Simlinker_PSAM
通用技术参考手册

北京芯凌科技有限公司

Beijing Simlinker Tech Co.,Ltd

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：

□ Simlinker/PSAM 简介

本章介绍了Simlinker/PSAM 的特点及体系结构，使您对Simlinker/PSAM 卡片有一个初步的了解。

□ Simlinker/PSAM 文件管理

本章从文件组织结构、文件格式、文件访问方式及各种类型文件的特点来详细描述了Simlinker/PSAM 的文件管理系统。

□ 卡片初始化设置

本章描述了Simlinker/PSAM 卡片初始化后的文件结构及使用方法。

□ Simlinker/PSAM 的安全体系

安全体系是Simlinker 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。本章从安全状态、安全属性、安全机制和密码算法四个方面详细描述了Simlinker/PSAM 的安全体系。

□ 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。

□ Simlinker/PSAM 发卡命令

1.2 参考文献

[1] 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。
[2] 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涉及的金融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）
PSAM ： 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. Simlinker/PSAM 简介

2.1 关于 Simlinker/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。

Simlinker/PSAM是由北京芯凌科技有限公司开发的智能卡操作系统，完全符合一下国际、国内标准：

♦ 识别卡，带触点的集成电路卡标准 《ISO7816-1/2/3/4》

Simlinker/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运算,以完成终端与卡之间的合法性认证功能。
♦ 支持中国人民银行认可的Single DES、Triple DES算法。
♦ 支持多种速率选择 可支持9600bps、38400bps等不同的通讯速率。

2.2 Simlinker 体系结构

2.2.1 卡片内部逻辑结构

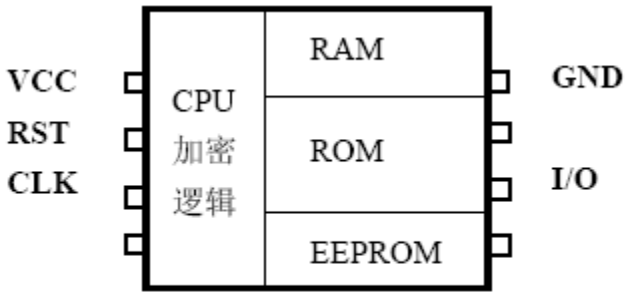


图 2-1 卡片内部逻辑结构

Simlinker 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。
Simlinker 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Simlinker 程序的区域。

♦ EEPROM
存放用户应用数据区域，Simlinker 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 Simlinker 功能模块划分

Simlinker 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Simlinker 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。

2.2.2 Simlinker/PSAM 命令集

表2.1 Simlinker/PSAM 命令集

编号	命令	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	D6	写二进制文件	ISO&PBOC
10	Update Record	00	DC	写记录文件	ISO&PBOC
11	Application Unblock	84	18	应用解锁	PBOC
12	Application Block	84	1E	应用锁定	PBOC
13	Init_For_Descrypt	80	1A	通用 DES 计算初始化	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 crypt	80	FA	通用图 DES 计算	PBOC
18	Erase DF	80	0E	擦除 DF	专有
19	Secure Calculation	80	1C	安全计算	PBOC&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. 文件管理

本章介绍Simlinker/PSAM 的文件系统，包括文件组织结构、文件结构、文件的访问方式及文件空间计算。其中文件结构与文件的访问方式是以文件类型为索引来叙述的。

3.1 文件组织结构

Simlinker/PSAM 的文件系统是由专用文件DF（Dedicated File）和基本文件EF

（Elementary File）组成的。

卡内数据的逻辑组织结构由专用文件（DF）的结构化分级组成。

♦ 在根处的DF 称作主文件（MF）。该MF 是必备的。

♦ 其他DF 是任选的。

MF（第1 级）为根DF，是必须有的，所有其他的文件都是它的分支。在MF 的下一级可以由DF 和EF 组成。我们将不包含子DF 的DF 称为ADF，包含子DF 的DF 称为DDF。

3.2 文件格式

3.2.1 概述

♦ Simlinker/PSAM 中的所有文件都是由文件头和文件体组成（如图3-1 所示）。文件头长度是16个字节，Simlinker/PSAM 用这些信息来管理文件。

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

图3-1 文件在EEPROM 中存放的格式

♦ 文件头用于存储文件类型、文件标识、文件大小和访问权限等内容（见表3.1）。文件体是存放数据的区域。

表3.1 文件头定义

描述	字节（byte）
文件类型	1
文件标识(FID)	2
文件大小	3
访问权限1	1
访问权限2	1
RFU	1
RFU	6
校验和（由COS 计算）	1

注：表*3.1* 中***RFU*** 字节对于不同类型的文件有不同的定义。对于文件头的详细描述见“***7.1 Create File*** 命令”。校验和由***COS*** 计算。

注意：文件格式是在建立文件时唯一确定的，所使用的命令是Create File.

3.2.2 文件类型

- Simlinker/PSAM 支持下列两种文件：
  ——专用文件(DF)。
  ——基本文件(EF)。
- 在根处的DF 称作主文件(MF)。该MF 是必备的。
- 定义了以下两种基本文件（EF）：

1、工作基本文件
用于存储不由卡所解释的数据(即用户数据)，包括二进制文件、定长记录文件、循环文件和变长记录文件。

2、内部基本文件
用于存储由卡所解释的数据，指为了管理和控制目的由卡分析和使用的数据，包括密钥文件。

- EF 支持的文件类型及相应的文件结构如表3.2 所示。

表3.2 文件类型字节的定义

类型字节（HEX）	文件描述	文件结构
38	MF 或DF	
28	二进制文件	透明文件
2A	定长记录文件	定长线性文件
2E	循环文件	循环文件
2C	变长记录文件	变长线性文件
3F	密钥文件（存放密钥和PIN，不允许外部访问）	变长线性文件

3.2.3 文件标识和文件名称

Simlinker/PSAM 是通过逻辑寻址而非物理寻址方式来管理文件的，支持通过文件名称和文件标识两种方式来访问文件。

3.2.3.1 文件标识（FID）

文件标识符（File Indentifier）是文件的标识代码，用2个字节来表示，在选择文件时只要指出文件标识符，Simlinker/PSAM就可以找到相应文件（KEY文件除外），同一目录下的文件标识符必须是唯一的。

□ 注意： MF 的文件标识均为’3F00’， KEY 文件标识均为‘0000’，‘FFFF’保留将来使用。同一目录下的文件标识符必须是唯一的。

3.2.3.2 短文件标识符SFI

短文件标识符由5 个二进制位组成，可选择的最大文件标识符为31。若文件需要用短文件标识符进行选择，则建立文件时就需将文件标识符取在1-31（00001-11111）之间。

3.2.3.3 文件名称

文件名称是指DF 名称，用于标识DF，卡中任何ADF 或DDF 可通过其DF 名称进行选择。ADF 的DF 名称对应其应用标识（AID），应用标识的格式可参考ISO/IEC 7816-5 的有关规定。应用标识的长度为5～16 字节，分为2 部分（见图3-4）：第一部分内容叫注册ID（Registered ID），长度为5 字节，由注册机构分配，包含国家代码、应用类别和应用提供商的标识号；第二部分（PIX）是可选的，由应用提供商定义，长度为0～11 字节。

AID	
RID	PIX
5 Byte	0...11 Byte

图3-2 应用标识编码

3.3 文件访问方式

- 通过文件标识符（FID ）进行访问
  在选择文件（Select File）时只要指出文件标识符，Simlinker/PSAM 就可以找到相应文件。（KEY文件不能通过文件标识进行选择）
- 通过短文件标识符（SFI）进行访问

短文件标识符选择可以通过Read Binary、Update Binary命令的参数P1来实现文件的选择：

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

若参数P1的高三位为100，则低5位为短的文件标识符。

［例］若P1为81H即10000001，其中高三位为100，则所选的文件标识符为0001。

短文件标识符选择还可以通过Read Record、Update Record、Append Record、命令的参数P2来实现文件的选择：

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

若P2的高五位不全为0，低三位为100，则高五位为短文件标识符。

［例］若P2为0CH即00001100，其中低三位为100，所选的文件标识符为0001。

♦ 通过DF 文件名称进行访问
在选择文件（Select File）时只要指出该DF 的文件名称，Simlinker/PSAM 就可以找到相应的DF。

3.4 专用文件（DF）

3.4.1 主文件（MF）

3.4.1.1 **定义**

在Simlinker/PSAM 中，在根处的DF 称作主文件(MF)。该MF 是必备的。它相当于DOS的根目录。

♦ IC 卡复位后，卡片自动选择MF 为当前文件。

♦ 在金融应用中，MF 与MF 下的目录文件（DIR 文件，一个记录型文件）一起构成支付系统环境（PSE），MF 的文件名称是1PAY.SYS.DDF01.

3.4.1.2 **文件头定义**

表3.3 MF 文件头定义

文件头	字节(Byte)	描述

文件类型	1	‘38’
文件标识(FID)	2	‘3F00’
文件大小	2	‘FFFF’，指自动将MF 空间建立为最大值
访问权限1	1	建立权限：在MF 下建立文件的权限
访问权限2	1	擦除权限：擦除MF 下所有文件的权限
RFU	1	‘FF’
RFU	8	‘FF’

3.4.1.3 文件操作命令

- 建立文件命令(Create File)
  在卡片无MF 时，必须首先建立MF 才能对卡片进行其它操作。
- 选择文件命令（Select MF）
  可以用Select File 命令通过文件标识符‘3F00’或文件名称1PAY.SYS.DDF01 来选择文件。
- 擦除DF 命令（Erase DF）
  在满足当前MF 的擦除权限时，可以用此命令擦除MF 下的所有文件(包括DF 或EF)，但MF 当前的访问权限、空间等信息并没有改变（即不能擦除MF 的文件头信息）。

注：若***MF*** 下无任何文件，则在该目录下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开***MF*** 再进入***MF*** 时，将遵循文件的访问权限。

3.4.2 专用文件（DF）

3.4.2.1 定义

在Simlinker/PSAM 中，专用文件DF 相当于DOS 的目录。每一个DF 下可以存放多个EF 和多个下级DF。

- 卡片可支持3 级目录（MF-DF-DF）。我们称包含下级目录的专用文件（DF）为DDF，不包含下级目录的专用文件为ADF.
- 任何一个DF 在物理上和逻辑上都保持独立，都有自己的安全机制和应用数据。
- DF 的个数仅受EEPROM 空间的限制。

3.4.2.2 文件头定义

表3.4 DF 文件头定义

文件头	字节（Byte）	描述

文件类型	1	‘38’
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”
文件大小	2	表示DF 文件体大小
访问权限1	1	建立权限：在MF 下建立文件的权限
访问权限2	1	擦除权限：擦除MF 下所有文件的权限
RFU	1	‘FF’
RFU	8	‘FF’

3.4.2.3 文件名称

见“3.2.3.3 文件名称”。

3.4.2.4 文件操作命令

- 建立文件命令(Create File)

  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

- 选择文件命令（Select MF）

  可以用Select File 命令通过文件标识符或DF 名称来选择文件。

- 擦除DF 命令（Erase DF）

  在满足当前DF 的擦除权限时，可以用此命令擦除DF 下的所有文件(包括DF、EF)，但DF

  当前的访问权限、空间等信息并没有改变（即不能擦除当前DF 的文件头信息），且DF 的文件名称也不能被擦除。

注：**若当前*DF* 下无任何文件，则在该*DF* 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开该*DF* 再进入此*DF* 时，将遵循文件的访问权限。**

3.5 工作基本文件

工作基本文件用于存储不由卡所解释的数据（即用户数据），包括二进制文件、定长记录文件、循环文件、钱包文件和变长记录文件。

3.5.1 二进制文件

3.5.1.1 定义

二进制文件为一个数据单元序列，数据以二进制为单位进行读写。

3.5.1.2 文件体结构▌透明文件

透明文件通常又叫二进制文件或流文件，即透明文件不处理任何内部结构。存储在文件中的数据通过使用地址偏移量访问（文件逻辑地址从0 开始）。

透明文件的结构如下图所示：

长度（单位Byte）

1 2 3 .....m

图3-3 透明结构

[例] 从一个10 字节的文件中读取偏移量为3 的5 个字节：

长度(单位Byte)

1 2 3 4 5 6 7 8 9 10

偏移量=3 数据

3.5.1.3 **文件头定义**

表3.5 二进制文件头定义

文件头	字节(Byte)	描述
文件类型	1	‘28’，安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”
文件大小	2	文件体长度
访问权限1	1	读权限
访问权限2	1	写权限
RFU	1	‘FF’
RFU	8	‘FF’

3.5.1.4 **文件操作命令**

- 建立文件命令（Create File ）
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用Select File 命令通过文件标识符来选择文件。
- 读二进制文件（Read Binary）
  当满足文件的读权限时，可以用Read Binary 命令读取文件信息。
- 写二进制文件（Update Binary）
  当满足文件的写权限时，可以用Update Binary 命令写入文件信息。

3.5.2 定长记录文件

3.5.2.1 **定义**

定长记录文件为具有固定长度记录的文件。

3.5.2.2 文件体结构▌定长线性文件

定长线性文件又叫定长记录文件，它的结构是相同长度的记录。不同的记录通过顺序号来区分访问。记录只能整条访问，不允许访问记录的部分数据。

3.5.2.3 文件头定义

表3.6 定长记录文件头定义

文件头	字节(Byte)	描述
文件类型	1	‘2A’，安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”
文件大小	2	字节1 表示记录总个数(2-254) 字节2 表示记录长度(≤178)
访问权限1	1	读权限
访问权限2	1	写权限
RFU	1	‘FF’
RFU	8	‘FF’

3.5.2.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

- 选择文件命令（Select File）
  可以用Select File 命令通过文件标识符来选择文件。

- 读记录文件（Read Record）
  当满足文件的读权限时，可以用Read Record 命令读取一条记录。

- 写记录文件（Update Record）
  当满足文件的写权限时，可以用Update Record 命令写（或更新）一条记录。

3.5.3 循环文件

3.5.3.1 定义

循环文件为具有固定长度记录的环行文件。

3.5.3.2 文件体结构▌循环文件

循环文件又叫循环记录文件。循环文件的每条记录都只有一个数据域，数据以记录为单位进行存储，记录长度最大为178 个字节。不同的记录通过顺序号或记录指针来区分访问，应用时只能顺序增加记录。当写记录时，当前写入的为第一条记录，则上一次写入的记录为第二条，依此类推，滚动写入。记录只能在文件头中所规定的范围内滚动写入，当写完最后一条记录时将覆盖最先写入的记录。

3.5.3.3 文件头定义

表3.7 循环文件头定义

文件头	字节(Byte)	描述
文件类型	1	‘2E’，安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”：
文件大小	2	字节1 表示记录总个数(2-254) 字节2 表示记录长度(≤178)
访问权限1	1	读权限
访问权限2	1	添加权限
RFU	1	‘FF’
RFU	8	‘FF’

3.5.3.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

- 选择文件命令（Select File）
  可以用Select File 命令通过文件标识符来选择文件。

- 读记录文件（Read Record）
  当满足文件的读权限时，可以用Read Record 命令读取一条记录。

- 写记录文件（Update Record）
  当满足文件的添加权限时，可以用Update Record 命令增加一条新记录。

3.5.4 变长记录文件

3.5.4.1 定义

变长记录文件为具有可变长度记录的文件。

3.5.4.2 文件体结构——变长线性文件

变长线性文件又叫变长记录文件。变长记录文件的数据以记录为单位进行存储，通过记录号或记录标识来选择每条记录。更新记录时，新的记录长度必须与卡中原有记录长度相同，否则本次更新无效。

一个文件中的记录数为2～254，不同的操作系统所支持的记录长度最大值不一样，Simlinker/PSAM支持的记录长度最大值为178 字节。

通常，变长记录以TLV（Tag-Length-Value）格式存在。在Simlinker/PSAM 中，变长记录文件和密钥文件都采用变长记录格式。

图3-6 变长记录文件头格式

文件头	字节(Byte)	描述
文件类型	1	‘2C’，安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”
文件大小	2	文件主体空间
访问权限1	1	读权限
访问权限2	1	追加权限/写权限
RFU	1	‘FF’
RFU	8	‘FF’

说明：

♦ 文件主体空间=所有记录长度和；

每条记录长度=1 字节记录标识符(T)+1 字节记录长度（L）+L 字节数据+1 字节校验码（由COS 计算）每条记录长度的最大为178 个字节。

3.5.4.4 文件操作命令

♦ 建立文件命令（Create File ）

当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

♦ 选择文件命令（Select File）

可以用Select File 命令通过文件标识符来选择文件。

♦ 读记录文件（Read Record）

当满足文件的读权限时，可以用Read Record 命令读文件中的记录。

♦ 写记录文件（Update Record）
当满足文件的写权限时，可以用Update Record 命令写（或更新）一条记录。

3.6 内部基本文件

用于存储由卡所解释的数据，指为了管理和控制目的由卡分析和使用的数据，包括密钥文件。

3.6.1 密钥文件（KEY 文件）

3.6.1.1 定义

存放密钥的文件，不可由外界读出。当满足文件的增加密钥权限时可以向文件中写入一条密钥；当满足密钥的使用权限时可在卡内进行相应的密码运算；当满足某条密钥的更改权限时可以修改此密钥。

注：

♦ 每个*DF* 下只能有一个*KEY* 文件，且必须最先被建立。在任何情况下密钥数据均无法读出。

♦ 若当前*DF* 下无任何文件，则在该*DF* 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开该*DF* 再进入此*DF* 时，将遵循文件的访问权限。

3.6.1.2 文件体结构——变长记录格式

一个KEY 文件中可以包含多种密钥，每种密钥可以有多个。在Simlinker/PSAM 中，密钥文件采用变长记录格式，数据项定义如下表所示，记录中的T、L 字节由COS 维护。

表3.9 KEY 文件记录格式

数据元		长度
T（由COS 维护）		1
L（由COS 维护）		1
Value	密钥头	5

	密钥值	不同的密钥类型长度不同

说明：

- 每条记录长度=1 字节TAG+1 字节的长度+5 字节的密钥头+密钥值的长度。
- 密钥头和密钥值的设置见“9.3 Write Key 命令”。

3.6.1.3 密钥头——密钥类型

表3.10 密钥类型

密钥名称	类型字节（HEX）	密钥名称	类型字节（HEX）
主控密钥	00	PBOC	方式一
维护密钥	01	PBOC	方式一
消费密钥	02	PBOC	方式一
PIN解锁密钥	03	PBOC	方式一
重装PIN密钥	04	PBOC	方式一
用户卡应用维护密钥	05	PBOC	方式一
MAC密钥	06	PBOC	方式一
加密密钥	07	PBOC	方式一
MAC、加密密钥	08	PBOC	方式一
解密密钥	09	PBOC	方式一
安全计算方式0密钥	0A	专有	方式一
安全计算方式1密钥	0B	专有	方式一
内部认证密钥	F0	专有	方式二
口令重装密钥	F8	专有	方式二
外部认证密钥	F9	专有	方式二
口令密钥	FA	专有	方式二

说明： 表中的“方式一”与“方式二”的具体含义见“9.3Write Key”。
所有密钥的装载与更新都必须采用加密带 MAC 方式（线路加密保护方式）。

3.6.1.4 文件头定义

表3.11 KEY 文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘3F’
文件标识(FID)	2	‘0000’
文件大小	2	所有密钥记录长度之和+5 字节保留空间
DF 短文件标识符	1	见表3.14
访问权限2	1	增加密钥权限
RFU	1	‘FF’
RFU	8	‘FF’

说明：

♦ DF 短文件标识符

表3.12 DF 短文件标识符

b7	b6	b5	b4	b3	b2	b1	b0	描述
0	0	0	X	X	X	X	X	当前DF 为DDF，低5 位为DDF 下目录基本文件的短文件标识符。
1	0	0	X	X	X	X	X	当前DF 为ADF，低5 位为发卡方专用数据文件的短文件标识符。
1	1	1	1	1	1	1	0	保留值

3.6.1.5 文件操作命令

♦ 建立文件命令（Create File ）
当满足卡片当前DF 的建立权限时，可以用Create File 命令创建文件。

♦ 增加或修改密钥命令（Write Key）
在满足密钥文件的增加密钥的权限时，可以用Write Key 命令向密钥文件中写入一条密钥（设置密钥头和密钥值）；在满足密钥的更改权限时可以用Write Key 命令更改密钥数据（即不能更改密钥头数据）。

注：不能用***Write Key*** 命令修改口令密钥。

♦ 对于不同的密钥类型，有其相应的命令，见“3.6.2. 密钥（KEY）和表3.15 密钥类型及命令”。
在满足密钥使用权限时才可使用相应的密钥进行认证或密码运算。

3.6.2 密钥（KEY）

3.6.2.1 主控密钥

在增加或修改密钥中，主控密钥是用于产生安全报文的密钥。

主控密钥也可以当作外部认证密钥使用，其错误计数器默认为‘33’，后续状态默认为‘0A’。

主控密钥涉及的命令如下：

外部认证命令（External Authenticate）

增加或修改密钥命令（Write Key）

3.6.2.2 维护密钥

在以安全报文方式访问文件时，维护密钥是用于产生安全报文的密钥。

维护密钥所涉及的命令如下：

读二进制文件（Read Binary）

写二进制文件（Update Binary）

读记录文件（Read Record）
写记录文件（Update Record）
增加记录（AppendRecord）
卡片锁定（CardBlock）
应用锁定（Application Block）
应用解锁（Application Unblock）

3.6.2.3 消费密钥

消费密钥是PSAM卡用于消费的密钥。
消费密钥支持密钥多级分散。
在消费交易过程中，消费密钥用于产生MAC1和验证MAC2，以保证用户卡与终端之间数据传输的完整性和双方之间的合法性认证。
消费密钥所涉及的命令如下：
MAC1计算（Init_SAM_For_Pruchase）
校验MAC2（Credit_SAM_For_Purchase）

3.6.2.4 PIN解锁密钥

PIN解锁密钥是用于解锁被锁定的用户卡口令密钥。
PIN解锁密钥支持多级分散。
在用户卡PIN解锁命令中，PIN解锁密钥用于加密数据和长生MAC。
PIN解锁密钥所涉及的命令如下：
通用DES计算初始化）Init_For_Descrypt)
通用DES计算（DES Crypt）

3.6.2.5 重装PIN密钥

重装PIN密钥适用于重装用户卡口令的密钥。
重装PIN密钥支持多级分散。
在用户卡重装口令中，重装PIN密钥用于产生MAC。
重装PIN密钥所涉及的命令如下：
通用DES计算初始化（Init_For_Descrypt）
通用DES计算（DES Crypt）

3.6.2.6 用户卡应用维护密钥

用户卡应用维护密钥是用于安全更新用户卡文件的密钥。
用户卡应用维护密钥支持多级分散。
在以安全报文方式访问用户卡中的文件时，用户卡应用维护密钥用于加密数据及产生MAC。
用户卡应用维护密钥所涉及的命令如下：
通用DES计算初始化（Init_for_Descrypt）

通用DES计算（DES Crytp）

3.6.2.7 MAC密钥

MAC密钥用于MAC计算
MAC密钥支持密钥多级分散。
MAC密钥所涉及的命令如下：
通用DES计算初始化（Init_For_Descrypt）
通用DES计算（DES Crypt）

3.6.2.8 加密密钥

加密密钥用于DES加密运算。
加密密钥支持密钥多级分散。
加密密钥所涉及的命令如下：
通用DES计算促使花）(Init_For_Descrypt)
通用DES计算（DES Crypt）

3.6.2.9 MAC、加密密钥

MAC、加密密钥用于MAC计算和DES加密运算。
MAC、加密密钥支持密钥多级分散。
MAC、加密密钥所涉及的命令如下：
通用DES计算初始化）Init_For_Descrypt)
通用DES计算（DES Crypt）

3.6.2.10 解密密钥

解密密钥用于MAX计算和DES解密运算。
解密密钥支持密钥多级分散。
解密密钥所涉及的命令如下：
通用DES计算初始化）Init_For_Descrypt)
通用DES计算（DES Crypt）

3.6.2.11 安全计算方式0密钥

安全计算方式0密钥是安全计算方式0中的加密密钥。
安全计算方式0密钥所涉及的命令如下：
安全计算（Secure Calculation）

3.6.2.12 安全计算方式1密钥

安全计算方式0密钥是安全计算方式1中的加密密钥。
安全计算方式1密钥所涉及的命令如下：

安全计算（Secure Calculation）

3.6.2.13 内部认证密钥

内部认证密钥是用于内部认证过程中的密钥。
乃不认证密钥所涉及的命令如下：
内部认证（Internal Authenticate）

3.6.2.14 口令重装密钥

口令重装密钥用来长生重装PIN'命令的MAC。
口令重装密钥所涉及的命令如下：
重装/修改口令密钥（Reload/Change PIN）

3.6.2.15 外部认证密钥

外部认证主要用于外部认证过程（卡对机具进行认证）中认证鉴别数据。
外部认证密钥如果被锁死将无法被解锁。
外部认证密钥所涉及的命令如下：
外部认证命令（External Authenticate）
在满足密钥的使用权限时，可以用External Authentication命令验证终端的合法性。

3.6.2.16 口令密钥（PIN）

PIN也是密钥的一种，只有卡片持有者知道此PIN值，用以实现卡片对持有者的鉴别。
口令长度是2到8字节。
正确核对口令后可使卡片达到指定的安全状态，以执行某个操作（如读文件等）。
每次核对口令失败时错误计数器自动减一，当正确核对口令后，错误次数技术其复位(恢复原值）。当错误计数达到0时，口令密钥自动被锁死。可以用响应的命令对被锁定口令进行口令解锁操作。
错误计数器的取值范围是1到15.
口令密钥所涉及的命令如下：
验证口令（Verify PIN）
验证并修改口令（Verify & Change PIN），适用于长度为8字节的口令密钥。
解锁口令（Unblock PIN），适用于长度为8字节的口令密钥。

3.6.3 密钥类型及命令集

表3.13 密钥类型及命令集

密钥类型（HEX） / 命令	主控密钥 00	维护密钥 01	消费密钥 02	PIN解锁密钥 03	重装PIN密钥 04	用户卡应用维护密钥 05	MAC密钥 06	加密密钥 07	MAC加密密钥 08	解密密钥 09	安全计算方式0密钥 0A	安全计算方式1密钥 0B	逻辑加密卡专有密钥 0C	内部认证密钥 F0	口令重装密钥 F8	口令密钥 FA	外部认证密钥 F9
Application Block		Y															
Application Unblock		Y															
Credit_SAM_For_Purchase			Y														
DES Crypt				Y	Y	Y	Y	Y	Y	Y							
External Authentication	Y																Y
Init_For_Descrypt				Y	Y	Y	Y	Y	Y	Y							
Init_SAM_For_Purchase			Y														
Internal Authentication														Y			
Reload/Change PIN															Y		
Secure Calculation											Y	Y					
Update Binary		Y															
Update Record		Y															
Verify PIN																Y	
Calculate Key													Y				
Write Key	Y																

说明：表格中Y表示命令可用于对应的密钥类型。
密钥类型用一个字节表示，如某个密钥类型为‘00’则表示该密钥为主控密钥。密钥类型在装载KEY文件时确定。

3.7 文件类型及命令集

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

表3.14 文件类型及命令集

文件类型（hex） / 命令	MF 38	DF 38	二进制 28	定长记录 2A	循环 2E	变长记录 2C	KEY文件 3F
Create	Y	Y	Y	Y	Y	Y	Y
Erase DF	Y	Y					

Read Binary			Y				
Read Record				Y	Y	Y	
Select File	Y	Y	Y	Y	Y	Y	
Update Binary			Y				
Update Record				Y	Y	Y	
Write Key							Y

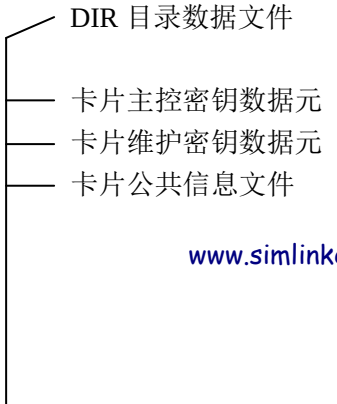
说明：
表格中Y表示命令可用于对应的文件类型。
文件类型表示文件内部结构组织形式，用一个字节来表示，如某个文件类型为28H则表示该文件为二进制文件。文件类型在建立文件时规定。

3.8 PSAM 卡文件结构

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

3.8.1 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：



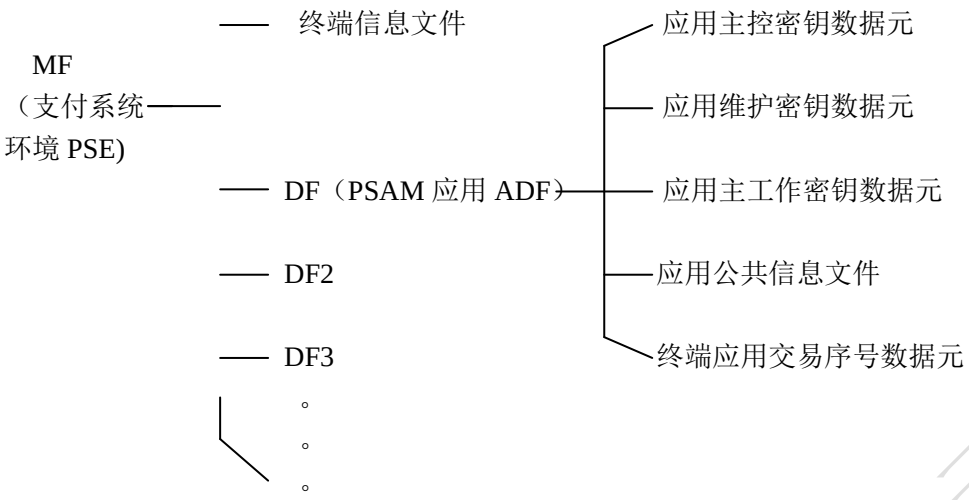


图 3-7　PSAM 卡文件结构（简要）

3.8.2　MF 区域说明

在 PSAM 卡的 MF 区域中，文件创建和密钥装载是在卡片主控密钥的控制下进行的。

3.8.2.1　目录数据文件

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

3.8.2.2　卡片主控密钥

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

创建卡片 MF 区域的文件；

装载卡片维护密钥、应用主控密钥；

更新卡片主控密钥、卡片维护密钥。

卡片主控密钥的控制可通过外部认证操作实现，也可通过安全报文的方式实现。

3.8.2.3　卡片维护密钥

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

安全更新记录文件；

安全更新二进制文件；

卡片维护密钥的控制通过安全报文的形式实现。

3.8.2.4　卡片公共信息文件

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

3.8.2.5 终端信息文件

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

3.8.3 ADF 区域说明

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

3.8.3.1 应用主控密钥

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

装载应用维护密钥、应用主工作密钥；

更新应用主控密钥、应用维护密钥。

应用主控密钥的控制可通过外部认证操作实现，也可通过安全报文的方式实现。

3.8.3.2 应用维护密钥

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

安全更新记录文件；

安全更新二进制文件；

进行应用解锁。

卡片维护密钥的控制通过安全报文的形式实现。

3.8.3.3 应用主工作密钥

应用主工作密钥用于卡片的交易，在应用主控密钥的控制下装载。

3.8.3.4 应用公共信息文件

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

3.8.3.5 终端应用交易序号数据元

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

终端应用交易序号只对本应用有效。

3.9 文件空间计算

如前所述，每个文件在EEPROM 中存放的格式如下：

16 字节文件头 （文件类型，文件标识符，文件主题空大小，权限，校验等）
文件主体

- 每个基本文件所占的EEPROM 空间=文件头+文件主体空间
- 定长、钱包和循环文件的主体空间=记录个数*（记录长度+1）
- 每个DF 所占的EEPROM 空间=DF 头16 字节+DF 下所有文件的空间和+DF 名称长度
- MF 的空间=MF 头16 字节+MF 下所有文件空间之和

3.10 安全报文传送

3.10.1 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，正阳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。

3.10.2 如何实现安全报文传送

3.10.2.1 文件

二进制文件、定长记录文件、变长记录文件、循环文件、普通钱包文件都可以采用安全报文传送。如对上述文件进行安全报文传送，只需要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

表3.18 文件类型设置

【例】建立文件杀死若需要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（详见Create File）

3.10.2.2 密钥

对于密钥也可以采用安全报文传送。

如对密钥进行安全报文传送（使用Write Key、Verify PIN），只需在安装密钥时改变密钥类型字节高两位即可。

密钥类型字节定义如下：

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

表 3.19 密钥类型设置

【例】对密钥若需要进行线路加密保护(DES&MAC)则将密钥类型最高位及次高位均置1，如外部认证密钥类型有‘39’编程‘F9’。

3.10.2.3 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Simlinker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）

——Simlinker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禁止数字‘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，则转到第五步；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。

如果该密钥长度为8字节，则依照图3-17的方式来产生MAC（根据在第三步中产生的数据长度不同，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3-18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字节长的的MAC。

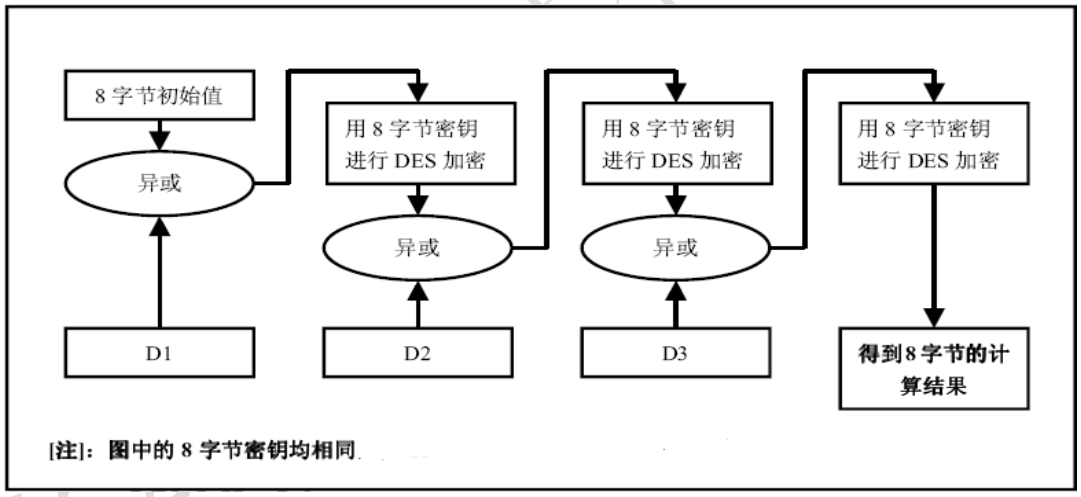


图 3.17 用Single DES密钥产生MAC的算法

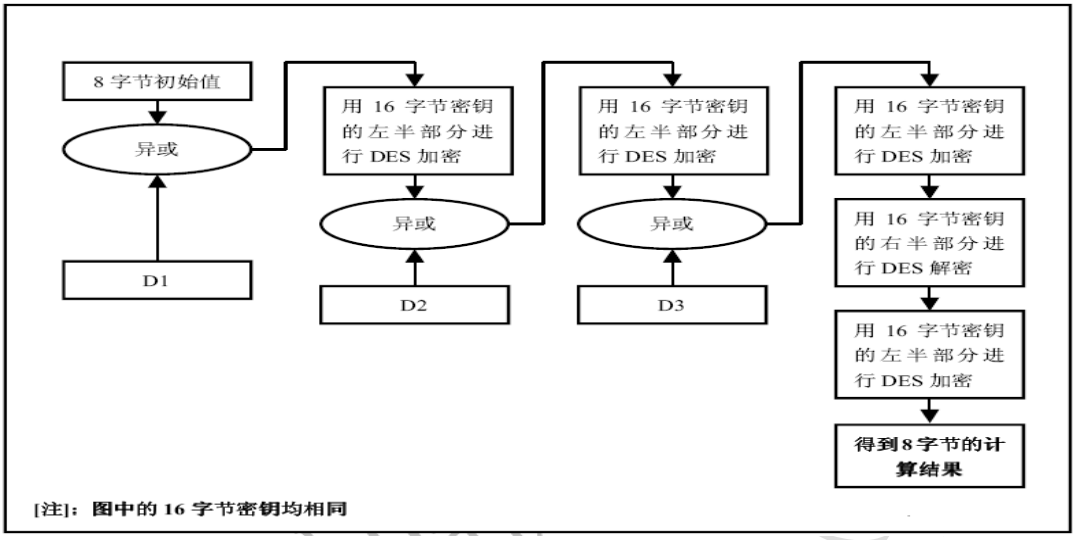


图 3.18 用Triple DES密钥产生MAC的算法

3.10.2.4 数据加密和解密

1. 数据加密

按照如下方式对数据进行加密：

第一步：用LD标识明文数据的长度，在明文数据前加上LD长生新的数据块。

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。最后一个数据块长度有可能不是8字节。

第三步：如果最后（或唯一）的数据块长度等于8字节，转到第四步；如果不足8字节，在右边添加16进制数字‘80’。如果长度已达到8字节，转到第四步；否则，在其右边添加16进制数字‘00’直到长度到达8字节。

第四步：对每一个数据块使用相应密钥进行加密。

如果该密钥长度为8字节，则依照图3-19的方式来加密数据块。

如果该密钥长度为16字节，则依照图3-20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数需连接在一起（加密后的D1,D2,D3等）。并将结果数据块插入到命令数据域。

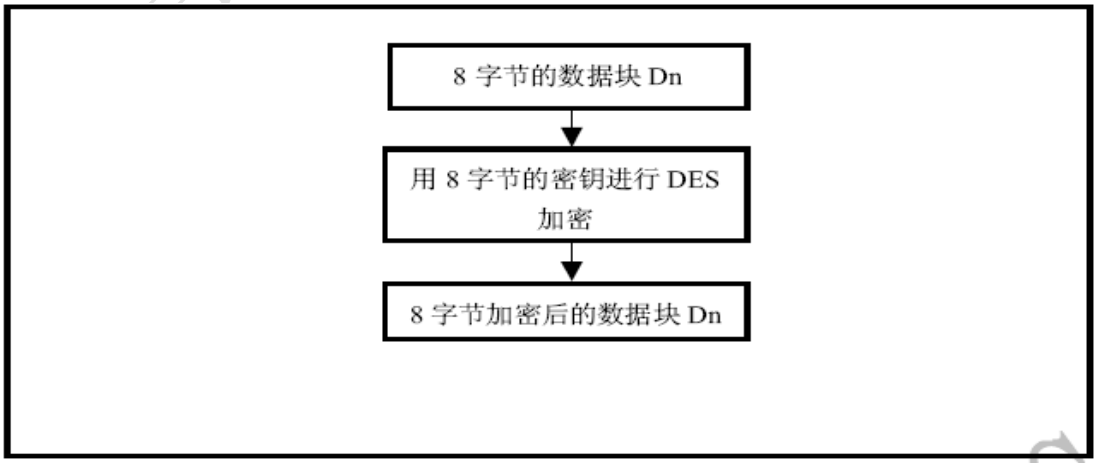


图 3.19 用Single DES密钥进行数据加密的算法

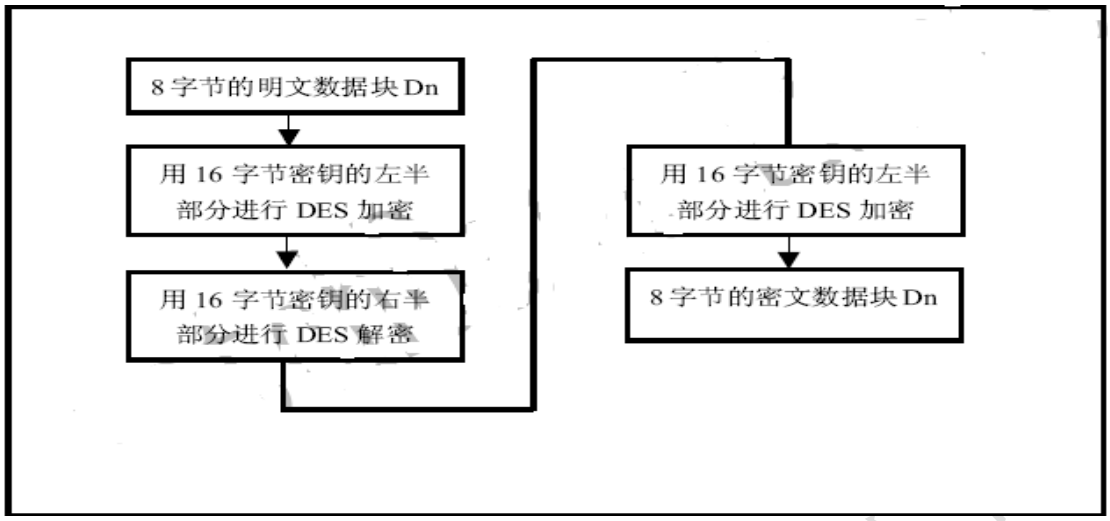


图 3.20 用Triple DES密钥进行数据加密的算法

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。

如果该密钥长度为8字节，则依照图3-21的方式来解密数据块。

如果该密钥长度为16字节，则依照图3-22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，D2等）连接在一起。

数据块由LD、明文数据、填充字符组成。

第四步：应为LD标识明文数据长度，因此，它被用来恢复明文数据。

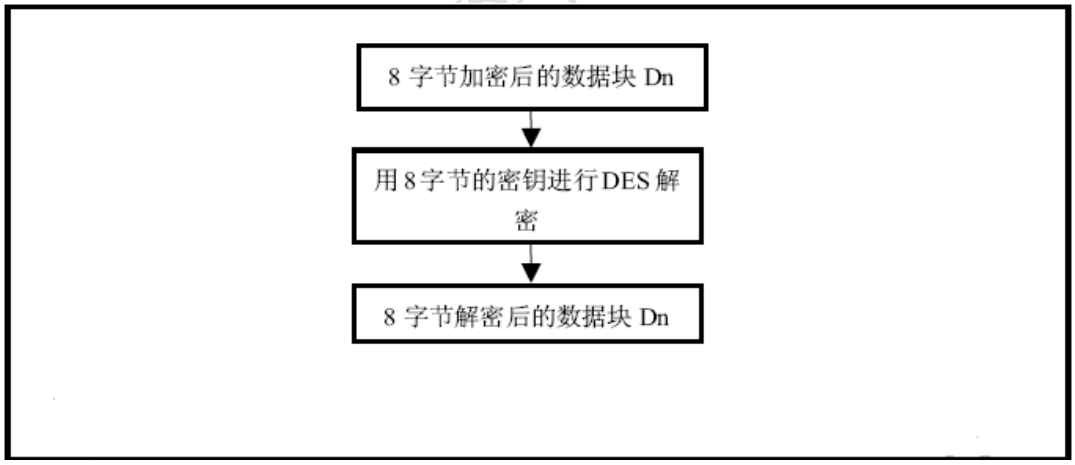


图 3.21 用Single DES密钥进行数据解密的算法

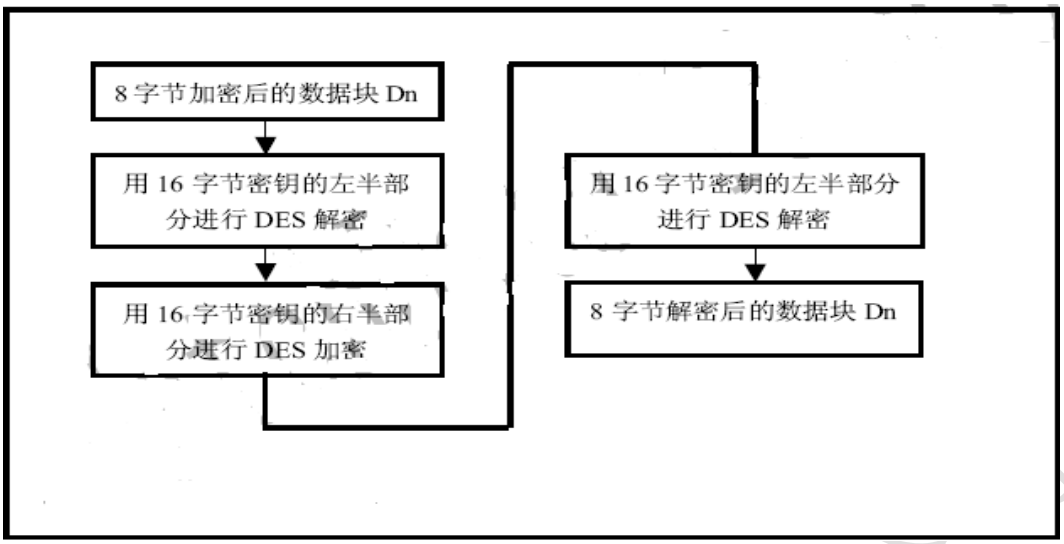


图 3.22 用Triple DES密钥进行数据解密的计算

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3-23描述了产生过程密钥的机制。数据数据是8字节，输入数据的定义见相关命令描述。

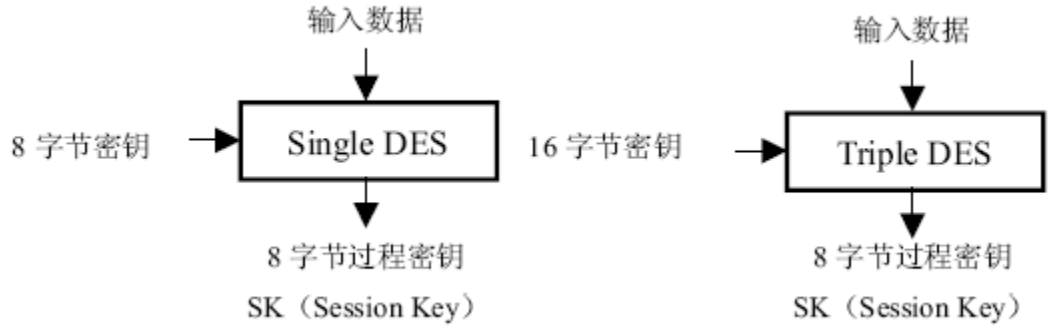


图 3.23 过程密钥的产生

4. 卡片初始化设置

4.1 卡片初始化

卡片初始化完成以下两个功能：

Simlinker/PSAM的参数设置

安装传输密钥

卡片初始化是在卡片制造厂家完成。在卡片初始化之前，只能使用卡片初始化指令。

4.2 卡片传输协议

卡片传输协议T=0.

4.3 卡片初始化后的文件结构

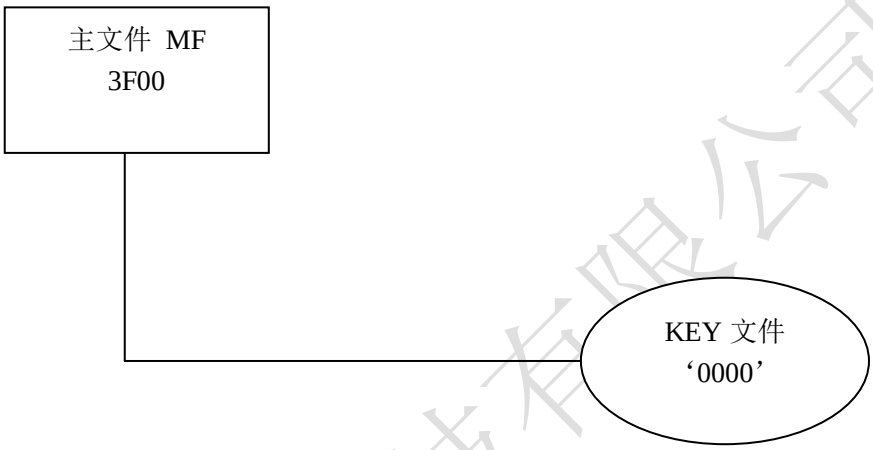


图**4-1** 卡片初始化文件结构

4.4 主文件（MF）

- MF 是卡片文件系统的根。

- 文件参数

  文件类型：‘38’
  文件标识符：‘3F00’
  文件大小：卡片已根据芯片最大空间建立MF
  MF 建立权：‘AA’
  MF 擦除权：‘AA’
  文件名称：1PAY.SYS.DDF01

4.5 KEY 文件

♦ KEY 文件里仅包含一条卡片传输密钥，以保证卡片运输过程中的安全。只有认证此密钥后才能进行发卡操作。

♦ 文件参数

文件类型：‘3F’
文件标识符：‘0000’
文件大小：‘1C’
MF 的短文件标识符：‘01’
密钥增加权限：‘AA’

4.6 卡片传输密钥

♦ 卡片传输密钥相当于卡片主控密钥。

♦ 只有认证卡片传输密钥后才能进行发卡操作。

♦ 密钥参数

密钥标识：00
密钥类型：‘F9’
使用权限：‘F0’
更改权限：‘AA’
后续状态：‘0A’
错误计数器：‘33’

♦ 密钥值

密钥长度：16 字节

注：如果您需要专用的卡片传输密钥，必须在批量订货时声明。由我公司代为生成唯一的专用卡片传输密钥。

4.7 使用说明

如前所述，卡片中MF 的建立和擦除权限已经预置为AA 且不可更改。只有卡片传输密钥认证通过后，安全状态寄存器达到状态‘0A’时，才能进行发卡操作。

卡片传输密钥认证通过后，有以下两种操作方式：

1）擦除MF 下的文件，重新建立卡片结构。

2）替换传输密钥值，后建立卡片结构。（替换传输密钥的方法见“9.3 Write Key 之方式一”）

5. Simlinker/PSAM 的安全体系

5.1 安全状态

安全状态是指卡在当前所处的一种安全级别。Simlinker/PSAM的MF和DF分别具有16种不同的安全状态。

Simlinker/PSAM在卡内部用两个4位寄存器来标识安全状态，每个寄存器的值可以是0至F之间的某一值。两个寄存器如下：

MF安全状态寄存器

它表示整个卡所处的安全级别。

DF安全状态寄存器

它表示当前应用所处的安全级别。

5.1.1 MF 安全状态寄存器

- 在以下几种情况下，MF 安全寄存器将被复位为0：
  [1] 卡片复位后；
  [2] 当在MF 下的核对口令或外部认证命令返回的错误状态为63CX.

- 应用目录的改变不会影响该寄存器的值。

- 只有MF 下的口令核对或外部认证通过后MF 的安全状态寄存器值才发生变化。

5.1.2 DF 安全状态寄存器

- 在以下几种情况下，DF 安全寄存器将被复位为0：
  [1] 卡片复位后。
  [2] 选择DF 后（如选择下级子目录或同级目录等）。

  [3] 当前DF 下的核对口令或外部认证命令返回的错误状态为63CX.

- 只有当前目录下的口令核对或外部认证通过后DF 的安全状态寄存器值才发生变化。若当前目录为MF，则当前目录的DF安全状态寄存器的值等于MF的安全状态寄存器值。

5.2 安全属性

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

安全属性又称访问权限，如下表所示：

表5.1 访问权限

文件类型	访问权限
MF/DF	建立/擦除
KEY 文件	增加
KEY 文件中的密钥	使用/更改
二进制文件	读/写
定长记录文件	读/写
循环文件	读/写
变长记录文件	读/写

每种文件访问权限在建立该文件（Create File）时用一个字节指定；每种密钥访问权限在增加密钥(Write Key)时用一个字节指定。

Simlinker的访问权限有别于其它任何操作系统的访问权限，它用一个区间来严格限制其他非法访问者。

假设当前安全状态寄存器的值用V来表示。

- 访问权限为‘0Y’时表示要求MF的安全状态寄存器的值大于等于Y。
  即：访问权限=‘0Y’ V>=Y

  [例] 如某文件读的权限为‘05’表示在对该文件进行读之前必须使MF的安全状态寄存器的值大于等于5. 即：文件的读权限=‘05’ V>=5

- 访问权限为‘XY’时（X不为0）表示要求当前目录的安全状态寄存器的值大于等于Y且小于等于X.
  [1] 当X>Y时
  即访问权限=‘XY’，且X>Y， 如此 Y≤V≤X

  [2] 当X=Y时,当前安全状态寄存器必须等于X.
  即访问权限=‘XY’，且X=Y， 如此 V=X=Y

  [3] 当X<Y时，表示禁止相应的操作。
  [例1] 如某文件写的权限为53表示对该文件进行写之前必须使当前目录的安全状态寄存器的值为3、4或5.
  [例2] 某文件读的权限为F0，写的权限为F1，代表可任意读取，写时必须满足当前目录的安全状态寄存器的值大于等于1.

5.3 安全机制

安全机制是指某种安全状态转移为另一种安全状态所采用的方法和手段。

为改变安全状态寄存器的值，必须通过某个密钥的口令或外部认证认证来实现；在密钥装载时，它的后续状态字（8bit）已经规定好了相应的安全状态，认证通过后，密钥的后续状态字节低4位将被置入安全状态寄存器。

- 在MF下认证通过后，将同时改变MF和当前目录的安全状态寄存器的值；
  在非MF下认证通过后，将只改变当前目录的安全状态寄存器值。
  为更好的理解Simlinker 的安全机制，下面举一例说明：
  设卡中某目录下有一个二进制文件，参数定义如下：
  读权限=‘F1’；
  写权限=‘F2’；
  该目录下有一个口令密钥，口令核对通过之后的后续状态为1；
  该目录下有一外部认证密钥，使用权限为11，外部认证通过之后后续状态为2。
  请看下面的操作及当前目录的状态寄存器的变化情况：

卡终端操作	方向	当前目录安全状态寄存器的值
选择 DF	→	0
	←	送返回信息
读二进制文件	→	0
	←	读的权限不满足，不允许读
验证口令	→	1
	←	口令核对正确
读二进制文件	→	1
	←	送出读出的数据
写二进制文件	→	1
	←	写的权限不满足，不允许写
外部认证	→	2
	←	外部认证正确
写二进制文件	→	2
	←	写成功
读二进制文件	→	2
	←	送出读出的数据

图5-1 访问权限控制

5.4 基于 DES 的加密算法

5.4.1 DES 加密算法

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

Single DES算法

Single DES算法是值使用单长度（8字节）密钥K对8字节块的输入数据X1，X2，X3……加密，得到8字节块的输入数据Y1，Y2，Y3……。其中，

$$Y1 = DES\ (K)\ [X1]$$

解密方式如下：

$$Y1 = DES^{-1}(K)[y1]$$

3DES算法（Triple DES算法）

3DES算法是指使用双长度（16字节）密钥K=（K1||K2）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：

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

5.4.2 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 3DES 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 3DES 运算

5.4.3 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 的左半部分为 LK，右半部分为 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；

5.4.4 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：
首先用可内密钥对最后 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做临时密钥。

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

Simlinker 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

Simlinker 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	SW1	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
93	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 Simlinker/PSAM 基本命令

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。

7.1.1 注意事项

在满足该外部认证密钥的使用权限且该密钥未被锁死时才可执行该命令。

7.1.2 命令报文

表 7.1 External Authentication 命令报文编码

代码	长度（byte）	值（Hex）	描述
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，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

命令报文数据域包括 8 字节加密后的随机数。

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 7.2External Authentication 命令响应状态码

SW1	SW1	意义
90	00	正确执行
63	CX	还剩 X 次可试机会
67	00	长度错误
69	81	不是外部认证密钥
69	82	密钥使用条件不满足
69	83	外部认证密钥锁死
6A	82	未找到 key 文件
93	02	安全信息不正确
94	03	密钥未找到

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 7.3Get 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

命令报文数据域不存在。

7.2.5 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

7.2.6 响应报文状态码

表 7.4 Get Response 命令响应状态码

SW1	SW1	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

7.3 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 7.5 Get Challenge 命令报文编码

代码	长度（byte）	值（Hex）	描述
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 7.6 Get Challenge 命令响应状态码

SW1	SW1	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 7.7 Inernal Authentication 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00	-
INS	1	88	-
P1	1	00	加密
		01	解密
		02	计算 MAC
P2	1	XX	DES 密钥标识号
Lc	1	XX	-
DATA	XX	XX…XX	认证数据
Le	1	00	-

说明：

P1=00，表示进行加密运算，密钥类型是 DES 加密密钥

P1=01，表示进行解密运算，密钥类型是 DES 解密密钥

P1=02，表示进行 MAC 运算，密钥类型是 DES&MAC 密钥

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 7.8 Internal Authentication 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	正确执行 XX 标识响应数据长度。可用 Get Response 命令取回响应数据（仅用于 T=0）
67	00	Lc 与钱包文件长度不一致
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	文件未找到
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	卡片
产生两个 8 字节随机数 RND		
送 RND 作内部认证	==》 《==	卡片用指定的 DES 加密密钥对随机数 RND 进行 DES 加密，产生鉴别数据 D1.即：D1=DES（KID，RND） 送 D1

用于卡片 DES 加密密钥相同的密钥 Cardkey 对 RND 进行 DES 加密，产生鉴别数据 D2，后比较 D1 和 D2 即： 1） D2=DES(Cardkey,RND) 2） D1?=D2		

图 7-1 内部认证过程

说明：

1. 终端自己产生或从 PSAM 卡申请 1 个 8 字节随机数 RND；
2. 终端向卡片发出内部认证命令，送入 RND 到卡片内；
   00 88 00 KID 08 RND
3. 卡片收到 RND 后，用卡内的相应密钥对随机数 RND 进行 DES 加密预算，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 进行 DES 加密，产生 8 字节鉴别数据 D2；
6. 终端比较 D1 和 D2，若一致则认证通过，不一致认证失败。

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 7.9 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	1	-	不存在
DATA	XX	-	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 7.10 Read Binary 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	正确执行 XX 标识响应数据长度。可用 Get Response 命令取回响应数据（仅用于 T=0）
67	00	长度错误
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
6A	82	文件未找到

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.

若 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。

7.6 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。

7.6.2 注意事项

- Read Record 命令只适用于定长记录文件、循环文件、钱包文件和变长记录文件。
- 访问二进制文件的命令如下：
  建立文件（Create File）
  选择文件（Select File）
  读记录文件(Read Record)/写记录文件(Update Binary)/增加记录(Append 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 7.11 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	控制参数，见说明
Lc	1	-	不存在
DATA	XX	-	不存在
Le	1	XX	‘00’或要读取的数据长度

说明

命令报文中的引用控制参数：

b7	b6	b5	b4	b3	b2	b1	b0	含　义
X	X	X	X	X				SFI
					1	0	0	P1 为记录的个数

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数据组成。

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 7.12 Read Record 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	正确执行 XX 标识响应数据长度。可用 Get Response 命令取回响应数据（仅用于 T=0）
67	00	长度错误
69	81	命令与文件结构不相符
69	82	读的条件不满足
6A	81	不支持此功能
6A	82	文件未找到
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。

7.7 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 MF、DDF 或 ADF。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 7.13 Select File 命令报文编码

代码	长度（byte）	值（Hex）	描述
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	分拣标识符或 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，标识按文件标识符选择（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，标识用 DF 名称选择，分如下两种情况：

——P2=00，标识第一个或仅有一个：

——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表示符或 DF 名称。表 6.21 成功。

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 6.21 和 6.22 所示。

表 7.14 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 6.22 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	发卡方自定义数据文件控制信息	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 7.15 Select File 命令响应状态码

SW1	SW1	意义
90	00	正确执行
61	XX	正确执行 XX 标识响应数据长度。可用 Get Response 命令取回响应数据（仅用于 T=0）
67	00	长度错误
6A	81	不支持此功能
6A	82	未找到文件
6A	86	参数 P1 P2 不正确

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）
- ♦ 只有满粗二进制文件写权限时才能执行此命令。

7.8.3 命令报文

表 7.16 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 标识要写入的字节数。
——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。
若为线路几米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“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 7.16 Update Binary 命令响应状态码

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

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。

在使用当前记录地址时，该命令将在修改记录成功后重新设定记录指针。

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：

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 7.17 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纪录
Le	-	-	不存在

说明：

参数 P2 的含义

b7	b6	b5	b4	b3	b2	b1	b0	含　义
X	X	X	X	X				SFI
					0	0	0	第一个记录
					0	0	1	最后一个记录
					0	1	0	下一个记录
					0	1	1	上一个记录
					1	0	0	记录号在 P1 中给出
其余值								RFU

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

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 7.18 Update Record 命令响应状态码

SW1	SW1	意义
90	00	正确执行
67	00	长度错误（Lc 域为空）
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
69	87	无安全报文
6A	81	不支持此功能
6A	82	未找到文件
6A	83	未找到记录
6A	84	文件无足够空间

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，校验时可以忽略该字段，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 7.19 Verify PIN 命令报文编码

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

说明：

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，则口令可试此时减 1，若口令已被锁死，则不能再执行该命令。

7.10.4 命令报文数据域

命令报文数据域由持卡者数据的口令密钥组成。

7.10.5 响应报文数据域

响应报文数据域不存在。

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 标识个人密码允许重试的次数；

当卡片回送 SW2=C0 时，标识不能重试口令密钥，此时再次使用 Verify PIN 命令，将返回失败状态 6983.

IC 卡可能回送的状态码入校所示：

表 7.20 Verify PIN 命令响应状态码

SW1	SW1	意义

90	00	正确执行
63	CX	还剩 X 此可试机会
62	83	口令密钥校验错误
67	00	长度错误
69	81	不是口令密钥
69	82	密钥使用条件不满足
69	83	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. Simlinker/PSAM 扩展命令

表 8.1 列出了 Simlinker/PSAM 扩展命令。

表 8.1Simlinker/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	Creadit_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 Appliction 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 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’）。

8.1.2 命令报文

表 8.1 Application Block 命令报文编码

代码	长度（byte）	值（Hex）	描述
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识以表明不允许执行 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。

用密钥标识为 00 的 16 字节维护密钥计算 MAC。

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 8.2 Application Block 命令响应状态码

SW1	SW1	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相应的限制将被取消。

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 8.3 Application Unblock 命令报文编码

代码	长度（byte）	值（Hex）	描述
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。
用密钥标识为 00 的 16 字节维护密钥计算 MAC。

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 8.4 Application Unblock 命令响应状态码

SW1	SW1	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 卡下点后自动消失，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
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“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“状态子 SW1SW2 意义”

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“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 8.6 DES Crypt 命令报文编码

代码	长度（byte）	值（Hex）	描述
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
Le	1	00	-

表 8.7 DES Crypt 命令引用控制参数 P1

b7	b6	b5	b4	b3	b2	b1	b0	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 b2 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“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 b0 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 b0 位为 1 时，且 P1 的 b1 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“状态字 SW1SW2 意义”。

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，进行加密得到 MAC。

8.5.2 命令报文

表 8.7Init_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 对卡片传来的下表数据加密生成 8 字节过程密钥 SK。

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“基于 DES 的加密算法”。

8.5.5 响应报文状态码

见“状态子 SW1SW2 意义”。

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_FOR_Purchase 命令产生的过程密钥 SK 校验 MAC2，过程如下：
检查 MAC 尝试计数器，如果 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，并回送烛台码“63CX”，标识剩余尝试计数器的新值；
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 命令陈宫执行后才能进行。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 8.9 Credit_SAM_For_Purchase 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	72	-
P1	1	00	-

P2	1	00	-
Lc	1	04	-
DATA	XX	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。
MAC 计算的初始值为 8 个字节的十六禁止数字“0”，方法见“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“状态子 SW1SW2 意义”。

8.6.6 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所示：

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

发出 MAC2→		
	MAC2 校验→	←发出校验结果

图 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 8.10 Reload/Change PIN 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	5E	-
P1	1	00	Reload PIN
		01	Change PIN
P2	1	00	-
Lc	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‘00’，方法见“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 7.32 Reload/change PIN 命令响应状态码

SW1	SW1	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	安全报文数据项不正确
93	03	应用永久锁定
94	03	密钥未找到

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“基于 DES 的加密算法”。

8.8.2 命令报文

表 8.12 Secure Calculation 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	1C	-
P1	1	00	加密方式
		01	解密方式（DOUBLE 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 8.13 Secure Calculation 命令响应状态码

SW1	SW1	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。
69	85	使用条件不满足（应用临时锁定）
6A	81	功能不支持（文件不可建立在 MF 或 DF）
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
94	03	密钥索引不支持

8.9 Calculate Key (计算 Mifare 密钥)

8.9.1 定义与范围

在 PSAM 卡的控制下，使用 Mifare one 卡作为用户卡，计算逻辑加密卡的扇区密钥。

8.9.2 命令报文

表 8.14 Calculate Key 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	FC	-
P1	1	00	标准方式
		=！00	扩展方式，P1 为内部认证密钥的标识
P2	1	XX	KID（逻辑加密卡专有密钥的标识）
Lc	1	0D-11	-
DATA	XX	XX…XX	数据

参数说明：

若 P1=00，按标准的建设部 SAM 专用命令进行认证及扇区密钥的计算，此方式下，P1 必须等于 00.

若 P1=！00，按扩展的建设部 SAM 专用命令进行认证及扇区密钥的计算，此方式下，P1 的值为逻辑加密卡认证密钥的标识。

P2=逻辑加密卡专有密钥的标识。

8.9.3 命令报文数据域

城市代码（2 字节）

卡片唯一序列号（4 字节）

流水号（2 字节）

认证 MAC（4 字节）

扇区标识 1（1 字节）

扇区标识 2（1 字节）

…….

扇区标识 5（1 字节）

8.9.4 响应报文数据域

响应报文数据域包括一下数据（按顺序返回）
扇区 1 的密钥值（6 字节）
扇区 2 的密钥值（6 字节）
…….
扇区 5 的密钥值（6 字节）

8.9.5 响应报文状态码

表 8.15 Calculate Key 响应报文状态码：

SW1	SW1	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。
69	85	使用条件不满足（应用临时锁定）
6A	81	功能不支持（文件不可建立在 MF 或 DF）
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
94	03	密钥索引不支持

8.9.6 命令使用说明

标准的建设部 SAM 专用命令

根据 P2 指定的 KID 查找逻辑加密卡专有密钥；

用查找到的密钥对数据域的前 8 个字节加密；

比较加密结果前 4 个字节和数据域中的 MAC，如果不同则返回错误；

再用此密钥对一下数据加密；

唯一号（4 字节）+流水号（2 字节）+MAC 高字节（1 字节）+扇区标识 1（1 字节）

取加密结果的高 6 字节为 Mifare 的一组密钥；

将加密数据中的扇区标识 1 换成扇区标识 2，3，4，5（如果有的话），计算相应密钥。

将生成的密钥依此按顺序送出即可。

所有算法采用 3DES，通讯速率为 38400bps，通讯协议为 T=0；

例：设卡中有 KID=01，密钥值为“12 34 56 78 9A BC DE F0 12 34 56 78 9A BC DE F0”的逻辑加密卡专有密钥；

因此发向 SAM 卡命令为：

80 FC 00 01 0E FE DC BA 98 76 54 32 10 4A B6 5B 3D 01 02

则返回结果为： 6C DF 72 41 82 27 18 41 9D 72 D0 C9

扩展的建设部 SAM 专用命令

P1 必须不为 00；

COS 内部按 P1 指定的 KID 查找逻辑加密卡认证密钥；

使用查找到的逻辑加密卡认证密钥对数据域的钱 8 个字节加密；

比较加密结果钱 4 个字节和数据域中的 MAC，如果不同则返回错误；

根据 P2 指定的 KID 查找逻辑加密卡专有密钥；

用查找到的逻辑加密卡专有密钥对一下数据加密；

唯一号（4 字节）+流水号（2 字节）+MAC 高字节（1 字节）+扇区标识 1（1 字节）；

取加密结果的高 6 字节为 Mifare 的一组密钥；

将加密数据中的扇区标识 1 换成扇区标识 2，3，4，5（如果有的话），计算响应的密钥。

将生成的密钥依此按顺序送出即可。

所有算法采用 3DES，通讯速率为 38400bps，通讯协议为 T=0；

例：设卡中有 01 号的逻辑加密卡专有密钥“12 34 56 78 9A BC DE F0 12 34 56 78 9A BC DE F0”；有 01 号的逻辑加密卡认证密钥 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF;

发向 SAM 卡命令为：

80 FC 01 01 0E FE DC BA 98 76 54 32 10 69 1C 58 65 01 02

则返回结果为：12 49 55 7A78 50 C1 1B 8C 30 70 9B

9. Simlinker/PSAM 发卡命令

- 此部分描述了Simlinker/PSAM 的发卡命令，以下各节将详细描述这些命令。
- 有关安全报文的操作见 “安全报文传送”。

表***9.1*** 列出了***Simlinker/PSAM*** 发卡命令。

表9.1 Simlinker/PSAM 发卡命令

序号	命令	CLA	INS	功能描述	兼容性
1	Create File	80	E0	建立文件（DF、EF）	专有
2	Erase DF	80	0E	擦除DF	专有
3	Write Key	84	D4	增加或改密钥	PBOC&专有

9.1 Create File（建立文件）

9.1.1 定义与范围

Create File 命令用于建立文件系统。请参见“3.4 专用文件、3.5 工作基本文件和3.6 内部基本文件”。

9.1.2 注意事项

- 在满足当前DF 的建立权限时，可用此命令建立DF 或EF。
- 每个DF 下只能有一个KEY 文件，且必须最先被建立。
- 当前DF 被擦除后，则在该DF 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开当前DF 再进入DF 时，将遵循文件的访问权限。
- 目录文件建立后不能自动被选择（MF 除外），需使用Select File 命令选择。

9.1.3 命令报文

表9.2 Create File 命令报文编码

代码	长度(byte)	值(Hex)	描述
CLA	1	80	-
INS	1	E0	-
P1P2	2	XXXX	文件标识（FileID）
Lc	1	XX	-
DATA	XX	XX....XX	文件控制信息（和DF 名称）
Le		-	不存在

注：***MF*** 的文件标识符必须是‘***3F00***’；
KEY 文件的文件标识符必须是‘***0000***’；

9.1.4 命令报文数据域

命令数据域中的所有权限设置请参见“5. Simlinker/PSAM 的安全体系”。

9.1.4.1 **主文件（MF）**

♦ P1 P2 参数固定为‘3F 00’

表9.3 MF 的文件控制信息

数据域	文件类型	文件空间	建立权限	擦除权限	8 字节传输代码
长度（byte）	1	2	1	1	8
值（HEX）	38	FFFF	XX	XX	FFFFFFFFFFFFFFFF

9.1.4.2 专用文件（**DF**）

表9.4 DF 的文件控制信息

DATA	文件类型	文件空间	建立权限	擦除权限	保留字	DF名称（可选）
长度(byte)	1	2	1	1	3	5~16
值（HEX）	38	XXXX	XX	XX	FFFFFF	DF 名称

9.1.4.3 基本文件（**EF**）

基本文件控制信息内容如下表所示。

表9.5 EF 的文件控制信息

数据域 / 文件类型	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte7
二进制文件	28	文件空间		读权限	写权限	‘FF’	‘FF’
定长记录文件	2A	2≤记录数≤254	记录长度≤178	读权限	写权限	‘FF’	‘FF’
循环文件	2E	2≤记录数≤254	记录长度≤178	读权限	写权限	‘FF’	‘FF’
变长记录文件	2C	文件空间=所有记录长度和 每条记录=记录长度+1 字节校验码（由COS 计算）		读权限	写权限	‘FF’	‘FF’
密钥文件	3F	文件空间=所有密钥记录长度之和+5 字节保留空间每条记录的计算方法见说明[2]		当前DF文件短标识符见说明[2]	增加权限	‘FF’	‘FF’

说明：

[1] 二进制文件、定长记录文件、变长记录文件、循环文件、（密钥文件除外）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。
基本文件数据域Byte1（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

[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。

【2】 **KEY** 文件
注：***KEY*** 文件标识符必须是‘***0000***’。
1）每条记录长度=1 字节TAG+1 字节的长度+5 字节的密钥头+密钥值的长度。
记录中的T、L 字节由COS 维护。
注：对于连接MF下密钥的KEY记录，则记录长度=1字节TAG+1字节的长度+1字节密钥类型。
记录中的T、L字节由COS维护。
2）DF文件短标识符
DF 文件短标识符如下表所示。

表9.6 DF 文件短标识符

b7	b6	b5	b4	b3	b2	b1	b0	描述
0	0	0	X	X	X	X	X	当前DF 为DDF，低5 位为DDF 下目录基本文件的短文件标识符。
1	0	0	X	X	X	X	X	当前DF 为ADF，低5 位为发卡方专用数据文件的短文件标识符。
1	1	1	1	1	1	1	0	保留值

9.1.5 响应报文数据域

响应报文数据域不存在。

9.1.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表9.7 Create File 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
6A	81	无MF 或卡片已锁定
6A	86	文件已存在
6A	84	空间不足
69	82	创建文件权限不满足
67	00	创建文件权限不满足
6E	00	无效的CLA

9.2 Erase MF（擦除目录文件 MF）

9.2.1 定义与范围

Erase MF 命令用于擦除MF 该指令仅对MF有效。

9.2.2 注意事项

- 在满足当前DF 的擦除权限时，可以用此命令擦除MF 下的所有文件(包括DF、EF)，但MF当前的访问权限、空间等信息并没有改变(即不能擦除当前DF 的文件头信息)，且MF 的文件名称也不能被擦除。
- 当前MF 下无任何文件时，则在该目录下可任意擦除DF 而不受擦除权限控制。
- 当前MF 被擦除后，则在该目录下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开当前DF 再进入DF 时，将遵循文件的访问权限。

9.2.3 命令报文

表9.8 Erase MF 命令报文编码

代码	长度(byte)	值(Hex)	描述
CLA	1	80	-
INS	1	0E	-
P1	1	00	-
P2	1	00	-
Lc	-	00	-
DATA	-	-	不存在
Le		-	不存在

9.2.4 命令报文数据域

命令报文数据域不存在。

9.2.5 响应报文数据域

响应报文数据域不存在。

9.2.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表9.9 Erase MF 命令响应状态码

SW1	SW2	描述
90	00	命令成功执行
65	81	写EEPROM 不成功
69	82	擦除权限不满足

9.3 Write Key（增加或修改密钥）

9.3.1 定义与范围

Write Key 命令可向卡中装载密钥或更新卡中已存在的密钥。本命令可支持8 字节或16字节的密钥，密钥写入必须采用加密的方式，在主控密钥的控制下进行。请参见“内部基本文件”。

9.3.2 注意事项

- 在满足当前DF 下KEY 文件的增加权限时，可用Write Key 命令向KEY 文件中写入密钥。
- 当满足密钥的修改权限时，可以对密钥值进行修改（口令密钥除外）。

9.3.3 命令报文

9.3.3.1 **方式一(命令报文报文编码符合《中国银行PSAM 卡规范》)**

表9.10 Write Key 命令报文编码的方式一（密钥装载与更新）

代码	长度(byte)	值(Hex)	描述
CLA	1	84	-
INS	1	D4	-
P1	1	00	-
P2	1	00	符合《中国银行PSAM卡规范》
		XX	高4位是密钥的使用权限，详细设置请参看说明； 低4为是密钥的修改权限，详细设置请参看说明。
Lc	1	XX	数据长度
DATA	XX	XX....XX	加密后的密钥信息、MAC
Le	-	-	不存在

说明：
P2：高4 位是密钥的使用权限，低4 位是密钥的修改权限。
如：P2=34h，表示密钥的使用权限必须大于等于‘3’且小于等于‘F’， 密钥的修改权限必须大于等于‘4’且小于等于‘F’。

9.3.3.2 **方式二（Simlinker/PSAM 专有命令编码）**

表9.11 Write Key 命令报文编码的方式二（密钥装载）

代码	长度(byte)	值(Hex)	描述
CLA	1	84	-
INS	1	D4	-
P1	1	01	-
P2		XX	密钥标识
Lc	1	XX	-

DATA	XX	XX....XX	加密后的密钥信息、MAC
Le	-	-	不存在

表9.12 Write Key 命令报文编码的方式二（密钥更新）

代码	长度(byte)	值(Hex)	描述
CLA	1	84	-
INS	1	D4	-
P1	1	00	-
P2		00	-
Lc	1	XX	-
DATA	XX	XX....XX	加密后的密钥信息、MAC
Le	-	-	不存在

9.3.4 命令报文数据域

9.3.4.1 **方式一**

表9.13 Write Key 命令报文数据域的方式一（包括密钥装载与更新）

数据域	密钥用途	密钥版本	算法标识	密钥值
长度（byte）	1	1	1	8/16

说明：

【1】密钥用途：

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

——0，主控密钥

——1，维护密钥

——2，消费密钥

——3，PIN解锁密钥

——4，重装PIN密钥

——5，用户卡应用维护密钥

——6，MAC密钥

——7，加密密钥

——8，MAC、加密密钥

——9，解密密钥

——0A，安全计算方式0

——0B，安全计算方式1

——0C，逻辑加密卡专有密钥

——0D，逻辑加密卡认证密钥

注：主控密钥可以被当作外部认证密钥，其错误计数器默认为33、后续状态默认为0A。

【2】 密钥算法标识

密钥算法标识指定了密钥所支持加密算法，长度1字节。密钥算法标识约定如下：

——0，3DES

——1，DES

——2-255，保留

【3】密钥版本

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

注：一个目录下只能有一个主控密钥和一个维护密钥，且它们的密钥版本必须为‘00’。

9.3.4.2 **方式二**

表9.14 Write Key 命令报文数据域的方式二（密钥装载）

数据域 / 密钥类型	**Byte 1**	**Byte 2**	**Byte 3**	**Byte 4**	**Byte 5**	**密钥长度（byte）**
内部认证密钥	F0	使用权限	更改权限	密钥版本号	算法标识	8/16
外部认证密钥	F9	使用权限	更改权限	后续状态	错误计数器	16
口令重装密钥	F8	使用权限	更改权限	FF	错误计数器	8/16
口令密钥	FA	使用权限	EF	后续状态	错误计数器	2～6（如果口令长度不足6个字节，后补‘FF’）

注：表中密钥版本号、后续状态等见说明***[4]***。

说明：

[1] 若应用目录下某类型密钥只有一个，则其密钥标识是‘**00**’，否则，应从‘**01**’顺序开始。在一个应用下：

- 只能有一个口令密钥和一个重装口令密钥，它们的密钥标识必须是00。
- 一个或多个外部认证密钥标识必须从 ‘01’顺序开始。
- 密钥标识不能是‘FF’。

[2] 术语解释：

- 使用权限

  指该密钥在使用时如核对、认证、运算时所需满足的条件。

例如：使用权为41 表示在使用该密钥时当前目录安全状态寄存器值必须大于等于1且小于等于4。

♦ 更改权限

指用WRITE KEY 更改密钥内容的权限,在满足该条件时可使用Write Key 更改密钥内

容，但不能改变错误计数器的值。

♦ 错误计数器

高半字节指出密钥可以连续错误的最多次数， 低半字节指出还可以再试的次数。如果连续错误错超过规定的次数，密钥自动被锁死。

例如：错误计数器的值为33，表示该密钥最多可以连续错误3 次，若输错一次则其值变为32，再错一次之后变为31，若下次核对或认证正确则该值变为33。使用解锁口令时，解锁口令正确后错误次数低半字节被设置成高半字节值，同时口令被修改。

解锁口令若错误，解锁口令允许再试次数减一，解锁口令和外部认证密钥锁死后无法被解锁。

♦ 后续状态

当口令核对成功或外部认证成功后，置安全状态寄存器值为后续状态的低半字。

♦ 解锁KID(指定需解锁的口令标识)

当解锁口令核对成功后,想要解开的口令密钥的密钥标识,即要解锁哪个口令密钥。

♦ 密钥版本号和算法标识由用户自己定义。

表9.15 Write Key 命令报文数据域方式二（密钥更新）

数据域	Byte1	Byte2	Byte3	密钥值长（**Byte**）
内容	密钥类型	密钥标识	00	密钥值
长度（byte）	1	1	1	8/16

说明：密钥类型的高2 位必须置为0，低6 位与密钥装载时的设置相同。
密钥标识必须与密钥装载时的设置相同。

9.3.4.3 密钥装载与更新

1、当装载MF 下的主控密钥时，分以下两种情况：

1）由厂家在卡片MF 的KEY 文件中已预先装入一条主控密钥(即卡片传输密钥,见“卡片初始化设置”），其密钥带有线路保护属性。用户可以在发卡中先认证或替换此密钥，后继续对卡片进行发卡操作。

2）在用户擦除MF 后，MF 下的主控密钥必须以明文方式装入，命令报文如下所示：

命令	CLA	INS	P1	P2	Lc	DATA
长度	1	1	1	1	1	21
值（hex）	80	D4	01	00	15	F9F0AA0A33+16 字节密钥值

当修改MF 下的主控密钥时，用MF 下的主控密钥加密数据和计算MAC。

2、当装载应用目录（MF 除外）下的主控密钥时，用上一级应用目录下的主控密钥加密数据和计算MAC。
当修改应用目录（MF 除外）下的主控密钥时，用当前应用目录下的主控密钥加密数据和计算MAC。

3、当装载/更新应用目录（MF 或DF）下的密钥（主控密钥除外）时，用当前应用下的主控密钥加密数据和计算MAC。

MAC 计算方法见“.安全报文传送”。

9.4.5 响应报文数据域

响应报文数据域不存在

9.4.6 响应报文状态码

见“6.4 状态字SW1SW2 意义”。

9.4.7 应用举例

例如：某ADF 下的主控密钥为KAct1，在该应用下写入一应用维护密钥K（16 字节），则命令报
文如下（该命令的前一条命令为取4 字节的随机数Rnd4）：
84 D4 00 00 1C Encrypt（KAct1，01 00 00 + K）[24 Bytes] + MAC（Rnd4+00 00 00 00，KAct1，
84 D4 ...Encrypt（KAct1，13 01 00 00 + K）[24 Bytes]）[4 Bytes]
响应状态为 9000