XX	-
DATA	XX	XX...XX	要加密的数据长度
Le	1	00	-

表 8.8 DES CRYPT 命令引用控制参数 P1

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

说明：

P1 值计算模式如下：

——0，无后续块加密

——1，最后一块 MAC 计算

——2，有后续块加密
——3，下一块 MAC 计算
——5，唯一一块 MAC 计算
——7，第一块 MAC 计算
——其他，保留

8.4.3 命令报文数据域

命令报文数据域包括要加密的数据。加密数据的长度为 8 的整数倍。

在 P1 的 b3 位为 1 时，待处理数据的前 8 个字节为 MAC 计算的初始值。

MAC 计算方法见“4.安全报文传送”，数据的填充在卡片外面进行，卡片只支持长度为 8 的整数倍数据的 MAC 计算。

8.4.4 响应报文数据域

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

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

8.4.5 响应报文状态码

见“6.4 状态字 SW1SW2 意义”。

8.4.6 应用举例

例如：以上一节例子为例，卡内已有一 TYPE = 63 密钥产生一临时密钥 SK，根据密钥的继承性，该 SK 可以用于进行 DES 和 MAC 运算，举用于计算 DES 的命令报文如下：

80 FA 00 00 08 11 22 33 44 55 66 77 88

响应报文和状态如下：

3DES（SK，11~88）[8 Bytes] 9000

8.5 Init_SAM_For_Purchase（MAC1 计算）

8.5.1 定义与范围

Init_SAM_For_Purchase 命令可支持多级消费密钥分散机制，产生《中国金融集成电路（IC）卡规范》中定义的 MAC1。根据银行 IC 卡试点技术方案，可以利用试点城市标识、成员行标识、卡片应用序列号、随机数和交易信息得到过程密钥，进而加密得到 MAC。

8.5.2 命令报文

表 8.9 Init_SAM_For_Purchase 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	80	-
INS	1	70	-
P1	1	00	-
P2	1	00	-
Lc	1	XX	14h+8*N（N=1，2，3）
DATA	XX	XX...XX	要处理的数据
Le	1	08	-

8.5.3 命令报文数据域

命令报文数据域包括的数据以下列顺序排列：

- 用户卡随机数，4 字节
- 用户卡交易序号，2 字节
- 交易金额，4 字节
- 交易类型标识，1 字节
- 交易日期（终端），4 字节
- 交易时间（终端），3 字节
- 消费密钥版本号，1 字节
- 消费密钥算法标识，1 字节
- 用户卡应用序列号，8 字节
- 成员银行标识，8 字节
- 试点城市标识，8 字节

8.5.4 响应报文数据域

响应报文数据域包括以下数据（按顺序返回）：

——4 字节的终端脱机交易序号

——4 字节的 MAC1

PSAM 卡产生脱机交易流程中 MAC1 的过程如下：

- PSAM 在其内部用 GMPK（全国消费主密钥）对试点城市标识分散，得到二级消费主密钥 BMPK；
- PSAM 在其内部用 BMPK 对成员行标识分散，得到成员行消费主密钥 MPK；
- PSAM 在其内部用 MPK 对卡片应用序列号分散，得到卡片消费子密钥 DPK；
- PSAM 在其内部用 DPK 对卡片传来的下表所示数据加密生成 8 字节过程密钥 SK。

数据	长度（字节）
伪随机数	4
电子存折或电子钱包脱机交易序号	2
终端交易序号的最右两个字节	2

- PSAM 在其内部用过程密钥 SK 对下表数据按 MAC 计算方法生成 MAC1，将 MAC1 传送出去。MAC 计算的初始值为 8 个字节的十六进制数字‘0’，方法见“4.安全报文传送”。

数据	长度（字节）
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

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

参与处理的终端机编号和终端交易序号由卡片操作系统从卡片中取得。

Init_SAM_For_Purchase 命令可支持多级消费密钥分散机制，消费密钥的分散过程由 Lc 和消费密钥共同确定，如果二者不一致，则返回错误信息。密钥分散方法见“5.基于 DES 的加密算法”。

8.5.5 响应报文状态码

见“6.4 状态字 SW1SW2 意义”。

8.5.6 应用举例

例如：有一密钥内容为 00~FF 的 TYPE（密钥用途） =62、Kv（密钥版本） =00 的密钥 GMPK，MF 下的终端公共信息文件内容为 01~06，进行第一次 MAC1 计算命令报文如下：

80 70 00 00 2C 11 22 33 44 00 00 00 00 00 01 06 19 99 07 20 12 30 59 00 00 19 98 08 17 00 00 00 30 11 22 33 44 55 66 77 88 88 77 66 55 44 33 22 11

响应报文及状态：

00 00 00 00 BA 22 E8 D4 9000

8.6 Credit _SAM_For_ Purchase（校验 MAC2）

8.6.1 定义与范围

Credit_SAM_For_Purchase 命令利用 Init_Sam_For_Purchase 命令产生的过程密钥 SK 校验 MAC2，过程如下：

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

在此过程中，所有的中间结果只保留在卡片内部，外界无法得到。

Credit_SAM_For_Purchase 命令必须在 Init_Sam_For_Purchase 命令成功执行后才能进行。

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

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

卡片的状态在命令执行后将复原为MAC1校验前的状态。

8.6.2 命令报文

表 8.10 Credit_SAM_For_Purchase 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	80	-
INS	1	72	-
P1	1	00	-
P2	1	00	-
Lc	1	04	-
DATA	04	XX...XX	MAC2
Le	-	-	不存在

8.6.3 命令报文数据域

命令报文数据域包括 4 字节的 MAC2。

MAC2 的计算过程：

MAC2由卡中过程密钥SK对（4字节交易金额）按MAC计算方法生成的。

MAC 计算的初始值为 8 个字节的十六进制数字 '0'，方法见 "4.安全报文传送"。

8.6.4 响应报文数据域

响应报文数据域不存在。

8.6.5 响应报文状态码

见“6.4 状态字 SW1SW2 意义”。

8.6.6 应用举例

例如：续上一节例子，MAC2 校验的命令报文如下：
80 72 00 00 04 30 D4 26 05
响应状态如下：9000

8.6.7 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：

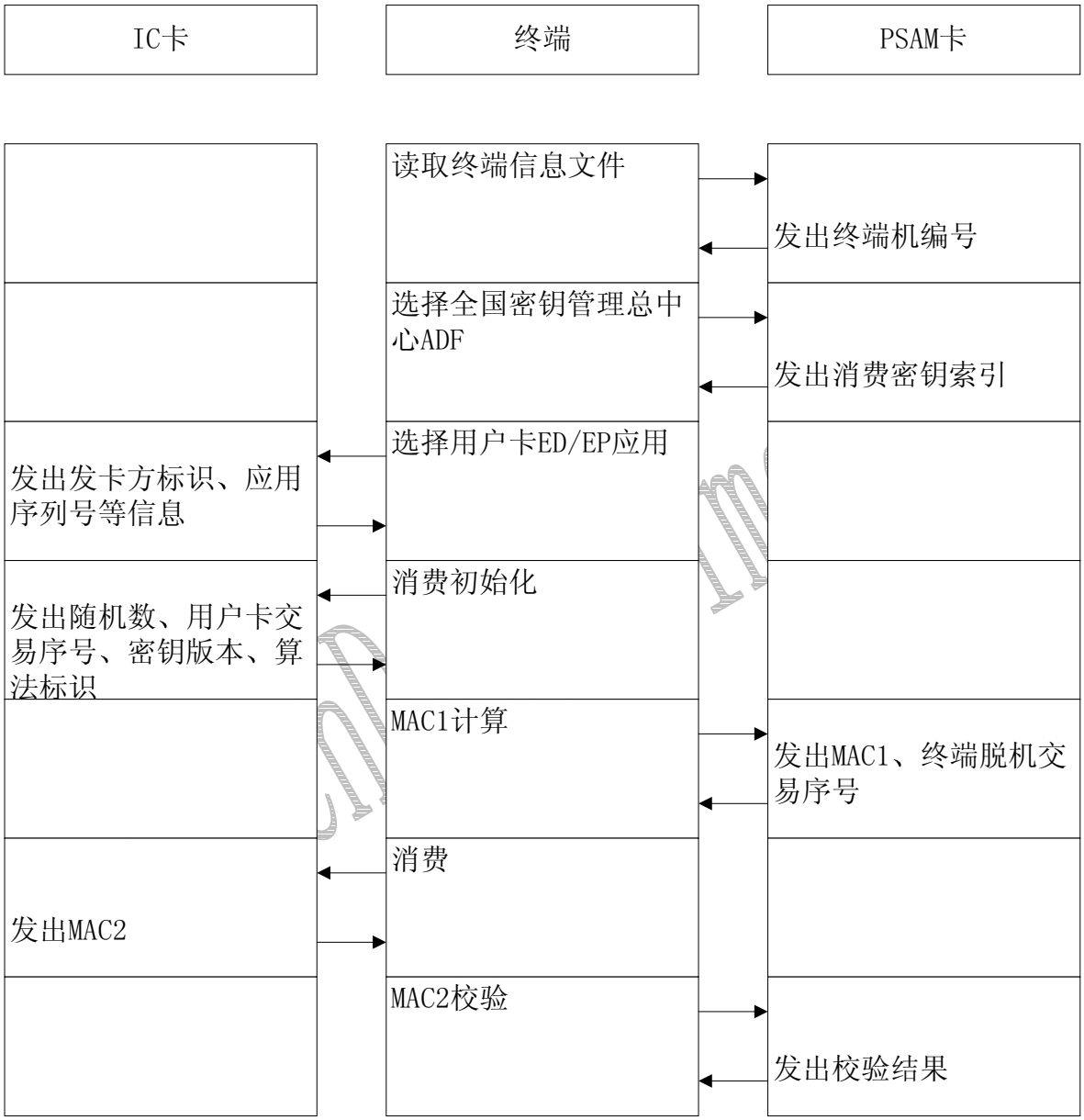


图 8-1 消费交易流程图

8.7 Reload/Change PIN（重装/修改口令密钥）

8.7.1 定义与范围

Reload/Change PIN命令用于发卡方重新给持卡人产生一个新的PIN。

Reload/Change PIN只能在能访问到重装口令密钥的发卡方终端或拥有原口令时才能够执行。

在成功执行 Reload/Change PIN 命令后，IC 卡必须完成以下操作：

1. 密钥错误尝试计数器复位。
2. IC卡的原密钥必须设置为新的值。

8.7.2 命令报文

表 8.11 Reload/Change PIN 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	80	-
INS	1	5E	-
P1	1	00	Reload PIN
		01	Change PIN
P2	1	00	-
Le	1	XX	-
DATA	XX	XX...XX	重装的 PIN 和报文鉴别码 MAC（Reload PIN） 旧口令 ‖ FF ‖ 新口令（Change PIN）
Le	-	-	不存在

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。

8.7.3 命令报文数据域

- 重装口令（Reload PIN）时包括 PIN 值和报文鉴别码 MAC
  此处的 MAC 是由重装口令密钥左右 8 字节异或运算的结果对口令 PIN 值进行 MAC 计算的结果。MAC 计算的初始值为 8 个字节的十六进制数字‘0’，方法见“4. 安全报文传送”。
- 修改口令（Change PIN）时包括原口令值和 FF 和新口令值。
  DATA 中“重装的 PIN”、“旧口令”和“新口令”长度是 2 到 6 个字节。

8.7.4 响应报文数据域

响应报文数据域不存在。

8.7.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 8.12 Reload/Change PIN 命令响应状态码

SW1	SW2	意义
90	00	正确执行
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
69	88	MAC 错误
93	03	应用永久锁定
94	03	密钥未找到

8.8 Secure Calculation（安全计算）

8.8.1 定义与范围

Secure Calculation命令利用密钥文件中的密钥对输入数据进行特定运算，输出结果。加密算法见“5.基于DES的加密算法”。

8.8.2 命令报文

表 8.13 Secure Calculation 命令报文编码

代码	长度 (byte)	值 (Hex)	描述 （Hex）
CLA	1	80	-
INS	1	1C	-
P1	1	00	加密方式
		01	解密方式（DOUBLE ONE WAY）
P2	1	XX	密钥版本
Lc	1	XX	8*N（N=2，3，4……）
DATA	XX	XX...XX	待运算数据
Le	1	08	-

8.8.3 命令报文数据域

命令报文数据域包括以下数据：

- 8 字节的 inputdata1；
- 8 字节的 inputdata2；
- 8 字节的 inputdata N-1。
- 8 字节的序列号

8.8.4 响应报文数据域

响应报文数据域包括8字节的运算结果。

8.8.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 8.14 Secure Calculation 命令响应状态码

SW1	SW2	意义
90	00	正确执行
61	**XX**	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
6A	81	无 MF 或卡片已锁定
94	03	密钥不存在
69	82	权限不满足
67	00	错误的数据长度
6E	00	无效的 CLA

附录 1 TimeCOS/PSAM 复位应答

- 在由终端发出复位信号以后，IC 卡以一串字节作为应答（即复位应答）。卡片通讯速率默认为 9600bps.
- 这些传输到终端的字节规定了卡和终端之间即将建立的通信特性。
- TimeCOS/PBOC 的复位信息完全符合 ISO 7816 规范。
  - 客户可以定制特殊的复位信息。

对于 T=0 通讯协议的卡，复位应答信息如下表所示：

表附录 11.1 T=0 协议

符号	值 (Hex)	说明	长度（byte）
TS	3B	正向约定，首先传送的是字符最低有效位	1
T0	6D	TB1 和 TC1 存在，历史字符为 13 个	1
TB1	00	无需额外编程电压 VPP	1
TC1	00	无需额外的保护时间	1
T1 ~ TD	XX	历史字符	13

说明：

- TS=‘3B’，它表示从 I/O 口传送数据时先传低位再传高位。
- T0=‘6D’，它的低半字节D表明有13个历史字符，高半字节6（0110）表示TB1、TC1存在，由于TD1不存在所以为T=0的通讯协议。

历史字符如下表所示：

表附录 11.4 复位信息中的历史字符

符号	值 (Hex)	意义
T1	‘W’（‘57’）	芯片厂商注册代码：WATCHDATA 的缩写
T2	‘D’（‘44’）	
T3-T5	XX…XX	由 TimeCOS 定义
T6-T7	XXXX	卡片制造机构注册标识号
T8	XX	OS 用途定义
T9~TD	XX…XX	卡序号，每卡该序号唯一