Simlinker/PBOC
用户卡技术参考手册

北京芯凌科技有限公司

BeijingSimlinkerTech 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/PBOC 简介

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

♦ Simlinker/PBOC 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/PBOC 的文件管理系统。

♦ 卡片初始化设置

本章描述了Simlinker/PBOC 卡片初始化后的文件结构及使用方法。

♦ Simlinker/PBOC 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/PBOC 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/PBOC 发卡命令

♦ 附录一 Simlinker/PBOC 的复位应答

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。
[3]《中国金融集成电路（IC）卡规范》V1.0，1998年1月，中国金融出版社出版。

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）。

♦ 圈存 Load
持卡人将其在银行相应帐户上的资金划转到电子存折或电子钱包中。圈存交易必须在金融终端上联机进行。一般情况下，圈存到电子存折中的资金计付活期利息，圈存到电子钱包中的资金不及付利息。

♦ 圈提 Unload
持卡人将电子存折中的部分或全部资金划回到其他在银行的相应帐户上，圈提交易必须在金融中终端上联机进行。

♦ 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。

♦ 取现 Cash Withdraw
取现交易允许持卡人从电子存折中提取先进。此交易必须在金融终端上进行，但可以脱机处理。只有电子存折应用支付此交易，且必须提交个人密码（PIN）。

♦ 透支限额 Overdraw Limit

“透支功能”是一种基于电子存折应用的有限信用功能。当电子存折中的实际金额不足时，它为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。修改透支限额交易必须在金融终端上联机进行，且必须提交个人密码（PIN）。

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. Simlinker/PBOC 简介

2.1 关于 Simlinker/PBOC

Simlinker/PBOC是由北京芯凌科技有限公司开发的智能卡（SmartCard）操作系统，完全符合以下国际标准：

♦ 识别卡，带触点的集成电路卡标准 《ISO7816-1/2/3/4》、EMV2000.

Simlinker/PBOC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，钱包文件 。
♦ 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。
♦ 接触界面支持多种速率选择 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

Simlinker 卡片芯片由以下四部分硬件模块组成：（见图2-1）

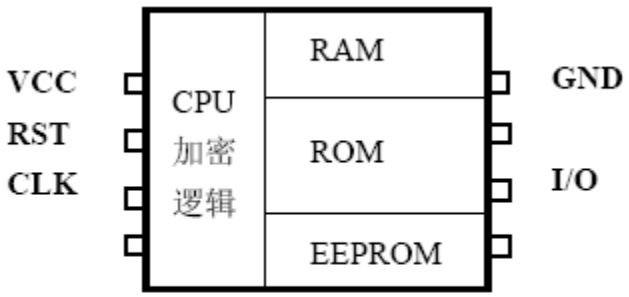


图 2-1 卡片内部逻辑结构

♦ 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
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。

2.2.3 Simlinker/PBOC 命令集

表2.1 Simlinker/PBOC 命令集

编号	命令	CLA	INS	功能描述	兼容性
1	Append Record	00/04	E2	增加记录	ISO&PBOC
2	Verify PIN	00/04	20	验证口令	ISO&PBOC
3	External Authentication	00	82	外部认证	ISO&PBOC
4	Get Challenge	00	84	取随机数	ISO&PBOC
5	Internal Authentication	00	88	内部认证	ISO&PBOC
6	Select File	00	A4	选择文件	ISO&PBOC
7	Read Binary	00/04	B0	读二进制文件	ISO&PBOC
8	Read Record	00/04	B2	读记录文件	ISO&PBOC
9	Get Response	00	C0	取响应数据	ISO&PBOC
10	Update Binary	00/04	D6	写二进制文件	ISO&PBOC
11	Update Record	00/04	DC	写记录文件	ISO&PBOC
12	Card Block	84	16	卡片锁定	PBOC
13	Application Unblock	84	18	应用解锁	PBOC
14	Application Block	84	1E	应用锁定	PBOC
15	PIN Unblock	80/84	24	个人密码解锁	PBOC
16	Initialize	80	50	初始化交易	PBOC
17	Credit For Load	80	52	圈存	PBOC
18	DebitForPurchase/CashWithdraw	80	54	消费/取现、圈提	PBOC
19	Update Overdraw Limit	80	58	修改透支限额	PBOC
20	Get Transaction Proof	80	5A	取交易认证	PBOC
21	Get Balance	80	5C	读余额	PBOC
22	Reload/Change PIN	80	5E	重装/修改个人密码	PBOC
23	UPDATE CAPP DATA CACHE	80	DC	更新复合消费数据	专有
24	DEBIT FOR CAPP PURCHASE	80	54	复合消费	专有
25	INITIALIZE FOR GREY LOCK	E0	7A	灰锁初始化	专有
26	GREY LOCK	E0	7C	灰锁	专有
27	INITIALIZE FOR GREY UNLOCK	E0	7A	联机解扣	专有
22	DEBIT FOR UNLOCK	E0	7E	脱机解扣	专有
23	GET LOCK PROOF	E0	CA	读取证明码	专有
23	Decrease	80/84	30	扣款	专有
24	Increase	80/84	32	存款	专有
25	Erase MF	80	0E	擦除 DF	专有
26	Write Key	80/84	D4	增加或修改密钥	专有
27	Creat File	80	E0	建立文件	专有

3. 文件管理

本章介绍Simlinker/PBOC 的文件系统，包括文件组织结构、文件格式、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/PBOC 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她的分支。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/PBOC 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/PBOC 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	7
校验和（由COS 计算）	1

注：表***3.1*** 中两个***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/PBOC 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。

♦ Simlinker/PBOC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
2F	钱包文件	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	变长线性文件

	问）	

3.2.3 文件标识和文件名称

Simlinker/PBOC 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/PBOC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/PBOC 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：

P	B7	B6	B5	B4	B3	B2	B1	B0
1	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：

P	B7	B6	B5	B4	B3	B2	B1	B0
2	短文件标识符					1	0	0

若P2的高五位不全为0，低三位为100，则高五位为短的文件标识符。

[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/PBOC 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/PBOC 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/PBOC 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2 级目录（MF-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：

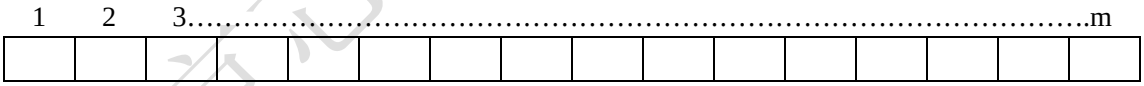
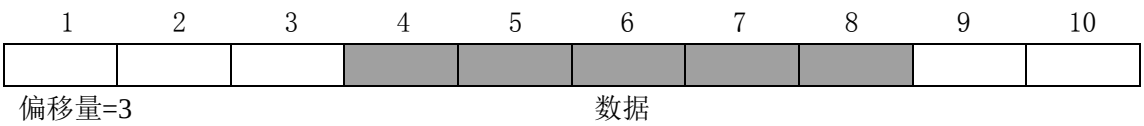


图3-3 透明结构

[例] 从一个10 字节的文件中读取偏移量为3 的5 个字节：



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
维护密钥标识	1	计算安全报文的密钥标识
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
维护密钥标识	1	计算安全报文的密钥标识
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
维护密钥标识	1	计算安全报文的密钥标识
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 普通钱包文件

3.5.4.1 定义

钱包文件的结构同循环文件，每条记录均为数值型，存款/扣款时用第一条记录（此记录号为1）的数值加上/减去交易金额，然后将新写的记录作为第一条记录。

3.5.4.2 文件体结构——循环文件

记录个数必须大于或等于2，记录长度必须小于8字节。

钱包文件中的金额是以二进制形式进行运算的，新建立的钱包文件余额为00。

存款/扣款时用第一条记录（此记录号为1）的数值加上/减去交易金额，然后将新写的记录作为第一条记录。

3.5.4.3 文件头定义

表 3.8 普通钱包文件头定义

文件头	字节（**Byte**）	描述
文件类型	1	‘2F’，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标识记录总个数（2-254） 字节2标识记录长度（<8 ）
访问权限1	1	扣款权限/读权限
访问权限2	1	存款权限
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘FF’

♦读权限

指使用 Read Record 命令读出指定记录的权限。

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。

3.5.5 电子存折/电子钱包文件

3.5.5.1 定义

- ♦ 电子存折（ED）

一种为持卡人进行消费、取现等交易而涉及的使用个人密码（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（EP）

一种为方便持卡人小额消费而涉及的金融IC卡应用。它支持圈存、消费以及查询余额交易。除圈存交易外，使用电子钱包进行的任何交易均不记录交易明细，且无需验证口令（PIN）。

3.5.5.2 文件体结构——循环文件

请参看3.4.5.2文件体结构——循环文件。

每条记录的数据项如下表所示：

表3.9 电子存折/电子钱包的文件结构

数据元	长度
余额	4
PBOC ED/EP脱机交易序号	2
PBOC ED/EP联机交易序号	2

注： 对于EP，余额有效长度是3个字节。

3.5.5.3 文件头定义

表 3.10 电子存折/电子钱包文件头定义

文件头	字节（**Byte**）	描述
文件类型	1	‘2F’，
文件标识(FID)	2	0001是电子存折，0002是电子钱包
文件大小	2	字节1表示目录总个数（必须等于2） 字节2表示目录长度（必须等于8 ）
访问权限	1	使用权限
TAC密钥标识符	1	在交易中需要使用的TAC密钥标识符
交易明细短文件标识符	1	用于保留交易明细的循环文件的短文件标识符
RFU	1	‘FF’

- 使用权限
  使用该金融专用钱包进行圈存、圈提等操作时满足的条件。
- 交易验证（TAC）密钥标识
  交易中用于生成交易验证码TAC的密钥标识符。
- 交易明细文件标识
  用于保存交易明细的循环文件的短文件标识符。有关交易明细文件内容见“附录 1” Simlinker/PBOC金融IC卡应用举例。

3.5.5.4 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。

。

3.5.6 变长记录文件

3.5.6.1 **定义**

变长记录文件为具有可变长度记录的文件。

3.5.6.2 **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/PBOC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/PBOC 中，变长记录文件采用变长记录格式。

图3-11 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
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘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。

3.5.6.3 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/PBOC 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3.12 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“7.3 Write Key 命令”。

注： 在 DF 下的 KEY 文件中增加一条链接 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。

见

3.6.1.3 **密钥头——密钥类型**

表3.13 密钥类型

密钥名称	类型字节（HEX）	密钥名称	类型字节(HEX)
DES加密密钥	30	外部认证密钥	39
DES解密密钥	31	修改透支限额密钥	3C
DESMAC密钥	32	圈提密钥	3D
内部密钥	34	消费密钥	3E
维护密钥	36	圈存密钥	3F
主控密钥	密钥标识为00的39密钥	口令（PIN）	3A
口令解锁密钥	37	解锁口令	3B
口令重装密钥	38		

3.6.1.4 **文件头定义**

表3.14 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	1	‘FF’

说明：

♦ DF 短文件标识符

表3.15 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 DES加密密钥

DES加密密钥是用于进行DES加密运算的密钥。
DES加密密钥所涉及的命令如下：
- 内部认证命令（Internal Authenticatte）

3.6.2.2 DES解密密钥

DES解密密钥是用于进行DES解密预算的密钥。
DES解密密钥所涉及的命令如下：
- 内部认证命令（Internal Authenticate）

3.6.2.3 DES&MAC密钥

DES&MAC密钥是用于进行MAC运算的密钥。

DES&MAC密钥所涉及的命令如下：

- ♦ 内部认证命令（Internal Authenticate）

3.6.2.4 内部密钥

内部密钥用于产生消费、取现和圈存交易中使用的交易验证码TAC。
内部密钥所涉及的命令如下：

- ♦ 圈存命令（Credit For Load）
- ♦ 消费/取现命令（Debit For Purchase/Cash Withdraw）
- ♦ 修改透支限额命令（Update Overdraw Limit）

3.6.2.5 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）

3.6.2.6 主控密钥

在以安全报文方式装载或更新密钥时，主控密钥是用于产生安全报文的密钥。
主控密钥所涉及的命令如下：

- ♦ 外部认证命令（External Authenticate）
- ♦ 增加或修改密钥命令（Write Key）

3.6.2.7 口令解锁密钥

在以安全报文方式访问口令时，口令解锁密钥是用于产生安全报文的密钥。
口令密钥解锁命令（PIN Unblock），适用于长度为2到6字节的口令密钥。
口令认证命令（VerifyPIN）
验证并修改口令（Verify&Change PIN）适用于长度为8字节的口令密钥。

3.6.2.8 口令重装密钥

口令重装密钥用来产生重装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），适用于标识为00、长度为2到6字节的口令密钥。

3.6.2.9 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。

3.6.2.10 修改透支限额密钥

修改透支限额密钥用来产生修改透支限额交易中使用的过程密钥SK,在修改透支限额交易中计算MAC和TAC。
修改透支限额密钥所涉及的命令如下：

- ♦ 修改透支限额初始化命令（Initialize For Update）
- ♦ 修改透支限额命令（Update Overdraw Limit）

3.6.2.11 圈提密钥

圈提密钥用来产生圈提交易中使用的过程密钥SK，在圈提交易中计算MAC。
圈提密钥所涉及的命令如下：

- ♦ 圈提初始化命令（Initialize For Unload）
- ♦ 圈提命令（Debit For Unload）

3.6.2.12 消费密钥

消费密钥用来产生消费/取现交易中使用的过程密钥SK，在消费/取现交易中计算MAC和TAC。
消费密钥所涉及的命令如下：

- ♦ 消费/取现初始化（Initialize For Purchase/Cash Withdraw）
- ♦ 消费/取现命令（Debit For Purchase/Cash Withdraw）

3.6.2.13 圈存密钥

圈存密钥用来产生圈存交易中使用的过程密钥SK，在圈存交易中计算MAC和TAC。
圈存密钥所涉及的命令如下：

- ♦ 圈存初始化命令（Initialize For Load）
- ♦ 圈存命令（Credit For Load）

3.6.2.14 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，错误次数计数器复位（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。
- ♦ 重装/修改口令密钥（Reload/Change PIN），适用于标识为00、长度为2到6字节的口令密钥。
- ♦ 口令密钥解锁（PIN Unblock），适用于长度为2到6字节的口令密钥。

全局PIN

如果某口令密钥被装载在MF下，且此口令密钥可以在指定的DF下使用，则该密钥为全局PIN。

在DF下，当满足全局PIN的使用权限时，可以核对该全局PIN，以改变当前安全状态寄存器的值；也可以使用其他相关命令对全局PIN进行操作，如验证并修改口令（Verify & Change PIN）等。

全局PIN的实现方法见“3.6.3 全局密钥”。

3.6.2.15 解锁口令密钥

解锁口令密钥用于解锁被锁定的8字节口令密钥。

解锁密钥锁定后无法被解锁。

解锁口令密钥所涉及的命令如下

- ♦ 解锁口令（Unblock）

3.6.3 全局密钥

如果某密钥被装载在MF下，且此密钥可以在指定的DF下使用，则该密钥为全局密钥。

实现方法

在DF下的KEY文件中增加一条连接MF下某一密钥的KEY记录，即Write Key命令中仅指明与MF下密钥相同的密钥标识和密钥类型，其真正的密钥属性和内容为MF下相对应的密钥类型和标识的密钥属性和内容。

应用方法

在DF下，当满足全局密钥的使用权限时，可以进行相应的操作；当满足全局密钥的修改权限时，可以使用Write Key命令更改密钥（口令密钥除外）。

3.6.4 主密钥与密钥分散

为了使应用系统在使用对称加密算法时获得最大的安全性，可以使每张卡片密钥在系统中具有唯一性，即卡片密钥=主控密钥对特定数据进行分散的结果。

对于 Single DES 主密钥，分散方法见图 3-9.

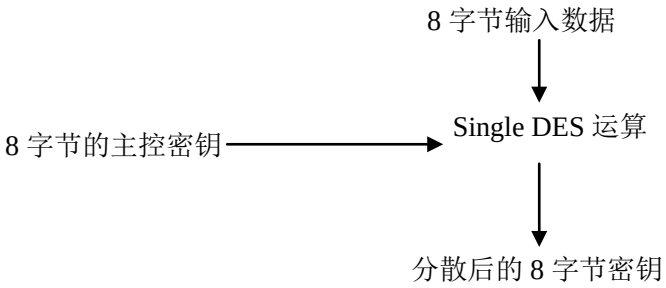


图 3.9 Single DES 密钥分散

对于 Triple DES 主密钥，分散方法见图 3-10.

左边的 8 字节输入数据=特定数据；

右边的 8 字节输入数据=特定数据按位求反。

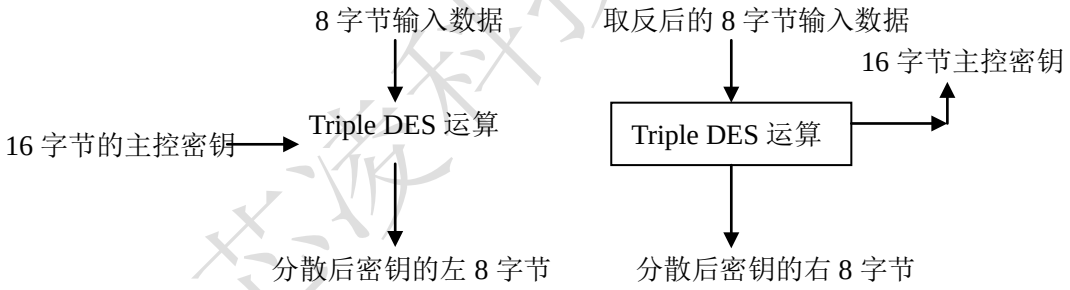


图 3-10 Triple DES 密钥分散

3.6.5 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 3-11 描述了产生过程密钥的机制，其中输入数据是 8 字节。

8 字节过程密钥 8 字节过程密钥
SK（Session Key） SK（Session Key）

图 3-11 过程密钥的产生

3.6.6 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	DES 加密 30	DES 解密 31	DES & MAC 32	内部密钥 34	维护密钥 36	主控密钥（标识为 00 的 39 密钥）	口令解锁 37	口令重装 38	外部认证 39	口令 3A	解锁口令 3B	修改透支限额 3C	圈提 3D	消费 3E	圈存 3F
Append Record					Y										
Application Block					Y										
Application Unblock					Y										
Card Block					Y										
Decrease					Y										
Increase					Y										
Credit For Load				Y											Y
Debit For Purchase/Cash Withdraw				Y										Y	
Debit For Unload													Y		
External Authentication						Y			Y						
Initialize For Puschase/cash Withdraw														Y	
Initialize For Load															Y
Initialize For Unload													Y		
Initialize For Update												Y			
Internal Authentication	Y	Y	Y												
PIN Unblock							Y								
Read Binary					Y										

Read Record					Y										
Reload/Change PIN								Y							
Unblock											Y				
Update Binary					Y										
Update OverdrawLimit				Y								Y			
Update Record					Y										
Verify & Change PIN										Y					
Verify PIN							Y			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/PBOC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/PBOC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	钱包 2F	变长记录 2C	KEY 文件 3F
Append Record					Y		Y	
Create	Y	Y	Y	Y	Y	Y	Y	Y
Credit For Load						Y		
Debit For Purchase/ Cash Withdraw						Y		
Debit For Unload						Y		
Erase DF	Y	Y						
Get Balance						Y		
Get Transaction Proff						Y		
Initialize For Cash Withdraw						Y		
Initialize For Load						Y		
Initialize For Purchase						Y		
Initialize For Unload						Y		
Initialize For Update						Y		
Read Binary			Y					
Read Record				Y	Y	Y	Y	
Select File	Y	Y	Y	Y	Y	Y	Y	
Update Binary			Y					
Update Overdraw Limit						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 Simlinker/PBOC 文件结构举例

Simlinker/PBOC 文件结构如下图所示：

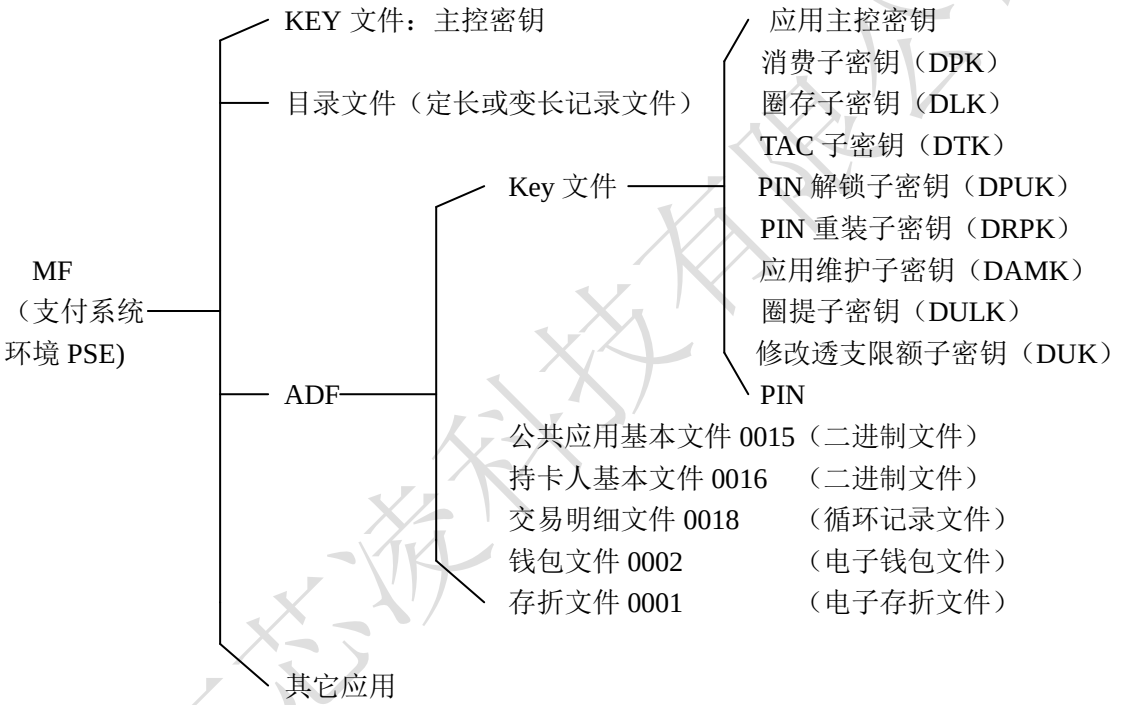


图 3-12 Simlinker/PBOC 文件结构举例（简要）

有关 PBOC 应用的详细内容（如命令代码、权限设置和文件信息等）见“附录 2 Simlinker/PBOC 金融 IC 卡应用举例”。

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，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。

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】建立文件时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。

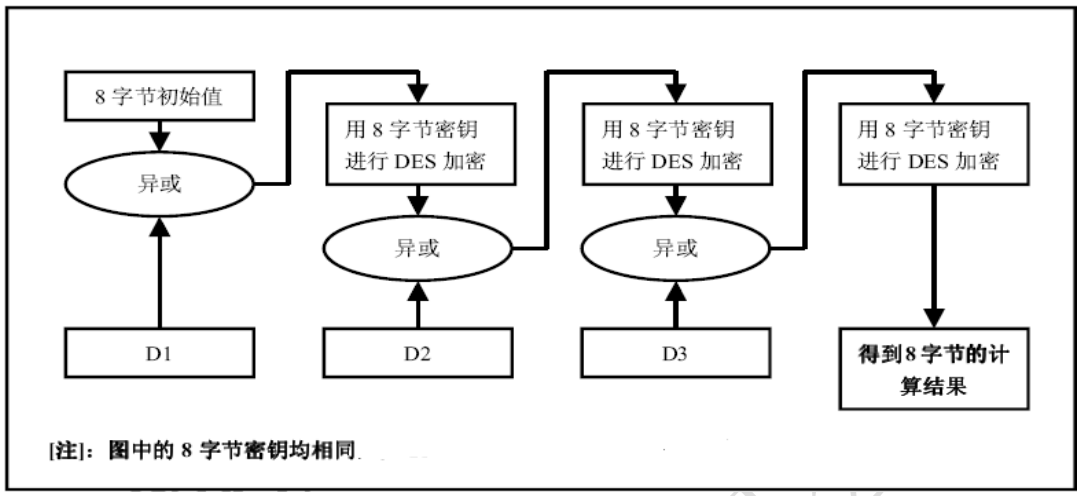


图 3.17 用Single DES密钥产生MAC的算法

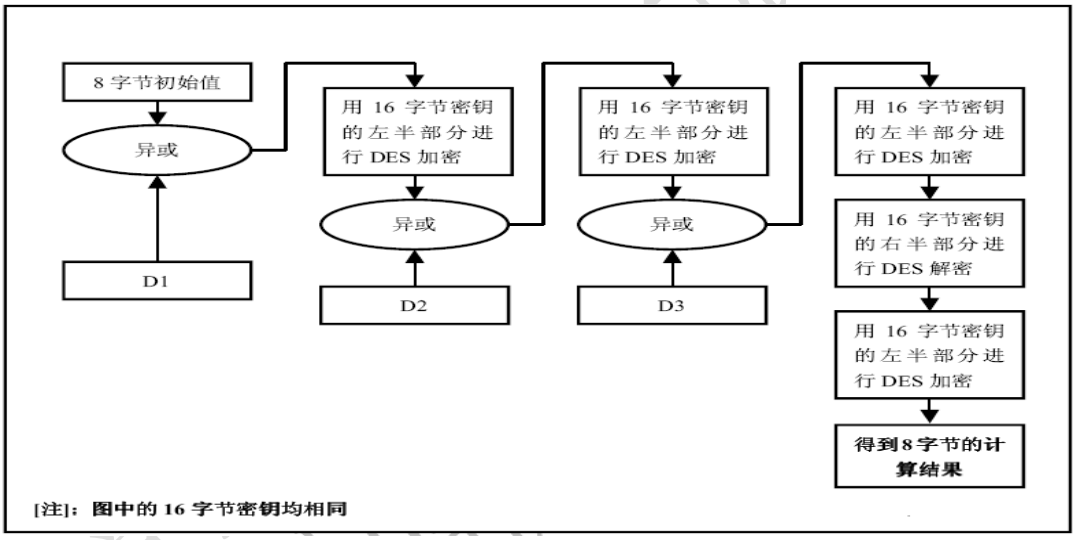


图 3.18 用Triple DES密钥产生MAC的算法

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顺序连接在一起（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

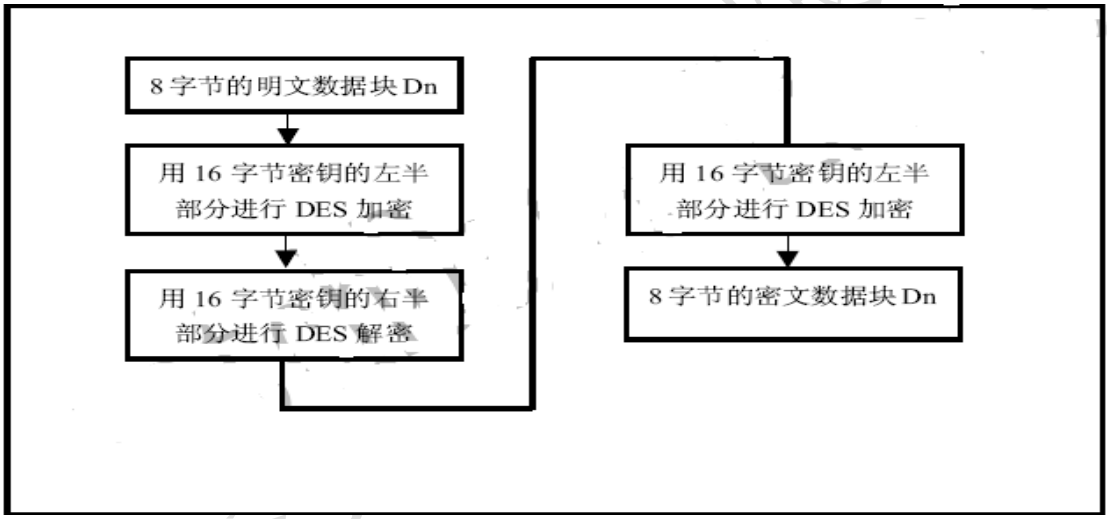


图 3.20 用Triple DES密钥进行数据加密的算法

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。

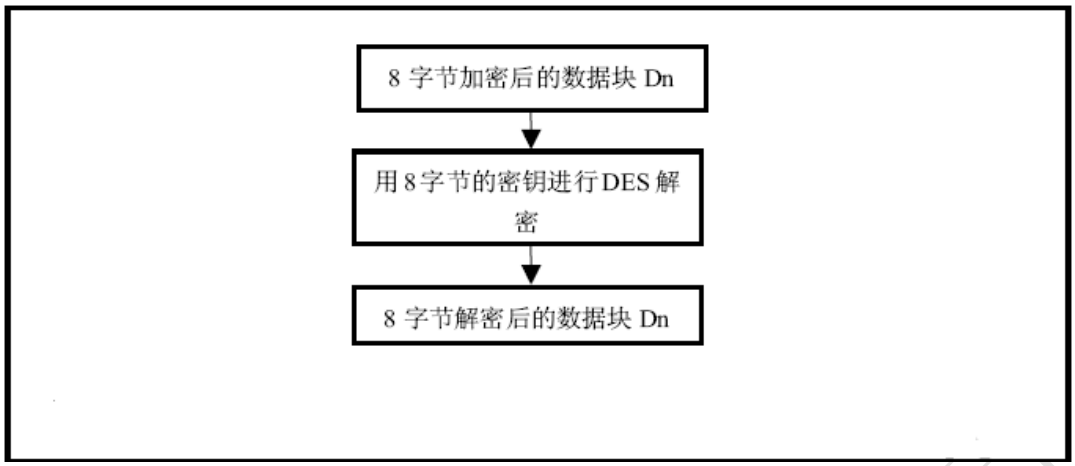


图 3.21 用Single DES密钥进行数据解密的算法

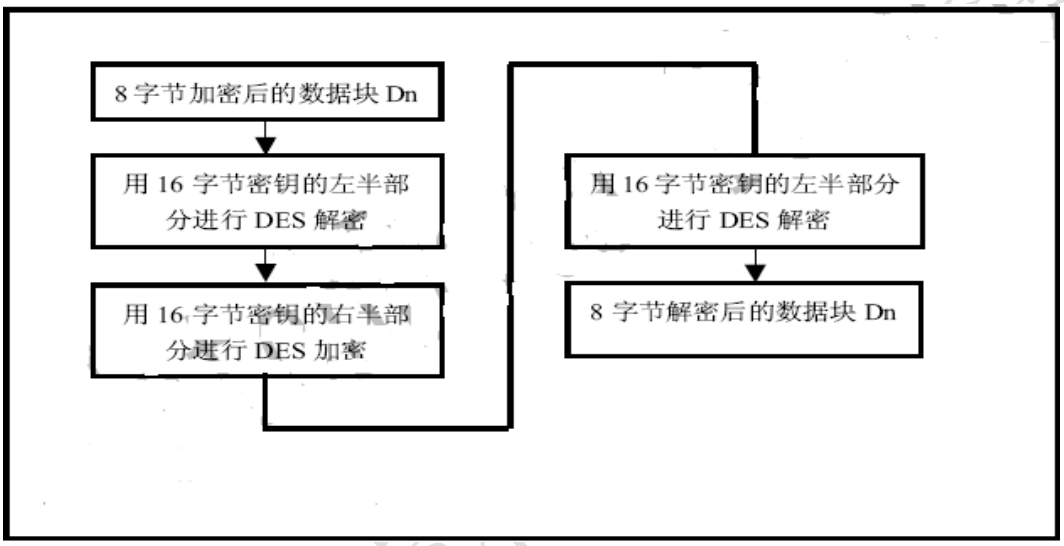


图 3.22 用Triple DES密钥进行数据解密的计算

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。

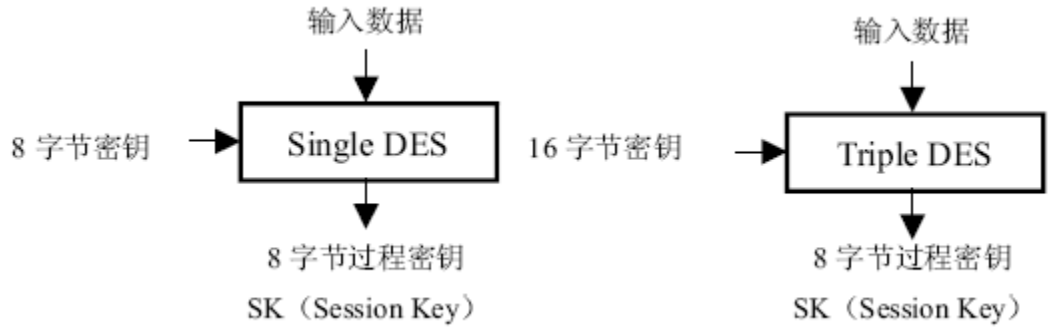


图 3.23 过程密钥的产生

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/PBOC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

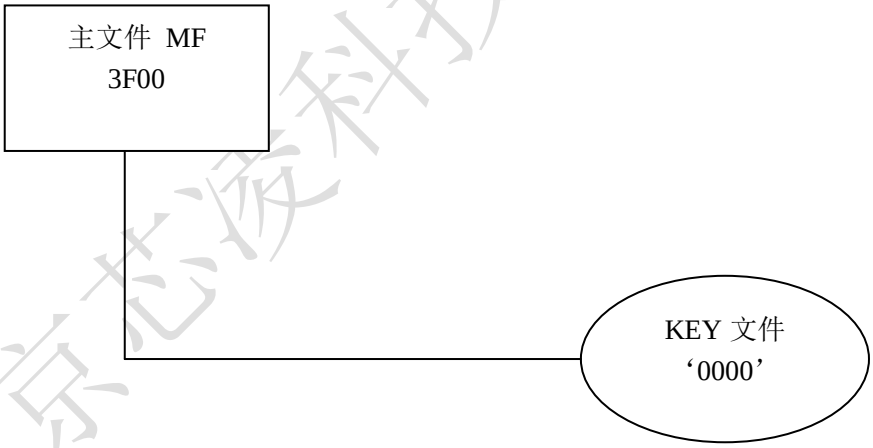


图4-1 卡片初始化文件结构

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
  - 默认密钥值：00112233445566778899AABBCCDDEEFF

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“7.3 Write Key 之方式一”）

有关外部认证的方法见外部认证（External Authentication）

5. Simlinker/PBOC 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/PBOC的MF和DF分别具有16

种不同的安全状态。

Simlinker/PBOC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
电子存折/电子钱包文件	使用
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5-2 访问权限控制

5.4 密码算法

Simlinker/PBOC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：

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

在建立DES密钥时，若密钥长度为8字节，则运算时使用Single DES算法，若密钥长度为16字节则运算是使用Triple DES算法。

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

Simlinker/PBOC在使用DES算法时使用ECB模式，若数据长度不是8的倍数时在计算过程中自动在数据后补80 00....00使其长度为8的倍数。

[例] 如果数据为12 23 34 56 78 89 90 A1 B1，由于数据长度不是8的倍数，所以在计算过程中自动将数据改写为12 23 34 56 78 89 90 A1 B1 80 00 00 00 00 00 00后再进行计算。

6. Simlinker 基本命令

6.1 Append Record（增加记录）

6.1.1 定义与范围

Append Record 命令用于对变长记录文件、循环文件追加记录。

6.1.2 注意事项

Append Record 命令适用于变长记录文件和循环文件。

- 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）
  增加记录（Apend Record）
- 只有满足记录文件读权限时才能执行此命令。
- 若循环文件记录已满则覆盖最早写入的记录，且新增加记录的记录号总为 1.

6.1.3 命令报文

表 6.1 Append Record 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	E2	-
P1	1	00	-
P2	1	XX	见说明
Lc	1	XX	-
DATA	XX	XX…XX	写入的数据
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	0	0	0	4-b8为短文件标识符
0	0	0	0	0	0	0	0	当前文件

Lc 标识要写入的字节数。

1．若为线路保护，Lc 为写入数据的长度+4 字节 MAC。

2．若为加密线路保护，Lc 为加密后数据的长度+4 字节 MAC。

6.1.4 命令报文数据域

命令报文数据域由追加记录组成。
若为线路保护则由追加记录附上 4 字节 MAC 码组成。
若为线路加密保护则由被加密过的记录数据附上 4 字节 MAC 码组成。
用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

6.1.5 响应报文数据域

响应报文数据域不存在。

6.1.6 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 6.2 Append Record 命令响应状态码

SW1	SW1	意义
90	00	正确执行
65	81	写 EEPROM 失败
67	00	长度错误（Lc 域为空）
69	81	当前文件不是循环文件或变长记录文件
69	82	不满足安全状态
6A	81	不支持此功能（无 MF 或 MF 已锁定）
6A	82	未找到文件
6A	83	未找到记录
6A	84	文件中存储空间不够（对变长记录文件）

6.1.7 应用举例

【1】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：往变长记录文件中增加 1 条记录标识为 AA 的记录，不进行线路保护。
命令：00 E2 00 08 0E AA 0C 11 22 33 44 55 66 77 88 99 AA BB CC
响应：9000
【2】 条件： 文件类型：循环文件；
文件标识符=0001
记录数=02；
记录长度=06；

建立时不采用线路保护；

设该文件为当前文件。

操作：往循环文件中追加 1 条记录，不进行线路保护。

命令：00 E2 00 00 06 11 22 33 44 55 66

响应：9000

6.2 External Authentication（外部认证）

6.2.1 定义与范围

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

6.2.2 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。

6.2.3 命令报文

表 6.3 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。

6.2.4 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。

6.2.5 响应报文数据域

响应报文数据不存在

6.2.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.4External 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

6.2.7 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；
后续张太=01；
16 字节密钥=00112233445566778899AABBCCDDEEFF
操作：外部认证
【步骤 1】取 8 字节随机数。
命令：00 84 00 00 08
响应：D3 89 BF 67 45 B9 35 50 9000
【步骤 2】卡终端用与外部认证密钥相同的密钥‘00112233445566778899AABBCCDDEEFF’对随机数进行加密，加密后的结果为 10B3315B20B50120
【步骤 3】卡终端将加密后的随机数送到卡中做外部认证。
命令：00 82 00 00 08 C1 8A 5B 4B 13 40 25 21
说明：其中 10 B3 31 5B 20 B5 01 20 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后续状态 01.

6.3 Get Response（取响应数据）

6.3.1 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。

6.3.2 注意事项

此命令只用于 T=0 通讯协议。

6.3.3 命令报文

表 6.5Get 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

6.3.4 命令报文数据域

命令报文数据域不存在。

6.3.5 响应报文数据域

响应报文数据域的长度由 Le 的值决定。

6.3.6 响应报文状态码

表 6.6 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

6.4 Get Challenge（取随机数）

6.4.1 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。

6.4.2 命令报文

表 6.17 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	04/08	要求卡片返回的随机数长度

6.4.3 命令报文数据域

命令报文数据不存在。

6.4.4 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。

6.4.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.8 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）

6.5 Internal Authentication（内部认证）

6.5.1 定义范围

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。

6.5.2 注意事项

在满足该密钥的使用条件时才能执行此命令

6.5.3 命令报文

表 6.9 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

6.5.4 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。

6.5.5 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。

6.5.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.10 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 文件中没有响应类型的密钥，卡片将返回‘9403’，即密钥未找到。

6.5.7 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 6-2 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。

6.5.8 应用举例

【1】条件：密钥标识号=01；
密钥类型是 DES 加密密钥；
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=00112233445566778899aabbccddeeff；
待加密数据 1122334455667788；
操作：内部认证即 DES 加密。
命令：00 88 00 01 08 1122223344556677
响应：6108
说明：对于 T=0 的卡片，6108 标识卡片要回送的数据长度，可以通过读响命令取返回数据。
命令：00 C0 00 00 08
响应：496BD7A351364453 9000

【2】条件：密钥标识号=01；
密钥类型是 DES 解密密钥；
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=00112233445566778899aabbccddeeff；
待加密数据 496BD7A351364453
操作：内部认证即 DES 解密。
命令：00 88 01 01 08 07 CB F6 15 E7 D7 2F 96
响应：6108
说明：对于 T=0 的卡片，6108 标识卡片要回送的数据长度，可以通过读响命令取返回数据。
命令：00 C0 00 00 08
响应：1122334455667788 9000

【3】条件： 密钥标识号=01；
密钥类型是 DES&MAC 解密密钥；
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=00112233445566778899aabbccddeeff；
待计算 MAC 数据 1122334455667788
操作：内部认证即计算 MAC。
命令：00 88 02 01 08 11 22 33 44 55 66 77 88

响应：6104

说明：对于 T=0 的卡片，6108 标识卡片要回送的数据长度，可以通过读响命令取返回数据。

命令：00 C0 00 00 04

响应：730B19B7 9000

说明：计算 MAC 的 8 字节初始值问 0000000000000000

6.6 Read Binary（读二进制文件）

6.6.1 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）。

6.6.2 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。

6.6.3 命令报文

表 6.11 Read Binary 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	B0	-
P1	1	XX	见说明
P2	1	XX	见说明
Lc	1	-	不存在（CLA=04 时除外）
DATA	XX	-	不存在（CLA=04 时，应包括 MAC）
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							

6.6.4 命令报文数据域

一般情况下，命令报文数据域不存在。
当使用安全报文时，命令报文数据域中应包含 MAC。
用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

6.6.5 响应报文数据域

响应报文数据域由读取的数据组成。
若为线路保护则由读取的数据附上 4 字节 MAC 组成。
若为线路加密保护则由被加密过的数据附上 4 字节 MAC 码组成。
注：文件被置成线路保护/线路加密保护时也允许明文读取，设置方法见“Create File”

6.6.6 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 6.12 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.

对于 T=0 的卡片，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。

6.6.7 应用举例

【1】 条件：文件类型;二进制文件；
文件表示符=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，步进行线路保护。
命令：00 B0 85 00 00
响应：6C08
说明：对于 T=0 的卡片，6C08 标识要求终端向 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：1122334455667788 9000

6.7 Read Record（读记录文件）

6.7.1 定义与范围

Read Record 命令用于读取记录文件的内容。

6.7.2 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)
- ♦ 只有满足二进制文件读权限时才能执行此命令。

6.7.3 命令报文

表 6.13 Read Record 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	B2	-
P1	1	XX	记录的个数
P2	1	XX	引用控制参数，见说明
Lc	1	-	不存在（CLA=04 时除外）
DATA	XX	-	不存在（CLA=04 时除外）
Le	1	XX	‘00’

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

6.7.4 命令报文数据域

当无安全报文使用时，命令报文数据域不存在。使用安全报文时，命令报文的数据域中应包含 MAC。MAC 的计算方法和长度由应用决定。

6.7.5 响应报文数据域

响应报文数据域由读取的数据组成。

6.7.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.14 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：

若 CLA=04，Le 被忽略，并返回整条记录内容。

若 CLA=00，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。

6.8 Select File（选择文件）

6.8.1 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。

6.8.2 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。

6.8.3 命令报文

表 6.15 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	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。

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。

6.8.4 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。

6.8.5 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 6.16 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

6.8.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.17 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

6.9 Unblock（解锁口令）

6.9.1 定义与范围

Unblock 命令用于解锁被锁定的 8 字节的口令。

6.9.2 注意事项

只有满足该解锁口令使用条件且该解锁口令未被锁死时才能执行此命令，该命令不改变安全状态寄存器的值。

6.9.3 命令报文

表 6.18 Unblock 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	2C	-
P1	1	00	-
P2	1	XX	解锁口令密钥标识
Lc	1	10	-
DATA	XX	XX…XX	8 字节解锁口令+8 字节新口令
Le	-	-	不存在

说明：

若解锁口令核对成功，则新口令值取代解锁口令指定的口令密钥的原有口令，且将口令错误计数器和解锁口令错误计数器恢复成原始值。

若解锁口令失败，则解锁口令可再试次数减 1，如果解锁口令锁死，解锁口令无法再被解锁。

6.9.4 命令报文数据域

报文数据域有 8 字节解锁口令，8 字节新口令组成。

6.9.5 响应报文数据域

响应报文数据域不存在

6.9.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.19Unblock 命令响应状态码

SW1	SW1	意义
90	00	正确执行
69	82	密钥的使用条件不满足
69	83	解锁口令密钥被锁死
6A	83	密钥未找到
6A	86	参数 P1 P2 不正确

6.9.7 应用举例

【1】条件：密钥标识号为 06 的口令解锁密钥；
使用权=0xF0；
错误计数器=0x33；
被锁死的口令密钥号=05；
8 字节的解锁口令=1122334455667788；
建立时不采用线路保护。

操作：密钥标识号为 05 的口令密钥被锁死，对它进行解锁，步进行线路保护。

命令：00 20 0006 10 11 22 33 44 55 66 77 88 01 02 03 04 05 06 07 08

6.10. Update Binary（写二进制文件）

6.10.1 定义与范围

Update Binary 命令用于写二进制文件。

6.10.2 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。

6.10.3 命令报文

表 6.20 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	10	-
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。

6.10.4 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“安全报文传送”。

6.10.5 响应报文数据域

响应报文数据域不存在。

6.10.6 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 6.21 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）

6.11 Update Record（写记录文件）

6.11.1 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。

6.11.2 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）

增加记录（Append Record）

♦ 只有满足记录文件写权限时才能执行此命令。

♦ 对于变长记录文件，更新记录时，新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。

6.11.3 命令报文

表 6.22 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：1.XXXXX 代表短文件标识符（SFI）；- - - - - 代表全 0 或短文件标识符
2.对于定长记录文件，P2 只能使用记录号在 P1 中给出，并且 P1 不能为 0

6.11.4　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。

6.11.5　响应报文数据域

响应报文数据域不存在。

6.11.6　响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.23 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

6.12 Verify PIN（验证口令）

6.12.1 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。

6.12.2 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。

6.12.3 命令报文

表 6.24 Verify PIN 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	00/04	-
INS	1	20	-
P1	1	00	-
P2	1	XX	口令密钥标识
Lc	1	02-08	-
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。

当口令长度为 8 字节时，可用 Unblock 命令对其进行解锁，使原来口令密钥文件恢复正常，同时口令错误计数器被恢复成初始值。

当口令长度为 01-08 字节时，可以用中国金融 IC 卡专用命令对其进行口令解锁，重装口令等操作。

6.12.4 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。

若为线路保护则由口令密钥附上 4 字节 MAC 码组成。

若为线路加密保护则由被机密过的口令密钥附上 4 字节 MAC 码组成。

用口令解锁密钥加密口令密钥和计算 MAC，方法见“安全报文传送”。

6.12.5 响应报文数据域

响应报文数据域不存在。

6.12.6 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 6.25 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

6.13 Verify & Change PIN（验证并修改口令）

6.13.1 定义与范围

Cerify & Change PIN 命令用于核对并修改 8 字节口令。

6.13.2 注意事项

在满足口令使用权限时，可以使用 Verify & Change PIN 命令由于核对并修改 8 字节口令。

6.13.3 命令报文

表 6.26 Verify & Change PIN 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	24	-
P1	1	00	-
P2	1	XX	口令密钥标识
Lc	1	10	-
DATA	XX	XX….XX	8 字节旧口令+8 字节新口令
Le	-	-	不存在

说明：

若核对成功，则安全状态寄存器被置为该口令密钥的后续状态，并用新口令取代旧口令，错误计数器被恢复；

若核对不成功，则可再试次数减 1，并且不修改口令值。

6.13.4 命令报文 数据域

命令报文数据域由 8 字节旧口令和 8 字节新口令组成。

6.13.5 响应报文数据域

响应报文数据域不存在。

6.13.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 6.27 Verify & Change 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
6A	82	KEY 文件未找到
6A	86	参数 P1 P2 不正确
93	02	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

6.14 Decrease（扣款）

6.14.1 定义与范围

Decrease 命令用于从记录长度小于 4 字节的钱包中扣款。

6.14.2 注意事项

Decrease 命令只适用于普通钱包。
访问普通钱包的命令如下：
建立文件（Create File）
选择文件（Select File）
存款/扣款（Increase/Decrease）
读记录文件（Read Record）
只有满足普通钱包文件扣款权限时才能执行此命令。

6.14.3 命令报文

表 6.28 Decrease 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80/84	-
INS	1	30	-
P1	1	00	-
P2	1	XX	见说明
Lc	1	XX	钱包文件的记录长度
DATA	XX	XX….XX	减少的金额
Le	-	-	-

说明：参数 P2 的设置如下所示：

b7	b6	b5	b4	b3	b2	b1	b0	含义
X	X	X	X	X	1	0	0	b3-b7 为短文件标识符
0	0	0	0	0	1	0	0	当前文件

6.14.4 命令报文数据域

命令报文数据域由减少的金额组成。
若为线路保护则由减少的金额附上 4 字节 MAC 组成。
若为线路加密保护则由被加密过的金额附上 4 字节 MAC 组成。
用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

6.14.5 响应报文数据域

响应报文数据域由 Lc 字节钱包中新的余额和 Lc 字节本次扣款金额组成。
若为线路保护则由新余额、扣款金额附上 4 字节 MAC 组成。
若为线路加密保护则由被加密过的新余额和扣款金额附上 4 字节 MAC 组成。

6.14.6 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 6.29Decrease 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。
65	81	写 EEPROM 不成功
67	00	Lc 与钱包文件长度不一致
69	81	不是钱包文件
69	85	扣款或存款条件不满足
69	87	无安全报文
6A	82	文件未找到
93	02	线路保护数据错误
94	01	金额不足

6.15 Increase（存款）

6.15.1 定义与范围

Increase 命令用于向记录长度小于 4 字节的钱包存款。

6.15.2 注意事项

Increase 命令只适用于普通钱包。
访问普通钱包的命令如下：
建立文件（Create File）
选择文件（Select File）
存款/扣款（Increase/Decrease）
读记录文件（Read Record）
只有满足普通钱包文件存款权限时才能执行此命令。

6.15.3 命令报文

表 6.30 Increase 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80/84	-
INS	1	32	-
P1	1	00	-
P2	1	XX	见说明
Lc	1	XX	钱包文件的记录长度
DATA	XX	XX….XX	增加的金额
Le	-	-	-

说明：参数 P2 的设置如下所示：

b7	b6	b5	b4	b3	b2	b1	b0	含义
X	X	X	X	X	1	0	0	b3-b7 为短文件标识符
0	0	0	0	0	1	0	0	当前文件

6.15.4 命令报文数据域

命令报文数据域由增加的金额组成。
若为线路保护则由增加的金额附上 4 字节 MAC 组成。
若为线路加密保护则由被加密过的金额附上 4 字节 MAC 组成。
用维护密钥加密数据和计算 MAC，方法见“安全报文传送”。

6.15.5 响应报文数据域

响应报文数据域由 Lc 字节钱包中新的余额和 Lc 字节本次存款金额组成。
若为线路保护则由新余额、存款金额附上 4 字节 MAC 组成。
若为线路加密保护则由被加密过的新余额和存款金额附上 4 字节 MAC 组成。

6.14.6 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 6.31Decrease 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。
62	83	文件校验错误
67	00	Lc 与钱包文件长度不一致
69	81	不是钱包文件
69	85	扣款或存款条件不满足
6A	82	文件未找到
93	02	线路保护数据错误
94	01	金额不足

6.15 Encrypt/Decrypt（分散动态密钥）

6.15.1 定义与范围

使用 35 密钥分散产生 RAM 中的动态工作密钥 30、32.

6.15.2 注意事项

只有 35 密钥才能在 RAM 中产生动态工作密钥。

6.15.3 命令报文

表 6.32 Encrypt/Decrypt 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	1A	-
P1	1	00	-
P2	1	XX	主工作密钥标识
Lc	1	08	-
DATA	XX	XX….XX	主密钥分散因子
Le	-	-	不存在

6.15.4 命令报文数据域

数据域	工作密钥的密文值
长度（byte）	08
值（hex）	XX….XX

6.15.5 响应报文数据域

无响应报文数据域

6.15.6 响应报文状态码

SW1	SW2	意义
90	00	命令执行成功
6A	86	参数错误
94	03	密钥未找到

6.16 Ecrypt/Decrypt (用动态工作密钥加密)

6.16.1 定义与范围

用 RAM 中的动态工作密钥对数据进行 DES 加密和 MAC 运算，并返回运算结果。

6.16.2 注意事项

动态工作密钥只能使用一次。

加密数据长度最长为 162 字节。

进行 MAC 计算时，数据长度范围 1—162 字节，数据后不需要补“80……00”,由系统内部自行补齐

6.16.3 命令报文

代码	长度（byte）	值（HEX）	描述
CLA	1	80	--
INS	1	FA	--
P1	1	00	加密
		01	MAC 计算（初始值默认为 8 字节 0）
		05	带初始值的 MAC 计算
P2	1	00	--
Le	1	XX	--
DATA	-	XX	计算数据
Le	-	-	不存在

6.16.4 命令报文数据域

代码	数据域值
P1=00/01	要加密的数据/要计算 MAC 的数据
P1=05	8 字节初始值+计算 MAC 的数据

6.16.5 响应报文数据域

响应报文数据域为加密或计算 MAC 的结果

6.16.6 响应报文状态码

SW1	SW2	意义

90	00	命令执行成功
67	00	错误长度
6A	86	参数错误
69	85	使用条件不满足

7. 中国金融 IC 卡专用命令

本部分 IC 卡命令完全符合《中国金融集成电路 IC 卡规范》。

交易的安全特性：《中国金融集成电路 IC 卡规范》规定在执行任何交易过程中，必须通过使用 MAC（根据不同的交易，在卡内生成相应的交易认证码）来保证交易数据在卡片、终端（PSAM 卡）和主机之间的完整性与交易方之间的合法性认证。

交易过程中所有 MAC 和 TAC 都是按 MAC 计算方法生成。MAC 计算的初始值为 8 个字节的十六进制数字‘0‘，方法见“安全报文传送”。

7.1 Appliction Block（应用锁定）

7.1.1 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’）。

对其它命令的响应根据不同的应用而定。

7.1.2 命令报文

表 7.1 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.

7.1.3 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。

7.1.4 响应报文数据域

响应报文数据域不存在。

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 7.2 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

7.2 Application Unblock（应用解锁）

7.2.1 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。

7.2.2 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。

7.2.3 命令报文

表 7.3 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

7.2.4 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。

7.2.5 响应报文数据域

响应报文数据域不存在。

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 7.4 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

7.3 Card Block（卡片锁定）

7.3.1 定义与范围

Card Block 命令使卡中所有应用永久失效。

当 Card Block 命令成功地完成后，所有后续的命令都将回送状态码“不支持此功能”即 6A81，且不执行任何其他操作。

7.3.2 命令报文

表 7.5 Card Block 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	84	-
INS	1	16	-
P1	1	00	-
P2	1	00	-
Lc	1	04	MAC 码长度
DATA	4	XX….XX	MAC
Le	-	-	不存在

7.3.3 命令报文数据域

命令报文数据域包括报文鉴别代码（MAC）数据元。
用密钥标识为 00 的 16 字节维护密钥计算 MAC。

7.3.4 响应报文数据域

响应报文数据域不存在。

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 Card Block 命令响应状态码

SW1	SW1	意义
90	00	正确执行
64	00	状态标志未改变
65	81	写 EEPROM 不成功
69	87	安全报文数据项对视
69	88	安全报文数据项不正确

7.4 Get Balance（读余额）

7.4.1 定义与范围

Get Balance 命令用于读取电子钱包或电子存折余额，实现查询余额交易。读取电子存折余额需验证口令密钥 PIN。

7.4.2 命令报文

表 7.7 Get Balance 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	5C	-
P1	1	00	-
P2	1	01	用于电子存折
		02	用于电子钱包
Lc	-	-	不存在
DATA	-	-	不存在
Le	1	04	要读取金额的长度

7.4.3 命令报文数据域

命令数据域不存在。

7.4.4 响应报文数据域

命令执行成功的响应报文 数据域如下所示：
电子存折或电子钱包余额（4 字节）

7.4.5 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 7.8 Get Balance 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	85	使用条件不满足
6A	81	功能不支持
6A	82	文件未找到

7.5 Get Transaction Prove（取交易认证码）

7.5.1 定义与范围

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

7.5.2 命令报文

表 7.9 Get Transaction Prove 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	5A	-
P1	1	00	-
P2	1	XX	要取 MAC 或交易验证码所对应的交易类型标识
Lc	1	02	-
DATA	2	XXXX	见命令报文数据域
Le	1	08	-

7.5.3 命令报文数据域

说明	长度（字节）
要取 MAC 或交易验证码所对应的当前电子存折或电子钱包联机或脱机交易序号	2

7.5.4 响应报文数据域

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

说明	长度（字节）
报文鉴别代码 MAC（可能不存在）	4
交易验证码 TAC	4

7.5.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.10 Get Transaction Prove 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）
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	82	文件未找到

93	02	MAC 无效
94	06	所需 MAC 不可用

7.5.6 防插拔功能

此功能保证卡片在交易处理中的任何情况下，仍能保持数据的完整性。

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

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

7.6 Initialize For Load（圈存初始化）

7.6.1 定义与范围

Initialize For Load 命令用于初始化圈存交易。

7.6.2 命令报文

表 7.11 Initialize For Load 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	50	-

P1	1	00	-
P2	1	01	用于电子存折 ED
		02	用于电子钱包 EP
Lc	1	0B	-
DATA	11	XX…XX	1 字节密钥标识符 4 字节交易金额 6 字节终端机编号
Le	1	10	-

7.6.3 命令报文数据域

圈存初始化命令报文数据域包括以下数据元：

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

7.6.4 响应报文数据域

此命令执行成功的响应报文数据域如下表：

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

MAC1 的计算过程：

i）有 Initialize For Load 命令指定的密钥对下表数据加密生成 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联机交易序号	2
8000	2

ii）MAC1 由卡中过程密钥 SK 对下表数据按 MAC 计算方法生成。

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。

数据	长度（字节）
电子存折或电子钱包旧余额	4
交易金额	4
交易类型标识（见下表）	1
终端机编号	6

表 7.13 交易类型标识

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

7.6.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.14Initialize For Load 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	功能不支持
6A	86	参数 P1 P2 错误
94	06	密钥未找到

7.7 Credit For Load（圈存）

7.7.1 定义与范围

Credit For Load 用于圈存交易。该命令只有在成功执行 Initialize For Load 之后才能执行。通过圈存交易，持卡人可将其在银行相应帐户上的资金划入电子存折或电子钱包中。这种交易必须在金融终端上联机进行并要求验证口令（无论电子存折还是电子钱包应用）。

7.7.2 命令报文

表 7.15 Credit For Load 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	52	-
P1	1	00	-
P2	1	00	-

Lc	1	0B	-
DATA	11	XX…XX	交易日期 交易时间 MAC2
Le	1	04	-

7.7.3 命令报文数据域

圈存命令报文数据域包括以下数据元：

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

MAC2 的计算过程

由圈存初始化时生成的过程密钥 SK 对下表数据按 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‘00‘，方法见“安全报文传送”

数据	长度（字节）
交易金额	4
交易类型标识（见表 7.13）	1
终端机编号	6
主机交易日期	4
主机交易时间	3

7.7.4 响应报文数据域

此命令执行成功的响应报文数据域如下表：

说明	长度（字节）
交易验证码 TAC	4

TAC 的计算过程：

TAC 由内部密钥 DTK 左右 8 字节异或运算的结果对下表数据按 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‘00‘。

数据	长度（字节）
电子存折或电子钱包新余额	4
电子存折或电子钱包联机交易序号（加 1 前）	2
交易金额	4
交易类型标识（见表 7.13）	1
终端机编号	6
主机交易日期	4
主机交易时间	3

7.7.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.16Credit For Load 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	01	命令不接受
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
93	02	MAC 无效

注：完成圈存后，Simlinker 将做如下操作：

把交易金额加在电子存折或电子钱包的金额上。

将电子存折联机交易序号或电子钱包联机交易序号加 1.

用下表的数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。

数据元	长度
电子存折/电子钱包联机交易序号（加 1 后）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

7.7.6 圈存交易流程

在进行圈存交易时，先选择银行应用，然后在银行应用下进行操作，整个过程如下所示：

IC 卡		终端		主机
设置当前应用标识 并送出应用序列号	← →	选择银行应用 将应用序列号送主机	 →	 主机保留卡片应用序列号
卡片产生过程密钥 SK，并利用 SK 计算 MAC1 将原余额、联机交	 ←-	发送圈存初始化命令 Initialize For Load		主机按终端指定密钥标识，使用相应的圈存主密钥对应用序列号分散得到圈存子密钥

易序号、密钥版本号、算法标识、4 字节伪随机数和 MAC1 送卡外	→	将收到的所有响应数据传送给银行主机	→	按卡片相同方法产生相同的过程密钥 SK，并校验 MAC1 的正确性
IC 卡用过程密钥 SK 验证 MAC2 的正确性。如果验证通过，则将交易金额加到余额上、更新交易明细记录、并用内部密钥前后 8 字节异或对新余额、交易类型标识、终端机编号、主机交易日期和时间进行 TAC 计算，产生 4 字节的 TAC 码、卡片联机交易序号加 1	←	终端接收主机交易日期和时间以及 MAC2，将其作为圈存命令的 DATA 域，发送圈存命令 Credit For Load 给 IC 卡。	←	如果 MAC1 校验正确，则主机联机交易序号加 1，并用 SK 对金额、交易类型标识、终端号、交易日期和时间进行 MAC 计算得到 MAC2 送终端，否则，交易终止。
将 TAC 码回送给终端	→	终端接收到 TAC 码，确认交易成功		

图 7-1 圈存交易流程

7.8 Initialize For Purchase/Cash Withdraw（消费/取现初始化）

7.8.1 定义与范围

Initialize For Purchase/Cash Withdraw 命令用于初始化消费交易。

7.8.2 命令报文

表 7.17 Initialize For Purchase/Cash Withdraw 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	50	-
P1	1	01	-消费初始化
		02	取现初始化
P2	1	01	用于电子存折 ED
		02	用于电子钱包 EP（取现交易不支持）

Lc	1	0B	-
DATA	11	XX…XX	1 字节密钥标识符 4 字节交易金额 6 字节终端机编号
Le	1	0F	-

7.8.3 命令报文数据域

消费/取现初始化命令报文数据域包括以下数据元：

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

7.8.4 响应报文数据域

此命令执行成功的响应报文数据域如下表：

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

7.8.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.18 Initialize For Purchase/Cash Withdraw 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）
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	82	文件未找到
94	01	余额不足

7.9 Debit For Purchase/Cash Withdraw（消费/取现）

7.9.1 定义与范围

消费/取现命令用于消费/取现交易。该命令只有在成功执行 Initialize For Purchase/Cash Withdraw 之后才能执行。

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

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

7.9.2 命令报文

表 7.19 Debit For Purchase/cash Withdraw 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	54	-
P1	1	01	-
P2	1	00	
Lc	1	0F	-
DATA	11	XX…XX	见下面命令报文数据域
Le	1	08	-

7.9.3 命令报文数据域

消费/取现命令报文数据域包括以下数据元：

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

MAC1 的计算过程：

i）有 Initialize For Purchase/Ccahs Withdraw 命令指定的密钥对下表数据加密生成 8 字节过程密钥 SK（SK 是在消费/取现初始化中生成的）。

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

ii）MAC1 由卡中过程密钥 SK 对下表数据按 MAC 计算方法生成。

数据	长度（字节）
交易金额	4
交易类型标识（见表 7.13）	1
终端机编号	6
终端交易日期	4
终端交易时间	3

7.9.4 响应报文数据域

此命令执行成功的响应报文数据域如下表：

说明	长度（字节）
交易验证码 TAC	4
MAC2	4

TAC 的计算过程：

TAC 由内部密钥 DTK 左右 8 字节异或的结果对下表数据按 MAC 计算方法生成的。

数据	长度
交易金额	4
交易类型标识	1
终端机编号	6
终端交易序号	4
终端交易日期	4
终端交易时间	3

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。

7.9.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.20 Debit For Purchase Cash Withdraw 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	01	命令不接受
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
93	02	MAC 无效
94	01	余额不足

注：完成消费交易后，Simlinker 将做如下操作：

从电子存折或电子钱包余额中扣减消费金额

将电子存折或电子钱包脱机交易序号加 1

用下表的数据组成一个记录，保存在所指定的记录长度为 23 字节的交易明细文件中（电子钱包不记录交易记录）

数据元	长度（字节）
电子存折脱机交易序号（加 1 后）	2
透支限额	3
交易金额	4
交易类型标识	1
终端机编号 6	6

终端交易日期	4
终端交易时间	3

7.9.6 消费交易流程

消费交易可以脱机进行，取现交易必须联机进行，且取现交易只能对电子存折进行，现以消费脱机交易为例说明其流程。有关 PSAM 卡的特性和指令见《Simlinker/PSAM 技术参考手册》，此外用到的 MAC1 计算及 MAC2 校验指令属于《Simlinker/PSAM 技术参考手册》范畴。

IC 卡		终端		PSAM 卡
设置当前应用标识 并送出应用序列号	← →	选择银行应用 接收应用序列号并保存		
卡片产生过程密钥 SK 将原余额、脱机交易序号、透支限额、密钥版本号、算法标识、4 字节伪随机数送卡外	← →	发送消费初始化命令 Initialize For Purchase 将接收到的有关数据作为 MAC1 计算命令的 DATA 域，送 MAC1 计算命令给 PSAM 卡。	 →	PSAM 卡按指定的密钥版本号，使用相应的消费主密钥对应用序列号分散得到消费子密钥。按卡片相同方法产生相同的过程密钥 SK，并计算产生 MAC1
IC 卡用过程密钥 SK 验证 MAC1 的正确性，如果验证通过，则将从余额扣除消费的金额；将卡片脱机交易序号加 1，更新交易明细记录。用 SK 对响应数据计算得到 4 字节的 MAC2；用内部密钥左右 8 字节异或运算的结果对响应数据计算得到 4 字节的 TAC 码	←	将终端号、交易日期和时间以及 MAC1 作为消费命令的 DATA 域，发送消费命令 Debie For Purchase 给 IC 卡	←	将 MAC1 回送给终端

将 MAC2 和 TAC 码回送给终端	→	终端接收到 TAC 码，确认交易成功，并将 MAC2 送 PSAM 卡校验 终端接收确认信息	→ ←	如果 MAC2 校验成功，则终端应记录该笔交易并发送确认信息给终端， PSAM 卡应用错误计数器减 1，当计数器值为 0 时，PSAM 卡将锁死。

图 7-2　消费交易流程

7.10　Initialize For Unload（圈提初始化）

7.10.1　定义与范围

Initialize For Unload 命令用于初始化圈提交易。

7.10.2　命令报文

表 7.21　Initialize For Unload 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	50	-
P1	1	05	-
P2	1	01	用于电子存折 ED
Lc	1	0B	-
DATA	11	XX…XX	1 字节密钥标识符 4 字节交易金额 6 字节终端机编号
Le	1	10	-

7.10.3　命令报文数据域

圈提初始化命令报文数据域包括以下数据元

说明	长度（字节）
密钥标识符（圈提密钥）	1

交易金额	4
终端机编号	6

7.10.4 响应报文数据域

此命令执行成功的响应报文数据域如下表：

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

i） 由 Initialize For Unload 所指定的密钥对下表数据加密生成 8 字节过程密钥 SK。

数据	长度（字节）
伪随机数	4
电子存折联机交易序号	2
8000	2

ii） MAC1 由卡中过程密钥 SK 对下表数据按 MAC 计算方法生成。

数据	长度（字节）
电子存折或电子钱包旧余额	4
交易金额	4
交易类型标识（见表 7.13）	1
终端机编号	6

7.10.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.22 Initialize For Unload 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	85	使用条件不满足
6A	81	功能不支持
6A	86	参数 P1 P2 错误

94	01	余额不足
94	03	密钥索引不支持

7.11 Debit For Unload（圈提）

7.11.1 定义与范围

Debit For Unload 用于圈提交易。该命令只有在成功执行 Initialize For Unload 之后才能执行。通过圈提交易，持卡人可以把电子存折中的部分或全部资金划到其在银行的相应帐户。这种交易必须在金融终端上联机进行并要求验证口令。

只有电子存折应用支持圈提交易。

7.11.2 命令报文

表 7.23 Debit For Unload 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	54	-
P1	1	03	-
P2	1	00	-
Lc	1	0B	-
DATA	11	XX…XX	主机交易日期 主机交易时间 MAC2
Le	1	04	-

7.11.3 命令报文数据域

圈提命令报文数据域包括以下数据元：

数据	长度（字节）
交易日期（主机）	4
交易时间（主机）	3

MAC2	4

MAC2 的计算过程：

MAC2 由圈提初始化时使用的过程密钥 SK 对下表数据按 MAC 计算方法生成的。

数据	长度(字节)
交易金额	4
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

7.11.4 响应报文数据域

此命令执行成功的响应报文数据域如下表:

说明	长度(字节)
MAC3	4

MAC3 的计算过程：

MAC3 由圈提初始化时生成的过程密钥 SK 对下表数据按 MAC 计算方法生成的。

数据	长度（字节）
电子存折新余额	4
电子存折联机交易序号（加 1 前）	2
交易金额	4
交易类型标识（见表 7.13）	1
终端机编号	6
主机交易日期	4
主机交易时间	3

7.11.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.24 Debit For Unload 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	01	命令不接受（无效状态）
6A	81	功能不支持
93	02	MAC 无效

注：完成圈提后，Simlinker 将做如下操作：

从电子存折余额中扣减交易金额。

将电子存折联机交易序号加 1.

用下表数据组成一个记录，保存在所指定记录长度为 23 个字节的交易明细文件中。

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

7.11.6 圈提交易流程

圈提交易只能够针对电子存折。交易流程见下表：

IC 卡		终端		主机
设置当前应用标识 并送出应用序列号	← →	选择银行应用 将应用序列号送主机	→	主机保留该卡应用序列号
卡片产生过程密钥 SK 用 SK 计算 MAC1	←	发送圈提初始化命令 Initialize For Purchase		主机按终端指定的密钥标识，使用相应的圈提主密钥对应用序列号分散得到圈提子密钥。
将原余额、联机交易序号、密钥版本号、算法标识、4 字节伪随机数和 MAC1 送卡外	→	将收到的所有响应数据传送给银行主机	→	按卡片相同方法产生相同的过程密钥 SK，并校验 MAC1 的正确性
IC 卡用过程密钥 SK 验证 MAC2 的正确性，如果验证通过，则将从电子存折上扣除交易的金额；将卡片联机交易序号加 1，更新交易明细记录。用 SK 对响应数据计算得到 4 字节的 MAC3；	←	终端接收主机交易日期和时间以及 MAC2，将其作为圈提指令的 DATA 域，发送圈提命令 Debit For Unload 给 IC 卡	←	如果 MAC1 校验正确，则主机联机交易序号加 1，并用 SK 对金额、交易类型标识、终端号、交易日期和时间进行 MAC 计算得到 MAC2 送终端，否则，交易终止。
将 MAC3 回送给终端	→	终端接收到 MAC3，送主机验证并保存 终端接收确认报文后，确认交易成功	→ ←	主机验证 MAC3。 如果 MAC3 验证正确，主机回送确认信息

图 7-3 圈提交易流程

7.12 Initialize For Update（修改透支限额初始化）

7.12.1 定义与范围

Initialize For Update 命令用于初始化修改透支限额交易。

7.12.2 命令报文

表 7.25 Initialize For Update 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	50	-
P1	1	04	-
P2	1	01	用于电子存折 ED
Lc	1	07	-
DATA	7	XX…XX	1 字节密钥标识符　6 字节终端机编号
Le	1	13	-

7.12.3 命令报文数据域

修改透支限额初始化命令报文数据域包括以下数据元：

说明	长度（字节）
密钥标识符（修改透支限额密钥）	1
终端机编号	6

7.12.4 响应报文数据域

此命令执行成功的响应报文数据域如下表所示：

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

MAC1 的计算过程：

i） 由 Initialize For Update 所指定的密钥对下表数据加密生成 8 字节过程密钥 SK。

数据	长度（字节）
伪随机数	4
电子存折联机交易序号	2
8000	2

ii） MAC1 由卡中过程密钥 SK 对下表数据按 MAC 计算方法生成。

数据	长度（字节）
电子存折余额	4
旧透支限额	3
交易类型标识（见表 7.13）	1
终端机编号	6

7.12.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.26 Initialize For Update 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	82	不满足安全状态
69	85	使用条件不满足
9A	81	功能不支持
6A	82	文件未找到
6A	86	参数 P1 P2 错误

94	03	密钥标识不支持

7.13 Update Overdraw Limit（修改透支限额）

7.13.1 定义与范围

Update Overdraw Limit 用于修改透支限额交易。该命令只有在成功执行 Initialize For Update 之后才能执行。

当电子存折中的实际金额不足时，透支功能为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。

修改透支限额交易必须在金融终端上联机进行。

只有电子存折应用支持修改透支限额交易。

7.13.2 命令报文

表 7.27 Update Overdraw Limit 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	80	-
INS	1	58	-
P1	1	00	-
P2	1	00	-
Lc	1	0E	-
DATA	14	XX…XX	见命令报文数据域
Le	1	04	-

7.13.3 命令报文数据域

修改透支限额命令报文数据域包括以下数据元：

数据	长度（字节）
新透支限额	3
发卡方交易日期	4

发卡方交易时间	3
MAC2	4

MAC2 的计算过程：
MAC2 由修改透支限额初始化时生成的过程密钥 SK 对下表数据按 MAC 计算方法生成的。

数据	长度
新透支限额	3
交易类型标识	1
终端机编号	6
主机交易日期	4
主机交易时间	3

7.13.4 响应报文数据域

此命令执行成功的响应报文数据域如下表：

说明	长度（字节）
交易验证码 TAC	4

TAC 的计算过程：
TAC 由内部密钥 DTK 左右 8 字节异或的结果对下表数据按 MAC 计算方法生成的。

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

7.13.5 响应报文状态码

IC 卡可能回送的状态码如下所示：
表 7.28 Update Overdraw Limit 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	01	命令不接受
69	82	不满足安全状态

69	85	使用条件不满足
9A	81	功能不支持
93	02	MAC 无效
94	01	金额不足

注：完成修改透支限额后，Simlinker 讲座如下操作：

将当前电子存折余额置为新的电子存折余额。

将电子存折联机交易序号加 1.

用下表的数据组成一个记录，保存在电子存折指定记录长度为 23 字节的交易明细文件中。

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

7.13.6 修改透支限额交易流程

修改透支限额只能对电子存折进行操作，且必须联机执行。

IC 卡		终端		主机
设置当前应用标识 并送出应用序列号	← →	选择银行应用 将应用序列号送主机	 →	主机保留该卡应用序列号
卡片产生过程密钥 SK 用 SK 计算 MAC1 将原余额、联机交易序号、密钥版本号、算法标识、4 字节伪随机数和 MAC1 送卡外	← →	发送修改透支限额初始化命令 Initialize For Purchase 将收到的所有响应数据传送给银行主机	 →	主机按终端指定的密钥标识，使用相应的圈提主密钥对应用序列号分散得到圈提子密钥。 按卡片相同方法产生相同的过程密钥 SK，并校验 MAC1 的正确性
IC 卡用过程密钥 SK 验证 MAC2 的正确性，如果验证通过，则交易金额加到余额上；更新透支限额；将卡片联机交易序号加 1；更新交易明细记录。用内部密钥左右 8 字节异或运算的结果对新余额、联机	←	终端接收主机交易日期和时间以及 MAC2，将其作为修改透支限额指令的 DATA 域，发送圈提命令 Update Overdraw Limit 给 IC 卡。	←	如果 MAC1 校验正确，则主机联机交易序号加 1，并用 SK 对金额、交易类型标识、终端号、交易日期和时间进行 MAC 计算得到 MAC2 送终端，否则，交易终止。

交易序号、交易金额、交易类型标识、终端机编号、主机交易日期和时间进行 TAC 计算，产生 4 字节的 TAC 码。				
将 TAC 回送给终端	→	终端接收到 TAC 码，确认交易成功		

图 7-4 修改透支限额交易流程

7.14 INITIALIZE FOR CAPP PURCHASE（复合消费）

7.14.1 定义与范围

INITIALIZE FOR CAPP PURCHASE 命令用于初始化复合应用消费交易。

7.14.2 命令报文

表 7.29 PIN Unblock 命令报文编码

代码	值
CLA	80
INS	50
P1	03
P2	02
Lc	0B
DATA	见下表
Le	0F

7.14.3 命令报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
密钥索引号	1
交易金额	4
终端机编号	6

7.14.4 响应报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
电子钱包余额	4
电子钱包交易序号	2
透支限额	3
密钥算法版本号（DPK）	1
密钥标识（DPK）	1
伪随机数	4

7.14.5 响应报文状态码

SW1	SW2	意义
90	00	执行成功
65	81	内存错误
69	85	长度错误
94	01	金额不足
94	02	交易计数器达到最大值
94	03	密钥索引不支持
94	08	应用灰锁锁定

7.15 UPDATE CAPP DATA CACHE （更新复合应用数据）

7.15.1 定义与范围

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

7.15.2 命令报文

代码	值
CLA	80
INS	DC
P1	复合应用类型标识符
P2	见表
Lc	后续数据长度
DATA	见下表
Le	不存在

UPDATE CAPP DATA CACHE 命令报文中的引用控制参数 P2 定义：

B8	B7	B6	B5	B4	B3	B2	B1	含义
0	0	0	0	0	—	—	—	RFU
X	X	X	X	X	—	—	—	SFI
1	1	1	1	1	—	—	—	RFU
—	—	—	—	—	0	0	0	第一个标识符出现的记录
—	—	—	—	—	X	X	X	RFU
其他值								RFU

7.15.3 命令报文数据域

此命令报文数据域由更新原有记录的新记录组成。

7.15.4 响应报文数据域

响应报文数据域不存在

7.15.5 响应报文状态码

应答报文可能的状态码如下：

SW1 SW2	意义
90 00	执行成功
65 81	内存失败
67 00	长度错误
69 81	命令与文件结构不相容
69 82	不满足安全状态
69 86	不满足命令执行的条件（不是当前的 EF）
6A 81	不支持此功能
6A 82	未找到文件
6A 83	未找到记录
6A 84	文件中存储空间不够
94 07	复合应用禁止

7.16 DEBIT FOR CAPP PURCHASE （复合消费）

7.16.1 定义与范围

DEBIT FOR CAPP PURCHASE 命令用于复合应用消费交易。

7.16.2 命令报文

DEBIT FOR CAPP PURCHASE 命令报文编码如下：

代码	值
CLA	80
INS	54
P1	01
P2	00
Lc	0F
DATA	见下表
Le	08

7.16.3 命令报文数据域

DEBIT FOR CAPP PURCHASE 命令报文的数据域 DATA：

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

MAC1 由过程密钥对（4 字节交易金额＋1 字节交易类型标识＋6 字节终端机编号＋4 字节主机交易日期＋3 字节主机交易时间+ 9 字节安全认证识别码）数据加密生成。
过程密钥由消费密钥对（4 字节伪随机数+2 字节电子钱包脱机交易序号+终端交易序号的最右两个字节）数据加密生成。

7.16.4 响应报文数据域

执行成功则应答报文如下：

说明	长度(字节)
TAC	4
MAC2	4

TAC 由消费密钥左右 8 位字节异或运算后对（4 字节交易金额＋1 字节交易类型标识＋6 字节终端机编号＋4 字节终端交易序号+4 字节主机交易日期＋3 字节主机交易时间）数据加密生成。
MAC2 由卡中过程密钥对 4 字节交易金额数据加密生成。

7.16.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
65	81	内存错误
67	00	长度错误
69	01	命令不接受(无效状态)
69	85	使用条件不满足
93	02	MAC 无效
94	01	金额不足

7.17 INITIALIZE FOR GREY LOCK （灰锁初始化）

7.17.1 定义与范围

INITIALIZE FOR GREY LOCK 命令用于初始化灰锁操作。

7.17.2 命令报文

INITIALIZE FOR GREY LOCK 命令报文编码如下：

代码	值
CLA	E0
INS	7A
P1	08
P2	01
Lc	07
DATA	见下表
Le	0F

7.16.3 命令报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
密钥索引号	1
终端机编号	6

7.16.4 响应报文数据域

执行成功则应答报文如下：

说明	长度(字节)
电子钱包余额	4
电子钱包交易序号	2
透支限额	3（全 0）
密钥版本号	1
算法标识	1
伪随机数	4

7.14.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
65	81	内存错误
69	01	命令不接受(无效状态)
69	85	使用条件不满足
94	03	密钥索引号不支持

7.18 GREY LOCK （灰锁）

7.18.1 定义与范围

GREY LOCK 命令用于灰锁电子钱包。

7.18.2 命令报文

GREY LOCK 命令报文编码如下：

代码	值
CLA	E0
INS	7C
P1	08
P2	00
Lc	13
DATA	见下表
Le	08

7.18.3 命令报文数据域

下表定义了命令报文的数据域 DATA：

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

MAC1 由过程密钥对（1 字节交易类型标识＋6 字节终端机编号＋4 字节主机交易日期

＋3 字节主机交易时间）数据加密生成。
过程密钥由（伪随机数+电子钱包脱机交易序号+终端交易序号的最右两个字节）的加密结果对（终端随机数+‘80000000’）数据加密生成。

7.18.4 响应报文数据域

执行成功则应答报文如下：

说明	长度(字节)
GTAC	4
MAC2	4

GTAC 由卡中过程密钥对（1 字节交易类型标识＋终端交易序号＋4 字节主机交易日期＋3 字节主机交易时间）数据加密生成。
MAC2 由卡中过程密钥对（4 字节电子钱包余额＋2 字节电子钱包脱机交易序号（加 1 前））数据加密生成。

7.18.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
64	00	状态标志位未改变
65	81	内存错误
67	00	长度错误
69	01	命令不接受(无效状态)
69	85	使用条件不满足
93	02	MAC 无效

7.19 INITIALIZE FOR GREY UNLOCK （联机解扣）

7.19.1 定义与范围

INITIALIZE FOR GREY UNLOCK 命令用于初始化联机解扣交易。

7.19.2 命令报文

INITIALIZE FOR GREY UNLOCK 命令报文编码如下：

代码	值
CLA	E0
INS	7A
P1	09
P2	01
Lc	07
DATA	见下表
Le	12

7.19.3 命令报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
密钥索引号	1
终端机编号	6

7.19.4 响应报文数据域

执行成功则应答报文如下：

说明	长度(字节)

电子钱包余额	4
电子钱包脱机交易序号	2
电子钱包联机交易序号	2
密钥版本号	1
密钥算法	1
伪随机数	4
MAC1	4

MAC1 由卡中过程密钥对（4 字节电子钱包余额＋2 字节电子钱包脱机交易序号＋1 字节交易类型标识＋6 字节终端机编号）数据加密生成。

过程密钥由 DULK 密钥对（伪随机数+电子钱包联机交易序号+‘8000’）加密生成。

7.19.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
65	81	内存错误
67	00	长度错误
69	01	命令不接受(无效状态)
69	85	使用条件不满足
6A	86	P1、P2 参数不正确
94	03	密钥索引号不支持

7.20 GREY UNLOCK （联机解扣）

7.20.1 定义与范围

GREY UNLOCK 命令用于联机解扣交易。

7.20.2 命令报文

GREY UNLOCK 命令报文编码如下：

代码	值
CLA	E0
INS	7E
P1	09
P2	00
Lc	0F
DATA	见下表
Le	04

7.20.3 命令报文数据域

下表定义了命令报文的数据域 DATA：

说明	长度(字节)
交易金额	4
交易日期	4
交易时间	3
MAC2	4

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

7.20.4 响应报文数据域

执行成功则应答报文如下：

说明	长度(字节)
MAC3	4

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

7.20.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
64	00	状态标志位未改变
65	81	内存错误
67	00	长度错误
69	01	命令不接受(无效状态)
69	85	使用条件不满足
93	02	MAC 无效
94	01	金额不足

7.21 DEBIT FOR UNLOCK （脱机解扣）

7.21.1 定义与范围

DEBIT FOR UNLOCK 命令用于对电子钱包进行解扣操作。

7.21.2 命令报文

DEBIT FOR UNLOCK 命令报文编码如下：

代码	值
CLA	E0
INS	7E
P1	08
P2	01
Lc	1B
DATA	见下表
Le	04

7.21.3 命令报文数据域

DEBIT FOR UNLOCK 命令报文的数据域 DATA：

说明	长度(字节)
交易金额	4
交易序号	2
终端机编号	6
终端交易序号	4
主机交易日期	4
主机交易时间	3
GMAC	4

GMAC 由过程密钥对（4 字节交易金额＋9 字节安全认证识别码）数据加密生成。

7.21.4 响应报文数据域

执行成功则应答报文如下：

说明	长度(字节)
TAC	4

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

7.21.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
64	00	状态标志位未改变
65	81	内存错误
67	00	长度错误
69	01	命令不接受(无效状态)
69	85	使用条件不满足
94	01	金额不足
93	02	MAC 无效
94	06	所需 MAC 和 TAC 不可用

7.22 GET LOCK PROOF （读取证明码）

7.22.1 定义与范围

GET LOCK PROOF 命令用于读取电子钱包应用的灰锁状态以及相关的证明码。

7.22.2 命令报文

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

代码	值
CLA	E0
INS	CA
P1	00 ：普通读取 01 ：清除 TACUF（交易验证码待读标志）
P2	00
Lc	不存在
DATA	不存在
Le	1E 或不存在

7.22.3 命令报文数据域

命令报文的数据域不存在。

7.22.4 响应报文数据域

正常状态 GET LOCK PROOF 命令执行成功的响应报文数据域：

说明	长度
状态字（＝‘00’表示当前应用无灰锁）	1
上次发生的解扣、联机解扣的交易类型标识	1
上次解扣、联机解扣的电子钱包（ ‘01’ ）	1
上次解扣、联机解扣的电子钱包余额	4
上次解扣、联机解扣的电子钱包的交易序号	2

上次解扣、联机解扣的终端机编号	6
上次解扣、联机解扣的日期	4
上次解扣、联机解扣的时间	3
上次解扣、联机解扣的交易金额	4
上次解扣的 TAC 或联机解扣的 MAC3	4

灰锁状态 GET LOCK PROOF 命令执行成功的响应报文数据域：

说明	长度
状态字（＝‘01’表示当前应用已灰锁）	1
灰锁的交易类型标识	1
被灰锁的电子钱包（ ‘01’ ）	1
被灰锁的电子钱包余额	4
被灰锁的电子钱包交易序号	2
执行 GREY LOCK 时的终端机编号	6
执行 GREY LOCK 时的日期	4
执行 GREY LOCK 时的时间	3
灰锁时的 MAC2	4
灰锁时的 GTAC	4

TAC 未读时 GET LOCK PROOF 命令执行成功的响应报文数据域：

说明	长度
状态字（＝‘10’表示当前应用 TAC 未读）	1
上次解扣的交易类型标识	1
上次解扣的电子钱包（ ‘01’ ）	1
上次解扣的电子钱包余额	4
上次解扣的电子钱包交易序号	2
上次执行解扣的终端机编号	6
上次执行解扣的日期	4
上次执行解扣的时间	3
解扣交易金额	4
上次解扣的 TAC	4

7.22.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
64	00	状态标志位未改变
65	81	内存错误
69	85	使用条件不满足
6A	86	P1、P2 参数不正确

7.23 GET MESSAGE （读取安全认证识别码）

7.23.1 定义与范围

GET MESSAGE 命令用于消费/取现交易。读取 CPU 卡中的安全认证识别码，即芯片安全区域内的安全认证识别码或芯片中的 MID ‖ UID0UID1UID2UID3 ‖ 四字节识别码，将安全认证识别码发送给 PSAM 卡进行认证。该命令在应在任意目录下都可以执行。

7.23.2 命令报文

GET MESSAGE 命令报文编码如下：

代码	值
CLA	80
INS	CA
P1	00
P2	00
Lc	09
DATA	不存在

7.23.3 命令报文数据域

命令报文数据域不存在。

7.23.4 响应报文数据域

执行成功则应答报文如下：

说明	长度
安全认证识别码	9

7.23.5 响应报文状态码

应答报文可能的状态码如下：

SW1	SW2	意义
90	00	执行成功
67	00	长度错误
6A	86	P1、P2 参数不正确
6D	00	INS 不支持或错误
6E	00	CLA 不支持或错误

7.24 PIN Unblock（口令解锁）

7.24.1 定义与范围

PIN Unblock 命令发卡方提供了解锁口令密钥的功能。
当 PIN Unblock 命令成功完成后，卡片将重置个人密码错误计数器的值。
命令中口令密钥的传递采用加密方式。

7.24.2 命令报文

表 7.29 PIN Unblock 命令报文编码

代码	长度（byte）	值（Hex）	描述
CLA	1	84	-
INS	1	24	-
P1	1	00	-
P2	1	01	-口令解锁密钥 ID
Lc	1	0C/14	-
DATA	12	XX…XX	加密的口令密钥数据元和报文鉴别码 MAC 数据元
Le	-	-	不存在

注：

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

7.24.3 命令报文数据域

命令报文数据域由口令密钥数据元和其后的报文鉴别代码 MAC 数据元组成。
用口令解锁密钥加密口令密钥和计算 MAC，方法见“安全报文传送”。

7.24.4 响应报文数据域

响应报文数据域不存在。

7.24.5 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.30 PIN 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
6A	82	KEY 文件未找到
6A	86	参数 P1 P2 不正确
69	88	安全报文数据项不正确
93	03	应用永久锁定
94	03	密钥未找到

7.25 Reload/Change PIN（重装/修改口令密钥）

7.25.1 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。

7.25.2 命令报文

表 7.31 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。

7.25.3 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。

7.25.4 响应报文数据域

响应报文数据域不存在。

7.25.5 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. 命令与应答

8.1 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	DATA

响应 *:*

SW1	SW2

8.2 命令格式

Simlinker 命令由4 字节的命令头和命令体组成，见图8-1。

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

图8-1 命令格式

8.2.1 命令头域

命令头定义板报文的内容如下表所示：

表8.1 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

8.2.2 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

8.3 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8-2 响应数据格式

8.4 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8.2 状态字SW1SW2

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。
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。

9. Simlinker/PBOC 发卡命令

- 此部分描述了Simlinker/PBOC 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/PBOC*** 发卡命令。

表9.1 Simlinker/PBOC 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 MF**	80	0E	擦除DF	专有
3	**Write Key**	80/84	D4	增加或修改密钥	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“ Simlinker/PBOC 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

数据域	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	28	文件空间		读权限	写权限	‘FF’	见 说 明

件							【2】
定长记录文件	2A	2≤记录数≤254	记录长度≤178	读权限	写权限	‘FF’	见说明【2】
循环文件	2E	2≤记录数≤254	记录长度≤178	读权限	写权限	‘FF’	见说明【2】
普通钱包文件	2F	2≤记录数≤254	记录长度=3或4	读/扣款权限	存款权限	‘FF’	见说明【2】
电子存折/电子钱包	2F	记录数=2	记录长度=8	使用权限	01	‘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]		‘0F’	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】对文件进行线路保护时所使用的维护密钥标识设置

基本文件数据域Byte7定义如下：

b7	b6	b5	b4	b3	b2	b1	b0
是否带线路保护读	1	1	1	读密钥标识符		写密钥标识符	

1）b7=1，表示该文件不支持带线路保护读，b3b2=11；
b7=0，表示该文件必须带线路保护读。

2）b6～b4位保留为1.

3）b3b2=11，表示用标识00的维护密钥；
b3b2=10，表示用标识01的维护密钥；
b3b2=01，表示用标识02的维护密钥；
b3b2=00，表示用标识03的维护密钥。

4）b1b0的设置方法与b3b2相同。

注：如果文件类型Byte1设置为不带线路保护，那么Byte7保留为‘FF’。
如果文件类型Byte1设置为带线路保护而b7设置为不带线路保护读，那么b3b2保留为1.

【3】 电子存折/电子钱包文件

注：电子存折的文件标识符必须是‘0001’；电子钱包的文件标识符必须是‘0002’；

【4】 **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	0	X	X	X	X	X	包含当前DF的A5模板的短文件标识符.
1	1	1	1	1	1	1	1	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（擦除主文件 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、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），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MF 再进入MF 时，将遵循文件的访问权限。

9.2.3 命令报文

表9.8 Erase DF 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	-	-	-
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 DF 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
6A	81	用此命令擦除DF时回送的错误信息

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“3.6 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

9.5.3.1 **方式一**

表9.15 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	80/84	-
INS	1	D4	-
P1	1	01	用于密钥装载
		3X	密钥类型，用于密钥更新
P2	1	XX	密钥标识
Lc	1	XX	数据长度
DATA	XX	XX....XX	密钥头+密钥值
Le	-	-	不存在

说明：

P2的设置见“9 密钥装载之说明【3】”

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’。

9.3.4 命令报文数据域

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

9.3.4.1 密钥装载

命令报文数据 = 密钥头（5 字节）+密钥值
若为线路加密保护，则由被加过密的数据附上 4 字节 MAC 码组成。（见说明【2】）
表 9.16 Write Key 之密钥装载命令报文数据域

数据域 / 密钥类型	Byte1	Byte2	Byte3	Byte4	Byte5	密钥长度（Byte）
DES 加密密钥	30	使用权限	更改权限	密钥版本号	算法标识	8/16
DES 解密密钥	31	使用权限	更改权限	密钥版本号	算法标识	8/16
DESMAC 密钥	32	使用权限	更改权限	密钥版本号	算法标识	8/16
内部密钥	34	使用权限	更改权限	密钥版本号	算法标识	8/16
维护密钥	36	使用权限	更改权限	FF	错误计数器	8/16
主控密钥	即密钥标识为 00 的外部认证密钥，其命令报文数据域同外部认证密钥					
外部认证密钥	39	使用权限	更改权限	后续状态	错误计数器	16
口令解锁密钥	37	使用权限	更改权限	FF	错误计数器	8/16
口令重装密钥	38	使用权限	更改权限	FF	错误计数器	8/16
修改透支限额密钥	3C	使用权限	更改权限	密钥版本号	算法标识	8/16
圈提密钥	3D	使用权限	更改权限	密钥版本号	算法标识	8/16
消费密钥	3E	使用权限	更改权限	密钥版本号	算法标识	8/16
圈存密钥	3F	使用权限	更改权限	密钥版本号	算法标识	8/16
口令密钥	3A	使用权限	EF	后续状态	错误计数器	2-8(对于金融目录下的口令，如

						果口令长度不足6个字节，后补FF)
解锁口令密钥	3B	使用权限	更改权限	指定需解锁的口令密钥标识	错误计数器	8

注：表中密钥版本号、后续状态等见说明【4】。

说明：

【1】 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 等），只需在安装密钥时改变 Byte1（密钥类型）字节高两位即可。

密钥数据域 Byte1（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

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由‘39’变为‘F9’。

注： 具有线路保护属性的密钥，必须用相应的线路保护模式装载与修改，但 MF 下的主控密钥装载除外。

【2】 以安全报文方式装载或修改密钥时所使用的密钥如下：

当装载 MF 下的主控密钥时，分以下两种情况：

i 由厂家在卡片 MF 的 KEY 文件中已经预先装入一条主控密钥（即卡片传输密钥，见“4.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。

ii 在用户擦除 MF 后，MF 下的主控密钥必须以明文方式装入，但可以设置密钥类型为线路保护方式，此后可以使用线路保护方式更新此密钥。

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。

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。

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”。

【3】 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：

只能有一个主控密钥、口令解锁密钥、一个重装口令密钥，它们的密钥标识必须是 00.

维护密钥做多可以有 4 个，密钥标识为 00-03.

对于金融应用下的口令，密钥标识为 00.

密钥标识不能是‘FF’。

[4] 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。

9.3.4.2 密钥更改

命令报文数据=新密钥值。

若为线路加密保护则由被加过密的数据附上 4 字节 MAC 码组成。

在满足密钥更改权限时可使用 Write Key 更改密钥内容，但不能改变错误计数器的值

口令密钥不允许使用此命令进行修改。

密钥被锁死不能使用该命令修改密钥。

9.3.5 响应报文数据域

响应报文数据域不存在

9.3.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 9.17 Write Key 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	82	权限（MF擦除权限）不满足
69	83	密钥被锁死
6A	82	KEY文件未找到
6A	83	密钥未找到
6A	84	KEY文件空间已满
93	02	修改密钥时线路保护错误

附录 A Simlinker/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.
- Simlinker/PSAM 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。

复位应答信息如下表所示：

表附录1.1 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	69	TB 和TC1 存在，历史字符为9 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-T9	XX	历史字符	9

说明：

· TS=‘3B’，它表示从I/O 口传送数据时先传低位再传高位。

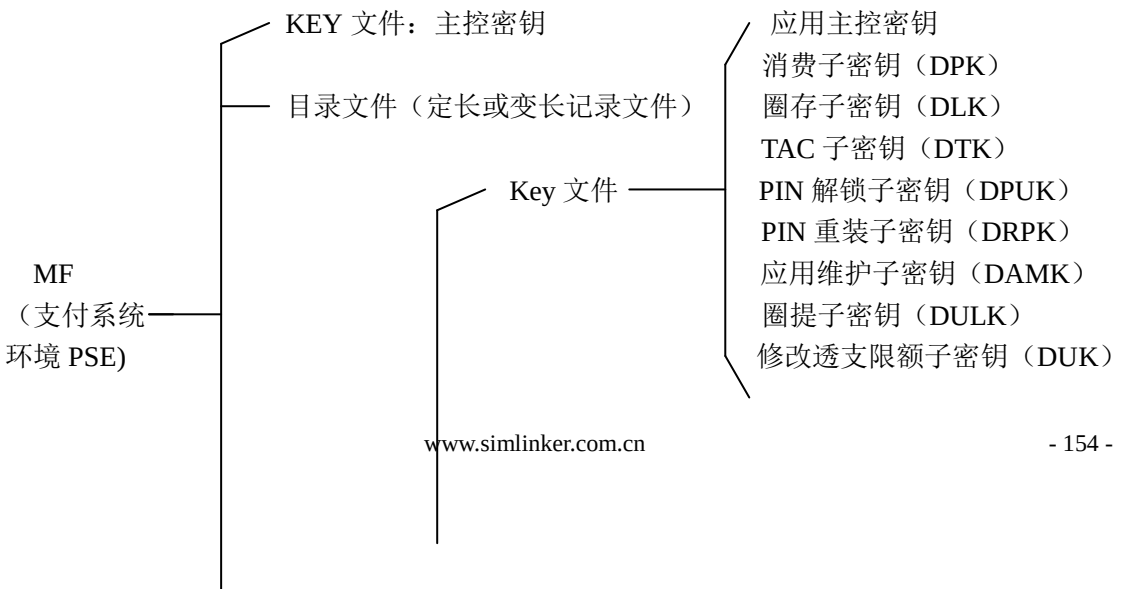
· T0=‘69’，它的低半字节9表明有9个历史字符，高半字节6（0110）表示TB1、TC1存在，由于TD1不存在所以为T=0的通讯协议。

表附录1.2 复位信息中的历史字符

符号	值（HEX）	意义
T1	‘P’（‘50’）	公司标识：PanSun 的缩写
T2	‘S’（‘53’）	
T3-T5	XX…XX	由Simlinker 定义
T6-T9	XX…XX	4 字节芯片序号，每卡该序号唯一

附录 B 电子存折/电子钱包应用的基本文件数据

Simlinker/PBOC 文件结构如下图所示：



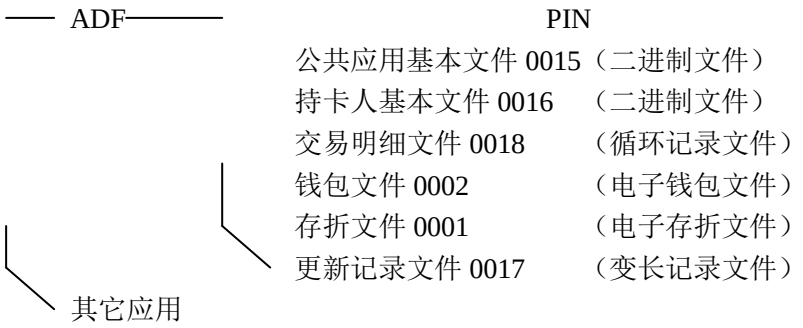


表 A-1 电子存折和电子钱包应用的公共应用基本数据文件

文件标示符	‘0015’	
文件类型	‘A8’（线路保护的二进制文件）	
文件主体空间	‘1E’	
读权限	‘F0’（自由读取）	
写权限	‘F0’（写二进制时必须使用 DAMK 进行线路保护，如连续三次执行此命令失败，IC 卡会送‘9303’即应用永久锁定）	
字节	**数据元**	**长度**
1-8	发卡方标识	8

9	应用类型标识	1
10	应用版本	1
11-20	应用序列号	10
21-24	应用启动日期	4
25-28	应用有效日期	4
29-30	发卡方自定义文件控制信息数据	2

表 A-2 电子存折和电子钱包应用的持卡人基本数据文件

文件标示符	‘0016’	
文件类型	‘A8’（线路保护的二进制文件）	
文件主体空间	‘27’	
读权限	‘F0’（自由读取）	
写权限	‘F0’（写二进制时必须使用 DAMK 进行线路保护，如连续三次执行此命令失败，IC 卡会送‘9303’即应用永久锁定）	
字节	**数据元**	**长度**
1	卡类型标识	1
2	本行职工标识	1

3-22	持卡人姓名	20
23-38	持卡人证件号码	16
39	持卡人证件类型	1

表 A-3 复合交易记录文件

文件标示符	‘0017’	
文件类型	变长记录文件	
文件大小		
读权限	‘F0’	
写权限	‘F0’	
字节	**数据元**	**长度**

用户自定义	用户自定义	用户自定义

表 A-4 电子存折和电子钱包应用的交易明细文件

文件标示符	‘0018’
文件类型	‘2E’（循环文件）
记录个数	‘0A’（该循环文件必须能够容纳至少十条消费、取现、圈存、圈提交易 记录）
记录长度	‘17’
读权限	‘F1’（必须先验证口令）

写权限	‘EF’（交易明细由 IC 卡维护，不允许外部对其修改）	
字节	**数据元**	**长度**
1-2	电子存折/电子钱包联机或脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标识	1
11-16	终端机编号	6
17-20	交易日期	4
21-23	交易时间	3