华大金融 PBOC2.0 双界面卡

用户参考手册

编　　号：HED-ICC-7.0.1.02-TD029_060707
支持算法：DES
COS 版本：MCOS3.5.3

北京中电华大电子设计有限责任公司

二 OO 六年七月

文档修订记录表

修订日期	修订人	批准人	修订内容
3/11/2008	葛晨	贺朋	1、ATQB 不同（P19） V97: ATQB 的 application data 区域不再返回 cos 版本信息，而是返回 00 00 00 00，未使用 2、case4 命令不同（P49） v97: 射频模式下，CASE4 的情况，命令格式可以是 CLA INS P1 P2 Lc DATA,也可以是 CLA INS P1 P2 Lc DATA Le 即可以加或不加 Le 字节； 射频模式下，CASE4 的情况，当 LE 错误时，返回 61XX

目录

声明

版本说明

序号	项目		
1.			
2.			
3.			
4.			
5.			

1. 引言

1.1. 编写目的

华大双界面卡配合华大自主开发的 MCOS/PBOC/SSC，支持金融环境，适用于金融领域中的应用。通过此用户手册可以帮助用户了解华大双界面卡的性能，熟悉使用华大双界面卡，配合应用的开发。

此用户手册适用于利用华大双界面卡进行应用设计与开发的人员使用。

1.2. 内容概述

本手册各部分内容包括：

- MCOS/PBOC/SSC 简介
  介绍华大双界面卡以及 MCOS/PBOC/SSC 的特性和所支持的文件结构特点。
- 安全管理
  描述了安全管理的基本概念，安全管理的实现方法，以及使用安全报文时命令的传送情况
- 命令与响应
  详细介绍了华大双界面卡支持的各种基本命令和专有命令的使用要求，以及命令执行的返回信息。
- 卡片个人化
  简单介绍了，在应用中进行卡片个人化的流程。
- 交易流程
  介绍华大双界面卡所支持的各种交易流程。

1.3. 定义

- 接口设备　Interface Device
  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
  为完成交易而在交易点安装的设备，用于同 IC 卡的连接。
- 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。

- 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。
- 明文 Plaintext
  没有加密的信息。
- 密文 Ciphertext
  通过密码系统产生的不可理解的文字或信号。
- 密钥 Key
  控制加密转换操作的符号序列。
- 加密算法 Cryptographic Algorithm
  为了隐藏或揭露信息内容而变换数据的算法。
- 认证机构 Certification Authority
  利用公开密钥和其他相关数据为所有者提供可靠校验的第三方机构。
- 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。
- DES 算法
  DES 是一个对称算法，加密和解密用的是同一算法。DES 的安全性依赖于所用的密钥。
- 保密密钥 Secret Key
  对称加密技术中仅供指定实体所用的密钥。
- 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。
- 电子钱包 Electronic Purse
  一种为方便持卡人进行小额消费而设计的 IC 卡应用，它支持圈存、消费等交易。除圈存外，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）。
- 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、取现等交易。
- 圈存 Load
  持卡人将其在银行相应账户上的资金划转到电子存折或电子钱包中。
- 圈提 Unload
  持卡人将其在电子存折中的部分或全部资金划回到其在银行的相应账户上。

1.4. 缩略语与符号

ADF	应用数据文件（Application Definition File）
AEF	应用基本文件（Application Elementary File）
AID	应用标识符（Application Identifier）
An	字母数字型（Alphanumeric）

ans	字母数字及特殊字符型（Alphanumeric Special）
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）
CLA	命令类别（Chip Card Payment Service）
CLK	时钟（Clock）
cn	压缩数字（Compressed Numeric）
DDF	目录数据文件（Directory Definition File）
DF	专用文件（Dedicated File）
DIR	目录（Directory）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
f	频率（Frequency）
GND	地(Ground)
IFS	信息域（Information Field）
INS	命令报文的指令字节（Instruction Byte of Command Message）
I/O	输入/输出（Input/Output）
Lc	终端发出的命令数据的实际长度（Exatct Length of Data Sent）
Le	响应数据中的最大期望长度（Maximum Length of Data Expected）
MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件（Mater File）
N	数字型（Numeric）
O	可选型（Optional）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
P3	参数 3（Parameter 3）
PIN	个人密码（Personal Identification Number）
RFU	保留为将来所用（Reserved for Future Use）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
TLV	标签、长度、值（Tag Length Value）
TAC	交易验证码（Transaction Authorization Cryptogram）
VCC	电源电压（Supply Voltage）
V_{PP}	Vpp 触点上的测量电压（Programming Voltage Message VCC Contact）

1.5. 参考资料

- ISO 7816-1: Identification cards - Integrated circuit(s) cards with contacts – Physical characteristics-1987/07/01
- ISO 7816-2: Identification cards - Integrated circuit(s) cards with contacts – Dimensions and location of the contacts-1998/05/15
- ISO 7816-3: Identification cards - Integrated circuit(s) cards with contacts – Electronic signals and transmission protocols-1989
- ISO 7816-4: Identification cards - Integrated circuit(s) cards with contacts – Inter-industry commands for interchange-1994/07/08
- ISO 7816-5: Identification cards - Integrated circuit(s) cards with contacts – Numbering system and registration procedure for application identifiers-1992/09/24
- ISO 7816-6: Identification cards - Integrated circuit(s) cards with contacts – Inter-industry data elements-1994/07/08
- EMV'96 Integrated Circuit Card Specification for Payment System
- EMV'96 Integrated Circuit Card Application Specification for Payment System
- 《中国金融集成电路（IC）卡规范 2.0》

2. 系统介绍

2.1. 特性

华大双界面卡是华大自主开发，拥有自主产权的一款高性能 CPU 卡，配合自主开发的高安全性的 CPU 卡操作系统 MCOS。

华大双界面卡具有以下特性：

- 符合带触点的集成电路卡标准《ISO/IEC 7816-1/2/3/4》
  符合《ISO/IEC14443》TypeB 非接触卡接口标准
  符合《中国金融集成电路（IC）卡规范 2.0》
- 一体化设计：接触接口和非接触接口共用一个 CPU 进行控制
- 接触模式和非接触模式自动选择
- 可靠性高 、操作方便快捷、防冲突
- 支持一卡多应用，各应用之间相互独立（多应用、防火墙功能）。
- 支持多级目录管理。
- 支持多种文件类型，包括透明文件、记录文件、安全文件、 循环文件、电子钱包文件及电子存折文件。
- 支持安全数据传输，提供明文、加密、校验和加密校验四种传输模式。
- 支持多种安全访问方式和权限（认证功能和口令保护）。
- 支持中国人民银行认可的 Single DES、Triple DES 算法。
- 支持中国人民银行规定的电子钱包和电子存折功能。
- 支持数据镜像及支付交易保护功能。
- 携带 DES 协处理器。
- 支持多波特率，最高波特率可达 78.13 Kbps。
- 8K EEPROM 存储容量。
- 10 年以上数据保持时间，10 万次以上重复擦写。
- 工作电压：5 V
- 工作温度：-25℃ ~ +70℃
- 时钟频率：1 ~ 5 MHz

2.2. 接触部分通讯传输机制

2.2.1. 复位应答（ATR）

卡片在出厂时，有卡片厂商来设定选择下列三种复位应答模式之一：

1．不支持模式选择（缺省）
2．Negotiable(协商)模式
3．Special（特殊）模式

2.2.1.1. 模式选择

根据设定的模式决定复位应答信息和通讯波特率。

1. 不支持模式选择

卡片在该模式下，复位应答返回后，只能以缺省波特率通讯。

COS 向接口设备发送复位应答序列，结构如下：

3B	6x（‘1’~‘F’）	00	00	历史字节（0~15 字节）

2. 支持模式选择，先进入 Negotiable(协商) 模式

1) 冷复位后，接收到 PPS ，则按协商后得到的 Fn 、Dn 进行通讯，此时，热复位将进入 Special 模式 （指定按 Fn , Dn 通讯），不能再切换模式。
2) 冷复位后，没有 PPS ，收到 APDU 命令，按缺省波特率 Fd、Dd 通讯，此时，热复位将进入 Special 模式 （指定按 Fd , Dd 通讯），不能再切换模式。
3) 冷复位后，没有 PPS ，没有收到 APDU 命令，此时，热复位将进入 Special 模式（指定按 Fi , Di 通讯），可以通过热复位继续切换到 Negotiable 模式。

冷复位 COS 向接口设备发送复位应答序列，结构如下：

3B	7x（‘1’~‘F’）	Fi Di	00	00	历史字节（0~15 字节）

PPS 协商后的热复位，COS 向接口设备发送复位应答序列，结构如下：

3B	Fx（‘1’~‘F’）	Fn Dn	00	00	10	80	历史字节（0~15 字节）

其中 Fn、Dn 值为协商的值。Fd <= Fn <= Fi ， Dd <= Dn <= Di 。

无 PPS，收到 APDU 命令后热复位，COS 向接口设备发送复位应答序列，结构如下：

3B	Fx（‘1’~‘F’）	Fd Dd	00	00	10	80	历史字节（0~15 字节）

无 PPS，直接热复位，COS 向接口设备发送复位应答序列，结构如下：

3B	Fx（‘1’~‘F’）	Fi Di	00	00	10	00	历史字节（0~15 字节）

3. 支持模式选择，先进入 Special（特殊） 模式

1) 冷复位后，收到 APDU 命令，按 Fi、Di 通讯，此时，热复位进入 Special 模式 （指定按 Fi , Di 通讯），不能再切换模式。

2) 冷复位后，没有收到 APDU 命令，此时，热复位将进入 Negotiable 模式（协商按 Fi , Di 通讯），可以通过热复位继续切换到 Special 模式。

冷复位 COS 向接口设备发送复位应答序列，结构如下：

3B	Fx（‘1’~‘F’）	Fs Ds	00	00	10	00	历史字节（0~15 字节）

收到 APDU 命令后热复位，COS 向接口设备发送复位应答序列，结构如下：

3B	Fx（‘1’~‘F’）	Fs Ds	00	00	10	80	历史字节（0~15 字节）

冷复位后直接热复位，COS 向接口设备发送复位应答序列，结构如下：

3B	7x（‘1’~‘F’）	Fi Di	00	00	历史字节（0~15 字节）

Fi = Fs , Di = Ds

2.2.1.2. PPS

2.2.1.2.1. 请求和响应的结构和内容

PPS 请求和响应分别包括一个初始字节 PPSS,后面是格式字节 PPS0,三个可选参数字节 PPS1,PPS2,PPS3 和一个检验字节 PCK 作为最后一个字节。

PPSS 标识了 PPS 请求或响应并等于’FF’。

PPS0 根据位 b5,b6,b7 是否等于 1 来指明可选字节 PPS1,PPS2,PPS3 是否存在。

PPS1 允许向卡建议 F 和 D 的值。PPS2 和 PPS3 留作未来使用。

PCK 的值是这样的，以致使所有字节 PPSS 至 PCK 的异或运算结果为空。

2.2.1.2.2. 处理流程

1) 接口设备发送 PPS-Request 序列到卡；

2) 如果卡接收到一个错误的 PPS-Request 序列（错误 PPS-Request 序列的定义是：PPSS＝‘FF’而其它部分有错。如果 ATR 后接口设备发送的第一个字节不是‘FF’，则不应视其为错误的

PPS-Request 序列，而应视其为正常命令的 CLA 字节），卡不应做任何响应；如果此时热复位，则按没有发送 PPS 的情况响应。

3) 如果卡接收到正确的 PPS-Request 序列，卡应发送一个 PPS-Response 序列；

2.2.1.3. 历史字节

注：历史字节由卡厂在对卡做初始化处理时嵌入卡系统， 格式和内容可自由定义。如用户无特殊要求，按顺序定义以下内容：

MID： 2 字节，芯片商注册标识号——‘0081’（中国华大）

MC2： 1 字节，COS 标识，ASCII 编码 ------‘4D’

MC1： 1 字节，COS 主版本号+次版本号，BCD 编码------‘48’

MC0： 1 字节，COS 修订版本号，BCD 编码------‘00’

2.3. 射频部分通讯传输机制

2.3.1. 射频接口概述

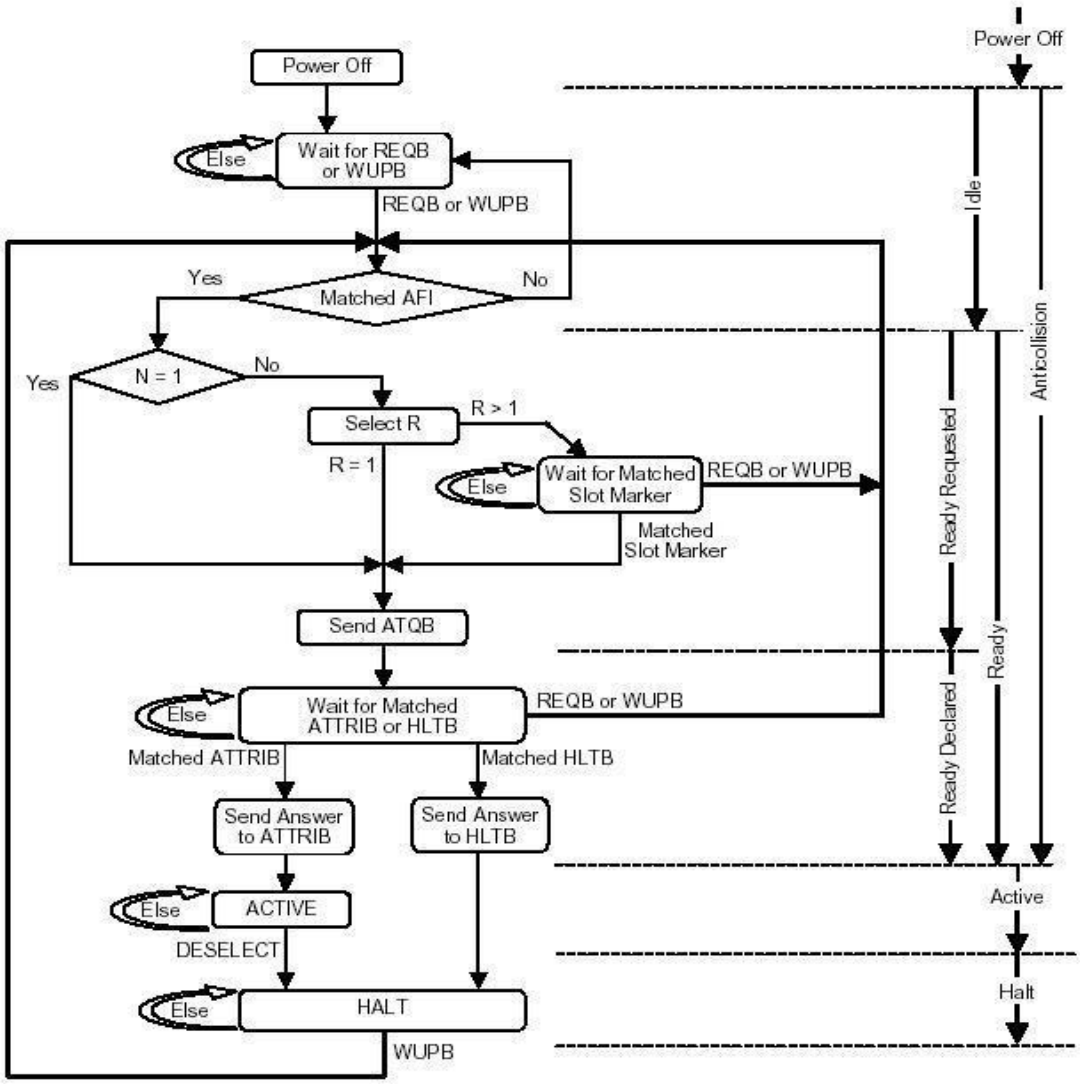
卡进入射频工作场并获得足够能量后，首先要完成防冲突处理流程，然后进入应用处理流程，处理应用层的命令。

2.3.1.1. 防冲突处理流程

卡感应到最小场强即进入 IDLE 状态，这时，卡被上电，只能响应 REQB/WUPB 命令。

收到正确的 REQB/WUPB 命令后即进入 READY-REQUESTED 状态,如果命令中的 AFI 与自己的 AFI 相符，则判断时隙数 N，如果 N=1,则返回 ATQB,进入 READY-DECLARED 状态。如果 N≠1，则在卡内产生一个 1-N 之间的随机数 R， 如果 R=1 则返回 ATQB,进入 READY_DECLARED 状态。如果 R>1 则等待时隙数为 R 的 SLOT_MARKER 命令后，发送 ATQB 命令，进入 READY_DECLARED 状态。此时，卡也可以响应 REQB/WUPB 命令，重新回到 READY-REQUESTED 状态。进入 READY_DECLARED 状态后，卡可识别 REQB/WUPB 命令，ATTRIB 命令，HALT 命令。当接收到 REQB/WUPB 命令，则又重新回到 READY-REQUESTED 状态。当接收到 HALT 命令，则进入 HALT 状态，此时，卡只响应 WUPB 命令。当接收到 ATTRIB 命令，如果与自己的 PUPI 不同，则仍处于 READY_DECLARED 状态，相同则返回响应，进入 ACTIVE 状态，此时，卡将只响应应用层命令和 DESELECT 命令。

下面是防冲突流程图：



2.3.1.2. 应用层处理流程

卡进入 ACTIVE 状态后，即进入了应用层处理流程，此时，只响应应用层命令和 DESELECT 命令。

应用层处理流程中，卡与读卡器的交互由三种数据块组成，分别是 I-BLOCK、 R-BLOCK、S-BLOCK。其中：

I-BLOCK 用来传输应用层的信息。

R-BLOCK 用来传输命令的应答(ACK /NAK)。

S-BLOCK 用来交换控制信息，包括两种类型：

其一，延长等候时间，包括 1 字节 INF。
其二，DESELECT 命令。

读卡器与卡之间的通讯有一定的规则，见下面：

交互过程中，第一块数据块总是由读卡器发出。
无论是卡或读卡器，当收到的 I-BLOCK 指示有后续块时，须返回 R(ACK)块。
S-BLOCK 只能成对出现。卡可发 S-BLOCK(WTX)来取代 I-BLOCK 或 R-BLOCK 应答,来请求延长等候时间。
卡如果收到 I-BLOCK,不是串传输，则应返回 I-BLOCK 应答。
卡如果收到 R(ACK)或 R(NAK),数据块号与当前数据块号相等，则上一次的 数据块被重发。
卡如果收到 R(NAK),数据块号与当前数据块号不同，则返回 R(ACK)。
卡如果收到 R(ACK),数据块号与当前数据块号不同，则继续传输。
当通讯错误和协议错误发生时，卡不做任何恢复，返回到接收模式，等待读卡器发送命令。
对于读卡器，除成串传输和 DESELECT 命令之外，当出现超时和无效数据块时，返回 R(NAK)。
对于读卡器，当成串传输时，当出现超时和无效数据块时，返回 R(ACK)。
对于读卡器，当发 DESELECT 命令没有返回时，可继续发 DESELECT 或忽略掉此卡。
当读卡器收到 R(ACK) 数据块时，如果块号与当前数据块号不同，则重发上一次的 I-BLOCK。
当读卡器收到 R(ACK) 数据块时，如果块号与当前数据块号相同，则继续传输。

读卡器和卡分别有自己当前的数据块号，规则如下：
对于读卡器: 初始数据块号为 0。
当收到的 R-BLOCK 或 I-BLOCK 为当前数据块号，则数据块号被翻转。
对于卡: 初识数据块号为 1。
当收到 I-BLOCK 时，翻转数据块号。
当收到 R-BLOCK(ACK)时，如果数据块号不为当前数据块号，翻转数据块号。

2.3.2. 射频通讯格式

2.3.2.1. 防冲突命令格式

ANTICMD	CRC
N Bytes	2 Bytes

ANTICMD：防冲突流程中的命令， N > 0。

2.3.2.2. 防冲突命令返回数据格式

DATA	CRC_ B

DATA：响应数据。

2.3.2.3. 应用层命令格式

协议头		命令应用数据单元	协议尾
PCB 1 Byte	CID 1 Byte（可选）	见表格 1	CRC 2 bytes

命令头				命令体		
CLA	INS	P1	P2	(Lc field)	数据域	(Le field)

表格 1 —— 命令应用数据单元

命令可以分为两种格式

格式	命令组成
2	CLA INS P1 P2 Le
3	CLA INS P1 P2 Lc Data

PCB： 协议控制字节
CID： 分配的 ID 号
CRC ： 帧校验码。

2.3.2.4. 应用层返回数据格式

协议头		响应数据单元	协议尾
PCB 1 Byte	CID 1 Byte（可选）	见表格 2	CRC 2 bytes

应答体	应答尾部

响应数据体	SW1	SW2

表格 2 —— 响应应用数据单元

PCB： 协议控制字节
CID： 卡分配的识别号
CRC ： 帧校验码。

2.3.3. 命令描述

2.3.3.1. 射频防冲突命令

防冲突命令只能在防冲突处理流程中使用，包括：

命令	功能描述
REQB/WUPB	建立通讯连接
Slot-MARKER	轮询命令
ATTRIB	分配卡识别号
HLTB	暂停卡命令

2.3.3.1.1. REQB/WUPB（建立通讯连接）

卡处于 IDLE、READY 状态响应 REQB 命令
卡处于 IDLE、READY、HALT 状态响应 WUPB 命令

2.3.3.1.1.1. 命令格式

05（Apf）	P1（AFI）	P2（PARAM）	CRC_B(2 bytes)

05：登录邀请
P1：应用类别号，编码如下：
00：全类别
2X：金融类别
其余：预留
P2：编码如下：

B8	b7	b6	b5	b4	b3	b2	b1
RFU				REQB/WUPB	时隙数		

b4 = 0 REQB 命令，卡处于 IDLE 或 READY 状态响应。
b4 = 1 WUPB 命令，卡处于 IDLE 或 READY 或 HALT 状态响应。

b3	b2	b1	N 时隙数（十进制）
0	0	0	1

0	0	1	2
0	1	0	4
0	1	1	8
1	0	0	16
RFU			缺省

2.3.3.1.1.2. 响应信息

卡内根据 P2 参数，产生 1 至时隙数之间的一个随机数 R，如果 R11，结束该命令，准备接收 Slot-MARKER 或新的 REQB/WUPB 命令；如果 R=1，按下列格式返回 ATQB：

50	PUPI 4 Bytes	IIN 4 Bytes	Protocol Info 3 Bytes	CRC_B 2 Bytes

PUPI： 伪唯一卡标识，由卡随机产生。

IIN： 芯片管理信息，由证卡内部提供。由 IIN 内容定义如下：

00 1 Byte	00 1 Byte	00 1 Byte	00 1 Byte

Protocol Info：该信息指示卡所支持的参数， 它的具体格式如下：

波特率 8 位	最大帧长度 4 位	协议类型 4 位	FWI 4 位	RFU 2 位	F0 2 位
00000000	1000	0001	1100	00	01

波特率： 支持双向 106Kbit/s

最大帧长度：256 字节

协议类型： 支持 ISO/IEC 14443-4

FWI： FWT = 1.237 Sec.

F0： 只支持 CID

2.3.3.1.2. Slot-MARKER（轮询）

在 REQB/WUPB 命令之后，读写机具可发送至多（N-1）个时隙数来定义每一个时隙的开始。时隙可以在读写机具收到对 REQB/WUPB 命令应答的返回数据结束（或无应答）之后被发送，以便标记下一个时隙的开始。

2.3.3.1.2.1. 命令格式

Apn	CRC_B

x5	2bytes

Apn：x 表示时隙数，编码 1-F 分别表示十进制时隙数：2-16。

2.3.3.1.2.2. 响应信息

如果 x 与上一条 REQB/WUPB 命令卡生成的时隙数匹配，则卡返回 ATQB。

2.3.3.1.3. ATTRIB（分配卡识别号）

读写机具发送的 ATTRIB 命令包括选择单个证卡所需要的信息。收到一个带有其标识符（PUPI）的 ATTRIB 命令的证卡即被选中，并分配到一个专用信道。在选中之后，该证卡仅响应带有其 CID（CID=00 表示通配）的命令。

2.3.3.1.3.1. 命令格式

1D	PUPI	P1	P2	P3	CID	CRC_B

PUPI： 伪唯一卡标识，由卡随机产生。

P1： 最小 TR0、TR1 时间，数据帧需要 SOF 和 EOF。

P2： 读卡器可接收的最大帧长度。

P3： 传输协议是否符合 ISO/IEC 14443-4。

CID： 读写机具为卡分配的识别号，取值范围为：00-0E。

2.3.3.1.3.2. 响应信息

1 字节		2 字节
MBLI	CID	CRC_B

MBLI：0

CID：回送卡接收到的 CID 参数。

2.3.3.1.4. HLTB 命令

使卡处于暂停状态，响应此命令后，卡只对 WUPB 命令有响应。

2.3.3.1.4.1. 命令描述

50	PUPI(4 bytes)	CRC_B(2 bytes)

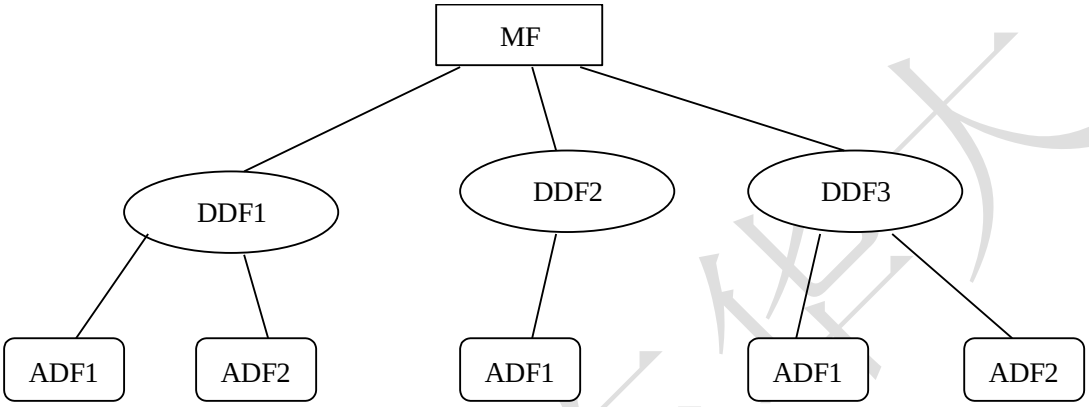
2.3.3.1.4.2. 响应信息

00	CRC_ B

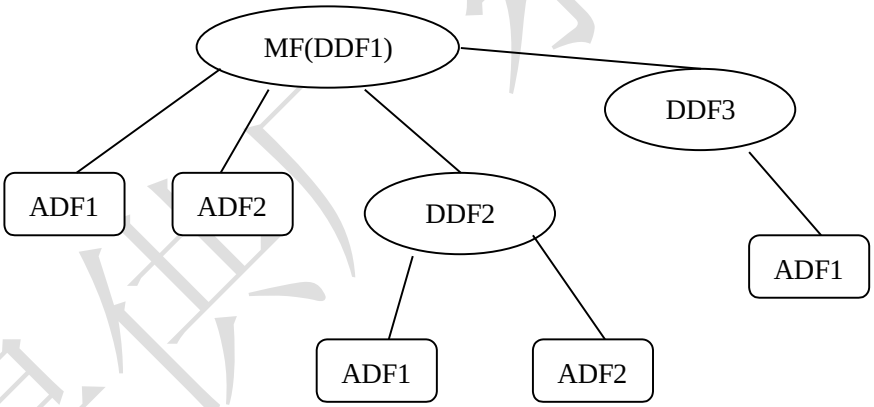
2.4. 一般性说明

本卡所支持的应用系统的组织架构如下：

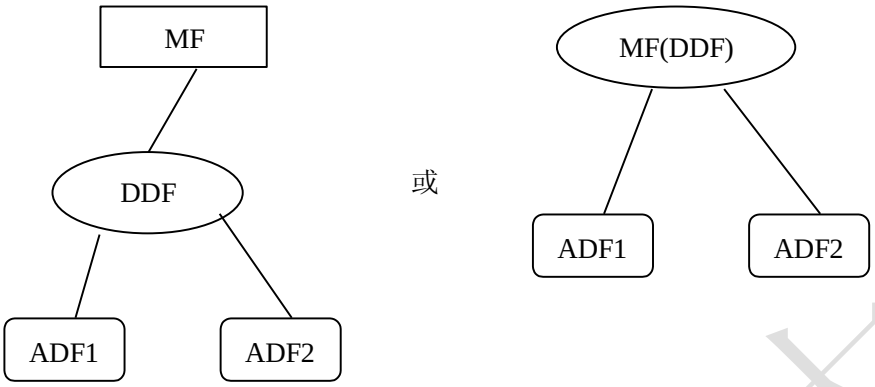
1．多应用平衡架构



2．多应用主次架构



3．单应用架构



2.4.1. 文件系统概述

华大双界面卡允许在可用空间内建立自己的文件系统。支持多层目录结构。在同层目录中文件不能有相同的 ID（标识符）。

三种专用文件（DF）类型：

MF： 根目录，是整个文件系统的根，同属应用环境类。MF 下可以有 EF（基本文件）、SF（安全文件）、DDF(目录文件)、ADF（应用文件）；

DDF： 目录文件，用于定义一个应用环境，它是应用的集合。DDF 下可以有 ADF、子 DDF、EF 和 SF 等结构。

ADF： 应用文件，用于定义具体应用。ADF 下可以有 EF 和 SF。

四种基本文件（EF）类型：

透明文件： 文件数据是通过连续空间中的字节地址进行存取。

记录文件： 数据以固定长度格式记录在文件中，文件内最多可以容纳 255 条记录。以明文方式存取时，最大记录长度可以 255 个字节；以安全方式存取时，最大记录长度为 64 个字节。记录文件有以下几种形式：

1、线性定长记录文件： 同一文件内的所有记录都是等长度的。

2、线性变长记录文件： 同一文件内的每个记录的长度可以不相等。支持 TLV 和 V 两种记录格式。

3、循环定长记录文件： 同一文件内的所有记录都是等长度的。支持对文件中的记录循环存取。

交易文件： 该类文件为特定格式文件。通过交易命令对这类文件进行操作。交易文件有以下几种形式：

1、电子存折文件： 完成圈存、消费等交易。执行交易命令前须提交用户口令。适用于金融环境。

2、电子钱包文件： 完成圈存和消费交易。执行圈存交易前须提交用户口令。适用于金融环境。

安全文件类型（SF）：

安全文件：该文件只能写入不能读出。文件内可存放密钥或口令。

应用环境：支持金融应用环境。

2.4.2. 支持多波特率

华大双界面卡支持多波特率通信。

2.5. 文件结构

下面定义了华大双界面卡支持的文件类型。所有文件的标识符（FID）不能为‘0000’和‘FFFF’。

2.5.1. MF 文件

MF 是根目录，是整个文件系统的根，同属应用环境类。可从任何应用内进入根目录 MF。在执行 FREEZE MF 命令之前，卡处于应用开发状态，可以重新建立 MF，为开发应用提供了调试的途径。

MF 文件头信息中的主要参数说明如下：

File-ID（2 字节）： 文件标识符。固定为’3F00’

App-Type（1 字节）： 环境类型 ’00’

RFU 保留字节（1 字节）： 固定为’00’

ATR-SFI（1 字节）： ATR 文件的短文件标识符。卡上电复位后，ATR 文件的内容，作为复位应答信息（ATR）的历史字节被发送。最大 15 个字节，该文件的类型为透明文件。如 ATR-SFI =’00’时，表示卡内不设置 ATR 文件，卡会给出缺省的 ATR 内容。

DIR-SFI（1 字节）： 目录文件的短文件标识符。该文件的类型为线性记录文件。
DIR-SFI =’00’时，表示 MF 下不设置目录文件。

FCI-SFI（1 字节）： FCI 文件的短文件标识符。选择应用时，FCI 文件的内容作为 SELECT FILE 命令的响应数据从卡内送出。FCI 文件的类型为透明文件。
FCI-SFI =’00’时，表示 MF 下不设置 FCI 文件。

ACw（1 字节）： MK 控制属性，控制 MK 重装方式。
(MK：MF 的主控密钥（卡片主控密钥/环境主控密钥）。短标识符为‘00’（KID=‘00’）。在 MF 下建立文件时，须认证此密钥。)

Write							
EPL	0	CER	CIPH	KT	0	0	0

bit7 EPL，当 EPL=’1’时，电子钱包消费记录交易明细。
bit6 保留‘0’。
bit5 CER，校验码（MAC）。当 CER=‘1’时，WRITE KEY 命令的数据域中要附有校验码（MAC）。

bit4	CIPH，数据加密。当 CIPH='1'时，WRITE KEY 命令的数据域为密文。
bit3	KT，标识 MF-Key 的长度，KT='0'时 MK 的长度为 8 字节，KT='1'时 MK 的长度为 16 字节。
bit2~bit0	保留'0'。

RLD-KID（1 字节）：MK 的重装密钥的短标识符。重装 MK 时，加密数据和计算 MAC 所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

BLK-KID（1 字节）：环境锁定密钥的短标识符。执行 CARD BLOCK 命令时，计算 MAC 所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

Limit-Value（1 字节）：密钥认证限制数。MK 的尝试次数，最大可设置为 15 次，Limit-Value 减为 0 时，密钥被锁定。Limit-Value 设置为 0 值时，限制数为无限大。

MF-Name（1-16 字节）：MF 的应用名称（可选）

2.5.2. DDF 文件

DDF 文件用于创建一个应用环境。在该环境下可建立若干与应用环境相关的 ADF、EF 和 SF 等，也可建立 DDF。在 DDF 下，只能选择其范围内直接的 DDF、ADF、EF 和 SF 文件。

DDF 文件头信息中的主要参数说明如下：

File-ID（2 字节）：文件标识符。

LNG（2 字节）：文件体空间

App-Type（1 字节）：环境类型 '00'

RFU 保留字节（2 字节）：固定为'0000'

DIR-SFI（1 字节）：目录文件的短文件标识符。该文件的类型为线性记录文件。DIR-SFI ='00'时，表示 DDF 下不设置目录文件。

FCI-SFI（1 字节）：FCI 文件的短文件标识符。选择 DDF 时，FCI 文件的内容作为 SELECT FILE 命令的响应数据从卡内送出。FCI 文件的类型为透明文件。FCI-SFI ='00'时，表示 DDF 下不设置 FCI 文件。

ACw（1 字节）：DDF 主控密钥控制属性，控制 DDF 主控密钥重装方式。
(MK：DDF 的主控密钥（环境主控密钥）。短标识符为'00'（KID='00'）。在 DDF 下建立文件时，须认证此密钥。)

Write							
EPL	0	CER	CIPH	KT	KP1	0	KACT

bit7 EPL，当 EPL=’1’时，电子钱包消费记录交易明细。

bit6 保留’0’

bit5 CER，校验码（MAC）。当 CER=’1’时，WRITE KEY 命令的数据域中要附有校验码（MAC）。

bit4 CIPH，数据加密。当 CIPH=’1’时，WRITE KEY 命令的数据域为密文。

bit3 KT，标识 MK 的长度，KT=’0’时 MK 的长度为 8 字节，KT=’1’时 MK 的长度为 16 字节。

bit2 KP1，标识 RLD-KID 所指密钥的位置，KP1=’0’时，RLD-KID 所指密钥在当前 DDF 下，KP1=’1’时，RLD-KID 所指密钥在父目录下。

bit1 保留’0’

bit0 MK 的有效性。

KACT=’0’表示不存在 MK。可通过父目录下的主控密钥按 ACw 定义的方式建立 MK。当卡复位后，在该应用环境下不可建立任何形式的应用和文件。

KACT=’1’表示 MK 已经存在。缺省值为全’0’。密钥长度由 KT 设定。

RLD-KID（1 字节）：MK 的重装密钥的短标识符。重装 MK 时，加密数据和计算 MAC 所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

BLK-KID（1 字节）：环境锁定密钥的短标识符。执行 CARD BLOCK 命令时，计算 MAC 所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

Limit-Value（1 字节）：密钥认证限制数。MK 的尝试次数，最大可设置为 15 次，Limit-Value 减为 0 时，密钥被锁定。Limit-Value 设置为 0 值时，限制数为无限大。

DDF-Name（1-16 字节）：DDF 的应用名称（可选）

2.5.3. ADF 文件

ADF 文件用于定义一个具体的应用。在该应用下可建立多个 EF 和 SF。

ADF 文件头信息中的主要参数说明如下：

File-ID（2 字节）：文件标识符。

LNG（2 字节）： 文件体空间

RFU 保留字节（4 字节）： 固定为’00000000’

FCI-SFI（1 字节）： FCI 文件的短文件标识符。选择 ADF 时，FCI 文件的内容作为 SELECT FILE 命令的响应数据从卡内送出。FCI 文件的类型为透明文件。FCI-SFI =’00’时，表示卡 ADF 下不设置 FCI 文件。

ACw（1 字节）： MK 控制属性，控制 MK 重装方式。

(MK：ADF 的主控密钥（应用主控密钥）。短标识符为‘00’（KID=‘00’）。在 ADF 下建立文件时，须认证此密钥。)

Write							
EPL	AV2	CER	CIPH	KT	KP1	KP2	KACT

bit7 EPL，当 EPL=’1’时，电子钱包消费记录交易明细。

bit6 AV2，当 AV2=’1’时，PBOC2.0 版本信息位于 FCI 专用信息之前；当 AV2=’2’时，版本信息位于 FCI 专用信息之后。

bit5 CER，校验码（MAC）。当 CER=’1’时，WRITE KEY 命令的数据域中要附有校验码（MAC）。

bit4 CIPH，数据加密。当 CIPH=’1’时，WRITE KEY 命令的数据域为密文。

bit3 KT，标识 MK 的长度，KT=’0’时 MK 的长度为 8 字节，KT=’1’时 MK 的长度为 16 字节。

bit2 KP1，标识 RLD-KID 所指密钥的位置，KP1=‘0’时，RLD-KID 所指密钥在当前 ADF 下，KP1=‘1’时，RLD-KID 所指密钥在父目录下。

bit1 PINL，PIN 权限和读权限的逻辑关系。PINL=‘0’时，为‘与’的关系；PINL=‘1’时，为‘或’的关系。

bit0 KACT，MK 的有效性。

KACT=‘0’表示不存在 MK。可通过父目录下的主控密钥按 ACw 定义的方式建立 MK。当卡复位后，又没有建立 MK，在该应用下不可建立任何形式的文件。

KACT=‘1’表示 MK 已经存在。缺省值为全‘0’。密钥长度由 KT 设定。

RLD-KID（1 字节）： MK 的重装密钥的短标识符。重装 MK 时，加密数据和计算 MAC 所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

BLK-KID（1 字节）： 应用锁定密钥的短标识符。在 ADF 下，执行 APPLICATION BLOCK

命令时，计算 MAC 所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

Limit-Value（1 字节）：密钥认证限制数。MK 的尝试次数，最大可设置为 15 次，Limit-Value 减为 0 时，密钥被锁定。Limit-Value 设置为 0 值时，限制数为无限大。

ADF-Name（1-16 字节）：ADF 的应用名称（可选）。

2.5.4. 透明文件

透明文件的文件体是一个连续的区域，以字节为存取单元。

透明文件头信息中的主要参数说明如下：

File-ID（2 字节）：文件标识符。以 SFI 访问时，文件标识符的低五位有效，只能访问到第一个文件。

LNG（2 字节）：文件体空间

RFU 保留字节（1 字节）：固定为’00’

ACr（1 字节）：文件的读控制属性。

READ							
PMK	CMK	CER	CIPH	0	0	PINL	MPIN

bit7 PMK，认证当前环境主控密钥（MK）。PMK=‘1’时，执行读命令前，必须通过当前环境（MF/DDF）主控密钥（MK）的认证。

bit6 CMK，认证当前应用主控密钥（MK）。CMK=‘1’时，执行读命令前，需要通过当前应用主控密钥（MK）的认证。在 MF/DDF 下执行读命令，该位无意义。

bit5 CER，校验码（MAC）。当 CER=’1’时，读命令的数据域中要附有校验码（MAC）。

bit4 CIPH，数据加密。当 CIPH=‘1’时，从卡内读出的数据为密文。

bit3-bit2 保留‘0’。

bit1 PINL，PIN 权限和读权限的逻辑关系。PINL=‘0’时，为‘与’的关系；PINL=‘1’时，为‘或’的关系。

bit0 MPIN，认证 PIN。MPIN=‘1’时，在执行读命令前，需要通过 PIN 的认证。

ACw（1 字节）： 文件的写控制属性

UPDATE							
PMK	CMK	CER	CIPH	DISA	DISU	PINL	MPIN

bit7 PMK，认证当前环境主控密钥（MK）。PMK=‘1’时，在执行写命令前，必须通过当前环境（MF/DDF）主控密钥（MK）的认证。

bit6 CMK，认证当前应用主控密钥（MK）。CMK=‘1’时，执行写命令前，需要通过当前应用主控密钥（MK）的认证。在 MF/DDF 下执行写命令，该位无意义。

bit5 CER，校验码（MAC）。当 CER=‘1’时，写命令的数据域中要附有校验码（MAC）。

bit4 CIPH，数据加密。当 CIPH=‘1’时，写命令的数据域为密文。

bit3 DISA，禁止添加。DISA=‘1’时，禁止向文件添加数据。

bit2 DISU，禁止修改。DISU=‘1’时，禁止修改文件内的数据。

bit1 PINL，PIN 权限和写权限的逻辑关系。PINL=‘0’时，为‘与’的关系；PINL=‘1’时，为‘或’的关系。

bit0 MPIN，认证 PIN。MPIN=‘1’时，在执行写命令前，需要通过 PIN 的认证。

Read-Right（2 字节）：文件的读权限。和 ACr 一起控制文件的读操作。高字节为全局读权限，低字节为局部读权限。

Write-Right（2 字节）：文件的写权限。和 ACw 一起控制文件的写操作。高字节为全局写权限，低字节为局部写权限。

RT-KID（1 字节）：读密钥的短标识符。执行读命令时，加密数据和计算校验码（MAC）所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

WT-KID（1 字节）：写密钥的短标识符。执行写命令时，加密数据和计算校验码（MAC）所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

2.5.5. 记录文件

记录文件中每条记录以固定长度记录数据。记录文件既可按记录号方式访问，也可按标签方式（TAG）访问。

记录文件头信息中的主要参数说明如下：

File-ID（2 字节）：文件标识符。以 SFI 访问时，文件标识符的低五位有效，只能访问到第一个文件。

RF（1 字节）：记录数据格式（‘01H’：TLV 格式；‘00H：非 TLV 格式’）。

ACr（1 字节）：文件的读控制属性。

READ							
PMK	CMK	CER	CIPH	0	0	PINL	MPIN

bit7 PMK，认证当前环境主控密钥（MK）。PMK=‘1’时，在执行读命令前，必须通过当前环境（MF/DDF）主控密钥（MK）的认证。

bit6 CMK，认证当前应用主控密钥（MK）。CMK=‘1’时，执行读命令前，需要通过当前应用主控密钥（MK）的认证。在 MF/DDF 下执行读命令，该位无意义。

bit5 CER，校验码（MAC）。当 CER=‘1’时，读命令的数据域中要附有校验码（MAC）。

bit4 CIPH，数据加密。当 CIPH=‘1’时，从卡内读出的数据为密文。

bit3-bit2 保留‘0’。

bit1 PINL，PIN 权限和读权限的逻辑关系。PINL=‘0’时，为‘与’的关系；PINL=‘1’时，为‘或’的关系。

bit0 MPIN，认证 PIN。MPIN=‘1’时，在执行读命令前，需要通过 PIN 的认证。

ACw（1 字节）：文件的写控制属性

ACw 定义为：

UPDATE							
PMK	CMK	CER	CIPH	DISA	DISU	PINL	MPIN

bit7 PMK，认证当前环境主控密钥（MK）。PMK=‘1’时，在执行写命令前，必须通过当前环境（MF/DDF）主控密钥（MK）的认证。

bit6 CMK，认证当前应用主控密钥（MK）。CMK=‘1’时，执行写命令前，需要通过当前应用主控密钥（MK）的认证。在 MF/DDF 下执行写命令，该位无意义。

bit5 CER，校验码（MAC）。当 CER=‘1’时，写命令的数据域中要附有校验码（MAC）。

bit4	CIPH，数据加密。CIPH=‘1’时，写命令的数据域为密文。
bit3	DISA，禁止添加。DISA=‘1’时，禁止向文件添加数据。
bit2	DISU，禁止修改。DISU=‘1’时，禁止修改文件内的数据。
bit1	PINL，PIN 权限和写权限的逻辑关系。PINL=‘0’时，为‘与’的关系；PINL=‘1’时，为‘或’的关系。
bit0	MPIN，认证 PIN。MPIN=‘1’时，在执行写命令前，需要通过 PIN 的认证。

Read-Right（2 字节）：文件的读权限。和 ACr 一起控制文件的读操作。高字节为全局读权限，低字节为局部读权限。

Write-Right（2 字节）：文件的写权限。和 ACw 一起控制文件的写操作。高字节为全局写权限，低字节为局部写权限。

RT-KID（1 字节）：读密钥的短标识符。执行读命令时，加密数据和计算校验码（MAC）所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

WT-KID（1 字节）：写密钥的短标识符。执行写命令时，加密数据和计算校验码（MAC）所用密钥的短标识符。该密钥的用途为传输密钥或主控密钥。

2.5.5.1. 线性定长记录文件

线性定长记录文件中的每条记录长度一致。

线性定长记录文件头信息中还需要以下参数：

RL（1 字节）：每条记录的长度。

RN（1 字节）：文件中可容纳的最大记录个数。

RE（1 字节）：当前记录个数。当前已存在的记录个数。在建立文件时，用户可设定一初始值，其值小于等于 RN。RE=’00’表示文件内无记录存在。

2.5.5.2. 线性变长记录文件

线性变长记录文件中的记录长度可以不一致。记录一旦建立添加，其长度不可改变。

线性变长记录文件头信息中还需要以下参数：

LNG（2 字节）：文件体空间。

2.5.5.3. 循环定长记录文件

循环定长记录文件中的每条记录长度一致。循环定长记录文件支持循环存取记录数据。

最新添加的一条记录，记录号为 1；上一条添加的记录， 记录号为 2；依此类推。

循环定长记录文件头信息中还需要以下参数：

RL（1 字节）： 每条记录的长度。

RN（1 字节）： 文件中可容纳的最大记录个数。

RE（1 字节）： 当前记录个数。当前已存在的记录个数。在建立文件时，用户可设定一初始值，其值小于等于 RN。RE='00'表示文件内无记录存在。

2.5.6. 交易文件

交易文件是一种特殊的文件结构。文件体为固定长度。只有交易命令才能对其操作。

2.5.6.1. 电子钱包(EP)文件

建立电子钱包(EP)文件时所用参数说明如下：

File-ID（2 字节）： 文件标识符。不能为'0000H'和'FFFFH'。

Bala-Limit（4 字节）： 余额上限。持卡人所能持有的最高金额值。

电子钱包文件是专用文件。只能建立在 ADF 下。文件体为固定长度。只有交易命令才能对其操作。

电子钱包文件体为 8 个字节。其内容定义为：

EP 脱机交易计数器（2 字节）： 电子钱包脱机交易的序号。

EP 联机交易计数器（2 字节）： 电子钱包联机交易的序号。

EP 余额（4 字节）： 电子钱包中可供支配的金额值。

与电子钱包文件相关的 KEY 和文件有：

DPKep： 消费密钥。其标识符固定为'02xxH'。其中'xx'为密钥索引号。密钥长度 16 个字节。

DLKep： 圈存密钥。其标识符固定为'09xxH'。其中'xx'为密钥索引号。密钥长度 16 个字节。

DTKep： 交易认证密钥（TAK）。其标识符固定为'0CxxH'。其中'xx'为密钥索引号。密钥长度 16 个字节。

List： 交易记录明细文件。为循环定长记录文件，其标识符固定为'0018H'。 文件体最小为记录长度 23 个字节，记录个数 10 条。

2.5.6.2. 电子存折(ED)文件

建立电子存折(ED)文件时所用参数说明如下：

File-ID（2 字节）： 文件标识符。不能为‘0000H’和‘FFFFH’。
Bala-Limit（4 字节）： 余额上限。持卡人所能持有的最高金额值。

电子存折文件是专用文件。只能建立在 ADF 下。文件体为固定长度。只有交易命令才能对其操作。

电子存折文件体为 11 个字节。其内容定义为：

ED 脱机交易计数器（2 字节）： 电子存折脱机交易的序号。
ED 联机交易计数器（2 字节）： 电子存折联机交易的序号。
ED 余额（4 字节）： 电子存折中可供支配的金额值。
透支限额（3 字节）： 最多允许透支的金额值。

与电子存折文件相关的 KEY 和文件有：

DPKed： 消费/取现密钥。其标识符固定为‘02xxH’。其中‘xx’为密钥索引号。密钥长度 16 个字节。
DLKed： 圈存密钥。其标识符固定为‘09xxH’。其中‘xx’为密钥索引号。密钥长度 16 个字节。
DULKed： 圈提密钥。其标识符固定为‘0AxxH’。其中‘xx’为密钥索引号。密钥长度 16 个字节。
DUKed： 修改透支限额密钥。其标识符固定为‘0BxxH’。其中‘xx’为密钥索引号。密钥长度 16 个字节。
DTKed： 交易认证密钥（TAK）。其标识符固定为‘0CxxH’。其中‘xx’为密钥索引号。密钥长度 16 个字节。
List： 交易记录明细文件。为循环定长记录文件，其标识符固定为‘0018H’。文件体最小为记录长度 23 个字节，记录个数 10 条。

2.5.7. 安全文件（内部）

安全文件只能写入不能读出。一个安全文件可存有多个密钥和口令。密钥和口令可通过 WRITE KEY 命令写入卡内。

标识符为‘00’的密钥定义为主控密钥。一个 DF 下只能有一个主控密钥。主控密钥的建立是随 DF 一起建立的，可通过 WRITE KEY 命令更新主控密钥值。详细内容请参照 WRITE KEY 命令。

建立安全文件时所用参数说明如下：

File-ID（2 字节）： 文件标识符。

LNG（2 字节）： 文件体空间。

ACw（1 字节）： 文件的写控制属性。

Reload				Append			
PMK	CMK	CER	CIPH	0	0	CER	CIPH

bit7 PMK，认证父目录主控密钥（MK）。PMK=‘1’时，在 ADF 下执行修改 KEY 命令前，需要通过父目录主控密钥（MK）的认证。如果在 MF/DDF 下执行修改 KEY 命令，则该位无意义。

bit6 CMK，认证当前主控密钥（MK）。CMK=‘1’时，执行修改 KEY 命令前，需要通过当前主控密钥（MK）的认证。

bit5 CER，校验码。当 CER=‘1’时，修改 KEY 命令的数据域中要附有校验码（MAC）数据。

bit4 CIPH，数据加密。当 CIPH=‘1’时，修改 KEY 命令的数据域为密文。

Bit3~bit2 保留‘0’。

bit1 CER，校验码。当 CER=‘1’时，新建 KEY 命令的数据域中要附有校验码（MAC）数据。用于计算校验码的 KEY 固定为当前主控密钥。

bit0 CIPH，数据加密。当 CIPH=‘1’时，新建 KEY 命令的数据域为密文。用于加密数据的 KEY 固定为当前主控密钥。

Write-Right（2 字节）： 密钥的修改权限。和 ACw 一起控制密钥的修改操作。高字节为全局修改密钥权限，低字节为局部修改密钥权限。详细说明参见“安全管理”一章。

WT-KID（1 字节）： 重装密钥的短标识符。执行修改密钥命令时，加密数据和计算校验数据所用 KEY 的短标识符。该密钥的用途为传输密钥，或主控密钥。

密钥分类定义如下：

密钥类型	适用范围
类型 1	内部认证密钥、外部认证密钥
类型 2	传输密钥
类型 3	交易密钥
类型 4	PIN

密钥数据信息格式：

字节数 / 类型	1	1	1	1	2	1	1	8 或 16
类型 1	用途	标识	版本	算法	Access-Right	Limit	SSB	Key-Data
类型 2	用途	标识	00	算法	Access-Right	Limit	00	Key-Data
类型 3	用途	索引	版本	算法	Access-Right	00	00	Key-Data
类型 4	用途	00	UBK	RLK	Access-Right	Limit	00	PIN（8）

注：

1、金融环境下，PIN 的有效长度 2~6 个字节。

2、对于类型 4 情况下的 PIN，数据信息格式中的 UBK 指的是解锁 PIN 密钥的标识符；RLK 指的是重装 PIN 密钥的标识符。

3、对于类型 4，标识为’00’ ，SSB 为’00’。

参数说明：

标识： 密钥的标识符。取值范围在‘00H’—‘7FH’之间。标识为‘00H’的密钥定义为主控密钥（MK）。

用途： 密钥用途定义如下：

用途	说明	密钥类型	相关命令
00	外部认证密钥	1	外部认证
01	传输密钥	2	“数据传输”
02	消费密钥	3	交易命令/计算命令
09	圈存密钥	3	交易/计算命令
0A	圈提密钥	3	交易/计算命令
0B	修改透支密钥	3	交易/计算命令
0C	交易认证密钥（TAC）	3	交易/计算命令
1C	内部认证密钥	1	内部认证
1F	口令	4	PIN 认证

索引： 密钥的引用序列号。

版本： 密钥的版本序号。

算法： 安全算法。’00’为 3DES 算法；’01’为单 DES 算法。

Access-Right： 密钥的使用权限。高字节为全局使用权限，低字节为局部使用权限。详细说

明参见“安全管理”一章。

Limit： 密钥认证限制数。连续认证失败的次数，最大设置为 15 次，Limit 减为 0 时，密钥和 PIN 被锁定或应用被永久锁定。Limit 设置为 0 值时，认证限制数为无限大。

SSB： 安全级别。详细说明参见“安全管理”一章。

Key-Data： 密钥数据。其有效长度为 8 字节或 16 字节。密钥的长度取决于加密算法。采用 3DES 算法的密钥长度为 16 字节，采用单 DES 算法的密钥长度为 8 字节。

PIN： 口令数据，其有效长度为 2~6 字节。第一次新建口令时，PIN 值为 8 字节其组成是：PIN 值=有效字节+填充数据’FF’（6~2 字节）。而更
PIN 时只输入有效值（2~6），不需要填充数据’FF’。
例如：PIN 值为‘1234’
新建口令：PIN 值=‘1234FFFFFFFFFFFF’
更新口令：PIN 值=‘1234’

UBK： 解锁密钥的短标识符。执行口令解锁命令时，加密数据和计算校验数据所用 KEY 的短标识符。该密钥的用途为传输密钥，或主控密钥。

RLK： 重装密钥的短标识符。执行口令重装命令时，加密数据和计算校验数据所用 KEY 的短标识符。该密钥的用途为传输密钥，或主控密钥。

3. 安全管理

3.1. 安全状态

安全状态是指卡当前所处的一种安全级别，卡的环境目录（DDF）和当前应用目录（ADF）分别具有 16 种不同的安全级别。在卡内用两个寄存器（16 位，每一位对应一个级别）表示整个环境的安全状态，称为全局安全状态字；两个寄存器（16 位，每一位对应一个级别）表示当前应用的安全状态，称为局部安全状态字。如果当前目录为 DDF 或 MF，局部安全状态无意义。四个寄存器的初始值为 0。

内存中安全状态字中的安全级别状态，是通过对 KEY/PIN 进行认证，认证成功后，将 KEY/PIN 记录中的安全级别字节（SSB）映射到相应的安全状态字来求得的，若密钥在 DDF 或 MF 下，则映射到全局安全状态字；若密钥在 ADF 下，则映射到局部安全状态字。SSB 的高 4 位表示安全级别区间的下限（1~15）， 低 4 位表示安全级别区间的上限（1~15），该字节值为‘XY’，表示认证成功后可以获得 X 至 Y 区间内的安全级别。映射的方法是：根据 SSB 指定的安全级别区间，对相应安全状态字中 X 至 Y 之间的所有位置 1。例如：SSB=‘46’，那么认证通过后，寄存器的第 4、5、6 位置‘1’；若 SSB=‘AD’，则认证通过后，寄存器的第 10、11、12、13 位置‘1’。

若 SSB 为‘00’或‘X’>‘Y’，表示对安全状态没有影响。

全局安全状态在当前 DDF 或 MF 整个工作期间有效，直到卡被重新复位或选择新的 DDF。局部安全状态只在一个 ADF 下有效，当从一个 ADF 变换到另一个 ADF（包括重新选择当前的 ADF）时，局部安全状态的内容被复位。

3.2. 文件访问权限

Right 定义了文件操作条件，2 个字节表示，高字节对应环境目录（DDF 或 MF）下的安全状态（或称全局安全状态），低字节对应当前 ADF 的安全状态（或称局部安全状态）。每个字节的高 4 位表示安全状态区间的下限（1~15）， 低 4 位表示安全状态区间的上限（1~15），该字节值为‘XY’， X ≤ Y 表示应获得相应安全状态字中 X 至 Y 区间内的安全级别；该字节值为‘0Y’，相应操作不受限制；若 X ≥ Y，表示相应操作被禁止。

综上所述，判别访问权限是否满足的方法是：

1. 如果 Right 字节为‘0X’格式，则满足访问条件；

2. 如果 Right 字节 X > Y，则无法满足访问条件，访问被禁止；

3. 如果 Right 字节 X ≤ Y，则检查安全状态字中 X 至 Y 区间内是否有‘1’存在，若有则满足访问条件；若无则不满足访问条件。

3.3. 数据交换模式

在卡的操作权限得到满足后，还要使用文件指定的数据交换模式才能正确地读写数据。

终端与卡之间的数据交换有四种模式：数据可以是明文、密文、明文加校验和密文加校验。命令根据被存取对象的存取模式控制字 ACx 采用相应的数据交换模式（如“READ BINARY”要根据当前透明文件的存取条件信息 ACwr 中指定的数据交换模式将数据读出）。

针对密文、明文加校验和密文加校验的数据交换模式，数据必须由 8/16 个字节组成一个数据块， 并以数据块为单位对数据加密或产生校验码 MAC。

安全数据交换的目的是保证数据的可靠性、数据完整性和对发送方的认证。数据完整性和对发送方的认证通过使用校验码来实现。数据的可靠性通过对数据域的加密来得到保证。

安全报文传送格式符合 ISO 7816-4 的规定，当 CLA 字节的后半字节等于十六进制‘4’时，表明对发送方命令数据要采用安全报文传送。对基本文件操作的命令报文数据是否使用安全报文传送取决于对 ACx 中 CER 和 CIPH 的设置。当 CER 和 CIPH 中的任一项为‘1’时，表明使用安全报文传送。

3.3.1. 明文模式

如果对数据传输的安全性、完整性以及对发送方的认证都没有要求，可以采用明文模式。数据交换中的明文模式就是命令报文的数据域中和响应报文的数据域中的数据不经过任何形式的变换处理直接传送。

3.3.2. 加密模式

如果侧重于数据在传输中的安全性，可以采用加密模式。数据交换中的加密模式就是命令报文的数据域中和响应报文的数据域中的数据先经过加密变换，然后再放在相应的数据域中传送。数据是如何加密的，请看下面数据加密一节。

3.3.3. 校验模式

如果侧重于数据在传输中的完整性和对数据发送方进行认证，可以采用校验模式。校验模式就是对命令报文的所有内容或响应报文的所有内容使用一个算法进行加密得到一个 4 字节的

校验码（MAC），然后把它放在命令报文或响应报文的数据域中发送。有关校验码的计算，请看下面 MAC 的计算一节。

3.3.4. 加密校验模式

如果既要求数据在传输中的安全性又要求数据在传输中的完整性和对数据发送方进行认证，可以采用加密校验模式。加密校验模式就是首先对命令报文数据域中或响应报文数据域中的数据进行加密；接着把命令报文数据域中或响应报文数据域中的明文数据替换为加密数据，再对命令抱文的所有内容或响应报文的所有内容使用一个算法进行加密得到一个 4 字节的校验码（MAC）；最后把报文数据域中或响应报文数据域中的数据替换为加密数据，再把校验码紧接在加密数据之后发送。数据域中的数据是怎样被加密的以及命令头和加密后的数据或加密后的响应报文数据是怎样作为输入数据产生校验码（MAC）的，请看下面加密数据和 MAC 的计算各节。

3.3.5. 模式控制字 Acx

文件的读、修改和添加等操作采用的具体模式是由文件头中的模式控制字 ACx 决定的。并且一旦确定某个存取功能的存取模式，以后将无法修改。对 ACx 的定义参见“文件结构”一节。当 ACx 中的 CER=‘1’时，表示安全报文传送必须使用校验模式；当 ACx 中的 CIPH=‘1’时，表示安全报文传送必须使用加密模式。

3.4. 安全计算

安全计算包括了华大双界面卡中涉及的各种安全算法。它们有：密钥分散计算，过程密钥计算、安全鉴别数据、校验码（MAC）的计算、数据加密和解密计算等。

校验码（MAC）总是命令或命令响应数据域中最后一个数据元素。规定 MAC 的长度为 4 个字节。当命令的数据域中要求带有 MAC 时，即命令安全报文传送，命令头中 CLA 字节的低半字节必须为十六进制数‘4’。

3.4.1. DES 算法

3.4.1.1. DES 在金融环境中的安全管理

3.4.1.1.1. 密钥分散的计算方法

密钥分散通过分散因子产生子密钥。

分散因子为 8 字节，将一个双长度的主密钥 MK，对分散数据进行处理，推导出一个双长度的子密钥 DK，如图 3-1-1 和图 3-1-2。

推导 DK 左半部分的方法是：

第一步： 将分散因子作为输入数据；
第二步： 将 MK 作为加密密钥；
第三步： 用 MK 对输入数据进行 3DEA 运算。

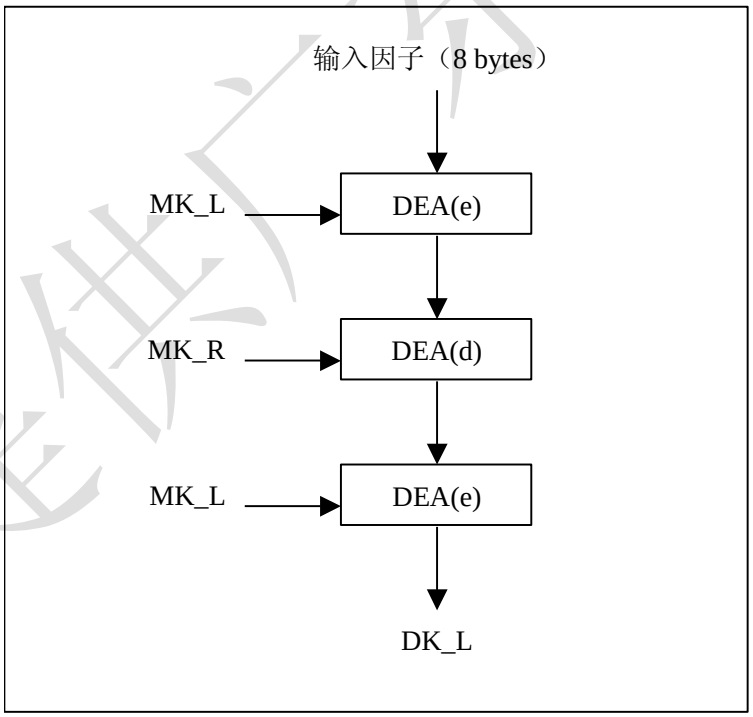


图 3-1-1 推导 DK 左半部分

推导 DK 右半部分的方法是：

第一步： 将分散因子求反，作为输入数据；

第二步： 将 MK 作为加密密钥；
第三步： 用 MK 对输入数据进行 3DEA 运算。

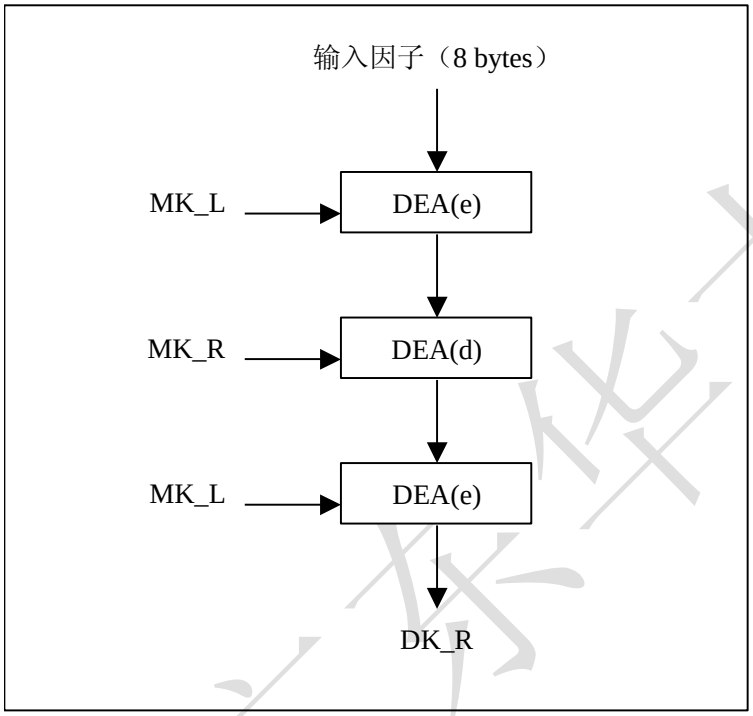


图 3-1-2 推导 DK 右半部分

3.4.1.1.2. 过程密钥的计算方法

3.4.1.1.2.1. 过程密钥的计算方法 1

该方法来源于 PBOC。

该方法是通过指定密钥对过程密钥输入因子（8 字节）进行 3DEA 或 DEA 计算产生过程密钥。如图 3-1-3 和图 3-1-4。

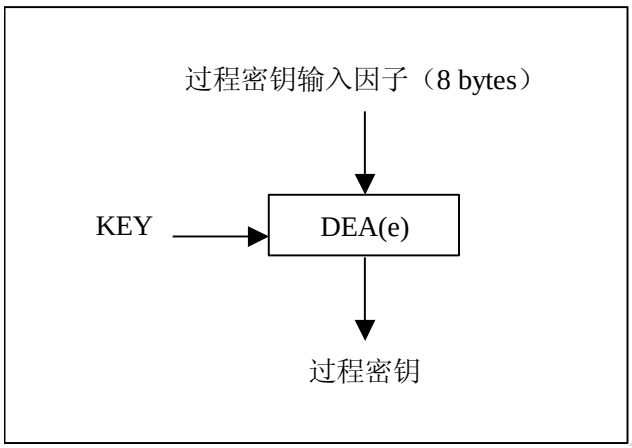


图 3-1-3 单倍长密钥产生过程密钥

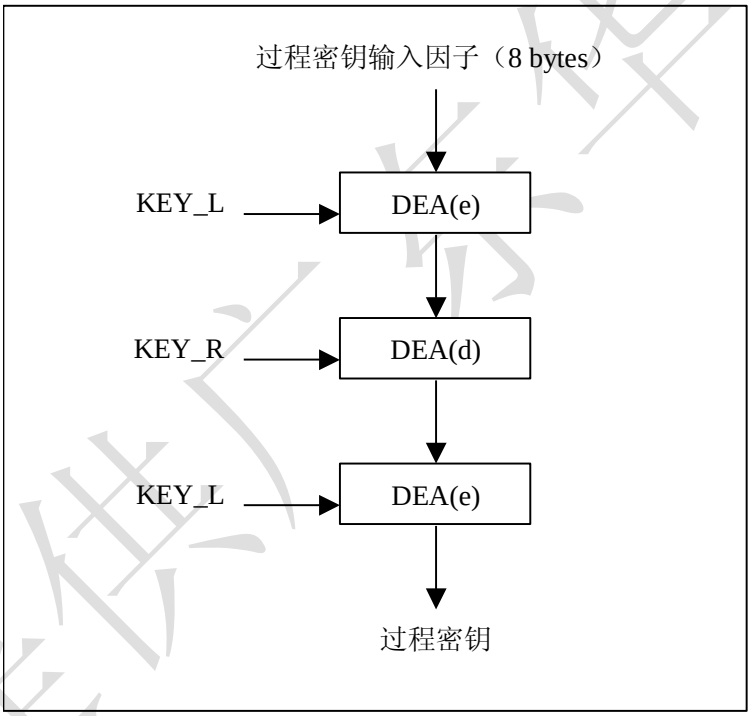


图 3-1-4 双倍长密钥产生过程密钥

3.4.1.1.2.2. 过程密钥的计算方法 2

该方法来源于 PBOC 标准。

该方法是通过对指定的双倍长密钥进行左右异或计算来产生单倍长过程密钥。如图 3-1-5。

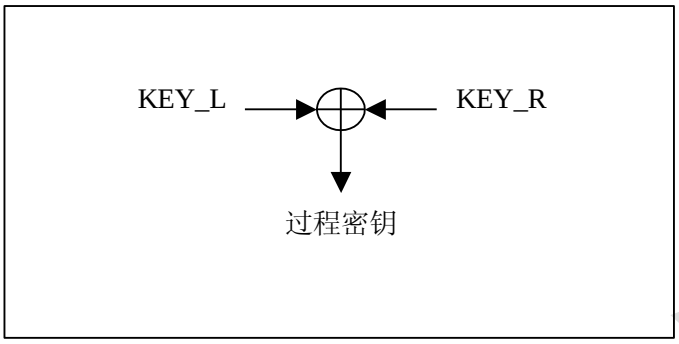


图 3-1-5 过程密钥产生

3.4.1.1.3. 鉴别数据的计算方法

该方法来源于 PBOC 标准。

该方法是通过指定的密钥（单倍长或双倍长）对鉴别数据输入因子（8 字节）进行 DEA 计算产生鉴别数据，供 IC 卡或接口设备进行验证。如图 3-1-6 和图 3-1-7。

按照如下方式使用 DEA 加密方式产生 MAC：

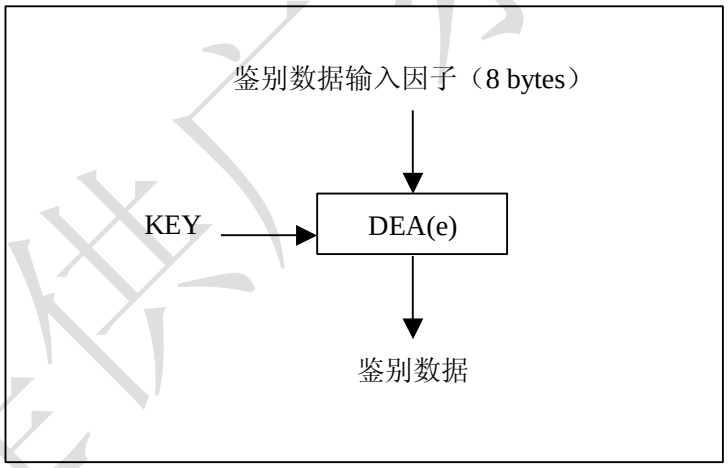


图 3-1-6 单倍长密钥的鉴别数据的计算

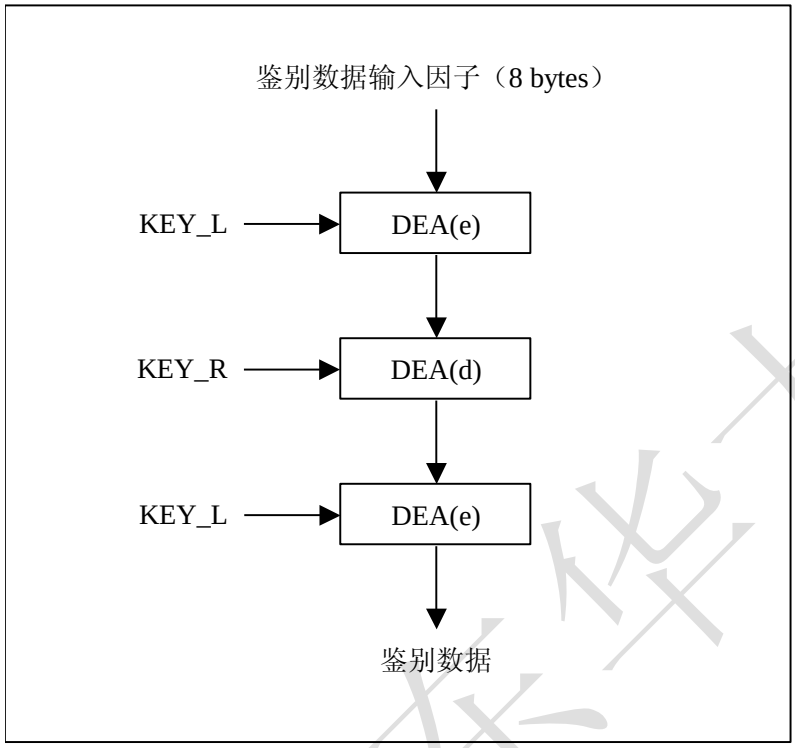


图 3-1-7　双倍长密钥的鉴别数据的计算

3.4.1.1.4.　MAC 的计算方法

3.4.1.1.4.1.　命令安全报文中的 MAC

该方法来源于 PBOC 标准。

命令安全报文中的 MAC 是使用命令的所有元素（包括命令头和命令数据域中的数据）来产生的。以保证命令连同数据能够正确完整地传送，并对发送方进行认证。

按照如下方式使用 DEA 加密方式产生 MAC：

第一步：　终端通过向 IC 卡发 GET CHALLENGE 命令获得一个 4 字节随机数，后补'00 00 00 00'作为初始值。

第二步：　将 5 字节命令头（CLA，INS，P1，P2，Lc）和命令数据域中的明文或密文数据连接在一起形成数据块。注意，这里的 Lc 应是数据长度加上将计算出的 MAC 的长度（4 字节）后得到的实际长度。

第三步：　将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。

第四步：　如果最后的数据块的长度是 8 字节的话，则在该数据块之后再加一个完整的 8 字节数据块'80 00 00 00 00 00 00 00'，　转到第五步。

如果最后的数据块的长度不足 8 字节，则在其后加入 16 进制数'80'，如果达到 8

字节长度，则转到第五步；否则接着在其后加入 16 进制数‘00’直到长度达到 8 字节。

第五步： 按照图 3-1-8 和图 3-1-9 所述的算法对这些数据块使用指定密钥进行加密来产生 MAC。

第六步： 最终取计算结果（高 4 字节）作为 MAC。

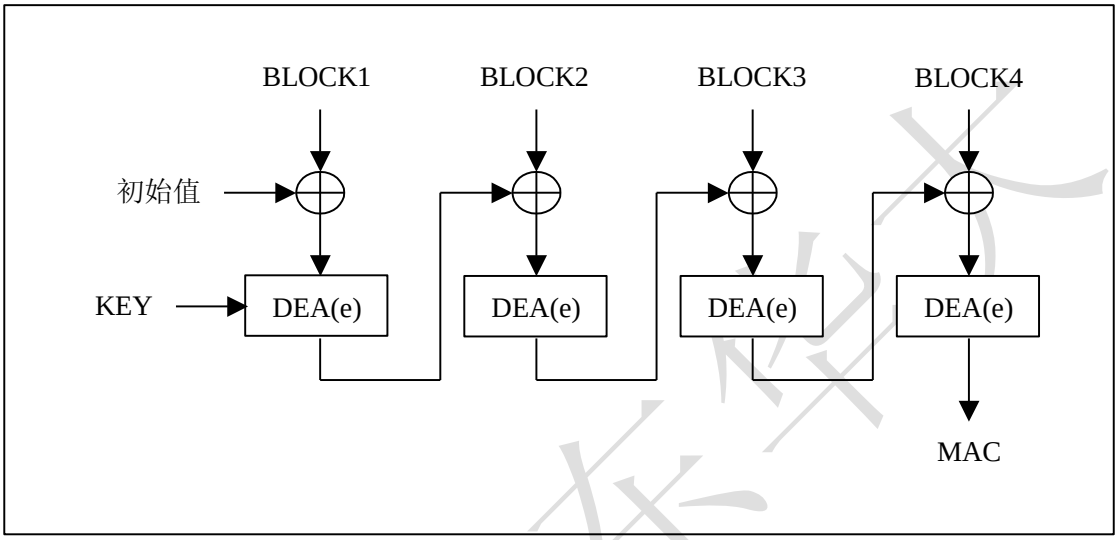


图 3-1-8 安全报文中单倍长密钥 MAC 计算

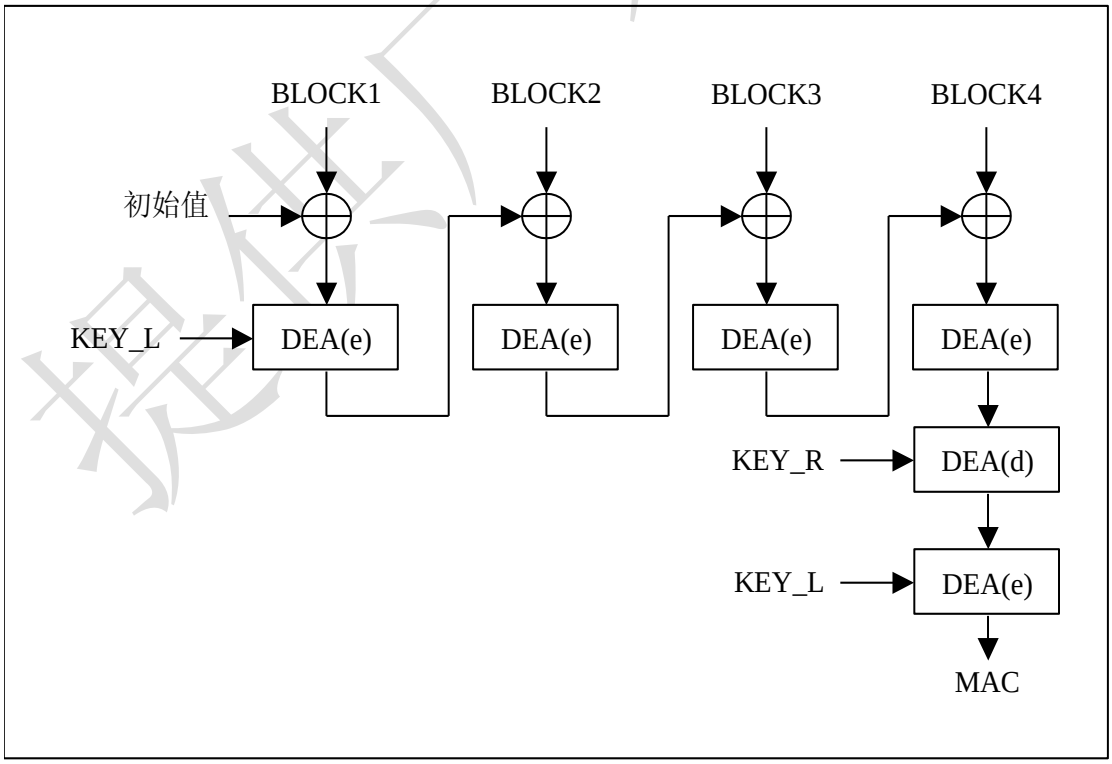


图 3-1-9 安全报文中双倍长密钥 MAC 算法

3.4.1.1.4.2. 交易中的 MAC

交易中的 MAC 计算使用此方法。计算方法分二步完成。先用指定密钥产生过程密钥（请参看 3.4.1.1.2 节过程密钥计算），再用过程密钥计算 MAC。

ED/EP 交易中的 MAC 是使用不同交易指定的数据元序列来产生的。从而保证交易的安全性。按照如下方式使用过程密钥 DEA 算法产生 MAC：

第一步： 将一个 8 字节长的初始值设定为 16 进制数‘00 00 00 00 00 00 00 00’

第二步： 将所有输入数据按指定顺序连接成一个数据块。

第三步： 将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。

第四步： 如果最后的数据块的长度是 8 字节的话，则在该数据块之后再加一个完整的 8 字节数据块‘80 00 00 00 00 00 00 00’，转到第五步。

如果最后的数据块的长度不足 8 字节，则在其后加入 16 进制数‘80’，如果达到 8 字节长度，则转到第五步；否则在其后加入 16 进制数‘00’直到长度达到 8 字节。

第五步： 按照图 3-1-10 所述的算法对这些数据块使用过程密钥（单倍长度）进行加密来产生 MAC。

第六步： 最终取计算结果（高 4 字节）作为 MAC。

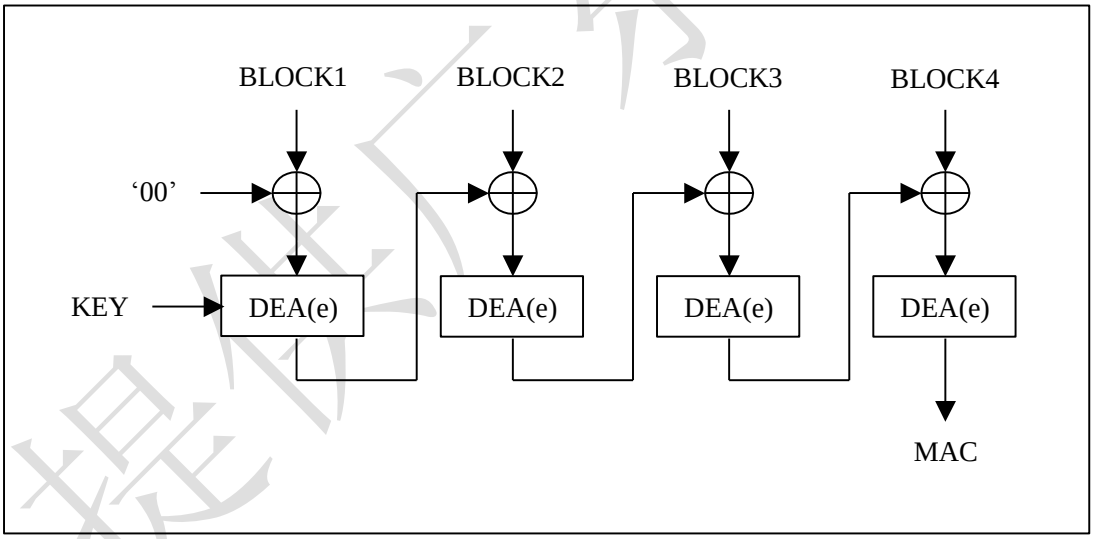


图 3-1-10 ED/EP 交易中的 MAC 算法

3.4.1.1.5. 数据加密的计算方法

按照如下方式对数据进行加密：

第一步： 用 L_D（1 字节）表示明文数据的长度，在明文数据前加上 L_D 产生新的数据块。

第二步： 将该数据块分成 8 字节为单位的数据块，表示为 BLOCK1、BLOCK2、BLOCK3、BLOCK4 等。最后的数据块有可能是 1~8 个字节。

第三步： 如果最后（或唯一）的数据块的长度是 8 字节的话，转到第四步；如果不足 8 字节，则在其后加入 16 进制数‘80’，如果达到 8 字节长度，则转到第四步；否则在其后加入 16 进制数‘00’直到长度达到 8 字节。

第四步： 按照图 3-1-11 和图 3-1-12 所述的算法使用指定密钥对每一个数据块进行加密。

第五步： 计算结束后，所有加密后的数据块依照原顺序连接在一起。

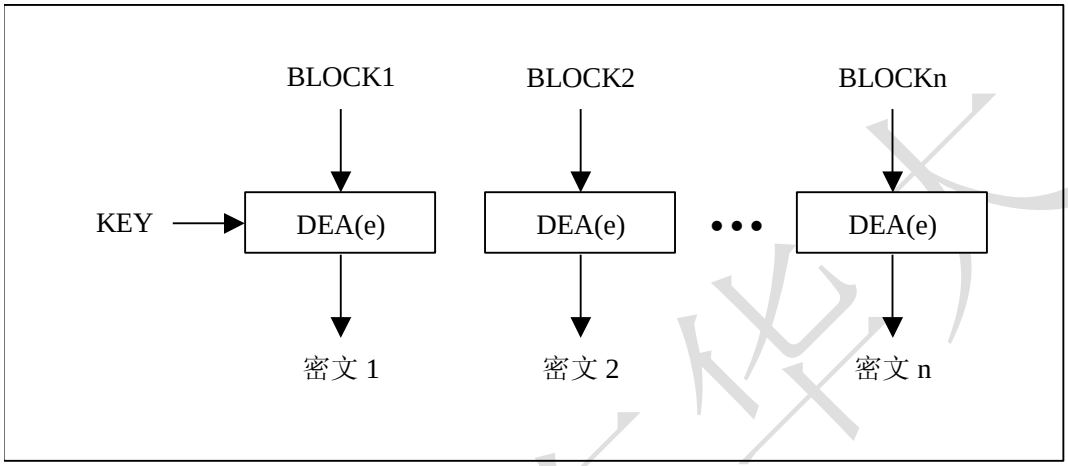


图 3-1-11 单倍长密钥 DEA 数据加密算法

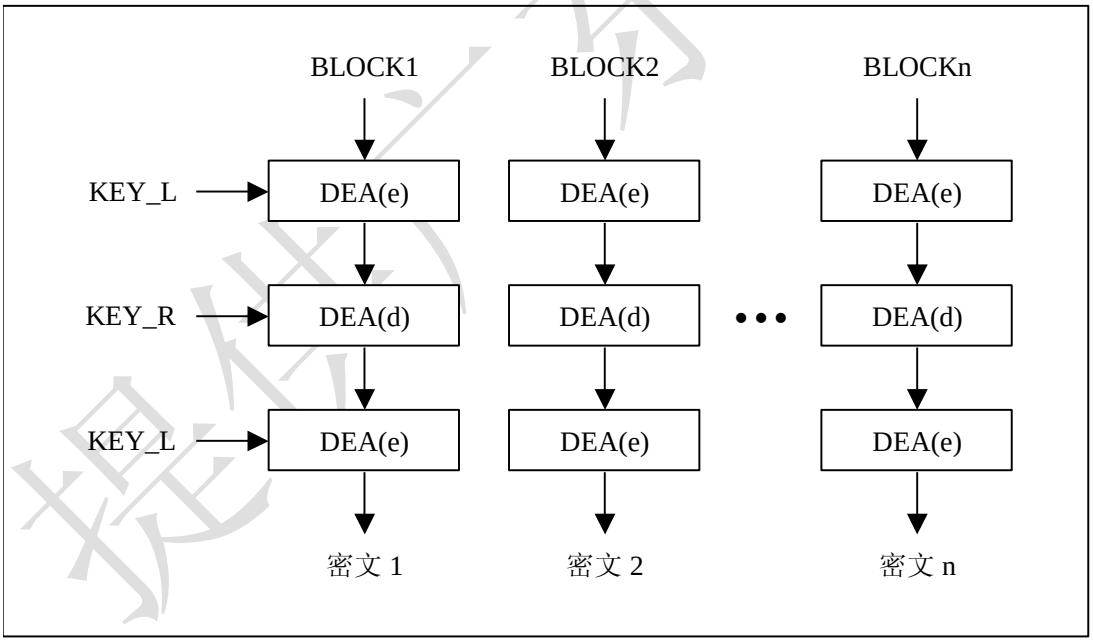


图 3-1-12 双倍长密钥 DEA 数据加密算法

3.4.1.1.6. 数据解密的计算方法

数据解密则采用相反的过程，如图 3-1-13 和图 3-1-14。

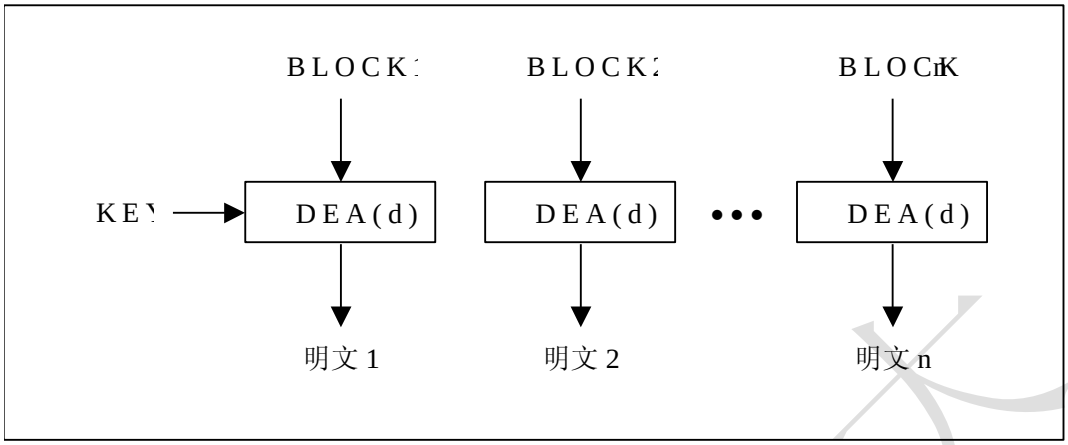


图 3-1-13 单倍长密钥 DEA 数据解密算法

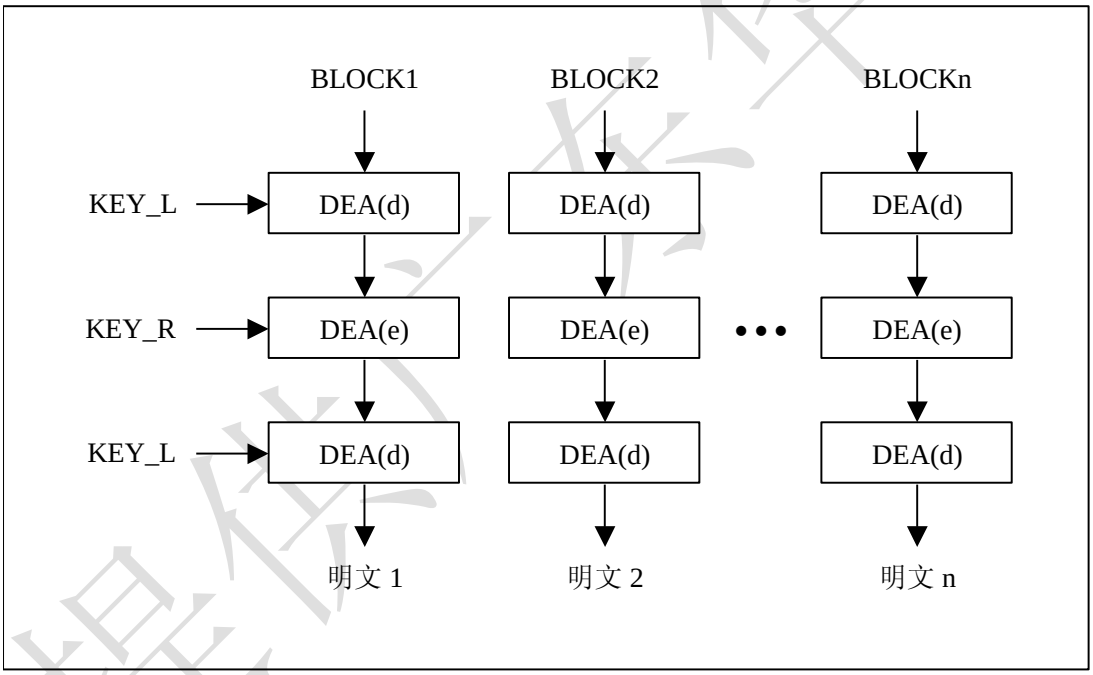


图 3-1-14 双倍长密钥 DEA 数据解密算法

3.5. 安全报文传送的命令情况

3.5.1. CASE 1

这种情况时，命令中没有数据送到卡（Lc）中，也没有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2

含安全报文的命令：	CLA	INS	P1	P2	Lc	MAC

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = MAC 的长度，4 字节。

3.5.2. CASE 2

这种情况时，命令中没有数据送到卡（Lc）中，有数据从卡中返回（Le）。

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

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = MAC 的长度，4 字节。

3.5.3. CASE 3

这种情况时，命令中有数据送到卡（Lc）中，没有数据从卡中返回（Le）。

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

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = 数据的长度 + MAC 的长度（4 字节）。

3.5.4. CASE 4

这种情况时，命令中既有数据送到卡（Lc）中，也有数据从卡中返回（Le）。

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

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = 数据的长度 + MAC 的长度（4 字节）。

注：

在射频模式下，CASE4 的情况下 Le 加不加均可。

4. 命令

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

4.1. 命令与响应的格式

4.1.1. 命令格式

命令由“命令头”和“命令体”组成

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

命令可分为四种情况：

格式	命令组成
CASE 1	CLA INS P1 P2
CASE 2	CLA INS P1 P2 Le
CASE 3	CLA INS P1 P2 Lc Data
CASE 4	CLA INS P1 P2 Lc Data Le

4.1.2. 响应格式

响应的格式：

数据	状态字	
DATA	SW1	SW2

DATA ：响应数据

SW1、SW2：卡片执行命令的返回值

4.2. COS 支持的命令集

4.2.1. 基本命令

4.2.1.1. APPEND RECORD 命令

4.2.1.1.1. 命令描述

APPEND RECORD 命令用于向记录文件中添加新记录。对循环记录文件，可无限添加记录；对其他记录文件，只能添加到文件的最后一条记录。

4.2.1.1.2. 使用条件和安全

APPEND RECORD 命令的执行必须满足访问文件的添加权限和添加属性。

4.2.1.1.3. 命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘E2’								
P1	‘00’								
P2	b8	b7	b6	b5	B4	b3	b2	b1	说 明
	0	0	0	0	0	0	0	0	当前的 EF 文件
	x	x	x	x	x	0	0	0	用 SFI 方式
Lc	DATA 域数据长度 **明文方式：** ‘00’< Lc ≤ ‘FF’ **加密方式：** ‘08’≤ Lc ≤ ‘70’（模 8） **校验方式：** ‘04’< Lc ≤ ‘73’ **校验加密方式：** ‘0C’≤ Lc ≤ ‘74’（模 8 + 4）								
DATA	明文方式： 新数据 加密方式： 被加密的新数据 校验方式： 新数据||MAC 校验加密方式：被加密的新数据||MAC								
Le	不存在								

当文件 ACw 中的 CER 和/或 CIPH 为‘1’时，必须使用安全报文传送；既 CLA 的后半字节等于十六进制‘4’。 若 CER=‘1’，则发送命令前，先要执行 GET CHALLENGE 命令，向卡申请一随机数作为 MAC 计算的初值。

4.2.1.1.4. 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	84	记录空间已满
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.1.5. 命令详解

条件 1： 文件标识符：0015（不是当前文件）
明文方式写入
记录长度为 0A

操作： 向记录文件中添加一条新的长度为 10 个字节的记录。
11223344556677889AA 为记录内容

命令： 00E200A80A11223344556677889AA

响应： 9000

条件 2： 文件标识符：0015
通过 SELECT FILE 选择该文件为当前文件
明文方式写入
记录长度为 0A

操作： 向记录文件中添加一条新的长度为 10 个字节的记录。
1122334455667788 99AA 为记录内容

命令： 00E200000A1122334455667788 99AA

响应： 9000

4.2.1.2. APPLICATION BLOCK 命令

4.2.1.2.1. 命令描述

APPLICATION BLOCK 命令执行成功后，锁定当前有效应用。锁定后的应用仍可以被选择（成功选择应用后，返回 SW1_SW2='6A81'），但被锁定应用下的文件是不可访问的，任何试图对文件的访问都将返回 SW1SW2='6A81'。锁定后的应用可通过 Get Response 命令得到 FCI 信息。如果应用被永久锁定返回 SW1SW2='9303'。

4.2.1.2.2. 使用条件和安全

APPLICATION BLOCK 命令的执行采用校验模式。计算校验码使用的 KEY 为 ADF 文件中的 BLK-KID 密钥。

4.2.1.2.3. 命令格式

代码	数 值
CLA	'84'
INS	'1E'
P1	'00'
P2	'00'锁定后可用 APPLICATION UNBLOCK 命令解锁 '01'永久锁定应用
Lc	'04'
DATA	信息认证码（MAC）
Le	不存在

4.2.1.2.4. 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
62	81	回送数据可能出错
62	83	选择文件无效
64	00	状态标志位未变
65	81	写 EEPROM 失败

67	00	Lc 长度错误
69	00	无信息提供
69	82	不满足安全状态
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC）数据错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定
93	03	应用永久锁定

4.2.1.2.5. 命令详解

操作： 锁定当前 ADF
条件 1： 要锁定的 ADF 为当前 ADF。
永久锁定。
步骤 1： 取 4 字节随机数
命令： 0084000004
响应： 08CDF316
步骤 2： 终端用该 ADF 文件中的 BLK-KID 密钥，对 841E000104 计算 MAC，
得到 MAC= 253814E4
步骤 3 应用锁定
命令： 841E000104253814E4
响应： 9000

4.2.1.3. CARD BLOCK 命令

4.2.1.3.1. 命令描述

成功执行 CARD BLOCK 命令后，应用环境被锁定。除 GET INFO 命令外，在锁定的应用环境内卡拒绝执行任何命令，返回状态信息'6A81'。

4.2.1.3.2. 使用条件和安全

命令的执行必须采用校验模式。使用 DDF 文件中 BLK-KID 所指定的密钥计算校验码。该命令必须在 DDF 下执行。

4.2.1.3.3. 命令格式

代码	数 值
CLA	'84'
INS	'16'
P1	'00'
P2	'00'
Lc	'04'
DATA	信息认证码（MAC）
Le	不存在

4.2.1.3.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
64	00	状态标志位未变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC）数据错误
6A	81	功能不支持

6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错

4.2.1.3.5. 命令详解

操作： 卡片锁定。
步骤 1： 取 4 字节随机数
命令： 0084000004
响应： 08CDF316
步骤 2： 终端用当前环境目录下的 BLK-KID 密钥，对 8416000004 计算 MAC，得到 MAC= 13060AC6
步骤 3 卡片锁定
命令： 8416000004130 60AC6
响应： 9000

4.2.1.4. CHANGE PIN 命令

4.2.1.4.1. 命令描述

CHANGE PIN 命令允许持卡人将当前个人密码更新为新的密码。可将有效的 PIN 更新为缺省 PIN，或将缺省 PIN 更新为有效 PIN。

4.2.1.4.2. 使用条件和安全

更新 PIN 命令中的数据域是以明文方式传送的。命令不受 PIN 的访问权限的限制。更新 PIN 时，要通过原 PIN 的认证。如果原 PIN 认证没有通过，不能完成 PIN 的更新，同时将 PIN 的限制计数器减一。

4.2.1.4.3. 命令格式

代码	值								
CLA	‘80’								
INS	‘5E’								
P1	‘01’								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	-	-	-	-	-	-	-	MF 或 DDF 下的 PIN
	1	-	-	-	-	-	-	-	ADF 下的 PIN
	-	x	x	x	x	x	x	x	PIN 标识符
	0	0	0	0	0	0	0	0	MPIN
Lc	‘05’–‘0D’								
Data	当前 PIN ||‘FF’|| 新的 PIN								
Le	不用								

4.2.1.4.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	含义
90	00	命令执行成功
63	Cx	验证失败，’x’ 表示重试次数
65	81	EEPROM 损坏，导致卡锁定

67	00	Lc 长度错
69	83	验证 PIN 锁定
69	85	使用条件不满足
6A	80	数据域参数不正确
6A	81	功能不支持
6A	86	P1，P2 参数不正确
6A	88	未找到 PIN 数据
6D	00	命令不存在
6E	00	命令类型错
93	03	应用永久锁定

4.2.1.4.5. 命令详解

操作： MPIN 修改。
条件： 旧 PIN：1234，新 PIN：9999
命令： 805E0100051234FF9999
响应： 9000

4.2.1.5. CLEAR DF 命令

4.2.1.5.1. 命令描述

CLEAR DF 命令删除 DF（包括 MF、DDF、ADF）文件体的内容。

4.2.1.5.2. 使用条件和安全

CLEAR DF 命令的执行必须通过相应 DF 下主控 MK 的认证。

4.2.1.5.3. 命令格式

代码	数 值
CLA	‘BF’
INS	‘CE’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	不存在

4.2.1.5.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

4.2.1.5.5. 命令详解

操作： 删除当前 DF 文件体的内容。
条件： 选择所要删除 的 DF ， 通过当前 DF 的 MK 认证
命令： BFCE0000
响应： 9000

4.2.1.6. CREATE FILE 命令

4.2.1.6.1. 命令描述

CREATE FILE 命令用于在卡内建立各种类型的文件，并为所建文件分配应用空间。执行一次 CREATE FILE 命令只能建立一个文件。

文件占用空间的计算方法：

用户数据空间 = EEPROM 容量-336 字节；
MF 文件 = 用户数据空间；
DDF、ADF 文件 = 48 字节+空间大小
透明、变长记录、定长记录、循环记录文件 = 16 字节 + 文件大小
安全文件 = 12 字节 + 文件大小
电子存折文件 = 20 字节
电子钱包文件 = 16 字节

4.2.1.6.2. 使用条件和安全

该命令的使用条件是：
1、卡经过了初始化；
2、建立 MF 前，应正确认证制造商密钥，初始的 MK 为‘0’值。
3、在 MF 下建立文件，必须通过 MF 的主控密钥 MK 的认证；
在 DDF 下建立文件，必须通过 DDF 的主控密钥 MK 的认证；
在 ADF 下建立文件，必须通过 ADF 的主控密钥 MK 的认证。

4.2.1.6.3. 命令格式

代码	数 值
CLA	‘80’
INS	‘E0’
P1	‘00’
P2	‘00’：MF 文件 ‘01’：DDF 文件 ‘02’：ADF 文件 ‘03’：透明文件 ‘04’：线性定长文件

	‘05’：线性变长文件 ‘07’：循环定长文件 ‘09’：电子钱包文件 ‘0A’：电子存折文件 ‘0B’：安全文件 其它保留
Lc	DATA 域的内容
MF	
11~27	文件标识符（File-ID）——2 字节（必须是‘3F00H’） 环境类型（App-Type）——1 字节 内部字节（RFU）——1 字节（‘00H’） ATR-SFI——1 字节 DIR-SFI——1 字节 FCI-SFI——1 字节 主控密钥控制属性 ACw——1 字节 RLD-KID——1 字节 BLK-KID——1 字节 主控密钥限制数（Limit）——1 字节 MF-Name——可选，最大 16 字节
DDF	
3~29	文件标识符（File-ID）——2 字节 文件体空间（LNG）——2 字节 环境类型（App-Type）——1 字节 内部字节（RFU）——2 字节（‘0000H’） DIR-SFI——1 字节 FCI-SFI——1 字节 主控密钥控制属性 ACw——1 字节 RLD-KID——1 字节 BLK-KID——1 字节 主控密钥限制数（Limit）——1 字节 DDF-Name——可选，最大 16 字节
ADF	
13~29	文件标识符（File-ID）——2 字节 文件体空间（LNG）——2 字节 内部字节（RFU）——4 字节（‘00000000H’） FCI-SFI——1 字节 主控密钥控制属性 ACw——1 字节 RLD-KID——1 字节

	BLK-KID——1 字节 主控密钥限制数（Limit）——1 字节 ADF-Name——可选，最大 16 字节
安全文件	
8	文件标识符（File-ID）——2 字节 文件体空间（LNG）——2 字节 WT-KID——1 字节 文件控制属性 ACw——1 字节 密钥的修改权限（Write-Right）——2 字节
透明 EF 文件	
13	文件标识符（File-ID）——2 字节 文件体空间（LNG）——2 字节 内部字节（RFU）——1 字节（‘00H’） 文件读控制属性 ACr——1 字节 文件写控制属性 ACw——1 字节 文件读权限（Read-Right）——2 字节 文件写权限（Write-Right）——2 字节 RT-KID——1 字节 WT-KID——1 字节
线性定长记录 EF 文件	
15	文件标识符（File-ID）——2 字节 记录长度（RL）——1 字节 最大记录个数（RN）——1 字节 预开记录个数（RE）——1 字节 内部字节（RFU）——1 字节（‘00H’） 数据格式（RF）——1 字节 文件读控制属性 ACr——1 字节 文件写控制属性 ACw——1 字节 文件读权限（Read-Right）——2 字节 文件写权限（Write-Right）——2 字节 RT-KID——1 字节 WT-KID——1 字节
线性变长记录 EF 文件	
14~14+n	文件标识符（File-ID）——2 字节 文件体空间（LNG）——2 字节 内部字节（RFU）——1 字节（‘00H’） 数据格式（RF）——1 字节 文件读控制属性 ACr——1 字节

	文件写控制属性 ACw——1 字节 文件读权限（Read-Right）——2 字节 文件写权限（Write-Right）——2 字节 RT-KID——1 字节 WT-KID——1 字节 第 1 条记录的长度 L1——1 字节（可选） 第 2 条记录的长度 L2——1 字节（可选） ……. 第 n 条记录的长度 Ln——1 字节（可选）
循环记录 EF 文件	
14	文件标识符（File-ID）——2 字节 记录长度（RL）——1 字节 最大记录个数（RN）——1 字节 预开记录个数（RE）——1 字节 数据格式（RF）——1 字节 文件读控制属性 ACr——1 字节 文件写控制属性 ACw——1 字节 文件读权限（Read-Right）——2 字节 文件写权限（Write-Right）——2 字节 RT-KID——1 字节 WT-KID——1 字节
电子钱包文件	
6	文件标识符（File-ID）——2 字节 余额上限（Bala-Limit）——4 字节
电子存折文件	
6	文件标识符（File-ID）——2 字节 余额上限（Bala-Limit）——4 字节
Le	不存在

4.2.1.6.4. 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态

69	85	使用条件不满足
6A	80	数据域参数不正确（建立同名文件）
6A	81	功能不支持
6A	84	空间已满
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.6.5. 命令详解

注：各类型文件 ACw 的设定请参考文件结构一章对各类型文件的 ACw 的定义

操作： 建立 MF

条件： 金融环境，
ATR-SFI=01
DIR-SFI=02，
FCI-SFI=15，
ACw=38（MK 长度为 16 字节，主控密钥用密文校验模式写入）
RLD-KID=02（主控密钥重装密钥标识），
BLK-KID=03（环境解锁密钥标识）
主控密钥限制次数为 3 次，
无 MF- NAME，
通过制造商密钥认证。

命令： 80E000000B3F00000001021538020303

响应： 9000

操作： 建立 DDF，金融环境

条件： 标识 DF01
空间 0600
DIR-SFI=02，
FCI-SFI=01，
ACw=38（MK 长度为 16 字节，主控密钥用密文校验模式写入），
RLD-KID=02（主控密钥重装密钥标识），
BLK-KID=03（环境解锁密钥标识），
主控密钥限制次数为 3 次，
无 DDF- NAME。

命令： 80E000010DDF0106000000000020138020303

响应： 9000

操作： 建立 ADF
条件： 标识为 00AD，
文件体空间 0500 字节，
FCI-SFI=15，
ACw=39（MK 长度为 16 字节，主控密钥用密文校验模式写入,MK 已经存在缺省为全 0），
RLD-KID=02（主控密钥重装密钥标识），
BLK-KID=03（环境解锁密钥标识），
主控密钥限制次数为 3 次，
ADF 文件名为 A00000000386980701
命令： 80E000021600AD0500000000001539020303A00000000386980701
响应： 9000

操作： 建立透明文件
条件： 文件标识为 0015，
文件体空间为 256 个字节，0100
ACr=20（文件用明文+MAC 方式读取，不需验证 PIN），
ACw=30（文件用密文+MAC 方式写入，不需验证 PIN），
读权限：0000（开放该文件的读权限）
写权限：0000（开放该文件的写权限）
RT-KID=05（读控制密钥），
WT-KID=06（写控制密钥）。
命令： 80E000030D00150100002030000000000506
响应： 9000

操作： 建立线性定长记录文件
条件： 文件标识为 0001，
每条记录的长度为 16 字节，
最多有 14 条记录，
不预开纪录，
ACr=01（记录用明文读出，需要 PIN 验证），
ACw=13（记录用密文写入，写入前需要验证 PIN 或满足写权限），
读权限：0000（开放该文件的读权限）
写权限：0033（ADF 的局部写权限级别为 3），
RT-KID=05（读控制密钥），
WT-KID=06（写控制密钥）。
命令： 80E000040F0001100E0000000113000000330506
响应： 9000
操作： 建立线性变长记录文件

条件： 文件标识为 0002，
文件体空间为 256 个字节，
ACr=20（记录用密文读出），
ACw=20（记录用密文方式写入），
读权限：0000，
写权限：0033（在 ADF 的局部写权限级别为 3），
RT-KID=05（读控制密钥），
WT-KID=06（写控制密钥）。
不预先设定记录长度。
命令： 80E000050E000201000000202000000033050 6
响应： 9000

操作： 建立循环记录文件
条件： 文件标识为 0003，
每条记录的长度为 16 字节，
最多有 14 条记录，
不预开纪录，
ACr=01（记录用明文读出，需要验证 PIN），
ACw=03（记录用明文写入，写入前需要验证 PIN 或满足写权限），
读权限：0000（开放该文件的读权限），
写权限：0033（在 ADF 的局部写权限级别为 3），
RT-KID=05（读控制密钥），
WT-KID=06（写控制密钥）。
命令： 80E000070E0003100E0000103000000330506
响应： 9000
操作： 建立电子钱包文件
条件： 文件标识为 EB00，
余额上限为 10000 元
命令： 80E0000906EB0000002710
响应： 9000
操作： 建立电子存折文件
条件： 文件标识为 ED00，
余额上限为 10000 元
命令： 80E0000A06ED0000002710
响应： 9000
操作： 建立安全文件
条件： 文件标识为 0011，
文件体空间为 256 个字节，
WT-KID=06（写控制密钥），

ACw=33（写入密钥和修改密钥采用密文校验模式），
写权限：0033（密钥修改权限级别为 3）。

命令： 80E0000B080011010006330033

响应： 9000

4.2.1.7. EXTERNAL AUTHENTICATE 命令

4.2.1.7.1. 命令描述

EXTERNAL AUTHENTICATE 命令的目的是 IC 卡验证外部接口设备的有效性，使接口设备对 IC 卡获得某种操作授权。

接口设备提供的认证数据应按以下规则产生：

金融应用环境	1、Lc = ‘08’ 2、用 GET CHALLENGE 命令向 IC 卡申请一组随机数。 3、用指定密钥对随机数作加密计算，产生认证数据。参见“安全计算”一节。

4.2.1.7.2. 使用条件和安全

EXTERNAL AUTHENTICATE 命令所使用的密钥（由 P2 参数指定）必须满足密钥的访问权限。密钥验证失败计数器减一。当计数器减为‘0’值时，密钥被锁定。

4.2.1.7.3. 命令格式

代码	数 值								
CLA	‘00’								
INS	‘82’								
P1	‘00’								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	全局密钥标识
	1	x	x	x	x	x	x	x	局部密钥标识
	0	0	0	0	0	0	0	0	当前 DF 下的 MK
Lc	‘08’								
DATA	认证数据（8 字节）								
Le	不存在								

4.2.1.7.4. 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
63	Cx	认证失败，还可认证 x 次
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.7.5. 命令详解

操作： 外部认证
条件： 外部认证密钥标识 01，对 MF 进行外部认证。
步骤 1： 取 8 字节随机数
命令： 0084000008
响应： 08CDF316E9DA2F96
步骤 2： 终端用与卡内用于外部认证的密钥相同的密钥对 8 字节随机数（08CD F316E9DA2F96）进行加密运算，产生认证数据（F26EE85B78806943）。
步骤 3： 发出外部认证命令
命令： 0082000108F26EE85B78806943
响应： 9000

4.2.1.8. FREEZE MF 命令

4.2.1.8.1. 命令描述

FREEZE MF 锁定对 MF 文件的重构。在应用的开发阶段，在没成功执行 FREEZE MF 命令之前，应用开发者可以反复对 IC 卡文件系统进行重构。在成功执行了 FREEZE MF 命令后，MF 重构功能被冻结。

4.2.1.8.2. 使用条件和安全

FREEZE MF 命令的执行必须在 MF 下，并且通过 MF 下主控 KEY 的认证。该命令成功执行后自动失效。

4.2.1.8.3. 命令格式

代码	数 值
CLA	‘BF’
INS	‘FE’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	不存在

4.2.1.8.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在

6E	00	CLA 错

4.2.1.8.5. 命令详解

在任何情况下，直接执行此命令即可。

4.2.1.9. GET CHALLENGE 命令

4.2.1.9.1. 命令描述

GET CHALLENGE 命令从 IC 卡中获取一组随机数，用于相关命令的安全认证。

4.2.1.9.2. 使用条件和安全

GET CHALLENGE 命令可无条件使用。

4.2.1.9.3. 命令格式

代码	数 值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	金融环境：‘04’或‘08’随机数长度

4.2.1.9.4. 响应信息

响应信息中的数据：

说 明	长度（字节）
随机数	4 或 8 或 10

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
67	00	Le 长度错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在

6E	00	CLA 错

4.2.1.9.5. 命令详解

在任何情况下，直接执行此命令即可。

4.2.1.10. GET INFO 命令

4.2.1.10.1. 命令描述

GET INFO 命令读取 IC 卡内的特征信息。

4.2.1.10.2. 使用条件和安全

GET INFO 命令可无条件使用。

4.2.1.10.3. 命令格式

代码	数 值
CLA	‘BF’
INS	‘C8’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	‘0F’

4.2.1.10.4. 响应信息

响应信息中的数据：

说 明	长度（字节）
芯片商注册标识号（‘8601’）	2
COS 标识符	1
COS 版本号	1
COS 版本修订号	1
EEPROM 空间	2
卡片状态	1
‘00’	1
当前目录类型	1
当前应用状态	1
当前目录空间	2

当前目录剩余空间	2

卡片状态：

——‘0A’，初始状态；
——‘0B’，开发状态；
——‘0C’，工作状态；
——‘0D’，锁定状态；
——‘0E’，EEPROM 损坏

当前目录类型：

——‘39’，MF
——‘3A’，DDF
——‘38’，ADF

当前规范类型：

——‘00’，PBOC 应用

当前应用状态：

——‘38’，工作状态
——‘78’，临时锁定状态
——‘B8’，永久锁定状态

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
67	00	Le 长度错误
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

4.2.1.10.5. 命令详解

在任何情况下，直接执行此命令即可。

4.2.1.11. GET RESPONSE 命令

4.2.1.11.1. 命令描述

GET REPONSE 命令从 IC 卡中向接口设备传送 APDU 的数据。

4.2.1.11.2. 使用条件和安全

GET REPONSE 命令无使用条件限制。

4.2.1.11.3. 命令格式

代码	数　值
CLA	‘00’
INS	‘C0’
P1	‘00’
P2	‘00’
Lc	不存在
DATA	不存在
Le	响应的最大数据长度

4.2.1.11.4. 响应信息

响应信息中的数据：

说 明	长度（字节）
响应数据	X

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	81	回送数据可能有错
67	00	Lc 或 Le 长度错误
6A	86	P1、P2 参数错
6C	xx	长度错误，‘xx’表示实际长度

6D	00	命令不存在
6E	00	CLA 错
6F	00	数据无效

4.2.1.12. INTERNAL AUTHENTICATE 命令

4.2.1.12.1. 命令描述

INITIALNAL AUTHENTICATE 命令的目的是 IC 卡向外部接口设备提供认证数据，以使接口设备对 IC 卡进行认证。

认证数据按以下规则产生：IC 卡对接口设备提供的数据作加密计算，同时将产生的认证数据回送给接口设备。

金融应用环境	1、Lc = ‘08’ 2、用指定密钥对随机数作加密计算，产生认证数据。参见“安全计算”一节。

4.2.1.12.2. 使用条件和安全

INTERNAL AUTHENTICATE 命令所使用的密钥（由 P2 参数指定）必须满足密钥的访问权限。

4.2.1.12.3. 命令格式

代码	数 值								
CLA	‘00’								
INS	‘88’								
P1	‘00’								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	全局密钥标识
	1	x	x	x	x	x	x	x	局部密钥标识
	0	0	0	0	0	0	0	0	当前 DF 下的主密钥标识
Lc	‘08’								
DATA	输入数据（8 字节）								
Le	‘08’（认证数据）								

4.2.1.12.4. 响应信息

响应信息中的数据：

说 明	长 度（字节）
认证数据	8

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
62	81	回送数据可能有错
64	00	标志状态位未变
67	00	Lc 长度错误
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.12.5. 命令详解

条件： 内部认证密钥标识 01，输入数据为 1122334455667788。
操作： 发出内部认证命令
命令： 00880001081122334455667788 08
响应： CD72DFC6E6D040A4

4.2.1.13. PIN CHANGE/UNLOCK 命令

4.2.1.13.1. 命令描述

PIN CHANGE/UNLOCK 命令为使用者提供了更改 PIN 和解锁 PIN 的功能。执行命令前，应先执行 GET CHALLENGE 命令。

4.2.1.13.2. 使用条件和安全

更改和解锁 PIN 时，命令的执行必须满足 PIN 的访问权限。如果更改 PIN，命令格式为密文校验模式。如果解锁 PIN，命令格式为校验模式。

对于金融 PIN 解锁请参看 PIN UNLOCK 命令。

对于金融 PIN 重装请参看 RELOAD PIN 命令。

4.2.1.13.3. 命令格式

代码	数 值								
CLA	‘84’								
INS	‘24’								
P1	‘00’								
P2	b8	B7	b6	b5	b4	b3	b2	b1	说 明
	0	-	-	-	-	-	-	-	MF 或 DDF 下的 PIN
	1	-	-	-	-	-	-	-	ADF 下的 PIN
								0	解锁 PIN，尝试计数器重置，但不修改 PIN
								1	更改 PIN，尝试计数器重置，同时修改 PIN
	0	0	0	0	0	0	0	-	MPIN
Lc	**校验方式：**’04’ **密文校验方式：**’0C’								
DATA	若 P2=’xxxxxxx0’，MAC 若 P2=’xxxxxxx1’，新 PIN 数据密文||MAC								
Le	不存在								

4.2.1.13.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	83	未找到 PIN
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.13.5. 命令详解

操作：　金融环境下对 PIN 解锁。
条件：　被锁定的 PIN 值：1234
通过 MPUK 按照”安全管理”一节的加密算法得到 PIN 密文：
83134983D3450BDE
通过 MPUK 按照”安全管理”一节的 MAC 计算得到 MAC：24A2B89D
命令：　842400000C83134983D3450BDE24A2B89D
响应：　9000

4.2.1.14. READ BINARY 命令

4.2.1.14.1. 命令描述

READ BINARY 命令用于读出透明文件的内容。当文件的 ACr 中的 CER 为‘1’时，应先执行 GET CHALLENGE 命令。

4.2.1.14.2. 使用条件和安全

READ BINARY 命令的执行必须满足访问文件的读权限和控制属性。

4.2.1.14.3. 命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘B0’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	1）不存在——明文方式 2）‘04’——校验方式								
DATA	1）不存在 2）MAC								
Le	期望返回的数据长度								

可能的命令/响应有：

CER	CIPH	命令	响应
0	0	00 B0 P1 P2 Le	明文数据 || SW1 SW2
0	1	04 B0 P1 P2 Le	密文数据 || SW1 SW2
1	0	04 B0 P1 P2 Lc MAC Le	明文数据 || SW1 SW2
1	1	04 B0 P1 P2 Lc MAC Le	密文数据 || SW1 SW2

4.2.1.14.4. 响应信息

响应信息中的数据为明文或密文数据。

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
61	xx	还有 xx 字节要返回
62	81	部分回送的数据可能有错
62	82	文件长度<Le
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6C	xx	Le 长度错误。‘xx’表示实际长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.14.5. 命令详解

操作 1： 读透明文件，直接通过 SFI 访问该文件。

条件： 假设该文件从头部开始的文件内容为：00112233445566778899AABBCCDDEE。
透明文件的标识为 0015（不是当前文件）。
期望读取的数据长度为 10 字节，
从文件的头部开始读该文件，

采用明文方式读取文件。

命令： 00B095000A

响应： 00112233445566778899

操作 2： 读透明文件。

条件： 透明文件的标识为 0016（通过 SELECT FILE 成为当前文件）。
期望读取数据长度为 10 字节，
从距离文件的头部 010B 个字节开始读该文件，
采用明文方式读取文件。
设距离文件的头部 010B 个字节开始的文件内容为：00112233445566778899AABBCCDDEEFF。

步骤 1： 选择该文件

命令： 00A40200020016

响应： 9000

步骤 2： 读文件

命令： 00B0010B0A

响应： 00112233445566778899

4.2.1.15. READ RECORD 命令

4.2.1.15.1. 命令描述

READ RECORD 命令读记录文件中指定的记录。即可通过指定记录号方式读取记录数据，也可通过记录标识符方式读取记录数据。当以 TLV 结构访问文件时，IC 卡视记录的第一个字节为‘T’，将整个记录返回。当文件的 ACr 中的 CER 为‘1’时，应先执行 GET CHALLENGE 命令。

4.2.1.15.2. 使用条件和安全

READ RECORD 命令的执行必须满足访问文件的读权限和控制属性。

4.2.1.15.3. 命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘B2’								
P1	记录号（‘00’表示当前记录） 记录标识符（‘00’表示按记录号指定第一条、最后一条、下一条、前一条）								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	-	-	-	当前文件
	x	x	x	x	x	-	-	-	通过 SFI 方式访问
	1	1	1	1	1	-	-	-	保留
	-	-	-	-	-	1	x	x	P1 作为记录号
	-	-	-	-	-	1	0	0	P1 指定的记录号
	-	-	-	-	-	1	0	1	从 P1 到记录尾
	-	-	-	-	-	1	1	0	从记录尾到 P1
	-	-	-	-	-	0	x	x	P1 作为记录标识符
	-	-	-	-	-	0	0	0	P1 指向相同标识符的第一条
	-	-	-	-	-	0	0	1	P1 指向相同标识符的最后一条
	-	-	-	-	-	0	1	0	P1 指向相同标识符的下一条
	-	-	-	-	-	0	1	1	P1 指向相同标识符的前一条
	其他值								保留
Lc	1) 不存在——明文方式 2)‘04’—— 命令报文校验方式								
DATA	1）不存在——明文方式								

	2）MAC——校验方式
Le	期望返回的记录数据

可能的命令/响应有：

CER	CIPH	命令	响应
0	0	00 B2 P1 P2 Le	明文数据 || SW1 SW2
0	1	04 B2 P1 P2 Le	密文数据 || SW1 SW2
1	0	04 B2 P1 P2 Lc MAC Le	明文数据 || SW1 SW2
1	1	04 B2 P1 P2 Lc MAC Le	密文数据 || SW1 SW2

4.2.1.15.4. 响应信息

响应信息中的数据为明文或密文数据。

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
61	xx	还有 xx 字节需要返回
62	81	回送的数据可能有错
64	00	标志状态位没变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效(未申请随机数)
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6C	xx	Le 错误，‘xx’表示实际长度
61	xx	射频模式下，CASE4 的情况，Le 错误，‘xx’表示实际

		长度
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.15.5. 命令详解

操作： 读取记录文件 0016 当中的第二条记录。
条件 1： 文件标识符为 0016 的记录文件中的第 2 条记录，该记录采用 TLV 格式，
该记录的内容为 2504AABBCCDD。
用明文方式读取。
方法 1： 通过短标识符选择记录文件，通过记录号读取记录
命令： 00B202B406
响应： 2504AABBCCDD
方法 2： 选择记录文件，通过记录号读取当前记录文件中指定的记录
步骤 1： 选择该文件
命令： 00A40200020016
响应： 9000
步骤 2： 读取该条记录
命令： 00B2020406
响应： 2504AABBCCDD
方法 3： 通过短标识符选择记录文件，通过记录标识符读取记录
命令： 00B225B006
响应： 2504AABBCCDD
条件 2： 标识符为 0016 的记录文件中包含 4 条记录，
其中第 1 条记录内容为 240400112233，
第 2 条记录为 2504AABBCCDD，
第 3 条记录为 260444556677，
第 4 条记录为 25048899EEFF，
该记录中的文件采用 TLV 格式，
读取记录用明文读取。
操作 1： 按照记录号递增的顺序，读取第二条记录以后的所有记录
方法 1： 通过 SFI 选择
命令： 00B202B512
响应： 2504AABBCCDD260444556677250488 99EEFF
方法 2： 选择当前文件，而后选择要求的记录
步骤 1： 选择该文件
命令： 00A40200020016

响应： 9000
步骤 2： 读记录
命令： 00B2020512
响应： 2504AABBCCDD26044455667725048899EEF
操作 2： 按照记录号递减的顺序，读取第二条记录以后的所有记录
方法 1： 通过 SFI 选择
命令： 00B202B612
响应： 25048899EEFF2604445566772504AABBCCDD
方法 2： 选择当前文件，而后选择要求的记录
步骤 1： 选择该文件
命令： 00A40200020016
响应： 9000
步骤 2： 读记录
命令： 00B2020612
响应： 25048899EEFF2604445566772504AABBCCDD
操作 3： 通过记录标识符，选择第四条记录
方法 1： 通过 SFI 方式
命令： 00B225B106
响应： 2504AABBCCDD
方法 2： 选择当前文件，而后选择要求的记录
步骤 1： 选择该文件
命令： 00A40200020016
响应： 9000
步骤 2： 读记录
命令： 00B2250106
响应： 25048899EEFF

4.2.1.16. SELECT FILE 命令

4.2.1.16.1. 命令描述

SELECT FILE 命令通过文件标识或应用名选择 IC 卡中的 MF、DDF、ADF 或 EF 文件。

4.2.1.16.2. 使用条件和安全

SELECT FILE 命令无使用条件限制。该命令不能用于选择安全文件（SF）。

4.2.1.16.3. 命令格式

代码	数　值
CLA	‘00’
INS	‘A4’
P1	‘00’通过 FID 选择 DF、EF，当 Lc=‘00’时，选 MF ‘01’通过 FID 选择 DF ‘02’通过 FID 选择当前 DF 下的 EF ‘03’选择父目录（Lc=‘00’） ‘04’通过 DF 名选择应用
P2	‘00’ ‘02’选择下一个文件（P1=04h 时）
Lc	P1=‘00’时，Lc=‘00’或‘02’ P1=‘01’~‘02’时，Lc=‘02’ P1=‘03’时，Lc=‘00’ P1=‘04’时，Lc=‘01’~‘10’
DATA	文件标识符（FID—2 字节） 应用名（App-Name，P1=‘04’）
Le	FCI 文件的信息长度（选择 DF 时）

4.2.1.16.4. 响应信息

响应信息的结构：
PBOC 规范：

下表定义了成功选择 PSE 后回送的 FCI：

标识	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名（1PAY.SYS.DDF01）	M
	‘A5’	FCI 数据专用模板	M
	‘88’	目录基本文件的 SFI	M
	‘9F0C’	FCI 文件内容	O

下表定义了成功选择 DDF 后回送的 FCI：

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘88’	目录基本文件的 SFI	M
	‘9F0C’	FCI 文件内容	O

下表定义了成功选择 ADF 后回送的 FCI：

标签	值		存在性
‘6F’	FCI 模板		M
	‘84’	DF 名	M
	‘A5’	FCI 数据专用模板	M
	‘9F0C’	FCI 文件内容	**O**
	9F08	版本信息	O

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
62	83	选择文件无效
62	84	FCI 格式与 P2 指定的不符
64	00	标志状态位没变
67	00	Lc 长度错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	87	Lc 与 P1-P2 不匹配
6D	00	命令不存在

6E	00	CLA 错
93	03	应用永久锁定

4.2.1.16.5. 命令详解

操作 1： 选择 MF
条件： MF 中的 DIR-SFI=02，MF 没有定义名称
命令： 00A4000000
响应： 6F078400A503880102
操作 2： 选择 MF 下的 ADF
条件： 当前环境在 MF 下，选择 MF 下文件标识符为 AD01 的 ADF 文件。
该 ADF 中不包含 FCI 文件，ADF 名为 AABBCCDD
命令： 00A4010002AD01
响应： 6F0B8404AABBCCDDA5039F0C00
操作 3： 选择 EF
条件： 选择当前 ADF 下文件标识符为 0016 的 EF 文件。
命令： 00A40200020016
响应： 9000
操作 4： 选择当前 ADF 的父目录 MF
条件： 当前的 ADF 的父目录为 MF。此 MF 中的 DIR-SFI=02，MF 没有名称。
命令： 00A4030000
响应： 6F078400A503880102
操作 5： 在 MF 下用应用名称选择 ADF
条件： 当前环境在 MF 下，选择 MF 下文件名称为 AABBCCDD 的 ADF 文件
此 ADF 的 FCI 文件内容：11223344556677889900
命令： 00A4040004AABBCCDD
响应： 6F158404AABBCCDDA50D9F0C0A11223344556677889900

4.2.1.17. UPDATE BINARY 命令

4.2.1.17.1. 命令描述

UPDATE BINARY 命令用于更新透明文件中的数据。当文件的 ACw 中的 CER 为‘1’时，应先执行 GET CHALLENGE 命令。

4.2.1.17.2. 使用条件和安全

UPDATE BINARY 命令的执行必须满足文件的访问权限和写控制属性。

4.2.1.17.3. 命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘D6’								
P1	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	x	x	x	x	x	x	x	当前文件高位地址
	1	0	0	x	x	x	x	x	通过 SFI 方式访问
P2	若 P1 的 b8=0，P2 为文件的低位地址 若 P1 的 b8=1，P2 为文件地址								
Lc	DATA 域数据长度 **明文方式：** ‘00’< Lc ≤ ‘FF’ **加密方式：** ‘08’≤ Lc ≤ ‘70’（模 8） **校验方式：** ‘04’< Lc ≤ ‘73 **校验加密方式：** ‘0C’≤ Lc ≤ ‘74（模 8 + 4）								
DATA	明文方式： 明文数据 加密方式： 密文数据 校验方式： 明文数据||校验码 校验加密方式：密文数据||校验码								
Le	不存在								

4.2.1.17.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是透明文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6B	00	起始地址超出范围
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.17.5. 命令详解

操作 1：　从文件头部更新标识为 0015 的透明文件，直接通过 SFI 访问该文件。
条件：　透明文件的标识为 0015
　　所要更新的数据长度为 16 字节，
　　从文件的头部开始更新文件，
　　采用明文方式写入文件，
　　所要更新的内容为：00112233445566778899AABBCCDDEEFF。
命令：　00D69500100011223344556677889 9AABBCCDDEEFF
响应：　9000
操作 2：　从中间更新标识为 0015 的透明文件。
条件：　透明文件的标识为 0015，
　　所要更新的数据长度为 16 字节，
　　从距离文件的头部 010B 个字节开始更新该文件，
　　采用明文方式读取文件，
　　更新的文件内容为：00112233445566778899AABBCCDDEEFF。
步骤 1：　选择该文件

命令： 00A40200020015
响应： 9000
步骤 2： 更新数据
命令： 00D6010B10001122334455667788 99AABBCCDDEEFF
响应： 9000

4.2.1.18. UPDATE RECORD 命令

4.2.1.18.1. 命令描述

UPDATE RECORD 命令用于更新记录文件中的数据。当文件的 ACw 中的 CER 为‘1’时，应先执行 GET CHALLENGE 命令。更新的记录长度必须等于原记录长度。循环定长记录文件的添加也可采用 P2=‘xxxxx011’方式实现。

4.2.1.18.2. 使用条件和安全

UPDATE RECORD 命令的执行必须满足文件的访问权限和写控制属性。

4.2.1.18.3. 命令格式

代码	数 值								
CLA	‘00’或‘04’								
INS	‘DC’								
P1	记录号（‘00’表示当前记录） 记录标识符（‘00’表示按记录号指定第一条、最后一条、下一条、前一条）								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	0	0	0	0	-	-	-	当前文件
	x	x	x	x	x	-	-	-	通过 SFI 方式访问
	1	1	1	1	1	-	-	-	保留
	-	-	-	-	-	1	x	x	P1 作为记录号
	-	-	-	-	-	1	0	0	P1 指定的记录号
	-	-	-	-	-	0	x	x	P1 作为记录标识符
	-	-	-	-	-	0	0	0	P1 指向相同标识符的第一条
	-	-	-	-	-	0	0	1	P1 指向相同标识符的最后一条
	-	-	-	-	-	0	1	0	P1 指向相同标识符的下一条
	-	-	-	-	-	0	1	1	P1 指向相同标识符的前一条
	任何其他值								保留
Lc	DATA 域数据长度 **明文方式：** ‘00’< Lc ≤ ‘FF’ **加密方式：** ‘08’≤ Lc ≤ ‘70（模 8） **校验方式：** ‘04’< Lc ≤ ‘73								

	校验加密方式： ‘0C’≤ Lc ≤‘74’（模 8 + 4）
DATA	明文方式： 明文记录数据 加密方式： 密文记录数据 校验方式： 明文记录数据||校验码 校验加密方式：密文记录数据|校验码
Le	不存在

4.2.1.18.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	81	当前文件不是记录文件
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	未选择文件
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	84	存储空间不够
6A	85	Lc 与 TLV 结构不匹配
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.18.5. 命令详解

操作 1： 更新记录文件 0016 当中的第二条记录。
条件： 该记录采用 TLV 格式，更新后记录的内容为 2504AABBCCDD，

用明文方式写入。
方法 1： 通过短标识符选择记录文件，通过记录号更新记录
命令： 00DC02B4062504AABBCCDD
响应： 9000
方法 2： 选择记录文件，通过记录号更新当前记录文件中指定的记录
步骤 1： 选择该文件
命令： 00A40200020016
响应： 9000
步骤 2： 更新该条记录
命令： 00DC0204062504AABBCCDD
响应： 9000
方法 3： 通过短标识符选择记录文件，通过记录标识符更新记录
命令： 00DC25B0062504AABBCCDD
响应： 9000
方法 4： 选择记录文件，通过记录标识符更新当前记录文件中的指定记录
步骤 1： 选择该文件
命令： 00A40200020016
响应： 9000
步骤 2： 更新该条记录
命令： 00DC2500062504AABBCCDD
响应： 9000
操作 2： 通过记录标识符，选择第四条记录并更新。
条件： 标识符为 0016 的记录文件中包含 4 条记录，采用 TLV 格式，
其中第 1 条记录内容为 240400112233，
第 2 条记录为 2504AABBCCDD，
第 3 条记录为 260444556677，
第 4 条记录为 25048899EEFF，
更新记录用明文方式，
要将第四条记录更新为 270411223344
方法 1： 通过 SFI 方式
命令： 00DC25B106270411223344
响应： 9000
方法 2： 选择当前文件，而后选择要求的记录
步骤 1： 选择该文件
命令： 00A40200020016
响应： 9000
步骤 2： 更新记录
命令： 00DC250106270411223344

响应： 9000

4.2.1.19. VERIFY PIN 命令

4.2.1.19.1. 命令描述

VERIFY PIN 命令的目的是 IC 卡验证终端提供的 PIN。

4.2.1.19.2. 使用条件和安全

执行 VERIFY PIN 命令前，必须满足 PIN 的访问权限。PIN 验证失败，其计数器减 1，当计数器为‘0’值时，PIN 被锁定。

4.2.1.19.3. 命令格式

代码	数 值								
CLA	‘00’								
INS	‘20’								
P1	‘00’								
P2	b8	b7	b6	b5	b4	b3	b2	b1	说 明
	0	-	-	-	-	-	-	-	MF 或 DDF 下的 PIN
	1	-	-	-	-	-	-	-	ADF 下的 PIN
	0	0	0	0	0	0	0	0	MPIN
Lc	PIN 长度： ‘02’—‘06’								
DATA	PIN 数据								
Le	不存在								

4.2.1.19.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
63	Cx	验证失败。‘x’表示可以重试的次数
64	00	标志状态位没变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态

69	83	认证 PIN 锁定
69	84	记录空间已满
69	85	使用条件不满足
6A	81	功能不支持
6A	86	P1、P2 参数错
6A	88	未找到 PIN 数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.19.5. 命令详解

操作 1： 认证 PIN
条件： 在当前 MF 下认证 PIN=’1234’。
命令： 00200000021234
响应： 9000
操作 2： 当前 DDF 下的 PIN
条件： 在当前 DDF 下认证 PIN=’1234’。
命令： 00200000021234
响应： 9000
操作 3： 当前 DDF 下的 PIN
条件： 在当前 ADF 下认证 PIN=’1234’ 。
命令： 00200080021234
响应： 9000

4.2.1.20. WRITE KEY 命令

4.2.1.20.1. 命令描述

WRITE KEY 命令用于建立和更新密钥及 PIN。
当 P1=‘00’时，“密钥信息”指的是安全文件定义的四种密钥结构。
当 P1=‘01’时，“密钥信息”指的是：用途＋标识＋版本＋密钥值。

4.2.1.20.2. 使用条件和安全

WRITE KEY 命令执行必须满足 KEY 和 PIN 的访问权限和写控制属性。不能通过该命令建立新的主控密钥。

4.2.1.20.3. 命令格式

代码	数　值
CLA	‘80’或‘84’
INS	‘D4’
P1	‘00’建立新密钥和 PIN（P2≠‘00’） ‘01’更新密钥和 PIN（P2=‘00’时表示主控密钥）
P2	安全文件标识
Lc	DATA 域的长度
DATA	明文方式：　明文密钥信息 加密方式：　密文密钥信息 校验方式：　明文密钥信息||校验码 校验加密方式：密文密钥信息|校验码
Le	不存在

4.2.1.20.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 EEPROM 失败

67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC 和密文）数据错误
6A	80	数据域参数错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到密钥数据
6A	84	文件空间已满
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.1.20.5. 命令详解

操作 1： 向标识符为 0015 的安全文件中写入密钥。
条件： 安全文件的标识符为 0015，
写入密钥为’00000000000000000000000000000000’，
密钥的用途：01，
标识：02，
版本：03，
采用 3DES 算法：00，
访问需要权限级别（Access-Right）：0033，
SSB：00
限制次数为 03，
明文方式写入密钥。
命令： 80D40015180102030000330003000000000000000000000000000000000000
响应： 9000
操作 2： 更新主控密钥。
条件： 写入密钥为’00000000000000000000000000000000’，
密钥的用途：00，
标识：00，
校验加密方式写入密钥。

步骤 1： 用 RLD-KID 标识的密钥作为加密密钥，对密钥信息进行加密计算。
加密方法参考“安全管理”一节中加密的算法
加密的信息为：
13000000000000000000000000000000000000000080000000
密钥密文信息为：
84DC92E51AB32094BCDE9853EFB21A324F8334F5BAE1DCF5

步骤 2： 取 4 字节随机数

命令： 0084000004

响应： 08CDF316

步骤 3： 计算 MAC：D2FBA183

步骤 4： 写入密钥

命令： 84D401001C84DC92E51AB32094BCDE9853EFB21A324F8334F5BAE1DCF5D2FBA183

响应： 9000

4.2.2. 金融专有命令

4.2.2.1. APPLICATION UNBLOCK 命令

4.2.2.1.1. 命令描述

APPLICATION UNBLOCK 命令执行成功后，解锁当前锁定的应用。

4.2.2.1.2. 使用条件和安全

此命令只能在金融应用环境下执行。

APPLICATION UNBLOCK 命令的执行采用校验模式。计算校验码使用的 KEY 为 ADF 文件中的 BLK-KID 密钥。执行此命令必须满足 BLK-KID 密钥的访问权限。

4.2.2.1.3. 命令格式

代码	数　值
CLA	‘84’
INS	‘18’
P1	‘00’
P2	‘00’
Lc	‘04’
DATA	信息认证码（MAC）
Le	不存在

4.2.2.1.4. 响应信息

响应信息中可能出现的状态码有：

SW1	SW2	说　明
90	00	命令执行成功
64	00	状态标志位未变
65	81	写 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态

69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC）数据错误
6A	81	功能不支持
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.2.1.5. 命令详解

操作： 解锁当前 ADF。
条件： 当前锁定的 ADF 为非永久锁定。
步骤 1： 取 4 字节随机数
命令： 0084000004
响应： 08CDF316
步骤 2： 终端用该 ADF 文件中的 BLK-KID 密钥，对 8418000004 计算 MAC，得到 MAC= 9BA006EB
步骤 3： 应用解锁
命令： 84180000049BA006EB
响应： 9000

4.2.2.2. CREDIT FOR LOAD 命令

4.2.2.2.1. 命令描述

CREDIT FOR LOAD 命令用于金融圈存交易。

4.2.2.2.2. 使用条件和安全

在执行 CREDIT FOR LOAD 命令之前，应先成功执行 INITIALIZE FOR LOAD 命令。

4.2.2.2.3. 命令格式

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

计算 MAC2 的数据包括：

—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

4.2.2.2.4. 响应信息

命令执行成功返回的数据包括以下内容：

—TAC 4 字节

计算 TAC 的数据包括：

—新余额 4 字节
—联机交易序号（加 1 前） 2 字节
—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
69	01	命令不接受（无效状态）
69	85	使用条件不满足
6A	81	功能不支持
6A	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	02	MAC 无效
93	03	应用被永久锁定

4.2.2.2.5. 命令详解

结果： 完成圈存操作
条件： 已经成功执行过 INITIALIZE FOR LOAD 命令
终端当前的日期：2003 ，10， 10
终端当前的时间：15 ： 30 ： 00
通过圈存交易中的过程密钥计算得到的 MAC2 ： EF23B213
（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算）
命令： ‘805200000B20031010153000EF23B213’
响应： 返回 TAC ： D1433650
（TAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用 TAC 密钥）

4.2.2.3. DEBIT FOR PURCHASE/CASH WITHDRAW 命令

4.2.2.3.1. 命令描述

DEBIT FOR PURCHASE/CASH WITHDRAW 命令用于金融消费/取现交易。

4.2.2.3.2. 使用条件和安全

执行 DEBIT FOR PURCHASE/CASH WITHDRAW 命令之前，应先成功执行 INITIALIZE FOR PURCHASE 命令或 INITIALIZE FOR CASH WITHDRAW 命令。

4.2.2.3.3. 命令格式

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
Lc	‘0F’
Data	终端交易序号（4 字节） 交易日期（4 字节） 交易时间（3 字节） MAC1（4 字节）
Le	‘08’（TAC＋MAC2）

计算 MAC1 的数据包括：

—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

4.2.2.3.4. 响应信息

命令执行成功返回的数据包括以下内容：

—TAC 4 字节

—MAC2 4 字节

计算 TAC 的数据包括：
—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节
—终端交易序号 2 字节
—交易日期 4 字节
—交易时间 3 字节

计算 MAC2 的数据包括：
—交易金额 4 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
69	01	命令不接受（无效状态）
69	85	使用条件不满足
6A	81	功能不支持
6A	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	02	MAC 无效
93	03	应用被永久锁定

4.2.2.3.5. 命令详解

结果： 完成消费或取现操作
条件 1： 已经成功执行过 INITIALIZE FOR PURCHASE 命令
得到终端交易序号 ： 00000001
终端当前的日期：2003 ， 10， 10
终端当前的时间：15 ： 30 ： 00
通过消费交易中的过程密钥计算得到的 MAC1 ： 11D3245B

（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算）

命令： ‘805401000F00000001200310101530000 11D3245B’

响应： 返回 TAC ： D1433650

（TAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用 TAC 密钥）

返回 MAC2：83270316

（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用消费交易中的过程密钥）

条件 2： 已经成功执行过 INITIALIZE FOR CASH WITHDRAW 命令

得到终端交易序号 ：00000001

终端当前的日期：2003 ，10， 10

终端当前的时间：15 ：30 ：00

通过取现交易中的过程密钥计算得到的 MAC1 ：132B1D45

（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算）

命令： ‘805401000F00000001200310101530000 132B1D45’

响应： 返回 TAC ： 210A2CB1

（TAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用 TAC 密钥）

返回 MAC2 ：FB2C1AE4

（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用消费交易中的过程密钥）

4.2.2.4. DEBIT FOR UNLOAD 命令

4.2.2.4.1. 命令描述

DEBIT FOR UNLOAD 命令用于金融圈提交易。

4.2.2.4.2. 使用条件和安全

在执行 DEBIT FOR UNLOAD 命令之前， 应先成功执行 INITIALIZE FOR UNLOAD 命令。

4.2.2.4.3. 命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘03’
P2	‘00’
Lc	‘0B’
Data	交易日期（4 字节） 交易时间（3 字节） MAC2（4 字节）
Le	‘04’（MAC3）

计算 MAC2 的数据包括：

—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

4.2.2.4.4. 响应信息

命令执行成功返回的数据包括以下内容：

—MAC3 4 字节

计算 MAC3 的数据包括：

—新余额 4 字节
—联机交易序号（加 1 前） 2 字节
—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
69	01	命令不接受（无效状态）
6A	81	功能不支持
6A	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	02	MAC 无效
93	03	应用被永久锁定

4.2.2.4.5. 命令详解

结果： 完成圈提操作
条件： 已经成功执行过 INITIALIZE FOR UNLOAD 命令
终端当前的日期：2003 ，10， 10
终端当前的时间：15 ：30 ：00
通过圈提交易中的过程密钥计算得到的 MAC2 ：453BC1F3
（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算）
命令： ‘805403000B20031010153000453BC1F3’
响应： 返回 MAC3：88B2FD12
（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用圈提交易中的过程密钥）

4.2.2.5. GET BALANCE 命令

4.2.2.5.1. 命令描述

GET BALANCE 命令用于查询电子存折或电子钱包余额。在电子存折余额中包括透支额。

4.2.2.5.2. 使用条件和安全

读取电子钱包，电子存折余额时需验证个人密码（PIN）。

4.2.2.5.3. 命令格式

代码	值
CLA	‘80’
INS	‘5C’
P1	‘00’
P2	‘01’：用于 ED； ‘02’：用于 EP；
Lc	不存在
Data	不存在
Le	‘04’

4.2.2.5.4. 响应信息

SW1	SW2	含义
90	00	命令执行成功
69	82	不满足安全状态
69	85	使用条件不满足
6A	81	功能不支持
6A	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定

4.2.2.5.5. 命令详解

结果： 得到电子存折或电子钱包的余额
条件 1： 查询电子存折余额，要求通过 PIN 验证
命令： 805C000104
响应： 返回余额：00002710
条件 2： 查询电子钱包余额
命令： 805C000204
响应： 返回余额：000003E8

4.2.2.6. GET TRANSACTION PROOF 命令

4.2.2.6.1. 命令描述

GET TRANSACTION PROVE 命令用于获取金融交易认证码（TAC 和 MAC）。

4.2.2.6.2. 使用条件和安全

在金融交易被迫中断时（掉电或提前拔卡），IC 卡会保持金融交易瞬间所处的状态和重要数据。重新插卡时，如果被中断的金融交易已经完成，执行该命令时返回上次金融交易的 TAC 和 MAC；如果未完成，则执行该命令时返回状态码‘9406’（所需 MAC 不可用）。

卡片在应用开发状态时不提供金融交易保护功能。金融交易被中断后，重新插卡执行该命令 IC 卡返回状态码‘9406’。

4.2.2.6.3. 命令格式

代码	值
CLA	‘80’
INS	‘5A’
P1	‘00’
P2	交易类型标识。
Lc	‘02’
Data	联机或脱机交易序号。
Le	‘08’

P2 交易类型：

01—ED 圈存
02—EP 圈存
03—圈提
04—ED 取款
05—ED 消费
06—EP 消费
07—ED 修改透支限额
08—信用消费

4.2.2.6.4. 响应信息

命令执行成功返回的数据包括以下内容：

—MAC 4 字节

—TAC 4 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
69	85	使用条件不满足
67	00	Le 长度错
6A	81	功能不支持
6A	86	P1 参数错
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定

4.2.2.6.5. 命令详解

结果： 取得交易认证码

条件： ED 圈存交易类型标识： 01

获得圈存联机交易序号：0001

命令： 805A0001020001

响应： 返回 MAC ： D1433650

返回 TAC： 83270316

4.2.2.7. INITIALIZE FOR CASH WITHDRAW 命令

4.2.2.7.1. 命令描述

INITIALIZE FOR CASH WITHDRAW 命令用于金融初始化取现交易。命令执行后 IC 卡为金融取现交易状态。

4.2.2.7.2. 使用条件和安全

INITIALIZE FOR CASH WITHDRAW 命令的执行仅对 DEBIT FOR PURCHASE/CASH WITHDRAW 命令有效。命令执行前，需要验证个人密码（PIN）。

4.2.2.7.3. 命令格式

代码	值
CLA	‘80’
INS	‘50’
P1	‘02’
P2	‘01’：用于 ED 取现交易； 其它值保留。
Lc	‘0B’
Data	密钥索引号（1 字节） 交易金额（4 字节） 终端机编号（6 字节）
Le	‘0E’

4.2.2.7.4. 响应信息

命令执行成功返回的数据包括以下内容：

—ED 余额 4 字节
—ED 脱机交易序号 2 字节
—透支限额 3 字节
—密钥版本号 1 字节
—算法标识 1 字节
—伪随机数 4 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
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	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定
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

4.2.2.7.5. 命令详解

结果： 用户卡获得取现初始化的状态
条件： 建立有电子存折文件
通过 PIN 验证
取现密钥索引：01
获得交易金额：000003E8
获得终端机编号 ：130000000001
命令： 805202010B01000003E8130000000001
响应： 返回
ED 余额： 00002710
ED 脱机交易序号： 0001
透支限额： 000000
密钥版本号： 01
算法标识： 00
伪随机数： 13D22145

4.2.2.8. INITIALIZE FOR LOAD 命令

4.2.2.8.1. 命令描述

INITIALIZE FOR LOAD 命令用于金融初始化圈存交易。命令执行后 IC 卡为金融圈存交易状态。

4.2.2.8.2. 使用条件和安全

INITIALIZE FOR LOAD 命令仅对 CREDIT FOR LOAD 命令有效。在 ED 操作前，需要验证个人密码（PIN）。

4.2.2.8.3. 命令格式

代码	值
CLA	‘80’
INS	‘50’
P1	‘00’
P2	‘01’：ED 圈存 ‘02’：EP 圈存
Lc	‘0B’
Data	密钥索引号（1 字节） 交易金额（4 字节） 终端机编号（6 字节）
Le	‘10’

4.2.2.8.4. 响应信息

命令执行成功返回的数据包括以下内容：

—ED 或 EP 余额 4 字节
—ED 或 EP 联机交易序号 2 字节
—密钥版本号 1 字节
—算法标识 1 字节
—伪随机数 4 字节
—MAC1 4 字节

计算 MAC1 的数据包括：

—旧余额 4 字节
—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
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	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定
94	02	交易计数器达到最大值
94	03	密钥索引不支持

4.2.2.8.5. 命令详解

结果： 用户卡获得圈存初始化的状态
条件： 建立有电子存折文件或电子钱包文件
对于电子存折文件，通过 PIN 验证
圈存密钥索引：01
获得交易金额：000003E8
获得终端机编号 ：130000000001
命令： 805000010B01000003E8130000000001 或
805000020B01000003E8130000000001
响应： 返回
余额： 00002710
联机交易序号： 0001
密钥版本号： 01

算法标识： 00
伪随机数： 13D22145
MAC1 ： 1BF234D1
（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用圈存过程密钥）

4.2.2.9. INITIALIZE FOR PURCHASE 命令

4.2.2.9.1. 命令描述

INITIALIZE FOR PURCHASE 命令用于金融初始化消费交易。命令执行后 IC 卡为金融消费交易状态。

4.2.2.9.2. 使用条件和安全

INITIALIZE FOR PURCHASE 命令仅 DEBIT FOR PURCHASE/CASH WITHDRAW 命令有效。在 ED 操作前，需要验证个人密码（PIN）。

4.2.2.9.3. 命令格式

代码	值
CLA	‘80’
INS	‘50’
P1	‘01’
P2	‘01’：用于 ED； ‘02’：用于 EP；
Lc	‘0B’
Data	密钥索引号（1 字节） 交易金额（4 字节） 终端机编号（6 字节）
Le	‘0F’

4.2.2.9.4. 响应信息

命令执行成功返回的数据包括以下内容：

—ED 余额 4 字节
—ED 脱机交易序号 2 字节
—透支限额 3 字节
—密钥版本号 1 字节
—算法标识 1 字节
—伪随机数 4 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	执行命令成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
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	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定
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

4.2.2.9.5. 命令详解

结果： 用户卡获得消费初始化的状态

条件： 建立有电子存折文件或电子钱包文件
对于电子存折文件，通过 PIN 验证
消费密钥索引：01
获得交易金额：000003E8
获得终端机编号 ：130000000001

命令： 805001010B01000003E8130000000001 或
805001020B01000003E8130000000001

响应： 返回
余额： 00002710
脱机交易序号： 0001
透支限额： 000000
密钥版本号： 01
算法标识： 00
伪随机数： 13D22145

4.2.2.10. INITIALIZE FOR UNLOAD 命令

4.2.2.10.1. 命令描述

INITIALIZE FOR UNLOAD 命令用于金融初始化圈提交易。命令执行后 IC 卡为金融圈提交易状态。

4.2.2.10.2. 使用条件和安全

INITIALIZE FOR UNLOAD 命令仅对 DEBIT FOR UNLOAD 命令有效。命令执行前，需要验证个人密码（PIN）。

4.2.2.10.3. 命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘05’
P2	‘01’：用于 ED 其它值保留。
Lc	‘0B’
Data	密钥索引号（1 字节） 交易金额（4 字节） 终端机编号（6 字节）
Le	‘10’

4.2.2.10.4. 响应信息

命令执行成功返回的数据包括以下内容：

—ED 余额 4 字节
—ED 联机交易序号 2 字节
—密钥版本号 1 字节
—算法标识 1 字节
—伪随机数 4 字节
—MAC1 4 字节

计算 MAC1 的数据包括：

—旧余额 4 字节
—交易金额 4 字节
—交易类型 1 字节
—终端机编号 6 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
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	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定
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

4.2.2.10.5. 命令详解

结果： 用户卡获得圈提初始化的状态
条件： 建立有电子存折文件
通过 PIN 验证
圈提密钥索引：01
获得交易金额：000003E8
获得终端机编号 ：130000000001
命令： 805005010B01000003E8130000000001
响应： 返回
ED 余额： 00002710
ED 联机交易序号： 0001
密钥版本号： 01

算法标识： 00
伪随机数： 13D22145

4.2.2.11. INITIALIZE FOR UPDATE 命令

4.2.2.11.1. 命令描述

INITIALIZE FOR UPDATE 命令用于金融初始化修改透支限额交易。命令执行后 IC 卡为金融修改透支限额交易状态。

4.2.2.11.2. 使用条件和安全

INITIALIZE FOR UPDATE 命令仅对 UPDATE OVERDRAW LIMIT 命令有效。命令执行前，需要验证个人密码（PIN）。

4.2.2.11.3. 命令格式

代码	值
CLA	‘80’
INS	‘50’
P1	‘04’
P2	‘01’
Lc	‘07’
Data	密钥索引号（1 字节） 终端机编号（6 字节）
Le	‘13’

4.2.2.11.4. 响应信息

命令执行成功返回的数据包括以下内容：

—ED 余额 4 字节
—ED 联机交易序号 2 字节
—旧透支限额 3 字节
—密钥版本号 1 字节
—算法标识 1 字节
—伪随机数 4 字节
—MAC1 4 字节

计算 MAC1 的数据包括：

—旧余额 4 字节
—旧透支限额 3 字节
—交易类型 1 字节
—终端机编号 6 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
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	86	参数 P1，P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	03	应用被永久锁定
94	02	交易计数器达到最大值
94	03	密钥索引不支持

4.2.2.11.5. 命令详解

结果： 用户卡获得修改透支限额初始化的状态
条件： 建立有电子存折文件
通过 PIN 验证
修改透支限额密钥索引： 01
获得终端机编号 ：130000000001
命令： 805004010701130000000001
响应： 返回
ED 余额： 00002710
ED 联机交易序号： 0001
就透支限额： 000000
密钥版本号： 01
算法标识： 00
伪随机数： 13D22145

MAC1 ： A2345FE

（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用修改透支限额的过程密钥）

4.2.2.12. PIN UNLOCK 命令

4.2.2.12.1. 命令描述

PIN UNLOCK 命令为使用者提供解锁 PIN 的功能。执行命令前，应先执行 GET CHALLENGE 命令。

4.2.2.12.2. 使用条件和安全

解锁 PIN 时，命令的执行必须满足 PIN 的访问权限。命令格式为密文校验模式。

4.2.2.12.3. 命令格式

代码	数 值
CLA	‘84’
INS	‘24’
P1	‘00’
P2	‘00’或者‘01’
Lc	‘0C’
DATA	旧 PIN 密文||MAC
Le	不存在

4.2.2.12.4. 响应信息

响应信息中可能返回的状态码有：

SW1	SW2	说 明
90	00	命令执行成功
65	81	写 EEPROM 失败
67	00	Lc 长度错误

69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	88	安全信息（MAC 和加密）数据错误
6A	81	功能不支持
6A	83	未找到 PIN
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

4.2.2.12.5. 命令详解

操作 1： 金融环境下对 PIN 解锁
条件： 被锁定的 PIN 值：1234
通过 MPUK 按照“安全管理”一节的加密算法得到 PIN 密文：83134983D3450BDE
通过 MPUK 按照“安全管理”一节的 MAC 计算得到 MAC：24A2B89D
命令： 842400010C83134983D3450BDE24A2B89D
响应： 9000

4.2.2.13. RELOAD PIN 命令

4.2.2.13.1. 命令描述

RELOAD PIN 命令用于重装 PIN。

4.2.2.13.2. 使用条件和安全

此命令只能在金融应用环境下执行。

RELOAD 命令执行必须满足 PIN 的访问权限和写控制属性。命令的数据域格式为明文校验。

4.2.2.13.3. 命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘00’
P2	‘00’
Lc	‘06’~‘0A’
Data	重装的 PIN 值 || MAC
Le	不存在

4.2.2.13.4. 响应信息

SW1	SW2	含义
90	00	命令执行成功
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 长度错
69	83	验证方法锁定
69	85	使用条件不满足
69	88	安全报文数据项不正确
6A	80	数据域参数不正确
6A	81	功能不支持

6A	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
6A	88	引用数据找不到
93	03	应用永久锁定

4.2.2.13.5. 命令详解

操作 1： 金融环境下对 PIN 重装
条件： 重装的新 PIN 值：1234
通过 MPUK 按照“安全管理”一节的 MAC 计算得到 MAC：24A2B89D
命令： 805E000006123424A2B89D
响应： 9000

4.2.2.14. UPDATE OVERDRAW LIMIT 命令

4.2.2.14.1. 命令描述

UPDATE OVERDRAW LIMIT 命令用于修改透支限额。修改透支限额表示允许持卡人透支消费的额度，是一种信用的体现。修改透支限额是金融机构为持卡人设定的透支额度。

4.2.2.14.2. 使用条件和安全

UPDATE OVERDRAW LIMIT 命令执行之前，必须成功执行 INITIALIZE FOR UPDATE 命令。

4.2.2.14.3. 命令报文

代码	值
CLA	‘80’
INS	‘58’
P1	‘00’
P2	‘00’
Lc	‘0E’
Data	新透支限额（3 字节） 交易日期（4 字节） 交易时间（3 字节） MAC2（4 字节）
Le	‘04’（TAC）

计算 MAC2 的数据包括：

—新透支限额 3 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

4.2.2.14.4. 响应信息

命令执行成功返回的数据包括以下内容：

—TAC 4 字节

计算 TAC 的数据包括：

—新余额 4 字节
—联机交易序号（加 1 前） 2 字节
—新透支限额 3 字节
—交易类型 1 字节
—终端机编号 6 字节
—交易日期 4 字节
—交易时间 3 字节

命令执行不成功，则只返回状态码 SW1 和 SW2。

SW1	SW2	含义
90	00	命令执行成功
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
65	81	EEPROM 损坏，导致卡锁定
67	00	长度错误
69	01	命令不接受（无效状态）
69	83	认证方法锁定
69	85	使用条件不满足
6A	81	功能不支持
6A	86	参数 P1、P2 不正确
6D	00	命令不存在
6E	00	命令类型错
93	02	MAC 无效
94	01	金额不足

4.2.2.14.5. 命令详解

结果： 完成修改透支限额操作
条件： 终端当前的日期：2003 ，10， 10
终端当前的时间：15 ： 30 ： 00
通过修改透支限额交易中的过程密钥计算得到的 MAC2 ： 453BC1F3

（MAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算）

成功执行 INITIALIZE FOR UPDATE 命令

新透支限额 ： 0003E8

命令： 805800000E0003E820031010153000453BC1F3

响应： 返回 TAC ：A2345FE

（TAC 计算参照“安全管理”一章中金融环境下交易 MAC 的计算，使用 TAC 密钥）

5. 卡片个人化

5.1. 卡片初始化

卡片初始化操作由卡片提供商来完成。

卡片初始化所要完成的任务：

1、向卡片写入制造商密钥，密钥用途是外部认证密钥。进行卡片个人化操作之前，需要认证此密钥获得权限，认证通过后，可以建立 MF，进行卡片个人化处理，之后此密钥自动作废。

2、写入卡片复位应答的初始历史信息。此历史信息在卡片个人化操作时，可以通过在 MF 下建立 ATR 文件替换为用户需要的信息。

5.2. 卡片个人化

卡片个人化是对卡片根据应用的需要所进行的操作。

卡片个人化所要完成的任务：

1、创建应用所需要的文件结构；

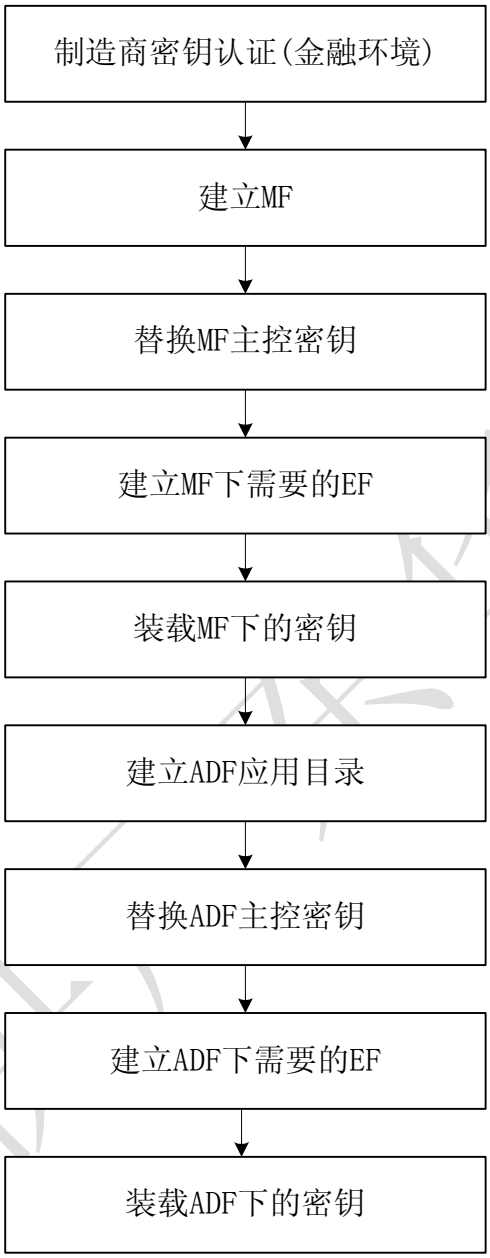
2、完成应用所需要的密钥的装载；

3、写入应用要求的数据。

经过个人化的卡片可以在实际应用中使用。

5.2.1. 卡片个人化流程

卡片个人化简易流程见下图：


制造商密钥认证(金融环境)
建立MF
替换MF主控密钥
建立MF下需要的EF
装载MF下的密钥
建立ADF应用目录
替换ADF主控密钥
建立ADF下需要的EF
装载ADF下的密钥

6. 交易流程

6.1. 金融应用交易流程

6.1.1. 交易预处理

图 6-1 给出了对电子存折/电子钱包应用的所有交易类型共有的预处理流程。

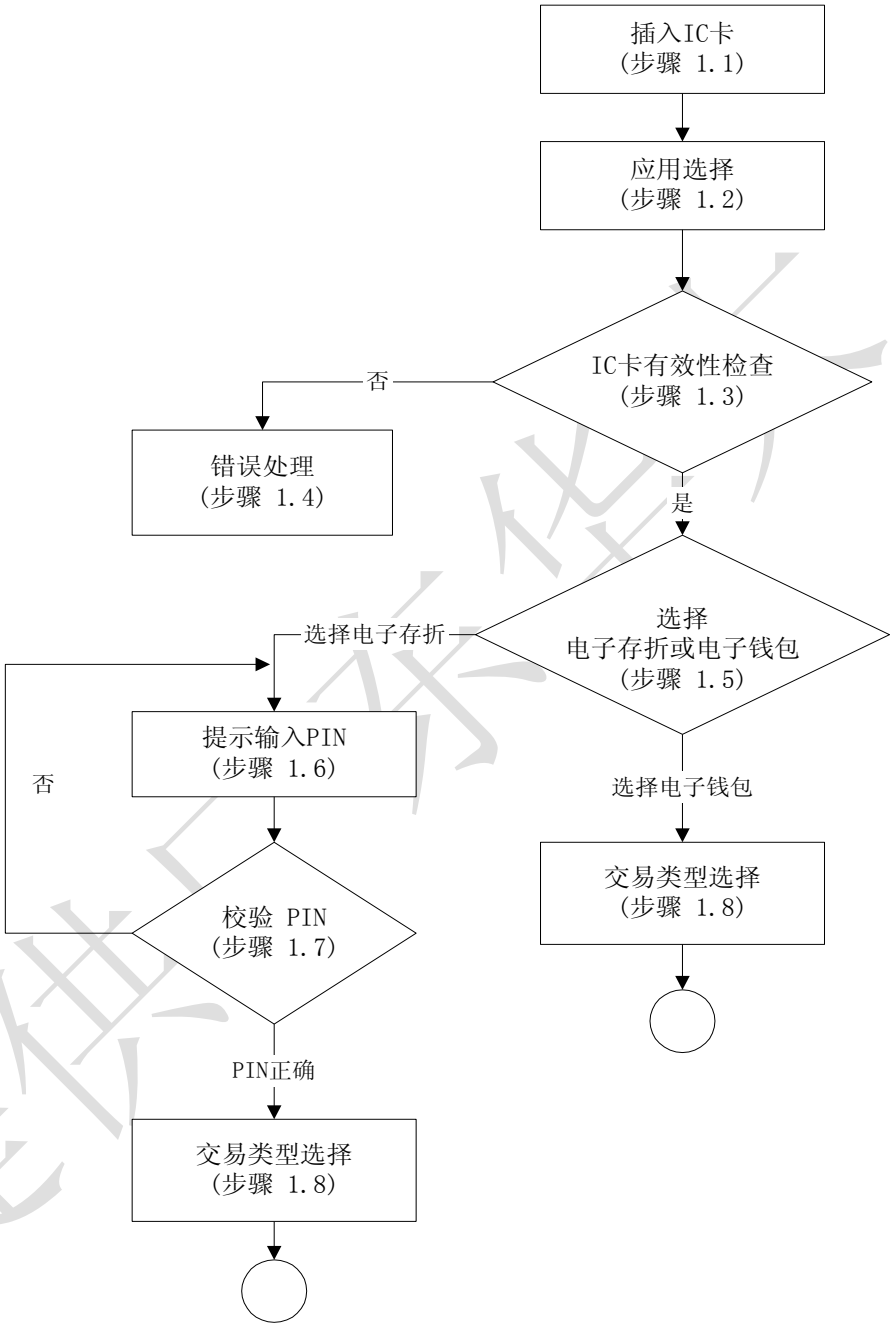

插入IC卡
(步骤 1.1)
应用选择
(步骤 1.2)
IC卡有效性检查
(步骤 1.3)
否
错误处理
(步骤 1.4)
是
选择
电子存折或电子钱包
(步骤 1.5)
选择电子存折
提示输入PIN
(步骤 1.6)
否
校验 PIN
(步骤 1.7)
PIN正确
交易类型选择
(步骤 1.8)
选择电子钱包
交易类型选择
(步骤 1.8)

图 6-1 交易预处理流程

6.1.1.1. 插入 IC 卡(步骤 1.1)

终端应具有检测 IC 卡是否已经插入读卡器的功能。如果 IC 卡已经插入，终端将继续执行 6.1.1.2 节的应用选择功能。

6.1.1.2. 应用选择(步骤 1.2)

执行 SELECT FILE 命令进行应用选择。

应用选择的执行过程请参见《中国金融集成电路(IC)卡规范》第 1 部分:卡片规范的“应用选择”部分。电子存折/电子钱包应用的应用标识符（AID）将由全国金融标准化技术委员会负责分配和维护。

成功地选择了电子存折/电子钱包应用后，IC 卡回送包含发卡方专用数据在内的文件控制信息 FCI。下表定义了此应用必备的发卡方专用数据。

数据字段的描述	长度 (字节)
发卡方机构标识符	8
应用类型标识	1
应用版本号	1
应用序列号	10
应用启用日期	4
应用有效日期	4
发卡方自定义 FCI 数据	2

应用类型标识 (ATI) 在应用选择时由 IC 卡回送给终端。 它标明电子存折/电子钱包应用在卡上的存在情况。

6.1.1.3. IC 卡有效性检查(步骤 1.3)

对于 SELECT 命令送回的数据，终端将对这些数据进行以下检查：

——该卡是否在终端存储的黑名单卡之列（使用发卡方标识和应用序列号）；

——终端是否支持该发卡方标识符；

——终端是否支持 IC 卡上的应用(使用应用类型标识(ATI)来检查)；

——终端是否支持从 IC 卡回送的应用版本号所代表的应用版本；

——应用是否在有效期内。

如果以上任一条件不满足，交易将按 6.1.1.4 节描述进行，否则按 6.1.1.5 中的描述进行。

6.1.1.4. 错误处理(步骤 1.4)

以上任一条件不满足时终端所作的处理不在本手册范围内。

6.1.1.5. 选择电子存折或电子钱包(步骤 1.5)

终端根据应用选择时获得的应用类型标识判别 IC 卡支持 ED、EP 的情况。

如果 IC 卡和终端只同时支持 ED 或 EP 之一，则终端将自动地选择到 ED 或 EP，继而进行 6.1.1.6 或 6.1.1.8 中所描述的步骤。

如果 IC 卡仅支持一种应用并且该应用不被终端支持，则该过程终止。

如果 IC 卡和终端彼此都支持 ED 和 EP 两种应用，终端应向持卡人提供选择 ED 或 EP 的过程，在这一过程中持卡人可以从中选择一种应用进行交易。

6.1.1.6. 提示输入持卡人密码（PIN）(步骤 1.6)

选择了电子存折/电子钱包的应用后，终端将提示持卡人输入 PIN。如果持卡人选择无需 PIN 校验，则终端应以发卡方默认的 PIN 作为持卡人的输入。

如果在此之前，终端通过其它方式获知持卡人无需 PIN 校验，则终端可以不提示持卡人输入 PIN，而以发卡方默认的 PIN 作为持卡人的输入。

6.1.1.7. 校验 PIN(步骤 1.7)

持卡人输入 PIN 后，终端将用 VERIFY 命令来校验持卡人输入的 PIN 是否正确。VERIFY 命令在本手册中命令部分定义。

当 IC 卡收到校验（VERIFY）命令后，它将进行以下操作：

——检查 PIN 尝试计数器。如果 PIN 尝试计数器为零时，PIN 被锁住且不能执行相应的命令。这种情况下，IC 卡返回状态‘6983’（认证方式锁定），终端结束交易过程。

——如果 PIN 没有被锁，将命令数据中的 PIN 和 IC 卡中存放的 PIN 进行比较。

——如果以上两 PIN 相同，IC 卡将 PIN 尝试计数器置为 PIN 重试的最大次数并返回状态‘9000’。IC 卡必须在断电之前或选择其他应用前记住 PIN 已经成功验证。交易处理按 6.1.1.8 节的描述继续进行。

——如果以上两 PIN 并不相同，IC 卡将 PIN 尝试计数器减 1 并返回状态‘63Cx’，这里’x’是 PIN 尝试计数器的新值。在这种情况下，终端将检查 x 的值。如果 x 是零，将终止交易并且卡片自动锁 PIN。否则，终端将提示重新输入 PIN 并且重复以上过程。

如果持卡人输入的 PIN 是正确的，交易流程执行 6.1.1.8 节。

6.1.1.8. 交易类型选择(步骤 1.8)

终端应该具备让持卡人选择交易类型的功能。每次交易最多只能选择一种交易类型。

对电子存折应用来说，持卡人应能选择如下交易类型：圈存、 圈提、消费、取现、修改透支限额、查询余额、查询明细。

对电子钱包应用来说，持卡人应能选择如下交易类型：圈存、消费、查询余额。

6.1.2. 圈存交易

通过圈存交易，持卡人可将其在银行帐户上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提交个人密码（PIN）（无论电子存折或电子钱包）。

6.1.2.1. 发出 INITIALIZE FOR LOAD 命令(步骤 2.1)

终端述发出 INITIALIZE FOR LOAD 指令启动圈存交易。

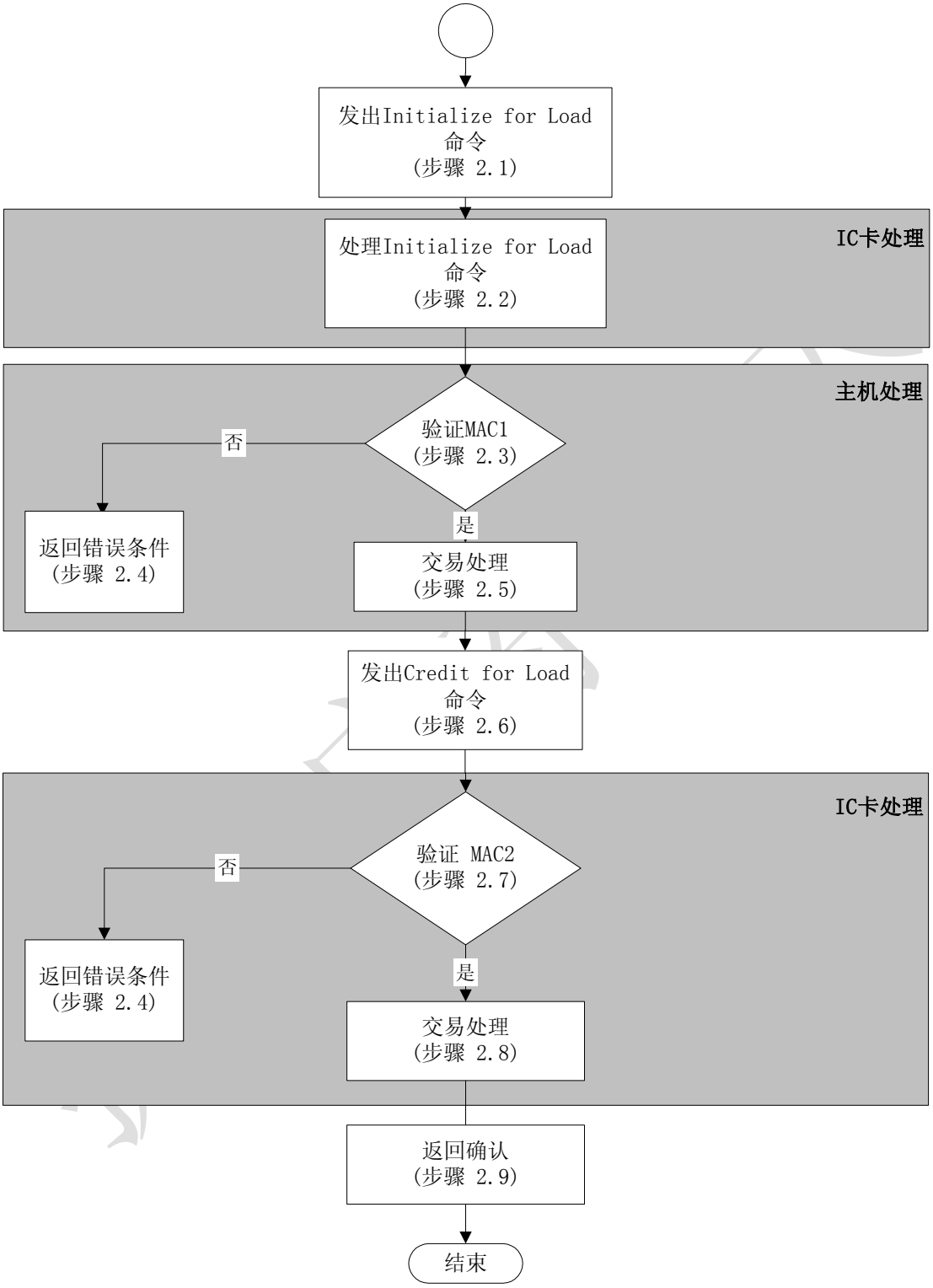


图 6-2 圈存交易处理流程

6.1.2.2. 处理圈存初始化(步骤 2.2)

收到圈存初始化命令后, IC 卡将进行以下操作：

——检查命令中包含的密钥索引是否能被 IC 卡支持。如果不支持，返回状态码‘9403’（不支持的密钥索引）且不返回其他数据，命令的处理结束。

——IC 卡产生一个伪随机数（ICC），过程密钥 SESLK 和一个报文验证码（MAC1 表示），以以供主机验证圈存交易和 IC 卡的合法性。

过程密钥 SESLK 被用于电子存折或电子钱包的圈存交易。过程密钥是用 DLK 密钥和安全管理一章中的机制产生的。用来产生过程密钥的输入数据如下:

SESLK：伪随机数（ICC）||电子存折联机交易序号或电子钱包联机交易序号||‘8000’

MAC1 的计算机制见安全管理一章。SESLK 作用于以下数据进行 MAC1 计算(按所列顺序):

——电子存折或电子钱包余额

——交易金额

——交易类型标识

——终端机编号

IC 卡将把 INITIALIZE FOR LOAD 命令的响应报文送给终端处理。如果 IC 卡返回的状态不是‘9000’，终端将终止交易。

6.1.2.3. 验证 MAC1(步骤 2.3)

收到圈存初始化命令的响应报文后, 终端把该响应报文定义的数据传给发卡机构主机。主机将生成 SESLK 并且确认 MAC1 是否有效。如果 MAC1 有效, 交易处理将按 6.1.2.5 节描述的继续执行。如果 MAC1 无效，交易处理将执行 6.1.2.4 中所描述的步骤节。

6.1.2.4. 返回错误状态(步骤 2.4)

如果出现使圈存交易不能被接受的条件，则主机应通知终端。送给终端的报文格式和内容，以及终端采取的动作在本手册的讨论范围以外。

6.1.2.5. 交易处理(步骤 2.5)

在确认能够进行圈存交易后，主机从持卡人在银行的相应帐户中减去持卡人输入的圈存金额。

主机也会产生一个报文验证码(MAC2 表示)，供 IC 卡对主机合法性进行检查。安全管理一章中描述了主机用来生成 MAC2 的机制。SESLK 作用于以下数据进行 MAC2 计算(按所列顺序):

——交易金额

——交易类型标识

——终端机编号
——交易日期 (主机)
——交易时间 (主机)

在成功地进行了圈存交易后，主机将电子存折联机交易序号或电子钱包联机交易序号加 1，并发送一个圈存交易接受报文给终端，其中包括 MAC2、交易日期（主机）和交易时间（主机）。

6.1.2.6. 发出 CREDIT FOR LOAD 命令(步骤 2.6)

在收到主机的圈存交易接受报文后，终端会发出 CREDIT FOR LOAD 命令给 IC 卡以更新卡上电子存折或电子钱包余额。

6.1.2.7. 验证 MAC2 (步骤 2.7)

收到 CREDIT FOR LOAD 命令后, IC 卡必须确认 MAC2 是有效的。如果 MAC2 有效,交易处理将执行 6.1.2.8 节。 如果 MAC2 无效，状态‘9302’（MAC 无效）会被返回给终端。终端对错误所应采取相应的动作。

6.1.2.8. 交易处理(步骤 2.8)

IC 卡将电子存折或电子钱包联机交易序号加 1，并且把交易金额加在电子存折或电子钱包的余额上。IC 卡必须全部成功地完成以上几个步骤或者一个也不完成。

在电子存折或电子钱包圈存交易中，IC 卡用以下数据组成的一个记录更新交易明细：
——电子存折或电子钱包联机交易序号
——交易金额
——交易类型标识
——终端机编号
——交易日期 (主机)
——交易时间 (主机)

TAC 的计算机制见安全管理一章。TAC 的计算不用过程密钥方式，它用 DTK 左右 8 位字节异或运算的结果对以下数据进行加密运算来产生(按所列顺序):

——电子存折或电子钱包余额
——电子存折或电子钱包联机交易序号（加 1 前）
——交易金额
——交易类型标识
——终端机编号
——交易日期（主机）
——交易时间（主机）

6.1.2.9. 返回确认(步骤 2.9)

在成功完成步骤 6.1.2.8 后， IC 卡将 CREDIT FOR LOAD 命令的响应报文 TAC 返回给终端。主机可以不马上验证 TAC。

6.1.3. 圈提交易

通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回到其相应账户上。这种交易必须在金融终端上联机进行并要求验证个人密码（PIN）。只有电子存折应用支持圈提交易。

6.1.3.1. 发出 INITIALIZE FOR UNLOAD 命令(步骤 3.1)

终端发出 INITIALIZE FOR UNLOAD 命令启动圈提交易。

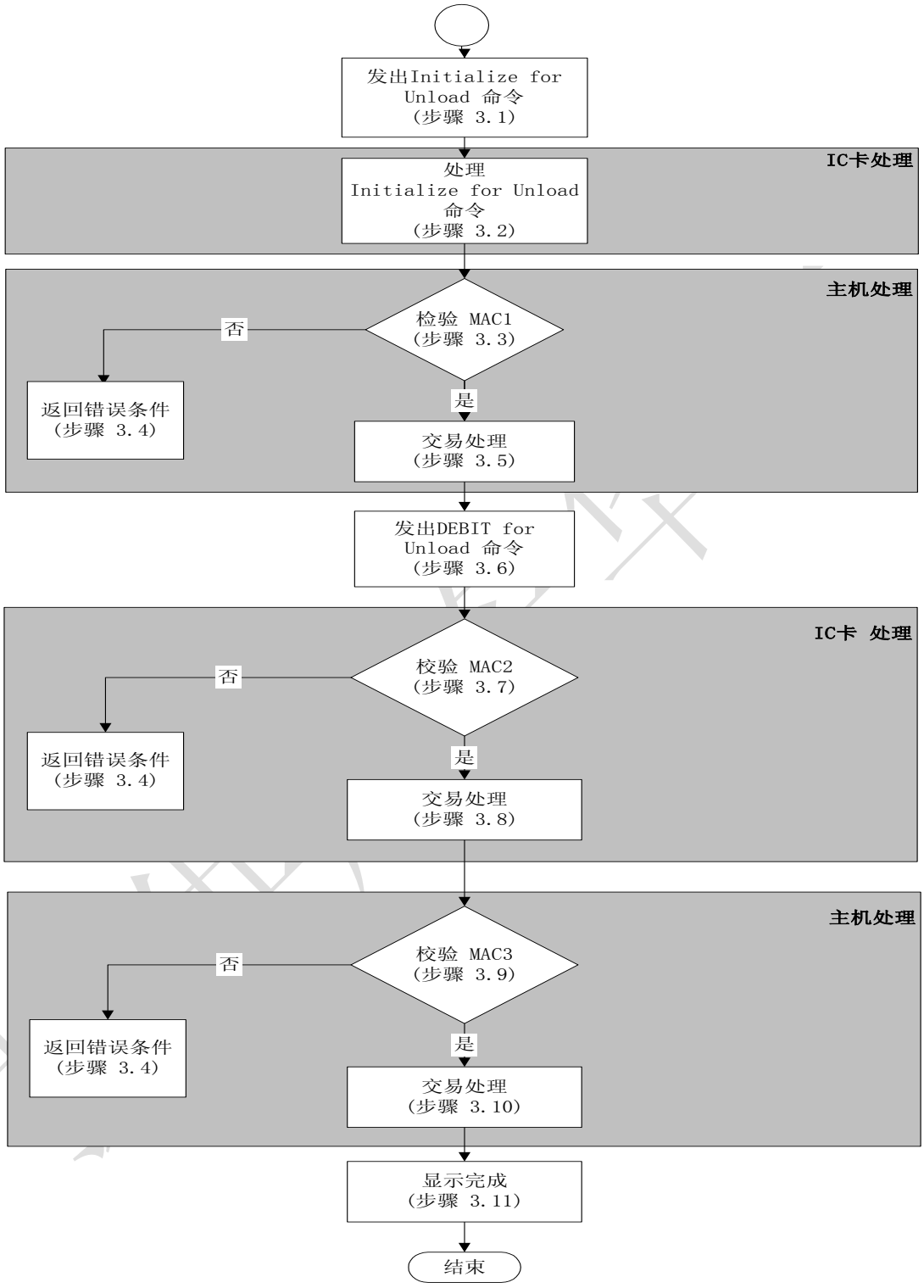


图 6-3 圈提交易处理流程

6.1.3.2. 处理 INITIALIZE FOR UNLOAD 命令(步骤 3.2)

收到 INITIALIZE FOR UNLOAD 命令后，IC 卡将进行一下操作：

——检查是否支持命令中提到的密钥索引号。如果不支持，则回送状态码‘9403’（不支持的密钥索引）。但不回送任何其他数据，命令处理结束。

——检查命令中包括的交易金额是否超过电子存折余额。如果超过，则回送状态码‘9401’（资金不足），但不回送任何其他数据。

在通过以上检查后，IC 卡将产生一个伪随机数（ICC）、过程密钥 SESULK 和一个报文鉴别码（MAC1），供主机验证圈提交易及 IC 卡的合法性。

SESULK 是用于电子存折圈提交易的过程密钥。该过程密钥是利用 DULK 并按照安全管理中过程密钥一节所描述的机制产生的。用来产生该过程密钥的输入数据如下：

SESULK：伪随机数（ICC）||电子存折联机交易序号||‘8000’

MAC1 的计算机制见安全管理一章。用 SESULK 对以下数据加密产生 MAC1（按所列顺序）：

—电子存折余额

—交易金额

—交易类型标识

—终端机编号

IC 卡应向终端回送前面所定义的 INITIALIZE FOR UNLOAD 命令的响应报文和状态码‘9000’。在收到 INITIALIAZE FOR UNLOAD 的响应报文后，终端将一个包含 INITIALIAZE FOR UNLOAD 响应报文数据域中规定的数据的圈提许可请求报文 MAC1 送往发卡方主机。

6.1.3.3. 验证 MAC1(步骤 3.3)

主机将产生 SESULK 并验证 MAC1 是否有效。如果 MAC1 有效，将执行 6.1.3.5 中的步骤。否则终端回送一个错误状态码，交易处理将转而执行 6.1.3.4 中所描述的步骤。

6.1.3.4. 回送错误状态(步骤 3.4)

如果不接受圈提交易，主机应通知终端。终端的处理方式不在本手册范围之内。

6.1.3.5. 主机处理(步骤 3.5)

主机确认能够进行圈提交易后，将产生一个报文鉴别码（MAC2），以供 IC 卡对主机合法性检查。下面列出包含在 DEBIT FOR UNLOAD 命令中从主机经由终端传到 IC 卡的数据。

MAC2 的计算机制见安全管理一章。用 SESULK 对以下数据进行加密（按所列顺序）产生 MAC2：

—交易金额

—交易类型标识
—终端机编号
—交易日期（主机）
—交易时间（主机）

主机向终端发送一个圈提交易接受报文，其中至少应包括交易日期（主机）、交易时间（主机）和 MAC2。

6.1.3.6. 发出 DEBIT FOR UNLOAD 命令(步骤 3.6)

终端收到主机的圈提交易接受报文后，向 IC 卡发出 DEBIT FOR UNLOAD 命令以更新卡上电子存折余额。

6.1.3.7. 验证 MAC2(步骤 3.7)

IC 卡必须确认 MAC2 是有效的。如果 MAC2 有效，交易处理将执行 6.1.3.8 中所描述的步骤。否则向终端回送状态码‘9302’（MAC2）无效。

6.1.3.8. 交易处理(步骤 3.8)

IC 卡将电子存折联机交易序号加 1，并从卡上的电子存折余额中扣减交易金额。IC 卡必须成功地完成以上所有步骤或者一个也不完成。

IC 卡将产生报文鉴别码（MAC3）。并通过 DEBIT FOR UNLOAD 命令的响应报文将以下数据经终端送往主机。

MAC3 的计算机制见安全管理一章。用 SESULK 对以下数据加密产生 MAC3（按所列顺序）：
—电子存折余额
—电子存折联机交易序号（加 1 前）
—交易金额
—交易类型标识
—终端机编号
—交易日期（主机）
—交易时间（主机）

IC 卡用以下数据组成的一个记录更新交易明细：
—电子存折联机交易序号（加 1 前）
—交易金额
—交易类型标识
—终端机编号
—交易日期（主机）

—交易时间（主机）

6.1.3.9. 验证 MAC3(步骤 3.9)

主机收到（经由终端）IC 卡回送的 MAC3 后，应确认 MAC3 是否有误。如果 MAC3 有效，交易处理将执行 6.1.3.10 中描述的步骤。否则将向终端回送一个错误状态码。

6.1.3.10. 交易处理(步骤 3.10)

发卡方主机将交易金额加在持卡人的相应银行账户上，并将主机的电子存折联机交易序号加 1。

主机向终端回送一个完成报文，表示持卡人的账户已更新。本手册不规定报文的内容和形式。

6.1.3.11. 显示完成(步骤 3.11)

在收到主机的完成报文后，终端将向持卡人显示交易完成信息。

如果需要，终端应能向持卡人提供交易纸凭证。

6.1.4. 消费交易

消费交易允许持卡人使用电子存折或电子钱包的余额进行消费。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。

6.1.4.1. 发出 INITIALIZE FOR PURCHASE 命令(步骤 4.1)

终端发出 INITIALIZE FOR PURCHASE 命令启动消费交易

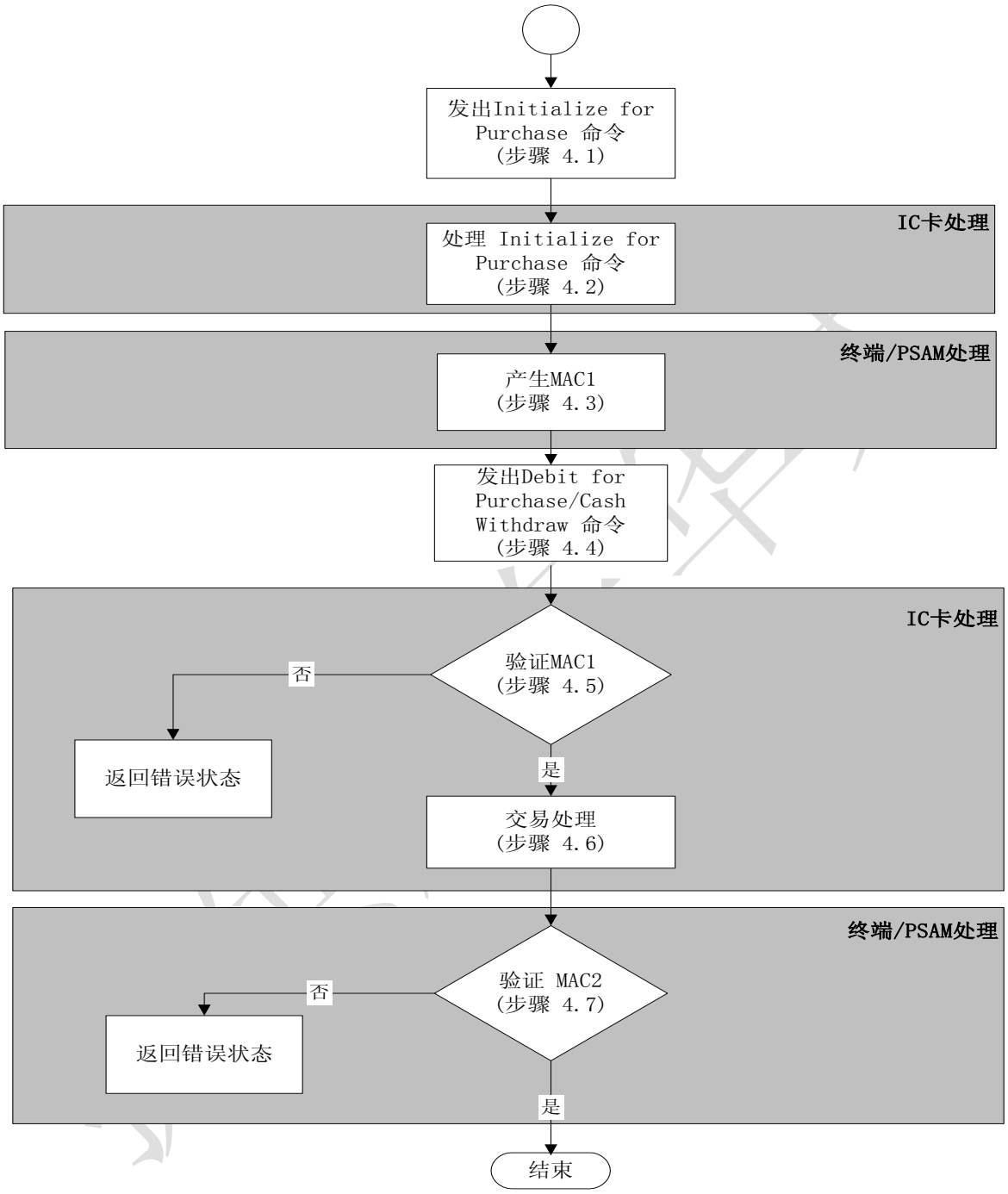


图 6-4 消费交易处理流程

6.1.4.2. 处理 INITIALIZE FOR PURCHASE 命令(步骤 4.2)

IC 卡收到 INITIALIZE FOR PURCHASE 命令后，IC 卡将进行以下操作：

——检查命令中包含的密钥索引是否被 IC 卡支持。如果不支持，返回状态码‘9403’（不支持的密钥索引）且不返回其他数据。

——检查电子存折余额或电子钱包余额是否大于或等于交易金额。如果小于交易金额，状态码‘9401’（资金不足）返回给终端，不返回其他数据。终端采取的措施不在本手册的范围内。

如果以上检验均无错误，IC 卡产生一个伪随机数（ICC），过程密钥 SESPK 以用于验证 MAC1。过程密钥是用 DPK 并按照安全管理一章中描述的机制产生的。用于生成过程密钥的输入数据如下：

SESPK：伪随机数（ICC）||电子存折脱机交易序号或电子钱包脱机交易序号||终端交易序号的最右两个字节。

6.1.4.3. 产生 MAC1(步骤 4.3)

使用伪随机数（ICC）和 IC 卡返回的电子存折脱机交易序号或电子钱包脱机交易序号，终端的安全存取模块（PSAM）将产生一样的过程密钥（SESPK）和一个报文认证码（MAC1），供 IC 卡来验证 PSAM 的合法性。

MAC1 的计算机制见安全管理一章。SESPK 作用于以下数据进行 MAC1 的计算(按所列顺序):

——交易金额
——交易类型标识
——终端机编号
——交易日期（终端）
——交易时间（终端）

6.1.4.4. 发出 DEBIT FOR PURCHASE/CASH WITHDRAW 命令 (步骤 4.4)

终端发出 DEBIT FOR PURCHASE/CASH WITHDRAW 命令。

6.1.4.5. 验证 MAC1(步骤 4.5)

在收到 DEBIT FOR PURCHASE 命令后，IC 卡要验证 MAC1 的有效性。如果 MAC1 是有效的, 交易处理将继续执行 6.1.4.6 节。如果 MAC1 是无效的，错误状态‘9302’（MAC 无效）被返回给终端。

6.1.4.6. 交易处理(步骤 4.6)

IC 卡从电子存折或电子钱包余额中扣减消费的金额，将电子存折或电子钱包脱机交易序号加 1。IC 卡必须全部成功地完成以上几个步骤或者一个也不完成，如果余额或序号的更新均没有成功，交易明细也不应被更新。

IC 卡产生一个报文验证码 (MAC2 表示)供 PSAM 对 IC 卡合法性进行检查。并通过 DEBIT FOR PURCHASE 命令响应报文回送以下数据，作为 PSAM 产生 MAC2 的输入数据。MAC2 的产生机制参见安全管理一章。用 SESPK 于以下数据进行加密产生 MAC2：

——交易金额

IC 卡按照安全管理一章中描述的机制用密钥 DTK 左右 8 字节异或运算后的结果产生 TAC。TAC 将被写入终端交易明细，以便后来传给主机进行交易验证。下面是用来生成 TAC 的数据，它们以明文形式包含在 CREDIT FOR PURCHASE 命令的响应报文中从 IC 卡传传到终端：

——交易金额
——交易类型标识
——终端机编号
——终端交易序号
——交易日期 (终端)
——交易时间 (终端)

对于电子存折消费交易，IC 卡将用以下数据组成的一个记录更新交易明细。

——电子存折脱机交易序号
——交易金额
——交易类型标识
——终端机编号
——交易日期 (终端)
——交易时间 (终端)

6.1.4.7. 验证 MAC2 (步骤 4.7)

收到从 IC 卡(经过终端)传来的 MAC2 后, PSAM 要验证 MAC2 的有效性。MAC2 验证的结果被传送到终端以便采取必要的措施。终端采取的措施不在本手册的范围之内。

6.1.5. 取现交易

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

6.1.5.1. 发出 INITIALIZE FOR CASH WITHDRAW 命令(步骤 5.1)

终端发出 INITIALIZE FOR CASH WITHDRAW 命令启动取现交易

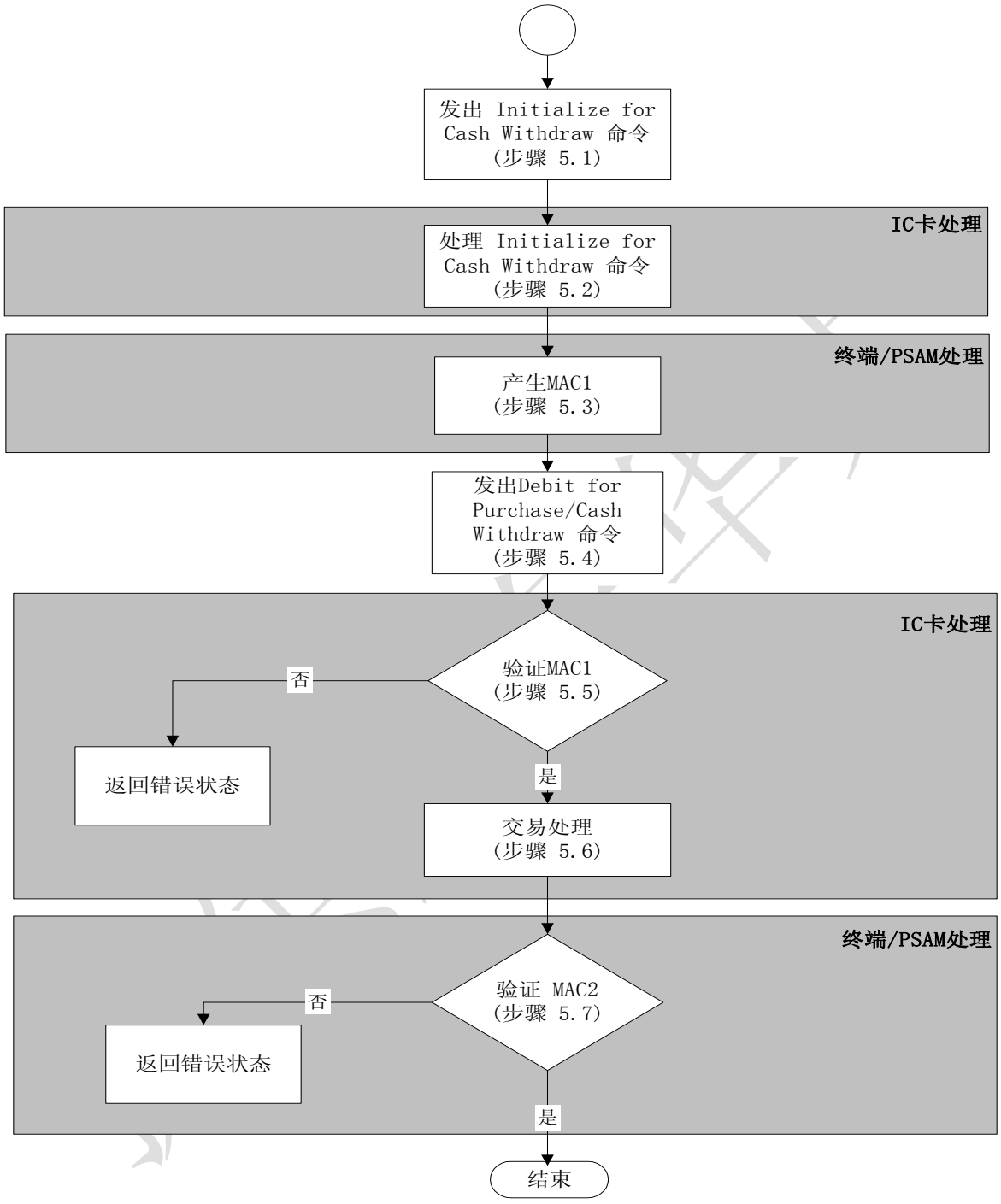


图 6-5 取现交易处理流程

6.1.5.2. 处理 INITIALIZE FOR CASH WITHDRAW(步骤 5.2)

收到 INITIALIZE FOR CASH WITHDRAW 命令后，IC 卡将进行以下操作：

——检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态码‘9403’ （不支持的密钥索引），但不回送其他数据。

——检查电子存折余额是否大于或等于交易金额。如果小于交易金额，状态码‘9401’（资金不足）返回给终端，不返回其他数据。终端采取的措施不在本手册的范围内。

对以上错误状态终端的处理不在本手册的范围内。

通过以上检查之后，IC 卡将产生一个伪随机数（ICC）和一个过程密钥 SESPK。该过程密钥是利用 DPK 并按安全管理一章描述的机制产生的。用于产生过程密钥的输入数据如下：SESPK：伪随机数（ICC）||电子存折脱机交易序号||终端交易序号的最右两个字节。

6.1.5.3. 验证 MAC1(步骤 5.3)

验证了交易金额有效之后，终端使用伪随机数（ICC）和 IC 卡回送的电子存折的脱机交易序号来产生相同的过程密钥（SESPK）和一个报文签别码（MAC1），供 IC 卡来验证 PSAM 的合法性。

MAC1 的计算机制见附录 B。用 SESPK 对以下数据加密产生 MAC1(按所列顺序):

——交易金额

——交易类型标识

——终端机编号

——交易日期（终端）

——交易时间（终端）

6.1.5.4. 发出 DEBIT FOR PURCHASE/CASH WITHDRAW 命令(步骤 5.4)

终端发出 DEBIT FOR PURCHASE/CASH WITHDRAW 命令。

6.1.5.5. 验证 MAC1(步骤 5.5)

在收到 DEBIT FOR PURCHASE/CASH WITHDRAW 命令后，IC 卡将验证 MAC1 的有效性。如果 MAC1 有效, 交易处理会继续执行 6.1.5.6 中所描述的步骤。否则将向终端回送错误状态码‘9302’（MAC 无效）。终端对错误状态的处理不在本手册范围以内。

6.1.5.6. 交易处理(步骤 5.6)

IC 卡从卡上的电子存折余额中扣减取现交易金额，将电子存折脱机交易序号加 1。IC 卡必

须成功地完成以上所有步骤或者一个也不完成，如果余额或序号的更新没有成功，交易明细也不应被更新。

IC 卡产生一个报文签别码 (MAC2)供 PSAM 对 IC 卡合法性进行检查。IC 卡通过 DEBIT FOR PURCHASE/CASH WITHDRAW 命令响应报文将以下数据送给 PSAM (通过终端) ，作为产生 MAC2 的输入数据。用 SESPK 对以下数据加密产生 MAC2：

——交易金额

IC 卡执照安全管理一章中描述的机制直接用 DTK 产生 TAC。TAC 将被写入终端交易明细，以便于主机进行验证。下面是用来产生 TAC 的数据，它们以明文形式包含在 CREDTE FOR PURCHASE/CASH WITHDRAW 命令的响应报文中从 IC 卡传送到终端：

——交易金额
——交易类型标识
——终端机编号
——终端交易序号
——交易日期 (终端)
——交易时间 (终端)

IC 卡将用以下数据组成的一个记录更新 IC 卡交易明细。

——电子存折脱机交易序号
——交易金额
——交易类型标识
——终端机编号
——交易日期 (终端)
——交易时间 (终端)

6.1.5.7. 验证 MAC2(步骤 5.7)

在收到从 IC 卡(经过终端)传来的 MAC2 后, PSAM 将验证 MAC2 的有效性。MAC2 验证的结果被传送到终端以便采取必要的措施。终端的处理不在本手册的范围之内。

6.1.6. 修改透支限额交易

“透支功能”是从技术上支持的一种基于电子存折应用的有限信用功能。当电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，且必须验证个人密码（PIN）。

是否使用“透支功能”以及允许透支的额度由发卡方决定。修改透支限额交易的具体业务做法和要求不在本手册的范围之内

如果透支限额存在，电子存折的余额是实际圈存余额与透支限额之和。

6.1.6.1. 发出 INITIALIZE FOR UPDATE 命令(步骤 6.1)

终端发出 INITIALIZE FOR UPDATE 命令启动后修改透支限额交易。

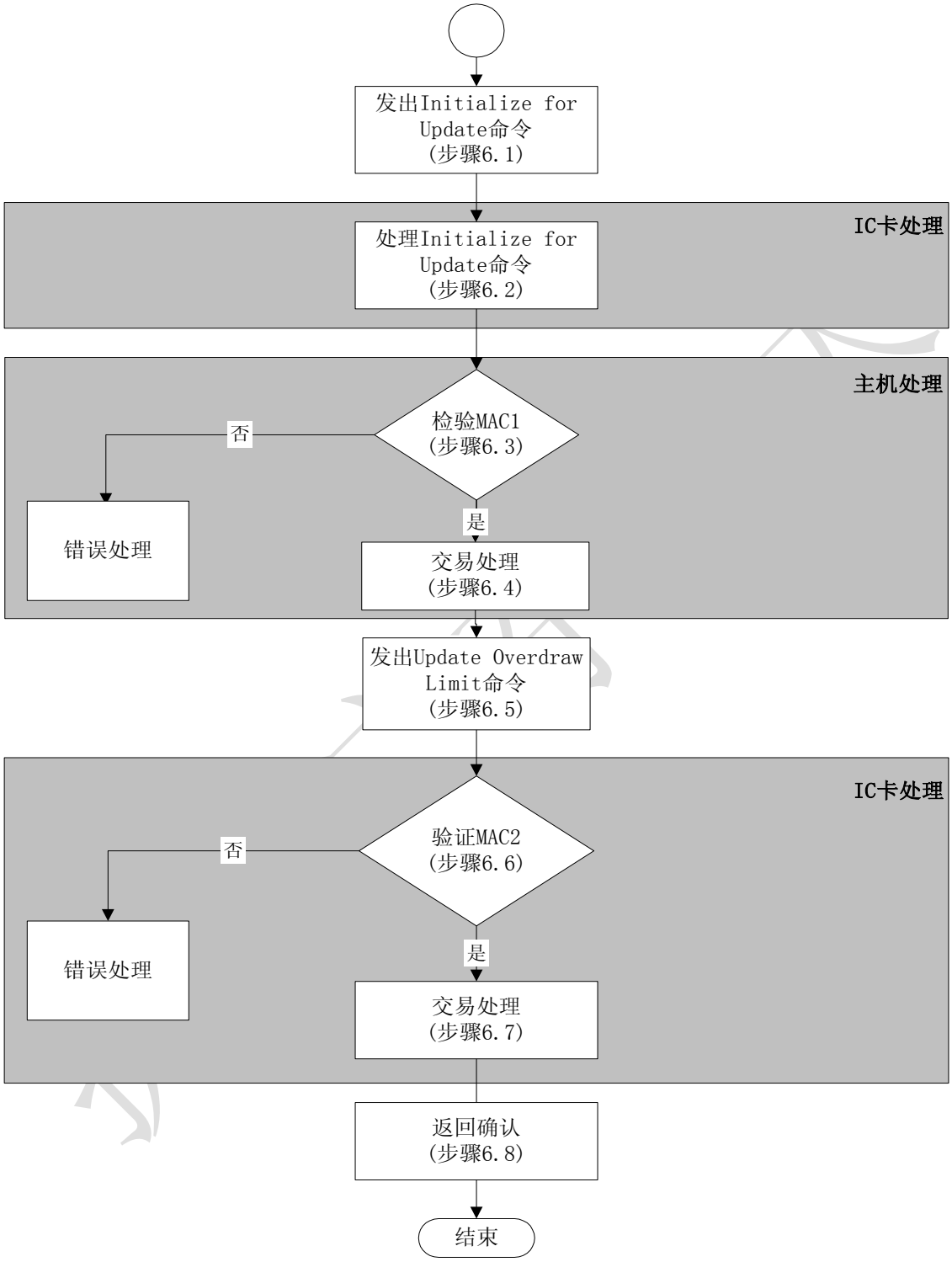


图 6-6 修改透支限额交易

6.1.6.2. 处理 INITIALIZE FOR UPDATE 命令(步骤 6.2)

收到 INITIALZE FOR UPDATE 命令后，IC 卡将进行以下操作：

——检查是否支持命令中提供的密钥索引号。如果不支持，则回送状态码‘9403’（不支持的密钥索引），但不回送其它数据。

终端对以上错误所做的处理不在本手册的范围内

在通过了以上检查之后，IC 卡将产生一个伪随机数（ICC）、一个过程密钥（SESUK）和一个报文鉴别码（MAC1）。该过程密钥是利用 DUK 并按安全管理一章中描述的机制产生的。用于产生过程密钥的输入数据如下：

SESUK：伪随机数（ICC）||电子存折联机交易序号||‘8000’

MAC1 的计算机制见安全管理一章。用 SESULK 对以下数据加密产生 MAC1（按所列顺序）：

—电子存折余额

—透支限额

—交易类型标识

—终端机编号

6.1.6.3. 验证 MAC1(步骤 6.3)

在收到 INITIALIZE FOR UPDATE 命令执行成功的响应报文后，终端应向主机传送 INITIALIZE FOR UPDATE 命令响应报文中定义的数据以及其他主机需要的数据以便于 MAC1 的验证。

利用终端传来的报文，主机将产生与 IC 卡相同的过程密钥（SESUK）来验证 MAC1。

如果 MAC1 有效，交易处理将执行 6.1.6.4 中所描述的步骤，否则，主机应向终端送错误状态码。终端针对错误状态所做的处理不在本手册的范围内。

6.1.6.4. 主机处理(步骤 6.4)

假定主机已经知道 IC 卡的透支限额。

基于 MAC1（或者其他由主机决定的验证标准）验证的结果，主机将决定是否允许修改透支限额。

如果主机拒绝交易，则应向终端发送一个拒绝报文，结束交易处理。

如果主机允许交易，则应生成一个报文鉴别码（MAC2），以供 IC 卡对主机合法性进行检查。

MAC2 的计算机制见安全管理一章。用 SESULK 对以下数据进行加密（按所列顺序）产生 MAC2：

—透支限额

—交易类型标识

—终端机编号

—交易日期（主机）
—交易时间（主机）
主机将电子存折联机交易序号加 1。
主机向终端发送一个至少包括新透支限额、交易日期（主机）、交易时间（主机）和 MAC2 的许可信息。

6.1.6.5. 发出 UPDATE OVERDRAW LIMIT 命令(步骤 6.5)

如果主机同意交易，终端将发出 UPDATE OVERDRAW LIMIT 命令。

6.1.6.6. 验证 MAC2(步骤 6.6)

IC 卡必须认证 MAC2 的有效性。如果 MAC2 有效，交易处理将执行 6.1.6.7 中所描述的步骤。否则向终端回送状态码‘9302’（MAC2）无效。终端对此错误状态所做的处理不在本手册的范围内。

6.1.6.7. 交易处理(步骤 6.7)

IC 卡将按照安全管理一章所描述的机制，直接用密钥 DTK 对以下数据加密产生一个 TAC：
——电子存折余额
——电子存折联机交易序号
——电子存折透支限额
——交易类型标识
——终端机编号
——交易日期（主机）
——交易时间（主机）
将当前电子存折余额置为新的电子存折余额，更新透支限额并使电子存折联机交易序号加 1。这三个修改必须全部完成，或一个也不完成。
——电子存折联机交易序号
——透支限额
——交易类型标识
——终端机编号
——交易日期（主机）
——交易时间（主机）
IC 卡通过响应报文将 TAC 和状态码‘9000’传送给终端。
IC 卡将用以下数据组成的一个记录更新 IC 卡交易明细。
——电子存折脱机交易序号

——透支限额
——交易类型标识
——终端机编号
——交易日期 (终端)
——交易时间 (终端)

6.1.6.8. 回送确认(步骤 6.8)

IC 卡在 UPDATE OVERDRAW LIMIT 命令中的响应报文中回送 TAC 和一个完成码，表明透支限额已经被成功更新。

6.1.7. 查询余额交易

持卡人可以通过终端或其他读卡设备读取电子存折/钱包中的余额。此交易一般脱机进行。在电子存折应用中进行此交易必须提交个人密码（PIN）。电子钱包则不需要。

终端通过 GET BLANCE 命令来实现查询余额交易。

6.1.8. 查询明细交易

持卡人可以通过终端或其他读卡设备读取电子存折中的交易明细记录。此交易一般采用脱机方式处理。交易时需提交个人密码（PIN）。

终端发出一个 READ RECORD 命令来获得交易明细。这个命令会回送某个交易明细记录中所含的所有数据。交易明细文件为循环记录文件，且至少包含 10 条记录。

交易明细中的记录用记录号寻址。记录号范围从 1 到 n，n 是文件中记录的最大个数。最近写入的记录号为 1，前一记录号为 2，如此类推直到 n。n 代表文件中最早写入的记录。

6.1.9. 应用维护功能

以下交易必须在有相应密钥的设备上执行。

6.1.9.1. 安全报文

电子存折/电子钱包应用涉及到的安全机制，请参考本手册安全管理一章，并作如下改动和增补：

——在传送一个包含安全报文的命令前，主机向终端发送一个报文，要求从 IC 卡获得一个随机数。终端向 IC 卡发出一个 GET CHALLENGE 命令。从 IC 卡回送的随机数被送往主机以用于安全报文处理。

——从 IC 卡回送的 4 字节随机数后缀以‘00 00 00 00’，所得到的结果作为初始值。

——不采用过程密钥。除去 UNBLOCK PIN 命令外，均用导出的应用维护密钥（DAMK）来计算 MAC。UNBLOCE PIN 命令采用导出的 PIN 解锁密钥来产生 MAC。

——全部采用双字节密钥的 3DEA 算法。

6.1.9.2. 卡片锁定

终端发出 CARD BLOCK 命令来锁定卡片。

此命令参照手册“命令”部分。其安全机制在 6.1.9.1 中描述。命令的成功执行使得 IC 卡中的所有应用无效。在这种情况下，进行应用选择将会回送状态码“6A81”（功能不被支持）。

6.1.9.3. 应用锁定

终端发出 APPLICATION BLOCK 命令来锁定应用。

此命令的用法由发卡方自行决定。

此命令参照手册“命令”部分。其安全机制在 6.1.9.1 中描述。在本手册所述的应用中，命令的成功执行导致 IC 卡中的电子存折/电子钱包应用无效。在这种状态下：

——选择此应用时，对 SELECT 命令 IC 卡回送文件控制信息（FCI）和状态码‘6A81’（功能不被支持）。

——在应用被选择后，除以下情况外，IC 卡对其它命令只回送状态码‘6985’（使用的条件不满足）：

a） 当用 SELECT 命令选择此应用或其他应用时；

b） 当用 GET CHALLANGE 命令为 UNBOLCK PIN 命令产生 MAC 时；

c） APPLICATION BLOCK 命令；

d） CARD BOLCK 命令；

如果在命令参数 P2 中指明永久性锁定此应用，IC 卡将设置一个内部标志以表明不允许执行 APPLICATION UNBLOCK 命令。

此命令的执行并不改变电子存折联机交易序号和电子钱包联机交易序号的值。

6.1.9.4. 应用解锁

终端发出 APPLICATION UNBLOCK 命令来对应用解锁，此命令参照手册“命令”部分，其安全机制在 6.1.9.1 中描述。

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并回送状态码‘9303’（应用永久锁定）。

如果在 APPLICATION UNBLOCK 命令中使用了永久锁定的选项，IC 卡将回送状态码‘6983’（认证方式锁定）且不再对应用解锁。

APPLICATION UNBLOCK 命令的成功执行，使应用重新恢复成有效状态。在此之后，该应用对所有命令的响应就像应用锁定和应用解锁没有执行过一样。

此命令的执行并不改变电子存折联机交易序号和电子钱包联机交易序号的值。

6.1.9.5. PIN 解锁

终端发出 UNBLOCK PIN 命令对 PIN 解锁，此命令参照手册“命令”部分，其安全机制在 6.1.9.1 中描述。

在命令报文中，P2 取‘01’值。使用 DPUK 对 PIN 数据加密（参考手册“安全管理”部分）。

如果 PIN 连续三次解锁失败，则 IC 卡将永久锁定此应用并回送状态码‘9303’（应用永久锁定）。

6.1.9.6. 二进制形式修改

终端文件的安全要求，发出 UPDATE BINARY 指令。

如果三次执行此命令均告失败，则 IC 卡将永久锁定此应用并回送状态码‘9303’（应用永久锁定）。

6.1.9.7. 更改 PIN

这个功能不需要 MAC，它可以在任意支持该命令的终端上执行。

当 IC 卡接到此命令时，它将：

——检查 PIN 尝试计数器。如果为 0，PIN 已锁定，此命令不能执行。在这种情况下，IC 卡回送状态码‘6983’（认证方式锁定）。

——如果 PIN 没有锁定，则命令中的‘当前 PIN’会和 IC 卡上存放的 PIN 比较。如果二者相

同，IC 卡将进行以下操作：

a）将 IC 卡上的 PIN 改为命令中的新 PIN；

b）将 PIN 尝试计数器置为 PIN 重试的最大次数。

——如果卡上的 PIN 和命令中的‘当前 PIN’并不相同，IC 卡将进行以下操作：

a）将 PIN 尝试计数器减 1；

b）回送状态码‘63Cx’，这里 x 是 PIN 尝试计数器的新值。如达到零，卡片自动锁 PIN。

6.1.9.8. 重装 PIN

终端发出 RELOAD PIN 命令来重装 PIN。

按照安全管理一章中的机制用密钥 DRPK 来产生一个 MAC。

当这个命令失败三次，应用被永久锁定。

6.1.10. 外部认证

EXTERNAL AUTHENTICATE 命令的目的是 IC 卡验证外部接口设备的有效性，使接口设备对 IC 卡获得某种操作授权。

接口设备提供的认证数据应按以下规则产生：

1、Lc = ‘08’

2、用 GET CHALLENGE 命令向 IC 卡申请一组随机数，作为认证数据输入因子（8 字节）。

3、用指定密钥对随机数作加密计算，产生认证数据（8 字节），参见“安全计算”一节。

IC 卡外部认证过程：

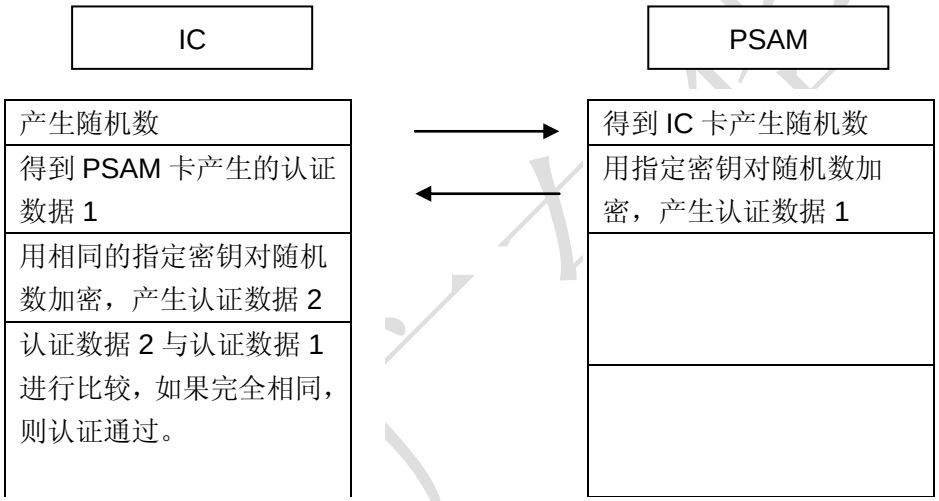


图 6-7 金融外部认证流程图

7. 防拔

卡片必须能够在交易处理中的任何情况下，甚至是在更新 EEPROM 过程中掉电的情况下，保持数据的完整性。这就需要在每次更新数据前对数据进行备份，并且在重新加电或进入感应区后自动地触发恢复机制。

在终端发给 IC 卡一个命令以更新余额时，卡片总会回送一个 MAC 或/和 TAC，以证明更新已经发生。

IC 卡必须在更新余额前计算 MAC 或/和 TAC，一旦余额更新成功，必须保证可以通过 GET TRANSCTION PROOF 命令获得此 MAC 或/和 TAC。如果防拔恢复已使余额恢复到更新前的数值，那么有关的加密数据不必再保留。接到更改余额的命令，这些加密数据可能被丢弃。

如果在命令已执行结束，而终端还未收到响应之前，卡片突然拔出，终端将会处于不知卡片是否更新的不定状态。这种情况下，终端应负责用 GET TRANSACTION PROOF 命令进行恢复。

如果卡片正在处理时被突然拔出，终端应提醒持卡人重新插入卡片。之后终端将检查发卡方标识和应用序列号以确认插入的卡片和前面拔出的卡片是否同一张卡。如果是同一张卡，终端发出 GET TRNSACTION PROOF 命令。假如 MAC 或/和 TAC 返回，终端即完成交易处理；如果 MAC 或/和 TAC 无法返回，则说明 IC 卡中的余额没有被修改。交易可以用适当的初始化命令重新开始。

附录 1：命令速查表

编号	命 令	类别	操作码	功能描述
基本命令集				
1	APPEND RECORD	00/04	E2	添加记录
2	APPLICATION BLOCK	84	1E	应用锁定
3	CARD BLOCK	84	16	环境锁定
4	CHANGE PIN	80	5E	持卡人更新密码
5	CLEAR DF	BF	CE	清除 DF 文件体
6	CREATE FILE	80	E0	建立文件
7	EXTERNAL AUTHENTICATE	00	82	外部认证
8	FREEZE MF	BF	FE	冻结 MF
9	GET CHALLENGE	00	84	取随机数
10	GET INFO	BF	C8	取卡的特征信息
11	GET RESPONSE	00	C0	取响应
12	INTERNAL AUTHENTICATE	00	88	内部认证
13	PIN CHANGE/UNLOCK	84	24	更改/解锁个人密码
14	READ BINARY	00/04	B0	读透明文件
15	READ RECORD	00/04	B2	读记录
16	SELECT FILE	00	A4	选择文件或应用
17	UPDATE BINARY	00/04	D6	修改透明文件内容
18	UPDATE RECORD	00/04	DC	修改记录
19	VERIFY PIN	00	20	验证个人密码
20	WRITE KEY	80/84	D4	装载/修改密钥
金融专有命令				
21	APPLICATION UNBLOCK	84	18	应用解锁
22	CREDIT FOR LOAD	80	52	圈存
23	DEBIT FOR PURCHASE/CASH WITHDRAW	80	54	消费/取现
24	DEBIT FOR UNLOAD	80	54	圈提
25	GET BALANCE	80	5C	读余额
26	GET TRANSACTION PROOF	80	5A	取交易认证
27	INITIALIZE FOR CASH WITHDRAW	80	50	取现初始化
28	INITIALIZE FOR LOAD	80	50	圈存初始化
29	INITIALIZE FOR PURCHASE	80	50	消费初始化

编号	命 令	类别	操作码	功能描述
30	INITIALIZE FOR UNLOAD	80	50	圈提初始化
31	INITIALIZE FOR UPDATE	80	50	修改透支限额初始化
32	PIN UNLOCK	84	24	解锁 PIN
33	RELOAD PIN	80	5E	重装个人密码
34	UPDATE OVERDRAW LIMIT	80	58	修改透支限额 6

附录 2：命令文件对应关系表

命令文件对应关系表：

编号	文件类型 / 命令	MF 文件	DDF 文件	ADF 文件	透明文件	记录文件	安全文件	电子钱包	电子存折
基本命令									
1	APPEND RECORD					√			
2	APPLICATION BLOCK			√					
3	CARD BLOCK								
4	CHANGE PIN						√		
5	CLEAR DF	√	√	√					
6	CREATE FILE	√	√	√	√	√	√	√	√
7	EXTERNAL AUTHENTICATE						√		
8	FREEZE MF	√							
9	GET CHALLENGE								
10	GET INFO								
11	GET RESPONSE								
12	INTERNAL AUTHENTICATE						√		
13	PIN CHANGE/UNLOCK						√		
14	READ BINARY				√				
15	READ RECORD					√			
16	SELECT FILE	√	√	√	√	√			
17	UPDATE BINARY				√				
18	UPDATE RECORD					√			
19	VERIFY PIN						√		
20	WRITE KEY						√		
金融专有命令									
21	APPLICATION UNBLOCK			√					
22	CREDIT FOR LOAD							√	√
23	DEBIT FOR PURCHASE/CASH WITHDRAW							√	√
24	DEBIT FOR UNLOAD								√
25	GET BALANCE								√
26	GET TRANSACTION PROOF							√	√

27	INITIALIZE FOR CASH WITHDRAW								√
28	INITIALIZE FOR LOAD							√	√
29	INITIALIZE FOR PURCHASE							√	√
30	INITIALIZE FOR UNLOAD								√
31	INITIALIZE FOR UPDATE								√
32	PIN UNLOCK						√		
33	RELOAD PIN						√		
34	UPDATE OVERDRAW LIMIT								√

附录 3：状态字节表

SW1	SW2	含义
90	00	命令执行成功
60	06	依据传输模式，所要读取的字节长度错
61	xx	正常处理。‘xx’表示可以通过后续 GET RESPONSE 命令得到的额外数据长度
62	81	回送数据可能出错
62	82	文件长度<Le
62	83	选择文件无效
62	84	FCI 格式与 P2 指定的不符
63	00	认证失败
63	Cx	验证失败， x =‘0’表示不提供计数器 x ≠‘0’表示重试次数
65	81	EEPROM 损坏，导致卡锁定
67	00	Lc 或 Le 长度错
69	00	无信息提供
69	01	命令不接受（无效状态）
69	81	命令与文件结构不相容
69	82	不满足安全状态
69	83	认证方法锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足
69	86	没有选择当前文件
69	88	安全报文数据项不正确
6A	80	数据域参数不正确
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到记录
6A	84	记录空间已满
6A	85	Lc 与 TLV 结构不匹配
6A	86	参数 P1、P2 不正确
6A	88	未找到引用数据
6B	00	参数错误（偏移地址超出了 EF）
6C	xx	长度错误（Le 错误； ‘xx’为实际长度）
61	xx	射频模式下，CASE4 的情况，Le 错误，‘xx’表示实际长度
6D	00	命令不存在
6E	00	命令类型错, CLA 错
6F	00	数据无效

93	02	MAC 无效
93	03	应用被永久锁定
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	06	所需 MAC 不可用
98	40	空间不够
98	50	文件已存在，或文件信息错误