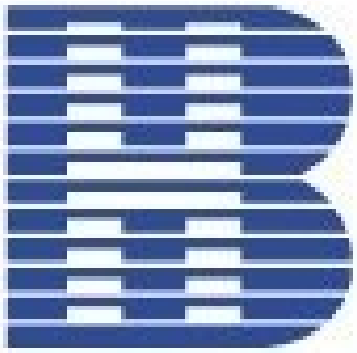
移动支付 PBOC2.0 电子钱包

用 户 手 册



恒宝股份有限公司

二零一零年三月

重要声明

随着 UranusPay ED/EP 卡片产品的升级，本手册内容会做相应的修改，恒宝股份有限公司保留在不通知情况下对本手册内容进行修改的权力。

手册变化动态

修改日期	版本号	主要变化内容描述	制订人
2006-07-07	1.0	初始创建 UranusPay EP 用户手册	赵志福
2006-08-28	1.1	修改文件结构，增加’EF11’文件	丁明勇
2009-7-14	1.2	确定 UranusPay ED/EP 用户参考手册新的目录结构	邓慧鹏
2010-1-27	1.3	修改创建文件指令	王鹏

目　　录

表格目录

图形目录

1 关于本手册

1.1 内容概述

本手册各部分内容概述如下：

- UranusPay ED/EP 应用简介
  本章介绍 UranusPay ED/EP 应用范围与特点，使用户对 UranusPay ED/EP 有一个初步了解。

- UranusPay ED/EP 应用文件结构
  本章介绍电子钱包应用文件组织、专用文件定义、密钥类型等。

- 安全报文传送
  本章描述安全报文基本概念，安全报文传送实现方法、MAC 计算、DES 加解密计算以及安全报文传送的命令情况。

- 命令与应答
  本章描述命令与应答结构，命令返回状态码 SW1SW2 的意义。

- UranusPay ED/EP 基本命令

- 中国金融 IC 卡专用命令
  本章描述 PBOC2.0 电子钱包应用基本命令与交易命令。

- 卡片交易状态
  本章具体列举卡片交易状态以及命令执行成功后的状态变化情况。

- 复位 ATR

注：有关 UranusPay ED/EP 文件系统、安全体系、卡片初始化设置、发卡命令与卡片技术性能指标参考《UranusPay DI 管理参考手册》

1.2 参考文献

- 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/IEC 14443-1：2000 《识别卡 无触点集成电路卡 接近式卡 第一部分：物理特性》
- ISO/IEC 14443-2：2000 《识别卡 无触点集成电路卡 接近式卡 第二部分：射频功率和信号接口》
- ISO/IEC 14443-3：2000 《识别卡 无触点集成电路卡 接近式卡 第三部分：初始化和防冲突》
- ISO/IEC 14443-4：2000 《识别卡 无触点集成电路卡 接近式卡 第四部分：传输协议》
- 《中国金融集成电路(IC)卡规范》送审稿 2004 ，中国人民银行

1.3 定义

T=0 协议
面向字符的异步半双工传输协议。

T=1 协议
面向块的异步半双工传输协议。

块 Block
包含两个或三个域（头域、信息域、尾域）的字符组。

冷复位 Cold Reset
当 IC 卡的电源电压和其它信号从静止状态中复苏且申请复位信号时，IC 卡产生的复位。

热复位 Warm Reset
在时钟（CLK）和电源电压（VCC）处于激活状态的前提下，IC 卡收到复位信号时产生的复位。

终端 Terminal
为完成金融交易而在交易点安装的设备，用于同 IC 卡的连接。它包括接口设备，也可包括其它部件和接口，例如与主机通讯的接口。

命令 Command
终端向 IC 卡发出的一条信息，该信息启动一个操作或请求一个应答。

连接 Concatenation
两个元素的连接是指将第二个元素附加到第一个元素的末尾。每个元素的字节在结果串中的排列顺

序与其从 IC 卡发送到终端的顺序相同，即：高位字节先送。每个字节位按照从最高位到最低位的顺序排列。一组元素或对象可以通过最先两个相连的方式连接成一个新元素，即第一个与第二个相连，再与第三个相连，…，依次类推。

响应 Response
IC 卡处理完成收到的命令报文后，回送给终端的报文。

金融交易 Financial Transaction
由于持卡者和商户之间的商品或服务交换行为而在持卡者、发卡机构、商户和收单行之间产生的信息交换、资金清算和结算行为。

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

集成电路 Integrated Circuit(IC)
设计用于完成处理和/或存储功能的电子器件。

集成电路卡(IC 卡) Integrated Circuit(s) Card
内部封装一个或多个集成电路的 ID－1 型卡(如 ISO7810、ISO7811 第 1 至第 5 部分、ISO7812 和 ISO7813 中描述的)。

报文 Message
由终端向卡或卡向终端发出的，不含传输控制字符的字节串。

报文认证码 Message Authentication Code
对交易数据及其相关参数进行运算后产生的代码。主要用于验证报文的完整性。

半字节 Nibble
一个字节的高四位或低四位。

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。

数字签名 Digital Signature
一种非对称加密数据变换，它使得接收方能够验证数据的原始性和完整性，保护发送和接收的数据不被第三方伪造，同时对于发送方来说，还可用以防止接收方的伪造。

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。

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。

电子钱包 Electronic Purse
一种为方便持卡人小额消费而设计的金融 IC 卡应用。它支持圈存、消费等交易。除圈存交易外，使用电子钱包进行的其它交易均不记录明细，且均无需提交个人密码(PIN)。

圈存 Load
持卡人将其在银行相应帐户上的资金划转到电子存折或电子钱包中。圈存交易必须在金融终端上联机进行 [1]。一般情况下，圈存到电子存折中的资金仍计付活期利息，圈存到电子钱包中的资金不计付利息。但具体作法由发卡方自行决定。

圈提 Unload
持卡人将电子存折中的部分或全部资金划回到其在银行的相应帐户上。圈提交易必须在金融终端上联机进行 [2]。

复合应用 Complex Application
结合电子钱包应用和其它应用的应用模式。

解扣出错计数器 GMAC Count
用于防止外界对 IC 卡进行恶意试探，在执行解扣指令时，IC 卡都会先对命令报文中的 GMAC 进行验证，如果正确则进行下一步的正常操作，并将出错计数器复位；连续出错 3 次时，IC 卡自动将当前应用锁定。

灰锁交易验证码 Grey-lock Transaction Authorization Code
IC 卡对电子钱包应用完成灰锁操作后，产生的一个安全验证码。

交易验证码待读标志 TAC Unread Flag
基于冗错考虑，当 IC 卡内部解扣操作已完成，而终端未读到 TAC 码时，交易中断，需要通过交易验证码待读标志的机制，通知下一个操作终端将这个未读 TAC 码取出，形成补充交易数据包上送主机。

终端随机数 Terminal Random
终端通过 PSAM 产生的随机数

1.4 缩略语

AID	应用标识符(Application Identifier)
ATI	应用类型标识(Application Type Identifier)
an	字母数字型(Alphanumeric)
ans	字母数字及特殊字符型(Alphanumeric Special)
b	二进制(Binary)
CCPS	芯片卡支付服务(Chip Card Payment Service)
CLA	命令报文的类别字节(Class Byte of the Command Message)
cn	压缩数字型(Compressed Numeric)
DEA	数据加密算法(Data Encryption Algorithm)

[1]在发卡方之间联网的情况下，可以在其他发卡方终端联行进行。
[2]在发卡方之间联网的情况下，可以在其他发卡方终端联行进行。

DF	专用文件(Dedicated File)
ED	电子存折(Electronic Deposit)
EF	基本文件(Elementary File)
EP	电子钱包(Electronic Purse)
FCI	文件控制信息(File Control Information)
INS	命令报文的指令字节(Instruction Byte of Command Message)
ISO	国际标准化组织(International Organization for Standardization)
Lc	终端发出的命令数据的实际长度(Exact Length of Data Sent)
Le	响应数据中的最大期望长度(Maximum Length of Data Expected)
MAC	报文认证码(Message Authentication Code)
MF	主控文件(Master File)
n	数字型(Numeric)
P1	参数1(Parameter 1)
P2	参数2(Parameter 2)
PIN	个人密码(Personal Identification Number)
PIX	专用应用标识扩展码(Proprietary Application Identifier Extension)
POS	销售点终端(Point of Service)
PSAM	销售点终端安全存取模块(Purchase Secure Access Module)
PSE	支付系统环境(Payment System Environment)
PVV	PIN校验值(PIN Verification Value)
RFU	保留为将来使用(Reserved for Future Use)
RID	已注册的应用提供者标识(Registered Application Provider Identifier)
RSA	一种非对称加密算法(Rivest,Shamir,Adleman)
SAM	安全存取模块(Secure Access Module)
SFI	短文件标识符(Short File Identifier)
SW1	状态码1(Status Word One)
SW2	状态码2(Status Word Two)
TAC	交易验证码(Transaction Authorization Crypogram)
TTI	交易类型标识(Transaction Type Identifier)
CCYYMM	年，月，日(Year, Month, Day)
3DES	3倍DES算法(Triple DES)
XX	1个字节16进制数
XXXX	2个字节16进制数
XX…XX	未知个字节16进制数

2 UranusPay ED/EP简介

2.1 关于UranusPay ED/EP

UranusPay ED/EP 是恒宝股份有限公司自主开发的双界面多应用智能卡操作系统，完全符合以下国内、国际规范：

- 识别卡，带触点的集成电路卡标准《ISO7816-1/2/3/4》
- 识别卡，无触点的集成电路卡标准《ISO14443-3/4》
- 中国金融集成电路(IC)卡标准

UranusPay ED/EP 操作系统具有以下特点：

- 接触式和非接触式接口共享卡片所有资源，如：微处理器、操作系统和存储空间等
- 卡片具备防冲突机制，支持多张卡片同时进入交易区；
- 支持多级目录结构，所建立的级数只取决于卡片空间和用户；
- 支持标准的文件类型，包括二进制、循环、定长、变长记录文件等；
- 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（信息机密性与完整性保护）；
- 支持多种安全访问方式和权限（认证功能和口令保护）；
- 支持中国人民银行认可的 Triple DES 算法、DES 算法；
- 支持多种保护数据，防止卡片被攻击的策略；
- 支持防插拔、防掉电功能；
- 支持多种通讯协议，接触界面支持 T=0 和 T＝1 协议，非接触界面支持 Type A 和 Type B 协议；
- 接触界面支持多种通讯速率，9600bps，38400bps 等多种不同的通讯速率；
- 非接触界面支持多种通讯速率，106kbps，212kbps，424kbps 等同多种不同的通讯速率。

2.2 UranusPay ED/EP命令集

编号	命　令	类别	操作码	功能描述
1	Read Binary	00	B0	读透明文件
2	Read Record	00	B2	读记录
3	Update Binary	00/04	D6	修改透明文件内容
4	Update Record	00/04	DC	修改记录
5	Append Record	00/04	E2	添加记录
6	Verify Pin	00	20	验证个人密码
7	External Authenticate	00	82	外部认证
8	Get Challenge	00	84	取随机数
9	Internal Authenticate	00	88	内部认证
10	Select	00	A4	选择文件或应用
11	Get Response	00	C0	取响应
12	Create File	80	E0	建立文件
13	Write Key	80/84	D4	装载/修改密钥

编号	命　令	类别	操作码	功能描述
14	Erase File	80	EE	删除文件
15	Initialize For Load	80	50	圈存初始化
16	Credit For Load	80	52	圈存
17	Initialize For Unload	80	50	圈提初始化
18	Debit For Unload	80	54	圈提
19	Initialize For Purchase	80	50	消费初始化
20	Initialize For Cash Withdraw	80	50	取现初始化
21	Debit For Purchase/Cash Withdraw	80	54	消费/取现
22	Initalize For Update	80	50	修改透支限额初始化
23	Update Overdraw Limit	80	58	修改透支限额
24	Get Balance	80	5C	读余额
25	Get Transaction Proof	80	5A	取交易认证
26	Change Pin	80	5E	持卡人更新密码
27	Card Block	84	16	环境锁定
28	Application Block	84	1E	应用锁定
29	Pin Unlock	84	24	解锁 PIN
30	Reload Pin	80	5E	重装个人密码
31	Application Unblock	84	18	应用解锁

表　2-1 UranusPay ED/EP 命令集

3 UranusPay ED/EP应用文件结构

本章描述 UranusPay ED/EP 应用文件结构，分别主要从文件组织、文件结构、密钥类型、专用文件定义等方面进行详细说明。

3.1 文件组织

图 3-1 PBOC ED/EP 文件组织

3.2 专用文件FID定义

文件名	FID	说明
电子存折 FID	EF01	二进制文件
电子钱包 FID	EF02	二进制文件
PBOC 交易 Proof 文件	EF03	二进制文件
余额上限文件	EF05	二进制文件，可读写，需要安全控制
PBOC 交易明细文件	EF18	定长循环记录文件,10 条记录
应用锁定原因 APP Lock Reason	EF21	二进制文件
持卡人基本数据文件	EF15	二进制文件
公共应用基本文件	EF16	二进制文件

表 3-1 PBOC ED/EP 专用文件 FID 定义

3.3 文件结构

◆ ED 和 EP 应用的公共应用基本数据文件（EF16）

文件标识(SFI)			‘21’ (十进制)
文件类型			透明
文件大小			30
文件存取控制		读 = 自由	改写 = 需要 安全信息
字节	数据元		长度
1-8	发卡方标识		8
9	应用类型标识		1
10	发卡方应用版本		1
11-20	应用序列号		10
21-24	应用启用日期		4
25-28	应用有效日期		4
29-30	发卡方自定义 FCI 数据		2

◆ ED 和 EP 应用的持卡人基本数据文件（EF15）

文件标识(SFI)			‘22’ (十进制)
文件类型			透明
文件大小			55
文件存取控制		读 = 自由	改写 = 需要 安全信息
字节	数据元		长度
1	卡类型标识		1
2	本行职工标识		1
3-22	持卡人姓名		20
23-54	持卡人证件号码		32
55	持卡人证件类型		1

◆ PBOC 交易明细文件（EF18）

文件标识 (SFI)		‘24’ (十进制)
文件类型		循环
文件存取控制		读 = PIN 保护 改写 = 不允许 [3]
记录大小		23
字节	数据元	长度
1-2	ED 或 EP 联机或脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标识	1
11-16	终端机编号	6

[3]交易明细由IC卡维护。不允许外部对其修改。

17-20	交易日期（终端）	4
21-23	交易时间（终端）	3

[说明]：外部能读，不能写

◆ 电子存折文件(EF01)

内容	字节数	说明
ED 脱机交易计数器	2	电子存折脱机交易序号
ED 联机交易计数器	2	电子存折联机交易序号
ED 余额	4	电子存折可供支配的金额
透支限额	3	最多允许透支的金额值

[说明]：外部不能读写，初始化值均为 0

◆ 电子钱包文件(EF02)

内容	字节数	说明
EP 脱机交易计数器	2	电子钱包脱机交易序号
EP 联机交易计数器	2	电子钱包联机交易序号
EP 余额	4	电子钱包可供支配的金额

[说明]：外部不能读写，初始化值均为 0

◆ PBOC 交易 PROOF 文件（保存 MAC，TAC）(EF03)

内容	字节数	说明
交易类型	1	
交易序号	2	
置有效标志位	1	
MAC	4	
TAC	4	保存 MAC

[说明]：外部不能读写，初始化值均为 0

◆ 余额上限文件 Balance Limit(EF05)

内容	字节数	说明
ED	4	圈存后 ED 余额(不包含透支限额)不能超过的余额上限
EP 上限	4	圈存后 EP 余额不能超过的余额上限

[说明]：外部能读写

◆ 应用锁定原因 APP LOCK REASON(EF21)

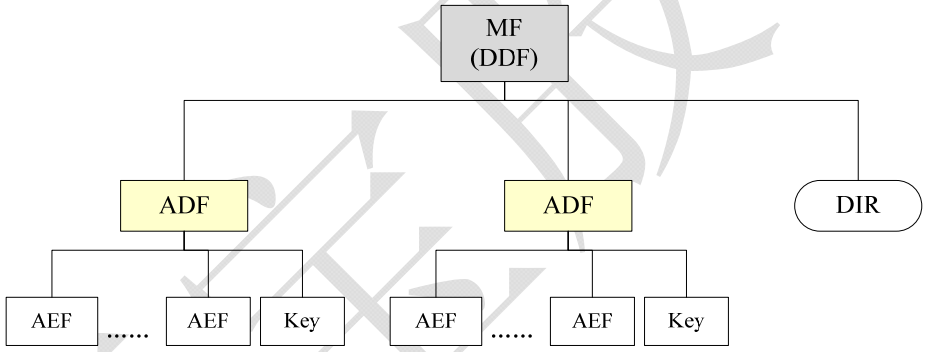
内容	字节数	说明
0	1	卡片锁定原因 00－正常 01－终端锁定黑卡 02－RFU
1－19	19	RFU

3.4 密钥类型定义

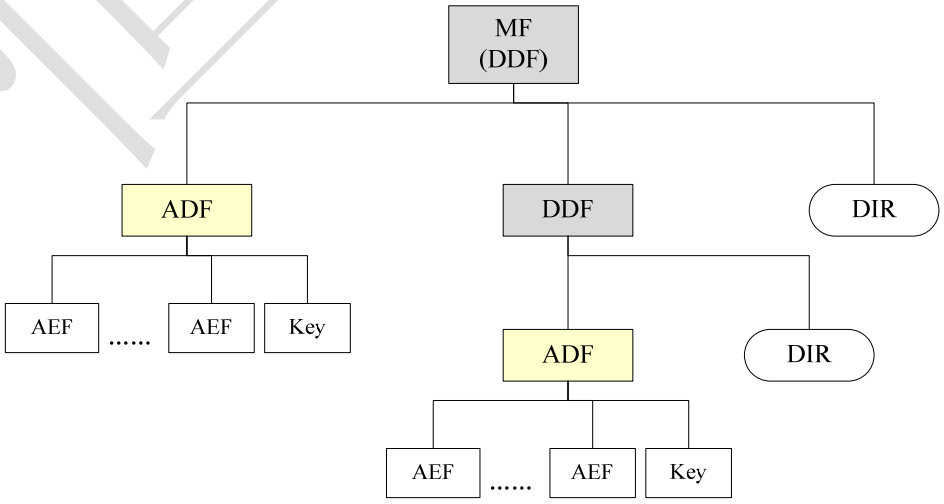
密钥名称	缩写	类型
TAC 密钥	DTK	25
圈存	DLK	26
消费	DPK	27
圈提	DULK	28
更新透支限额	DUK	29
PIN	PIN	3A
重装 PIN	DRPK	38
应用维护密钥	DAMK	36
外部认证密钥	DEAK	39
PIN 解锁密钥	DPUK	37

表 3-2　PBOC ED/EP 应用密钥类型

3.5 单环境多应用



3.6 多环境多应用



4 安全报文传送

4.1 安全报文传送的概念

UranusPay ED/EP 提供以下四种报文传输方式：

- 明文
- 密文
- MAC
- 密文 MAC

后三种属于安全报文传输，密文传输可以保证数据的私密性，MAC 传输可以保证数据传输的完整性和可靠性。

文件采用哪种报文传输方式在Create File命令参数域“安全属性”中指定，具体请参考《UranusPay DI 管理参考手册》。

> ✧ 当采用安全保文传输时，命令的 CLA 的低 4 位应当为十六进制数 ‘4’
> ✧ 采取哪种数据传输方案，完全由用户根据实际的情况确定
> ✧ 高安全性是以降低速度，增加实现难度来换取的，所以并不是安全性越高越好，而是一定要根据具体的情况来确定。

4.1.1 明文传输

当对数据传输时的私密性、完整性、可靠性没有要求时，可以采用明文传输的方式。采用明文传输命令的数据域和响应的数据域均是明文，不需要做数据变换。

4.1.2 密文传输

当只对数据传输时的私密性有要求时，尽量采用密文传输的方式。密文传输可以使数据被安全算法加密，防止未经授权的第三方获取数据信息。

UranusPay ED/EP 只要求对命令中的数据域进加密，响应中的数据域（读的结果）是不加密的。加密时，从 APDU 中的 “Lc || DATA”进行加密，并将加密后的密文长度 作为新的 Lc 使用.

具体如何实现数据加密的方法参考 4.3.5 节。

4.1.3 MAC传输

当只对数据传输时的完整性、可靠性有要求时，尽量采用 MAC 传输的方式。MAC 传输可以保证数据传输时不被篡改。

MAC 传输采用在命令数据域中增加 4 字节的校验码的方式实现保证数据传输时不被篡改。

计算 MAC 时，使用 4 字节的随机数并补 4 字节的 00，作为初始值，对 APDU 中的所有数据项计算 MAC。

具体如何实现计算 MAC 的方法参考 4.3.4 节。

4.1.4 密文MAC传输

当对数据传输时的私密性、完整性、可靠性均有要求时，采用密文 MAC 传输的方式。

这种方式先实现对数据进行加密，然后对加密后的数据进行计算 MAC 的方式来保证数据的私密性、完整性、可靠性。

4.2 如何实现安全报文传送

4.2.1 文件

UranusPay ED/EP 中所有的文件均由文件头和文件体构成。

- 文件头：描述、管理文件体的属性，包含定义了文件大小，文件类型，安全机制等等控制信息，DF 和 EF 的文件头在用户空间中都占用 16 字节的大小。
- 文件体：存储具体的文件内容。

文件头	标识、大小、类型、安全机制等属性
文件体	内容

文件头可能包含如下的域，具体情况还需要视不同的文件类型而定：

域	长度	描述
文件类型	1	定义文件的类型
文件标识	2	定义文件的标识号
文件大小	2	定义文件体能够存储的字节数
访问权限 1	1	不同类型文件实际含义不同
访问权限 2	1	不同类型文件实际含义不同
RFU	1	不同类型文件实际含义不同
安全属性	1	不同类型文件实际含义不同

4.2.2 密钥

对于密钥，也可以采用安全报文形式传送。

如果对密钥进行安全报文形式传送（使用 WriteKey 和 Verify Pin），只需要在安装密钥时，改变密钥类型字节的安全属性（高两位）即可。

密钥类型字节定义如下：

b7	b6	b5	b4	b3	b2	b1	b0	
1	**x**	x	x	x	x	x	x	MAC 线路保护
x	**1**	x	x	x	x	x	x	DES 线路加密

密钥类型的高两位，表示密钥的安全属性，

最高位为 1，表示在建立或修改时，需要使用 MAC

次高位为 1，表示在建立或修改时，需要线路加密传输

举例：

对密钥进行线路加密保护（DES&MAC），则将密钥类型的最高 2 位置 1，如：外部认证密钥由‘39’变为‘F9’。

4.3 安全计算（DES在金融环境中的安全管理）

安全计算包括密钥分散计算，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’。

4.3.1 密钥分散

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 4-1 和图 4-2。

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。

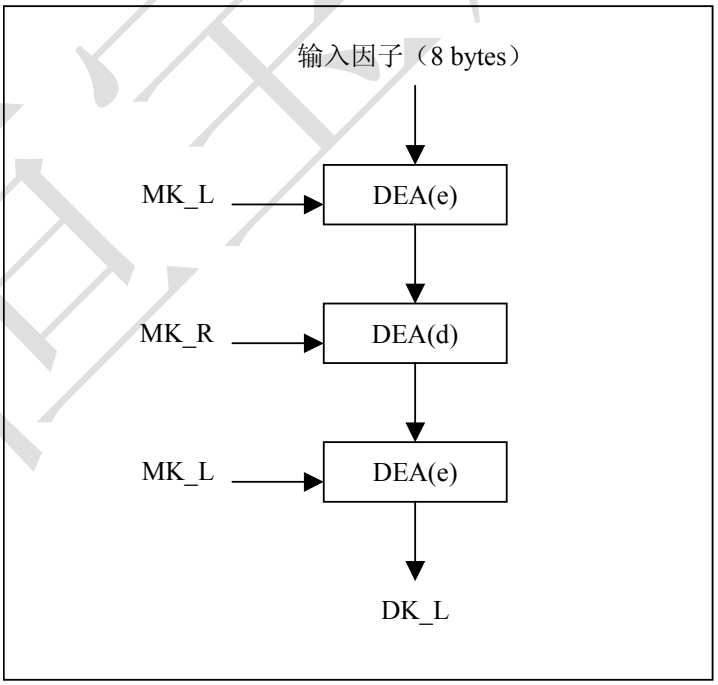


图 4-1 生成子密钥左半部分

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。

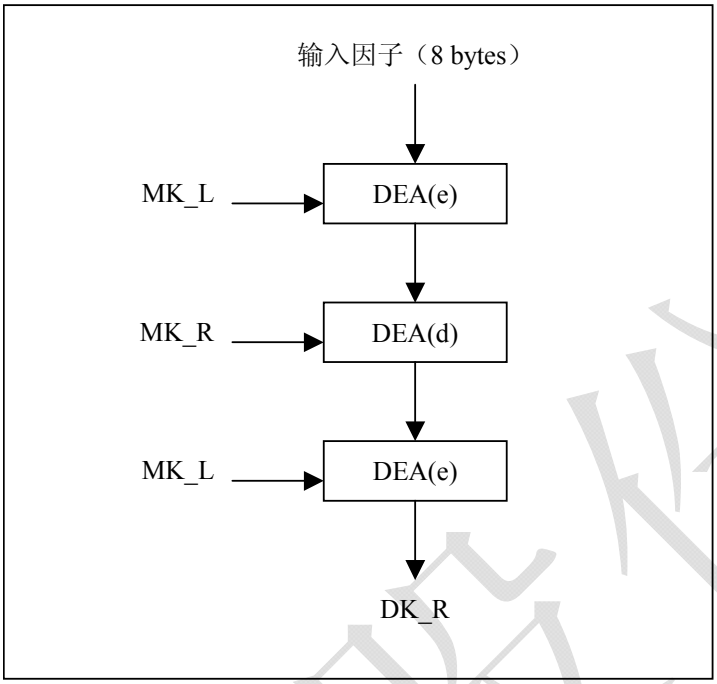


图 4-2 生成子密钥右半部分

4.3.2 过程密钥

4.3.2.1 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 4-3 和图 4-4。

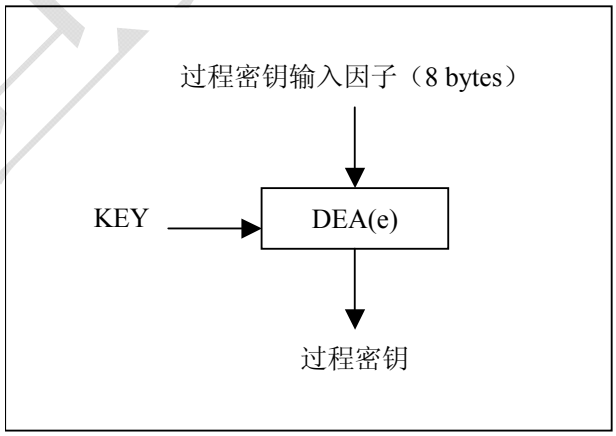


图 4-3 单倍长密钥产生过程密钥

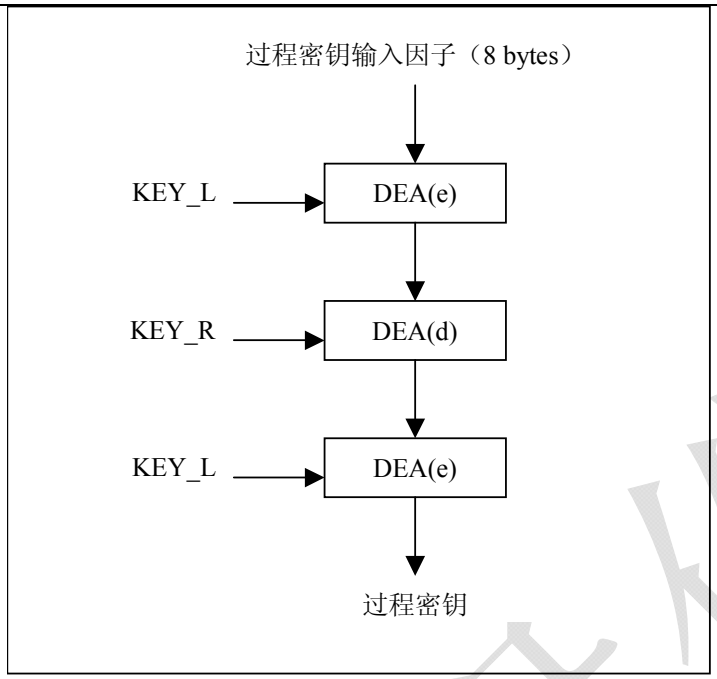


图 4-4 双倍长密钥产生过程密钥

4.3.2.2 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 4-5。

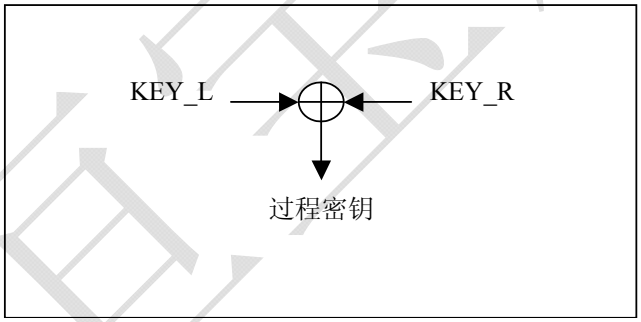


图 4-5 过程密钥产生

4.3.3 鉴别数据

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 4-6 和图 4-7。

按照如下方式使用 DEA 加密方式产生 MAC：

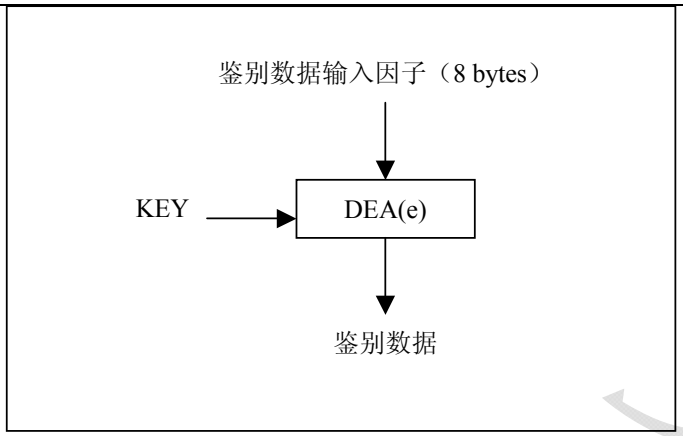


图 4-6　单倍长密钥的鉴别数据的计算

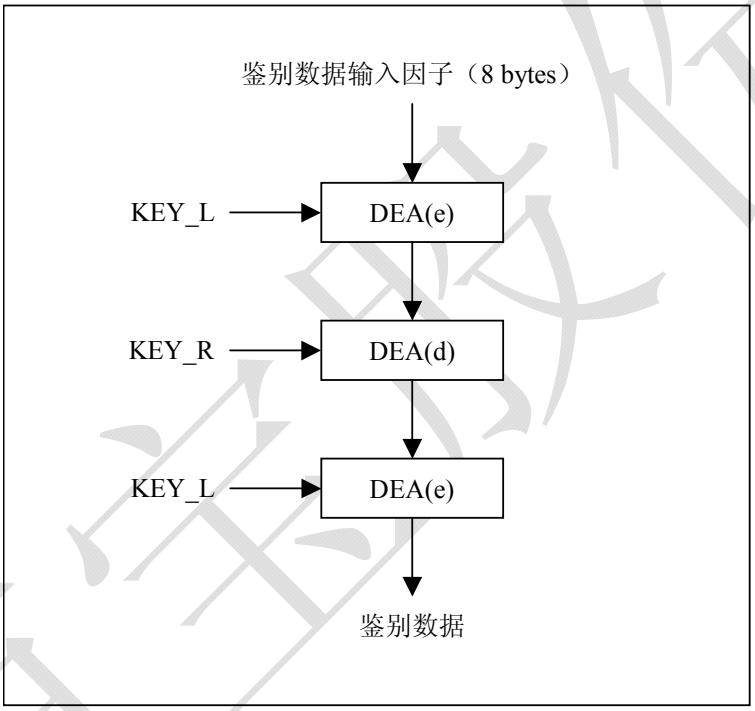


图 4-7　双倍长密钥的鉴别数据的计算

4.3.4 MAC

4.3.4.1 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 4-8 和图 4-9 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。

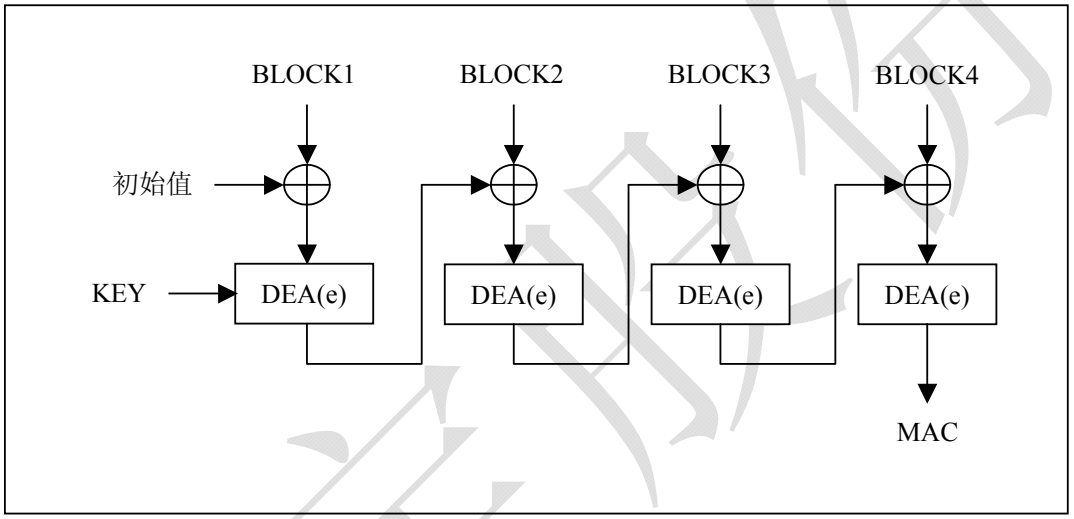


图 4-8 安全报文中单倍长密钥 MAC 计算

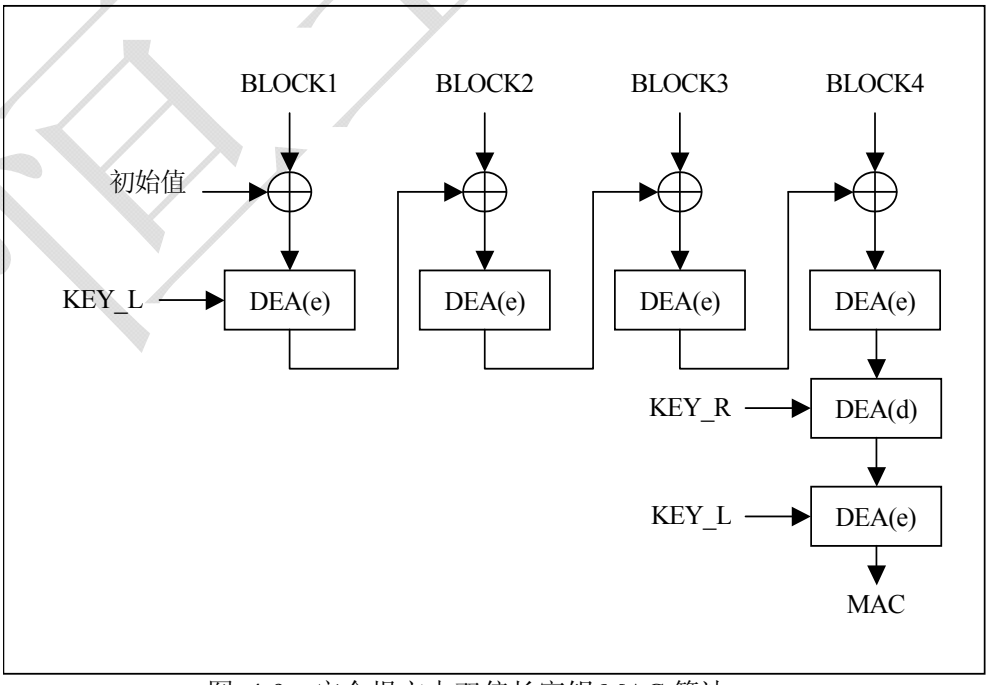


图 4-9 安全报文中双倍长密钥 MAC 算法

4.3.4.2 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 5.4.2 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 4-10 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。

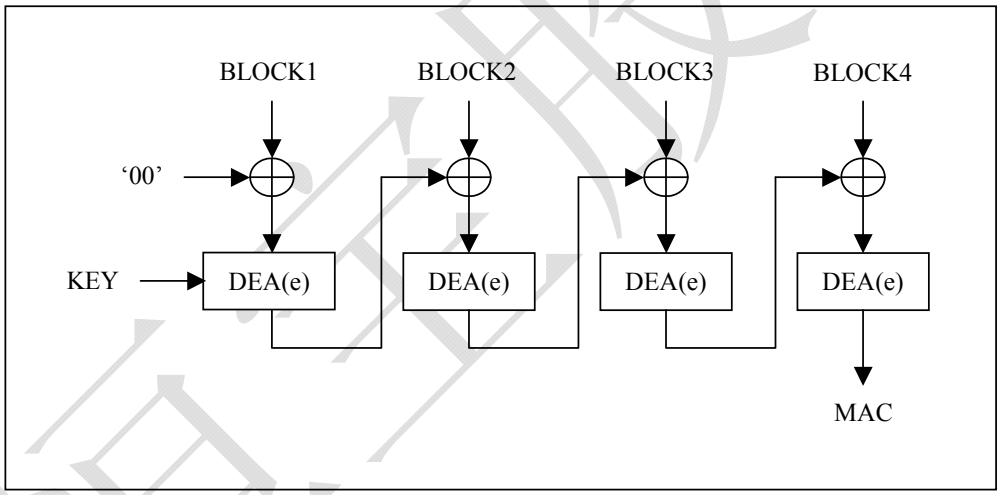


图 4-10　ED/EP 交易中的 MAC 算法

4.3.5 数据加密

按照如下方式对数据进行加密：

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

第二步：将该数据块分成 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 4-11 和图 4-12 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。

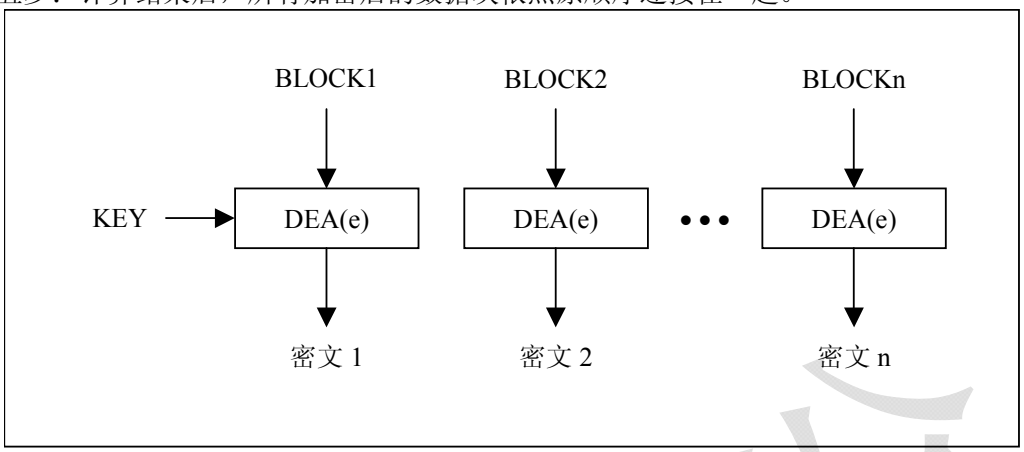


图 **错误！未找到引用源。**-11　单倍长密钥 DEA 数据加密算法

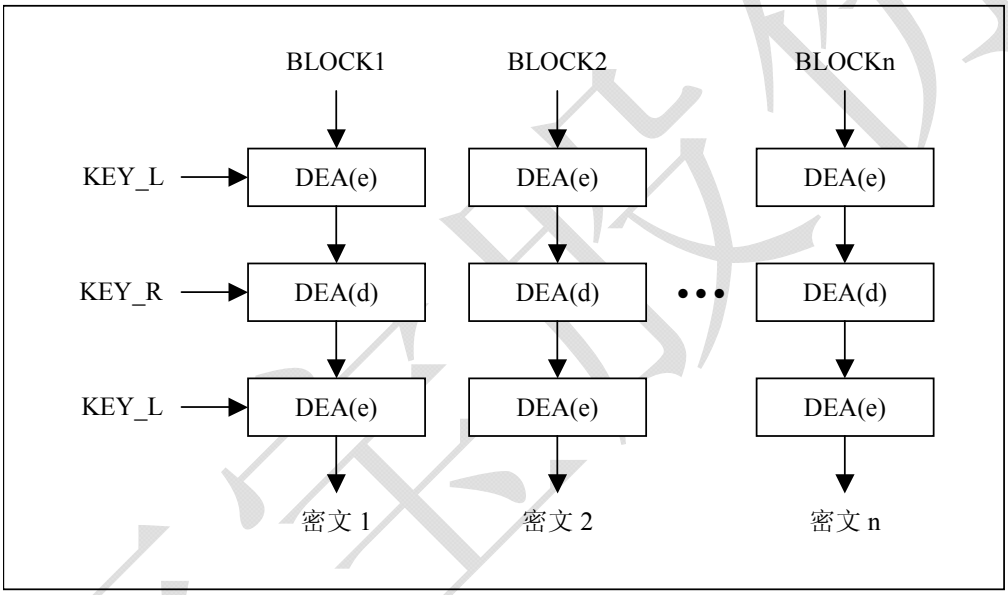


图 4-12　双倍长密钥 DEA 数据加密算法

4.3.6 数据解密

数据解密则采用相反的过程，如图 4-13 和图 4-14。

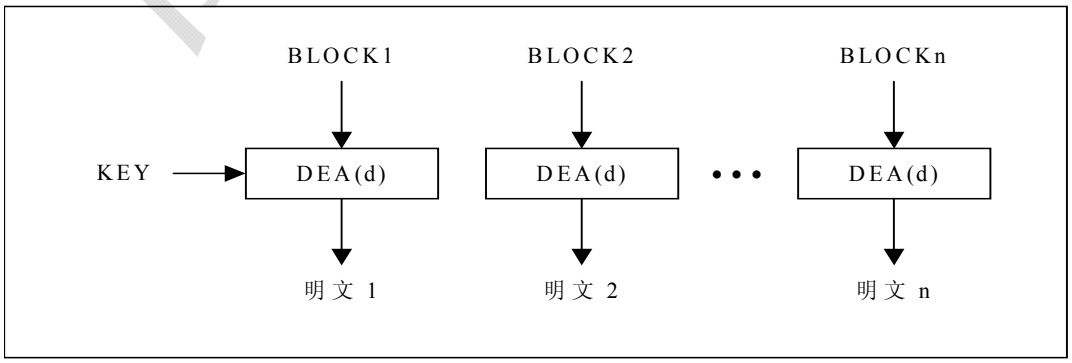


图 4-13　单倍长密钥 DEA 数据解密算法

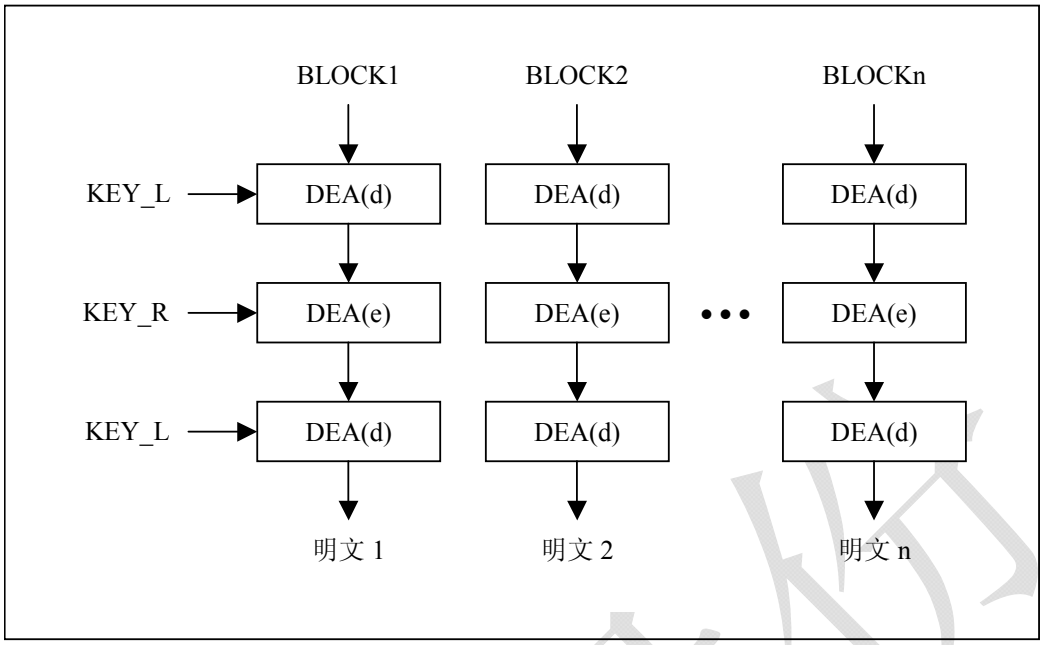


图 **错误！未找到引用源。**-14　双倍长密钥 DEA 数据解密算法

4.4 安全报文传送的命令情况

Case 1：没有数据送到卡（Lc）中，也没有数据从卡中（Le）返回。

不含安全报文的命令：

CLA	INS	P1	P2

含安全报文的命令：

CLA	INS	P1	P2	Lc	MAC

安全报文传送：CLA 字节的低四位必须是 04。
Lc 是 MAC 的长度（4 字节）。

Case 2：命令中没有数据送到卡中，也有数据从卡中返回。

不含安全报文的命令：

CLA	INS	P1	P2	Le

含安全报文的命令：

CLA	INS	P1	P2	Lc	MAC	Le

安全报文传送：CLA 字节的低四位必须是 04。
Lc 是 MAC 的长度（4 字节）。

Case 3：命令中有数据送到卡中，但没有数据从卡中返回。

不含安全报文的命令：

CLA	INS	P1	P2	Lc	Data

含安全报文的命令：

CLA	INS	P1	P2	Lc	Data	MAC

安全报文传送：CLA 字节的低四位必须是 04。
Lc=数据长度+MAC 的长度（4 字节）。

Case 4：命令中有数据送到卡中，也有数据从卡中返回。

不含安全报文的命令：

CLA	INS	P1	P2	Lc	Data	Le

含安全报文的命令：

CLA	INS	P1	P2	Lc	Data	MAC	Le

安全报文传送：CLA 字节的低四位必须是 04。

Lc=数据长度+MAC 的长度（4 字节）。

4.5 应用举例

[1]命令：写二进制文件（Update Binary）
线路保护模式：DES&MAC
维护密钥值：5741544348444154415469 6D65434F53
条件：文件标识符=03
文件主体空间=8 字节
文件建立时采用线路加密保护

[2]操作：写二进制文件，写入数据：1122334455667788
Step1: 取 4 字节随机数，计算 MAC 用
命令： 00 84 00 00 04
响应：46 4E 84 AF 9000
Step2: 写二进制文件，写入数据：1122334455667788
命令：04 D6 83 00 14 68 7E 0F 83 F6 A9 85 80 C4 01 5C EB 8D 00 F3 8B 1C AB E2 B9
说明：68 7E 0F 83 F6 A9 85 80 C4 01 5C EB 8D 00 F3 8B 为使用维护密钥对数据 08 11 22 33 44 55 66 77 88 80 00 00 00 00 00 00 加密后的结果，加密方法见 4.3.5；1C AB E2 B9 为使用维护密钥对命令报文生成的 4 字节 MAC 码，计算方法见 4.3.4。
响应：9000

5 命令与应答

5.1 命令与响应格式

从终端发出的命令和卡片响应的信息必须符合以下 4 种格式。

格式 1：

命令：

CLA	INS	P1	P2	00

响应：

SW1	SW2

格式 2：

命令：

CLA	INS	P1	P2	Le

响应：

Le 字节的 Data	SW1	SW2

格式 3：

命令：

CLA	INS	P1	P2	Lc	Data

响应：

SW1	SW2

格式 4：

命令：

CLA	INS	P1	P2	Lc	Data	Le

响应：

Le 字节的 Data	SW1	SW2

5.2 命令格式

命令由 4 字节的命令头和命令体组成。

命令头				命令体		
CLA	INS	P1	P2	Lc	Data	Le

5.2.1 命令头域

命令头定义报文的内容如下表所示：

代码	长度（bytes）	值(hex)	描述
CLA	1	X0	不带安全报文的命令
		X4	带安全报文的命令
INS	1	XX	指令代码

P1	1	XX	参数 1
P2	1	XX	参数 2

5.2.2 命令体

命令体中的各项是可选的。
Lc　　命令数据域中 Data 的长度，不可超过 178 字节。
Data　 命令和响应中的数据域
Le　　响应数据中期望数据的长度

5.3 响应数据格式

命令的应答由数据和状态字组成。其中返回数据域是可选项，SW1SW2 是卡片执行命令的返回代码，任何命令的返回信息都由至少由 1 个状态字组成。

数据	状态字	
响应中接收的数据位串	SW1	SW2

5.4 状态字SW1SW2 意义

状态字说明了命令的处理情况，即命令是否被正确执行，如未被正确执行，原因是什么。
状态字由 2 部分组成。
SW1　表示命令处理状态
SW2　表示命令处理限定

编码	说明	编码	说明
9000	成功	6986	没有 EF 被选择
6E00	CLA 不支持或错误	6988	线路保护错误
6D00	INS 不支持或错误	6A80	数据域有错误
6700	长度错误	6A81	无 MF 或者卡片锁定
6900	CLA 与线路保护属性不匹配	6A82	文件未找到
6901	状态机不满足	6A83	记录未找到
6981	文件类型不匹配	6A84	空间不足
6982	安全状态不满足	6A85	Lc 与 TLV 结构不相容
6983	密钥锁定	6A86	参数错误
6984	引用数据无效	6A88	未找到引用数据
6985	使用条件不满足	6A89	文件已经存在(FID 重复)
9302	MAC 无效	6A8B	KEY 文件没有建立
9401	资金不足	6B00	偏移超出范围
9403	不支持的密钥索引	6F00	无响应数据
9406	所需 MAC 和 TAC 不可用	63CX	验证失败，还剩下 X 次尝试机会
6300	校验错误	6CXX	LC 应该为 XX
61XX	取响应，XX 为返回数据长度		

表 5-1 状态字 SW1SW2 说明

6 UranusPay ED/EP基本命令

本章描述 UranusPay ED/EP 基本命令，有关安全报文的操作参考第 4 章。

UranusPay ED/EP 基本命令列表

编号	命　令	类别	操作码	功能描述	兼容性
1	Read Binary	00	B0	读透明文件	ISO&PBOC
2	Read Record	00	B2	读记录	ISO&PBOC
3	Update Binary	00/04	D6	修改透明文件内容	ISO&PBOC
4	Update Record	00/04	DC	修改记录	ISO&PBOC
5	Append Record	00/04	E2	添加记录	ISO&PBOC
6	Verify Pin	00	20	验证个人密码	ISO&PBOC
7	External Authenticate	00	82	外部认证	ISO&PBOC
8	Get Challenge	00	84	取随机数	ISO&PBOC
9	Internal Authenticate	00	88	内部认证	ISO&PBOC
10	Select	00	A4	选择文件或应用	ISO&PBOC
11	Get Response	00	C0	取响应	ISO&PBOC
12	CreateFile	80	E0	创建文件	ISO&PBOC
13	Erase File	80	EE	删除文件	ISO&PBOC
14	Write Key	80/84	D4	装载/更新密钥	ISO&PBOC

6.1 Create File创建文件

6.1.1 定义与范围

Create File 命令用于创建卡片中的全部文件系统，包括 MF、DF/ADF、EF 文件。

6.1.2 注意事项

- 每个卡片只存在一个 MF 文件。
- ADF/DF 和 EF 的数量没有限制，它取决于卡片的可用空间和用户应用。
- 在满足 MF 或者父 ADF/DF 的创建权限的条件下，才能成功创建子 DF 或 EF。
- MF 下文件标识为 0000 和 0001 的记录文件是唯一的密钥文件，密钥文件应该首先建立。
- 在预个人化阶段，任何权限不生效。
- DF 文件被成功建立后，不被设置为当前目录文件。
- MF、EF 文件被成功建立后，会自动被设置为当前文件，对于 EF 文件，需要清除当前记录指针。
- EFArr（安全记录文件）只能建立在，MF 下和 ADF 下，对应 FID 为 2F06 和 6F06
- 当创建 EF 时其 SFI（Short File Identifier）的合法范围是 0x01-0x1E,否则文件将不能创建成功
- 在创建文件时要确保当前 DF 下所建文件的 SFI（Short File Identifier），FID（File Identifier），

AID（Application Identifier）的唯一性

- 不同 DF 下可建立重名 DF 或 EF
- 只能在 3G 模式下

6.1.3 命令报文

命令	长度(Byte)	值（Hex）	描述
CLA	1	80	指令类型
INS	1	E0	指令码
P1	1	XX	参见注 1
P2	1	01/02/03	
P3	1	XX	参见注 2

表 6-1 Create File 命令报文

注 1：建立 EF 时，P1 定义

B8	B7	B6	B5	B4	B3	B2	B1	描述
0	-	-	-	-	-	-	-	文件体初始数据为全‘FF’
1	-	-	-	-	-	-	-	文件体初始数据为全‘00’
	0							非共享文件文件头
	1							共享文件文件头
						0	0	创建 MF
						0	1	创建 DF/ADF
						1	0	创建 EF（bit 8 只在创建 EF 时有效）

注 2：

P1	P3	描述
00	08+XX	建立 MF，XX 表示 AID 长度，如果没有 AID，则 P3=09，AID=00
01	08+XX	建立 MF，XX 表示 AID 长度，如果没有 AID，则 P3=09，AID=00
82/02	0A	建立 EF

注 3：

P1	P2	描述
01	01	建立 PSE，DDF
	02	建立 ADF，用于 PBOC 钱包应用
	03	建立 ADF，用于建设部钱包应用

6.1.4 命令报文数据域

命令报文数据域为创建文件信息，可分为以下情况：

- **MF 文件创建信息：**

字节	描述
1	文件描述符（见下表 0）
2-3	文件标识（3F00）
4	相关的 SFI 文件

5	属性字节 2（见下表 2）
6-8	安全属性定义（读，写，安全属性）
9-X	AID

文件描述符：

B8	B7	B6	B5	B4	B3	B2	B1	描述
	0							非共享文件
	1							共享文件
		0	0	0				普通文件
		0	0	1				内部文件
		1	1	0				DF
		1	1	1				ADF
					0	0	1	二进制文件
					0	1	0	定长文件
					1	1	0	循环文件

表 2：属性字节 2（生命周期状态）定义如下：

B8	B7	B6	B5	B4	B3	B2	B1	描述
							1	创建文件状态
						1	1	初始化状态
					1		1	用户状态—激活
					1		0	用户状态—去活
				1	1			终止状态

- **DF 文件创建信息**

字节	描述
1	文件描述符
2-3	文件标识
4	相关的 SFI 文件
5	属性字节 2（见上表 2）
6-8	安全属性定义（读，写，安全属性）
9-X	AID

注 2：DF 文件标识不能为 3F00。

- **EF 文件创建信息**

字节	描述
1	文件描述符
2	记录数
3	记录长度
4	SFI
5-6	FID
7	属性字节（上表 2）
8-10	安全属性定义（EFarr FID + Rec NO）

6.1.5 响应报文数据域

响应报文数据域不存在。

6.1.6 响应报文状态码

SW1SW2	描述
90 00	命令正常结束，执行成功
67 00	长度错误
69 82	权限不满足
6B 00	参数 P1P2 错误
6A 81	功能不支持
6A 84	空间不足
65 81	存储器错误
6F 00	FID，SFI，AID 重名

6.2 Erase File删除文件

6.2.1 定义和范围

删除指令成功执行后，将删除非电信下的全部应用。

6.2.2 命令报文

命令	长度(Byte)	值（Hex）	描述
CLA	1	80	指令类型
INS	1	EE	指令码
P1	1	00	
P2	1	00	
P3	1	08	

表 6-2 Erase DF 命令报文

6.2.3 命令报文数据域

从卡中取出随机数。

令随机数为明文，传输密钥为加密密钥进行 3DES 加密运算，得出数据域（认证码）。

6.3 Select选择文件

6.3.1 定义和范围

Select 命令通过文件名或 AID 来选择 IC 卡中的 DF（MF/DDF/ADF）或 EF。

6.3.2 注意事项

- 正确选择 MF 后，MF 安全寄存器将被复位为 0.
- 正确选择 MF 下各个 DF 后，DF 安全寄存器将被复位为 0，MF 安全寄存器的值不变.
- 应用锁定后，不能使用 Select 命令选择。

6.3.3 命令报文

代码	值
CLA	‘00’
INS	‘A4’
P1	‘00’：按 FID 选择（P2 必须等于 00） ‘01’：按 FID 选择 DF ‘02’：按 FID 选择 EF ‘04’：按文件名选择 DF
P2	‘00’第一个或仅有一个， ‘02’选择下一个（按文件名选择），
Lc	‘02’，P1=’00’ ‘05’-’10’， P1=’04’
Data	文件标识符或 DF 文件名
Le	选择 DF 时，为 FCI 文件信息长度

表 6-3 Select 命令报文

6.3.4 命令报文数据域

命令报文数据域应包括所选择的 PSE 名、DF 名、AID 或文件标识符 FID。

6.3.5 响应报文数据域

响应报文数据域应包括所选择的 DDF 或 ADF 的文件控制信息（FCI）.
下表定义了成功选择 DDF 后回送的 FCI：

标　志	值	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M
‘88’	目录基本文件的 SFI	M

表 6-4 SELECT DDF 的响应报文(FCI)

下表定义了成功选择 ADF 后回送的 FCI：

标　志	值	存在方式
‘6F’	FCI 模板	M
‘84’	DF 名	M
‘A5’	FCI 专用数据	M（社保应用无此项）
‘9F0C’	发卡方自定数据的 FCI	O（社保应用无此项）

表 6-5 SELECT ADF 的响应报文(FCI)

下表定义了 ADF 回送的‘A5’中包含的数据，其中必须包含标签为’9F08’的应用版本号，其数值由全国金融标准化技术委员会负责定义和维护

‘A5’	FCI 数据专用模板		M
	‘50’	应用标签	O
	‘87’	应用优先指示符	O
	‘9F08’	应用版本号	M
	‘9F12’	应用优先名称	O

表 6-6 SELECT ADF 的应答报文中的 FCI 数据专用模板

6.3.6 响应报文状态码

成功执行响应为‘9000’

IC 卡可能回送的错误状态码如下表所示：

编码	说明
6E00	CLA 不支持或错误
6D00	INS 不支持或错误
6700	长度错误
6985	所选文件被锁
9303	应用已锁定
6A81	无 MF 或者卡片锁定
6A82	文件未找到
6A86	参数错误
61XX	取响应，XX 为返回数据长度

表 6-7 Select 响应报文状态码

6.3.7 命令执行逻辑

检查 CLA 是否为“00”（6E00）
如果无 MF 或者卡片锁定，返 6A81
如果 P1＜3（根据 FID 查找）
检查 Lc 是否为 2（6700）
检查 P2 是否为“00”（6A86）
获取 FID
根据 FID 查找文件（6A82）
检查找到的文件类型 MF，DDF，ADF 或 EF
如果为 DF（MF，DDF，ADF）
设置 DF 标志位
检查是否为锁定的应用
如果是临时锁定的应用，返 6A81
否则返 9303
组织数据并返回
如果为 EF，返 9000
如果 P1 为 03，返 6A86
如果 P1 为“04”
检查 Lc 是否在[5，16]区间内（6700）
检查 P2 是否为“00”，“02”（6A86）
如果 P2 为“00”，根据 AID 查找第一个符合条件的文件（6A82）
如果 P2 为“02”，查找下一个符合条件的文件（6A82）
如果选中的文件为 DF 文件
设置 DF 标志位
如果是锁定的应用
如果是临时锁定的应用，返 6A81
否则返 9303
否则，组织数据并返回
如果选中的为 EF，则返 9000
如果 P1 为其它值，返 6A86

6.3.8 应用举例

条件 1：
操作：按 FID 选择 ADF
命令：00 A4 00 00 ADF1
响应：6134
命令：00 C0 00 00 34
响应：
6F328409A00000000386980701A5259F0801029F0C1E626400223333000103010001200108170000000012001010120011231556690000
说明：6134 表示后续有 0x34 字节数据需要取出，执行取响应命令将数据取出

操作：按文件名选择 ADF
命令：00 A4 04 00 09 A00000000386980701
响应：6134

命令：00 C0 00 00 34
响应：6F328409A00000000386980701A5259F0801029F0C1E6264002233330001030100012001081700000001200101012001123155669000
说明：6134 表示后续有 0x34 字节数据需要取出，执行取响应命令将数据取出

条件 2：
操作：按 FID 选择 DDF
命令：00 A4 00 00 02 DDF1
响应：6117
命令：00 C0 00 00 17
响应：6F15840E315041592E5359532E4444463031A5038801019000
说明：6117 表示后续有 0x17 字节数据需要取出，执行取响应命令将数据取出
操作：按文件名选择 DDF
命令：00 A4 04 00 0E 315041592E5359532E4444463031

响应：6117
命令：00 C0 00 00 17
响应：6F15840E315041592E5359532E4444463031A5038801019000
说明：6117 表示后续有 0x17 字节数据需要取出，执行取响应命令将数据取出

条件 3：
操作：选择 MF
命令：00 A4 00 00 02 3F00
响应：6109
命令：00 C0 00 00 09
响应：6F078400A5038801009000
说明：6109 表示后续有 0x09 字节数据需要取出，执行取响应命令将数据取出

条件 4：
操作：选择 EF
命令：00 A4 00 00 02 EF01
响应：9000
说明：响应 9000 说明此文件选择成功

6.4 Read Record 读记录文件

6.4.1 定义和范围

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

6.4.2 注意事项

- Read Record 命令适用于读取定长记录文件、循环记录文件、变长记录文件。
- 只有满足记录文件读权限时才能执行此命令。

6.4.3 命令报文

代码	值
CLA	‘00’
INS	‘B2’
P1	记录号
P2	引用控制参数(见下表)
Lc	不存在
Data	不存在
Le	‘00’或 要读取的记录的长度

表 6-8 Read Record 命令报文

下表定义了命令报文中的引用控制参数

P2								
B8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**含　义**
X	X	X	X	X				文件短标识符 SFI
0	0	0	0	0				当前文件
					1	0	0	按记录号访问

表 6-9 Read Record 命令引用控制参数 P2

6.4.4 命令报文数据域

命令报文中没有数据域。

6.4.5 响应报文数据域

Read Record 命令的响应报文数据域由读取的记录组成。

6.4.6 响应报文状态码

成功执行响应为‘9000’

IC 卡可能回送的错误状态码如下表所示：

编码	说明
6E00	CLA 不支持或错误

6D00	INS 不支持或错误
6700	长度错误
6981	文件类型不匹配
6982	安全状态不满足
6985	使用条件不满足
6986	没有 EF 被选择
6A81	功能不被支持
6A82	文件未找到
6A83	记录未找到
6A86	参数错误
6CXX	长度错误，Lc 应该为 XX

表 6-10 Read Record 响应报文状态码

6.4.7 命令执行逻辑

如果 CLA 不为“00”，返回 6E00
判断 P2 的合法性（6A86）
如果所要读取的是根据 SFI 来选择文件
获取 FID
根据 FID 查找文件（6A82）
如果所要读取的是当前文件（P1 不为 0 返 6A86）
读当前文件
判断所获取文件的文件类型是否匹配（6981）
检查权限（6982）
对变长记录文件和定长记录文件进行读取
如果数据响应模式为非社保模式（P2&03=04）
查找指定记录（6A83）
读取记录数据并获取记录长度。
如果数据响应模式为社保模式（P2&03=05，06）(多条连续记录的一次读取操作)（05，06 表示读取多条记录的顺序，05 为顺序，06 为逆序）
查找指定记录文件
获取指定记录数据的长度
如果 LC 大于记录数据的实际长度，返回 6CXX
如果 LC 为 0：
如果响应数据的长度大于 255,则分批做出响应并记录需响应的剩余记录数据的起始位置
否则，返回 6CXX
记录数据响应模式
组织数据并返回

6.4.8 应用举例

条件 1：**文件类型：定长记录文件**
文件标识符＝0001；
记录数＝3 条
记录长度＝12 个字节；
建立时不采用线路保护.
操作：读出定长记录文件中记录号为 02 的记录，不进行线路保护.

命令：00 B2 02 0C 00
响应：610C
说明：此文件的 L_C 应该为 0C，获取文件长度后，可根据需要读取文件中所需长度的数据。
命令：00 C0 00 00 0C
响应：11 22 33 44 55 66 77 88 99 AA BB CC 9000

条件 2：**文件类型：循环文件**
文件标识符＝0003；
记录数＝3 条
记录长度＝12 个字节；
建立时不采用线路保护.
操作：读出循环文件中记录号为 01 的记录，即最新写入的记录，不进行线路保护.
命令：00 B2 01 1C 00
响应：610C
说明：此文件的 L_C 应该为 0C，获取文件长度后，可根据需要读取文件中所需长度的数据。
命令：00 C0 00 00 0C
响应：11 22 33 44 55 66 77 88 99 AA BB CC 9000

条件 3：**文件类型：变长记录文件**
文件标识符＝0007；
建立时不采用线路保护.
操作：读出变长记录文件中的记录，不进行线路保护.
命令：00 B2 01 3C 00
响应：6104
说明：此文件的 L_C 应该为 04，获取文件长度后，可根据需要读取文件中所需长度的数据。
命令：00 C0 00 00 04
响应：11 22 33 44 9000

6.5 Read Binary 读二进制文件

6.5.1 定义和范围

Read Binary 命令用于读取二进制文件的内容(或部分内容)。

6.5.2 注意事项

- Read Binary 命令只适用于二进制文件.
- 只有满足二进制文件读权限时才能执行此命令.

6.5.3 命令报文

代码	值
CLA	‘00’
INS	‘B0’
P1	见下列说明

P2	从文件中读取的第一个字节的偏移地址
Lc	不存在；
Data	不存在；
Le	要读取的长度

表 6-11 Read Binary 命令报文

下表定义了命令报文中的引用控制参数：

P1								**P2**
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	
1	0	0	X	X	X	X	X	文件的偏移量
			短文件标识符					
0	文件偏移量 其中 P1 的低 7 位为偏移地址的高位							

表 6-12 Read Binary 命令引用控制参数

6.5.4 命令报文数据域

命令报文中没有数据域。

6.5.5 响应报文数据域

响应报文数据域由读出的数据组成。

6.5.6 响应报文状态码

IC 卡可能回送的错误状态码如下表所示：

编码	**说明**
6E00	CLA 不支持或错误
6D00	INS 不支持或错误
6700	长度错误
6981	文件类型不匹配
6982	安全状态不满足
6986	没有 EF 被选择
6A81	功能不被支持
6A82	文件未找到
6A86	参数错误
6B00	偏移超出范围
6CXX	长度错误，Lc 应该为 XX

表 6-13 Read Binary 响应报文状态码

6.5.7 命令执行逻辑

根据 P1 来判断文件选择方式。

如果所要读取的是根据 SFI 来选择文件

获取 SFI
根据 SFI 查找文件（6A82）
如果所要读取的是当前文件（P1 不为 0 返 6A86）
读取当前文件
获取文件头信息并判断文件类型（6981）
检查权限（6982）
从 APDU 指令中获取偏移量并判断偏移量的合法性（6B00）
如果 LC 大于文件体长度或等于“0”（6CXX）（XX 部分为文件体长度）
读取相应数据段，组织数据并返回。

6.5.8 应用举例

条件：文件类型：二进制文件
文件标识符：0005
文件主体空间的大小=8 字节
操作：读出自偏移量 00 开始到文件结束的所有数据，不进行线路保护。
命令：00 B0 85 00 00
响应：6108
说明：此文件的 L_C 应该为 08，获取文件长度后，可根据需要读取文件中所需长度的数据。
命令：00 C0 00 00 08
响应：11 22 33 44 55 66 77 88 9000

6.6 Update Record 修改记录文件

6.6.1 定义和范围

Update Record 命令用于更新定长或变长记录文件。

6.6.2 注意事项

- Update Record 命令适用于更新定长或变长记录文件。
- 只有满足记录文件写权限时才能执行此命令.
- 对于变长记录文件，更新记录时，新的记录长度必须与卡中原有记录长度相同，否则本次更新无效.
- 该指令在用户阶段不可使用。

6.6.3 命令报文

代码	值
CLA	‘00’ 或‘04’
INS	‘DC’
P1	记录号
P2	见说明

Lc	后续数据域的长度
Data	记录数据
Le	不存在

表 6-14 Update Record 命令报文

b8	b7	b6	b5	b4	b3	b2	b1	含　义
X	X	X	X	X				按 SFI 访问
0	0	0	0	0				当前文件
					1	0	0	记录号在 P1 中给出
其余值								RFU

表 6-15 Update Record 命令引用控制参数 P2

6.6.4 命令报文数据域

命令报文数据域由更新原有记录的新记录组成。

6.6.5 响应报文数据域

响应报文数据域不存在。

6.6.6 响应报文状态码

成功执行响应为‘9000’

IC 卡可能回送的错误状态码如下表所示：

编码	说明
6E00	CLA 不支持或错误
6D00	INS 不支持或错误
6581	内存失败（修改失败）
6700	长度错误
6981	文件类型不匹配
6982	安全状态不满足
6985	使用条件不满足
6986	没有 EF 被选择
6988	线路保护错误
6A80	数据域有错误
6A81	不支持此功能
6A82	文件未找到
6A86	参数错误
6A83	记录没有找到
6A84	文件中存储空间不够
6A85	Lc 与 TLV 结构不相容

表 6-16 Update Record 响应报文状态码

6.6.7 命令执行逻辑

检查 P2 的低三位是否为 100（6A86）
如果所要读取的是根据 SFI 来选择文件
获取 SFI
根据 SFI 查找文件（6A82）
如果所要读取的是当前文件（如果 P1 不为 0 则返 6A86）
读取当前文件
判断 LC 是否不为 0（6700）
判断文件类型是否匹配（6981）
检查权限（6982）
检查是否需要线路保护
判断 CLA 是否为 04（6A86）
查找应用维护密钥
密钥文件没找到（6A82）
密钥记录没找到（6A83）
检查权限（6982）
检查密钥是否锁死（9303）
判断随机数(6984)
校验 MAC，如果 MAC 错误，错误计数器减 1
如果错误计数器不为 0(6988)
如果错误计数器为 0（9303）
如果 MAC 正确
更新指定位置的二进制文件数据
重置错误计数器
如果是循环记录文件
追赶加记录后，修改指针
如果是定长记录
查长记录位置并更新记录
如果是变长记录
查长记录位置并更新记录
返回

6.6.8 应用举例

条件：文件类型：定长记录文件
文件标识符=0002
记录数=3 条
记录长度=12 个字节
建立时不采用线路保护
操作：写定长记录文件，不进行线路保护。
命令：00 DC 01 14 0C 11 22 33 44 55 66 77 88 99 AA BB CC
响应：9000
说明：‘11 22 33 44 55 66 77 88 99 AA BB CC’为写入的数据。

条件：文件类型：变长记录文件
文件标识符=0001

建立时不采用线路保护
操作：写变长记录文件，不进行线路保护。
命令：00 DC 00 0C 05 11 22 33 44 55
响应：9000
说明：‘11 22 33 44 55’为写入的数据。

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

6.7 Update Binary 修改二进制文件

6.7.1 定义和范围

Update Binary 命令用以写/修改二进制文件。

6.7.2 注意事项

- Update Binary 命令只适用于二进制文件。
- 只有满足二进制文件写权限时才能执行此命令.
- 该指令在用户阶段不可使用。

6.7.3 命令报文

代码	值
CLA	‘00’或‘04’
INS	‘D6’
P1	见说明
P2	要修改的第一个字节的偏移地址
Lc	后续数据域的长度
Data	写入/修改用的数据+报文认证码(MAC)数据元(4 字节)
Le	不存在

表 6-17 Update Binary 命令报文

CLA = ‘00’ 不需要安全报文。
CLA = ‘04’ 需要安全报文。

下表定义了命令报文中的引用控制参数：

P1	P2

b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0	SFI					欲读文件的偏移量
0	当前文件（欲写）的偏移量 其中 P1 低 7 位为偏移地址的高位							

表 6-18 Update Binary 命令引用控制参数

6.7.4 命令报文数据域

命令报文数据域为要写入的新的数据。

6.7.5 响应报文数据域

响应报文数据域不存在。

6.7.6 响应报文状态码

成功执行响应为‘9000’

IC 卡可能回送的状态码如下表所示：

编码	说明
6E00	CLA 不支持或错误
6D00	INS 不支持或错误
6700	长度错误
6581	内存失败（修改失败）
6981	文件类型不匹配
6982	安全状态不满足
6985	使用条件不满足
6986	没有 EF 被选择
6988	线路保护错误
6A81	不支持此功能
6A82	文件未找到
6A86	参数错误
6B00	偏移超出范围

表 6-19 Update Binary 响应报文状态码

6.7.7 命令执行逻辑

根据 P1 判断文件选择方式（6A86）
如果所要读取的是根据 SFI 来选择文件
获取 FID
根据 FID 查找文件（6A82）
如果所要读取的是当前文件（P1 不为 0 返 6A86）
读当前文件
获取文件头信息并判断文件类型（6981）

检查权限
判断偏移量的合法性（6B00）
判断 LC 是否不为 0（6700）
检查是否需要线路保护
判断 CLA 是否为 04（6A86）
查找应用维护密钥
密钥文件没找到（6A82）
密钥记录没找到（6A83）
检查权限（6982）
检查密钥是否锁死（9303）
判断随机数(6984)
校验 MAC，如果 MAC 错误，错误计数器减 1
如果错误计数器不为 0(6988)
如果错误计数器为 0（9303）
如果 MAC 正确
更新指定位置的二进制文件数据
重置错误计数器
检查更新字段（编移量+LC）是否超出文件体的范围（6B00）
修改指定数据段并返回。

6.7.8 应用举例

条件：文件类型：二进制文件
文件标识符＝0005
文件主体空间的大小＝8 个字节
建立时不采用线路保护.
操作：写二进制文件
命令：00 D6 85 00 08 11 22 33 44 55 66 77 88
响应：9000

6.8 Verify PIN校验个人密码

6.8.1 定义和范围

Verify PIN 命令用于校验命令数据域中的个人密码的正确性。
如 PIN 文件位于某一应用下，当此应用被锁定时，禁止校验 PIN;如 PIN 文件位于 MF 下，当应用被锁定后可以执行校验 PIN 命令。

6.8.2 注意事项

需要满足 PIN 的使用权限。

6.8.3 命令报文

代码	值
CLA	‘00’
INS	‘20’
P1	‘00’
P2	口令密钥标识号 社保应用：’00’
Lc	口令的长度，2-6 社保应用：’00’或’02’ ～’08’
Data	外部输入的个人密码
Le	不存在

表 6-20 Verify PIN 命令报文

P2=’00’表示无特殊限定符被使用。在 IC 卡上，VERIFY 命令在处理过程中应明确知道如何去寻找个人密码。

6.8.4 命令报文数据域

命令报文数据域由持卡者输入的个人密码组成。

6.8.5 响应报文数据域

响应报文数据域不存在。

6.8.6 响应报文状态码

成功执行响应为‘9000’

IC 卡可能回送的警告状态码如下表所示：

SW1	SW2	含　义
‘63’	‘Cx’	校验失败，‘x’表示允许重试的次数

IC 卡可能回送的状态码如下表所示：

Verify PIN 错误状态

SW1	SW2	含　义
‘69’	‘83’	认证方法(个人密码)锁定
‘69’	‘84’	引用数据无效
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘67’	‘00’	长度错误

表 6-21 Verify PIN 响应报文状态码

6.8.7 命令执行逻辑

判断 CLA（6E00）
检查 P1，P2（6A86）
如果 Lc 小于 2 且不等于 0 或 Lc 大于 8，返 6700
查找 PIN 密钥
如果密钥文件未找到（6A82）
如果密钥记录未找到（6A83）
检查权限（6982）
判断 PIN 是否锁定（6983）
如果 Lc 为 0（社保，PIN 为 N 个 FF）
校验 PIN 值
如果校验成功，设置安全状态并返回
如果校验失败（63CX）
如果 Lc 不为 0，校验 PIN
如果校验失败
清空安全状态
如果错误次数不为 0，返 63CX
如果错误次数为 0，返 6300
如果校验成功，设置安全状态并返回。

6.8.8 应用举例

条件：文件类型：二进制文件
　　文件标识=0005
　　文件主体空间的大小=8 个字节；
　　建立时不采用线路保护
操作：写二进制文件
命令：00 D6 85 00 08 11 22 33 44 55 66 77 88
响应：9000

6.9 Internal Authentication 内部认证

6.9.1 定义和范围

Internal Authentication 命令提供了利用接口设备发来数据和自身存储的相关密钥进行数据认证的功能，在这里指的是使用密钥对数据进行加密。

6.9.2 注意事项

在满足该密钥的使用条件时才能执行此命令。

6.9.3 命令报文

代码	值
CLA	‘00’
INS	‘88’
P1	‘00’
P2	密钥索引
Lc	认证数据的长度 社保应用：‘10’~’11’
Data	认证数据
Le	响应数据的长度 社保应用：‘00’

表 6-22 Internal Authentication 命令报文

6.9.4 命令报文数据域

命令报文数据域的内容是应用专用的认证数据。

6.9.5 响应报文数据域

响应数据为使用指定密钥对认证数据加密形成的数据。

6.9.6 响应报文状态码

IC 卡可能回送的错误状态码如下表所示：

SW1	SW2	含　义
‘67’	‘00’	长度错误
‘69’	‘82’	不满足安全状态
‘69’	‘85’	不满足使用条件
‘6A’	‘82’	文件未找到
‘6A’	‘83’	密钥未找到
‘6A’	‘86’	参数 P1 P2 不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

表 6-23 Internal Authentication 响应报文状态码

6.9.7 内部认证过程

序号	终端	方向	卡片
1	产生两个 8 字节随机数 RND_{IFD}		

2	送 RND_{IFD} 作内部认证	⟶	卡片用指定的 DES 加密钥对随机数 RND_{IFD} 进行 DES 加密运算，产生鉴别数据 D1 。即 D1=DES(KID, RND_{IFD})
3		⟵	送 D1
4	用与卡片认证密钥相同的密钥 Cardkey 对 RND_{IFD} 进行 DES 加密得到鉴别数据 D2．即： D2=DES(Cardkey, RND_{IFD}) D1?= D2		

图 **错误！未找到引用源。**-1 内部认证过程

6.9.8 命令执行逻辑

For SSSE

检查 CLA 是否为“00”（6E00）
检查 P1 是否为“00”（6A86）
检查 Lc 是否为 16 或 17（6700）
根据 P2 获取密钥 ID
根据 Lc 的不同，采用不同的密钥查找方式
查找内部认证密钥（6A82，6A83）
检查权限（6982）
对数据域中的前 8 个字节进行加密
以加密后的数据为密钥对数据域中的后 8 个字节进行加密
将最后所得的加密数据返回

For PSE

检查 CLA 是否为“00”（6E00）
检查 P1 是否为“00”（6A86）
检查 Lc 是否在(0,0xF0)范围内（6700）
根据 P2 获取密钥 ID
查找内部认证密钥（6A82，6A83）
检查权限（6982）
对数据域中的数据进行加密
将所得的加密数据返回

6.9.9 应用举例

条件：密钥标识号=01
密钥类型：DES 加密密钥；
使用权限=0xF0
更改权限=0XEF
算法标识=01
密钥版本号=01
16 字节的密钥=‘5741544348444154415469 6D65434F53’

待加密数据=‘1122334455667788’。

操作：内部认证即 DES 加密。

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

响应：6108

说明：对于 T=0 的卡片，6108 表示卡片要回送的数据长度，可以通过 Get Response 命令取返回数据。

命令： 00 C0 00 00 08

响应：07 CB F6 15 E7 D7 2F 96 9000

6.10External Authentication 外部认证

6.10.1定义和范围

External Authentication 命令用以验证外部设备的有效性，如果验证成功，则获得相应的操作权限。执行此命令前，需要先执行取随即数的命令。

6.10.2注意事项

在满足该外部认证密钥的使用权限且密钥未被锁死时才可执行该命令。

6.10.3命令报文

代码	值
CLA	‘00’
INS	‘82’
P1	‘00’
P2	密钥索引号
Lc	8
Data	8 字节的随即数密文
	8 字节鉴别数据＋8 字节鉴别所需原始信息
Le	不存在

表 6-24 External Authentication 命令报文

说明：

将命令中的数据用指定外部认证密钥解密，然后与先前产生的随机数进行比较，

若一致则表示认证通过，置安全状态寄存器为该密钥规定的后续状态值，错误计数器恢复成初始值；

若不一致则表示认证失败，可再错次数减一，且不改变安全状态寄存器的值。

6.10.4命令报文数据域

命令报文数据域中包含 8 字节的随机数密文数据.

6.10.5响应报文数据域

响应报文数据域不存在。

6.10.6响应报文状态码

IC 卡可能回送的警告状态码如下表所示：

SW1	SW2	含　义
‘63’	‘Cx’	鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’）

IC 卡可能回送的状态码如下表所示：

SW1	SW2	含　义
‘67’	‘00’	Lc 不正确
‘69’	‘83’	认证方法锁定
‘69’	‘84’	引用数据无效
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	参数 P1 P2 不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

表 6-25 External Authentication 错误状态

6.10.7外部认证过程

外部认证是卡片对机具的认证，流程如下：

序号	终端	方向	卡片
1	取 8 字节随机数（Get Challenge）	→	卡片内部产生随机数 RND_{ICC}
2		←	送随机数 RND_{ICC}
3	用与卡片认证密钥相同的密钥 Cardkey 对送随机数 RND_{ICC} 进行加密得到鉴别数据 D1．即：D1=DES(Cardkey, RND_{ICC})		

4	送鉴别数据 D1 作外部认证.	⟶	卡片用指定的外部认证密钥对 D1 进行解密运算，产生鉴别数据 D2，后比较 D2 和 RND_{ICC}．即 $D2=DES^{-1}(KID,DI)$ $D2?= RND_{ICC}$
5		⟵	送比较结果(即 SW1SW2)，若比较正确，则置安全状态寄存器值为该密钥后续状态.

图 **错误！未找到引用源。**-2 外部认证过程

6.10.8 命令执行逻辑

For SSSE

判断 CLA 是否为 0（6E00）
判断 P1 是否为 0（6A86）
判断 Lc 是否为 16 或 17（6700）
查找外部认证密钥（9403）
判断随机数(6984)
由外部认证密钥对随机数加密生成过程密钥，后由过程密钥对原始数据进行加密得到验证密文，该密文与数据域中验证密文进行比较：
如果数据不相等
清空安全状态
随机数标志清 0
错误计数器减 1
返回 63CX
如果数据相等
设置安全状态为成功
随机数标志清 0
重置错误计数器并返回 9000

For PSE

判断 CLA 是否为 0（6E00）
判断 P1 是否为 0（6A86）
判断 Lc 是否为 8（6700）
查找外部认证密钥（9403）
检查权限（6982）
判断随机数(6984)
检查密钥是否锁死（6983）
加密之前获取的随机数并和数据域中的随机数密文进行比较
如果数据不相等
清空安全状态
随机数标志清 0
错误计数器减 1
返回 63CX
如果数据相等
设置安全状态为成功
随机数标志清 0

重置错误计数器并返回 9000

6.10.9应用举例

条件：
外部密钥标识号＝01
使用权限＝0x00;
更改权限＝0xFF;
错误计数器＝0x33;
后续状态＝01
16 字节的密钥＝’57 41 54 43 48 44 41 54 41 54 69 6D 65 43 4F 53’
操作：
外部认证
步骤：
Step1:取 8 字节随机数.
命令：00 84 00 00 08
响应：D3 89 BF 67 45 B9 35 50 9000
Step2:卡终端用与外部认证密钥相同的密钥’57 41 54 43 48 44 41 54 41 54 69 6D 65 43 4F 53’对随机数进行加密，加密后的结果为 C1 8A 5B 4B 13 40 25 21.
Step3:卡终端将加密后的随机数送到卡中作外部认证.
命令：00 82 00 01 08 C1 8A 5B 4B 13 40 25 21
响应：9000
说明：成功执行后置安全状态寄存器 b1 位值为该外部认证密钥的后续状态 01.

6.11Get Challenge 取随机数

6.11.1定义和范围

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

6.11.2命令报文

代码	值
CLA	‘00’
INS	‘84’
P1	‘00’
P2	‘00’
Lc	不存在
Data	不存在
Le	‘04’～’10’

表 6-26 Get Challenge 命令报文

6.11.3命令报文数据域

命令报文数据域不存在。

6.11.4响应报文数据域

响应报文数据域包括随机数，长度为 4 字节或 8 字节。

6.11.5响应报文状态码

IC 卡可能回送的状态码如下表所示：

SW1	SW2	含　义
‘67’	‘00’	Le 长度错
‘6A’	‘81’	不支持此功能
‘6A’	‘86’	参数 P1 P2 不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

表 6-27 Get Challenge 响应报文状态码

6.11.6命令执行逻辑

判断 CLA 是否为“84”（6E00）
检查 P1，P2 是否为 0（6A86）
检查 Lc 是否非 0 且小于 0x10（6700）
获取随机数
组织数据并返回

6.12Get Response 取响应

6.12.1定义和范围

当 APDU 不能用现有协议传输时，Get Response 命令提供了一种从卡片向接口设备传送 APDU(或 APDU 的一部分)的传输方法.
当前一条指令返回 61XX 时，设备使用此指令从 IC 卡取响应数据.

6.12.2注意事项

前一条指令返回为 61XX 时可以使用。
如果 Le 的值为零，在附加数据有效时，卡片必须回送状态码’6CXX’，否则回送状态码’6F00’

6.12.3命令报文

代码	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

表 6-28 Get Response 命令报文

6.12.4命令报文数据域

命令报文数据域不存在。

6.12.5响应报文数据域

响应报文数据域的长度由 Le 的值决定。
如果 Le 的值为零，在附加数据有效时，卡片必须回送状态码’6CXX’，否则回送状态码’6F00’。

6.12.6响应报文状态码

IC 卡可能回送的警告状态码如下表所示：

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

IC 卡可能回送的错误状态码如下表所示：

SW1	SW2	含　义
‘67’	‘00’	长度错误(Le 不正确)
‘6A’	‘86’	参数 P1 P2 不正确
‘6C’	‘XX’	长度错误(Le 不正确，’XX’表示实际长度)
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘6F’	‘00’	数据无效

表 6-29 Get Response 响应报文状态码

6.12.7命令执行逻辑

检查 CLA 是否为 0（6E00）
检查 P1，P2 是否为 0（6A86）

检查实际的响应数据是否不为 0（6F00）
如果当前应用环境为社保卡且上次的 APDU 指令为读记录指令：
根据响应模式的不同来决定记录数据中各条记录的顺序为“顺序”或“逆序”
如果响应数据的长度大于 255，则需要分批响应并记录需响应的剩余记录数据的起始位置。
否则，返回指定长度的数据
如果 Lc 大于实际的响应数据长度或者 Lc 为 0，返回 6CXX
如果 Lc 小于实际的响应数据长度，则返回指定长度的数据

6.12.8应用举例

条件：
钱包文件（二进制）标识＝0001
步骤：
Step1:向钱包存入 1 元钱
命令：80 52 00 00 0B 1122334455667788991122
响应：6104
说明：对于 T=0 的卡片，6104 表示卡片要回送的数据长度，可以通过 Get Response 命令取返回数据.
Step2: 取响应数据
命令：00 C0 00 00 04
响应：A4072FBF 9000
说明：A4072FBF 为圈存返回的 TAC

6.13Append Record 添加记录

6.13.1定义和范围

用于对循环文件或变长记录文件添加记录。

6.13.2注意事项

1. Append Record 命令适用于循环文件和变长记录文件。
2. 只有满足记录文件读权限时才能执行此命令
3. 若循环文件记录已满则覆盖最早写入的记录，且新增加的记录的记录号总为
4. 该指令在用户阶段不可使用。

6.13.3命令报文

代码	值
CLA	‘00’或‘04’
INS	‘E2’
P1	‘00’

P2	当 P2=00000000 时，为当前 EF 当 P2=XXXXX000，且 XXXXX 不全等时，为 SFI。
Lc	数据字节数
Data	增加的纪录
Le	不存在

表 6-30 Append Record 命令报文

6.13.4 命令报文数据域

要追加的记录的数据

6.13.5 响应报文状态码

SW1	SW2	含义
90	00	正确执行
65	81	写 EEPRROM 失败
67	00	长度错误（Lc 域为空）
69	81	当前文件不是循环文件或变长纪录文件
69	82	不满足安全状态
6A	81	不支持此功能（无 MF 或 MF 已锁定）
6A	82	未找到文件
6A	83	未找到纪录
6A	84	文件中存储空间不够（对变长纪录文件）

表 6-31 Append Record 响应报文状态码

6.13.6 命令执行逻辑

检查 P1 是否为“00”（6A86）
检查 P2 低三位是否为“000”（6A86）
根据 P2 获取 SFI
如果 SFI 为 0，则当前文件为所要查找的文件
如果 SFI 不为 0，根据 SFI 查找文件(6A82)
检查 Lc 是否为 0（6700）
检查文件类型（6981）
检查读写权限（6982）
检查是否需要线路保护
　　判断 CLA 是否为 04（6A86）
　　查找应用维护密钥
　　密钥文件没找到（6A82）
　　密钥记录没找到（6A83）
　　检查权限（6982）
　　检查密钥是否锁定（9303）
　　判断随机数(6984)
　　校验 MAC，如果 MAC 错误，错误计数器减 1

如果错误计数器不为 0（6988）
如果错误计数器为 0（9303）
如果 MAC 正确
重置错误计数器
追加记录并返回。

6.13.7应用举例

- **文件类型：变长记录文件**
  文件标识符=0001
  建立时不采用线路保护
  操作：往变长记录文件中增加 1 条长度为 14 字节的记录，不进行线路保护。
  命令：00 E2 00 08 0E AA 0C 11 22 33 44 55 66 77 88 99 AA BB CC
  响应：9000

- **文件类型：循环文件**
  文件标识符=0001
  记录数=02
  记录长度=06
  建立时不采用线路保护
  设该文件为当前文件
  操作：往循环文件中增加 1 条记录，不进行线路保护。
  命令：00 E2 00 00 06 11 22 33 44 55 66
  响应：9000

6.14Write Key 装载/更新密钥

6.14.1定义和范围

Write Key 用于建立和更新密钥（包含 PIN）。

6.14.2注意事项

- 该指令在用户阶段不可使用。
- 密钥的安装和更新涉及到多种情况，下面将一一说明：

当建立安全文件，安装密钥时，如果当前目录或者上级目录不存在主控密钥的话，这时使用 Write Key 命令安装密钥只能采用明文方式安装密钥。

1. 在选择进入一个 DF 后，如果已经存在安全文件了，则安装密钥需要满足安全文件头中定义的增加权限要求。
2. 安装密钥的时候可以采用明文或者使用线路保护，如果使用线路保护的话，则采用的安全机制要和 KEY 文件头中定义的安全机制一致。
3. 修改密钥的时候，需要满足密钥的修改权限，采用的安全机制必须和密钥类型中定义的安全机制保持一致。

4. 在安装或修改密钥的时候，所用的线路保护密钥为当前 DF 下的主控密钥，如果当前 DF 下无密钥，必须先建立当前应用主控密钥，建立当前应用主控密钥用上级 DF 中的主控密钥。

6.14.3命令报文

域	长度	值	说明
CLA	1	‘80’/ ‘84’	84 为密文
INS	1	‘D4’	
P1	1	‘XX’	‘01’ ：安装密钥 ‘02’ ：更新密钥方法 2 其他：‘密钥类型’：更新密钥，更新密钥方法 1
P2	1	KID	KID 密钥标识符
Lc	1	‘XX’	DATA 域的长度
DATA	Lc	‘XX’… ‘XX’	
Le			不存在

表 6-32 Write Key 命令报文

6.14.4命令报文数据域

安装密钥时，DATA 数据域包括：

域	字节数	说明
密钥类型	1	
使用权限	1	
修改权限	1	
密钥版本/错误记数	1	
算法标识/后续状态	1	
密钥值	2-16	

表 6-32 Write Key 命令报文数据域

注：如果安装密钥时，DATA 数据域只有一个字节的密钥类型，则此密钥是全局密钥，表示引用的是 MF 下密钥类型和密钥标识都相同的密钥。

方式 1 修改密钥：DATA 数据域包括：

域	字节数	说明
密钥值	2-16	

方式 2 修改密钥：DATA 数据域包括：

域	字节数	说明
密钥类型	1	
使用权限	1	
修改权限	1	
密钥版本/错误记数	1	
算法标识/后续状态	1	
密钥值	2-16	

6.14.5 响应报文数据域

无

6.14.6 响应报文状态码

此命令执行成功的状态码是'9000'。
错误状态

SW1	SW2	含　　义
'6A'	'82'	文件未找到
'6A'	'83'	KEY 未找到
'6A'	'84'	空间不足
'6A'	'86'	参数错误
'67'	'00'	长度错误
'69'	'00'	CLA 与线路保护属性不匹配
'69'	'82'	安全状态不满足

表 6-33 Write Key 响应报文状态码

6.14.7 应用实例

格式 1：安装密钥
命令：80 D4 01 00 15 39 00 00 FF 0F 11223344556677889900112233445566
响应：9000
说明：安装密钥，此例中是类型为 39、标识是 00 的主控密钥，39 中的高 3 位都是 0，说明更新此密钥时要线路保护方式为'明文'，密钥长度为 16 字节

格式 2：方法 1 修改密钥
命令：80 D4 39 00 10 00111177665544338899112233445511
响应：9000
说明：修改类型为 39、标识为 00 的主控密钥，此方法只能修改密钥值

格式 3：方法 2 修改密钥
命令：80 D4 02 00 15 39 00 00 33 01 00111177665544338899112233441111
响应：9000
说明：修改类型为 39、标识为 00 的主控密钥，此方法除类型和标识，其它值都可以修改

7 UranusPay ED/EP金融专用命令

本章描述 UranusPay ED/EP 金融专用命令（交易 APDU 命令），并描述了相应的交易命令表以及交易类型标识表。

CLA	INS	P1	P2	说明	
80	50	00	0X	初始化	圈存 Ini Load
		01	0X		消费 Ini Purchase
		02	01		取现 Ini Cash Withdraw
		03	02		复合消费 Capp Purchase
	52	00	00	圈存 Load	
	54	01	00	消费/取现 Purchase/CashWithdraw	
		03	00	圈提 Unload	
		01	00	复合消费 Debit For Capp Purchase	
	58	00	00	修改透支限额 Update Overdraw Limit	
	5A	00	XX	取交易认证 Get Transaction Proof	
	5C	00	0X	读余额 Get Balance	
	5E	00	00	重装个人密码 Reload PIN	
		01	00	修改个人密码 Change PIN	
	DC	XX	XX	取认证识别码（建设部专用）	

UranusPay ED/EP 金融专用交易命令列表

7.1 Initialize For Load圈存初始化

7.1.1 定义和范围

Initialize For Load命令用于初始化圈存交易。

7.1.2 命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘00’
P2	‘01’ 用于 ED， ‘02’ 用于 EP 其他值保留。
L_c	‘0B’
Data	见说明

L_e	‘10’

表 7-1 Initialize For Load 命令报文

7.1.3 命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

表 7-2 Initialize For Load 命令报文

7.1.4 响应报文数据域

说明	长度（字节）
ED 或 EP 余额	4
ED 或 EP 联机交易序号	2
密钥版本号（DLK）	1
算法标识（DLK）	1
伪随机数（IC 卡）	4
MAC1	4

表 7-3 Initialize For Load 响应报文数据域

MAC1 计算如下：

1) 生成 8 字节过程密钥 SK：由 Initialize For Load 命令指定下的密钥对下表的数据加密生成 8 字节过程密钥 SK。

数据	长度（字节）
伪随机数	4
电子存折或电子钱包联机交易序号	2
‘8000’	2

2) 生成 MAC1：采用步骤 1 中的过程密钥 SK 对下表的数据按照 4.3.4MAC 中的 MAC 计算方法生成 MAC1。

数据	长度（字节）
电子存折或电子钱包旧余额	4
交易金额	4
交易类型标识（参考附录 3）	1
终端机编号	6

7.1.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

Initialize For Load错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误

‘69’	‘85’	使用条件不满足
‘6A’	‘81’	功能不支持
‘6A’	‘86’	P1、P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘03’	密钥索引不支持
‘69’	‘82’	不满足安全状态
‘93’	‘03’	应用被永久锁定

表 7-4 Initialize For Load 响应报文状态码

7.2 Credit For Load圈存

7.2.1 定义和范围

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

7.2.2 命令报文

代码	值
CLA	‘80’
INS	‘52’
P1	‘00’
P2	‘00’
L_c	‘0B’
Data	见说明
L_e	‘04’

表 7-5 Credit For Load 命令报文

7.2.3 命令报文数据域

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

表 7-6 Credit For Load 命令报文数据域

MAC2 的计算如下：

采用 Initialize For Load 圈存初始化时生成的过程密钥 SK 对下表达数据按 MAC 计算方法生成的。

数据	长度（字节）
交易金额	4
交易类型标识（参考附录 3）	1
终端机编号	6

主机交易日期	4
主机交易时间	3

7.2.4 响应报文数据域

说明	长度（字节）
交易验证码 TAC	4

表 7-7 Credit For Load 响应报文数据域

TAC 的计算如下：

TAC 由内部密钥 DTK 左右 8 字节异或运算的结果对下表的数据按 MAC 计算方法生成的。

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

7.2.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

CREDIT FOR LOAD错误状态

SW1	SW2	说 明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效
‘93’	‘03’	应用被永久锁定
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确

表 7-8 Credit For Load 响应报文状态码

注：完成圈存后，UranusPay ED/EP 将作如下操作：

- 把交易金额加在电子钱包或电子存折的余额上
- 将电子存折联机交易序号或电子钱包联机交易序号加 1
- 用数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。交易明细文件由哪些数据组成具体请参考章节 3 的文件结构。

7.2.6 圈存交易流程

序号	IC 卡	方向	终端	方向	主机
1	设置当前应用标识	←	选择银行应用		
2	并送出应用序列号	→	将应用序列号送主机	→	主机保留该卡片应用序列号
3	卡片产生过程密钥 SK,并利用 SK 计算得到 MAC1	←	发送圈存初始化命令 Initialize For Load		主机按终端指定的密钥标识，使用相应的圈存主密钥对应用序列号分散得到圈存子密钥。
4	将原余额、联机交易序号、密钥版本号、算法标识、4 字节伪随机数和 MAC1 送卡外	→	将收到的所有响应数据传送给银行主机	→	按卡片相同方法产生相同的过程密钥 SK，校验 MAC1 的正确性
5	IC 卡用过程密钥 SK 验证 MAC2 的正确性，若验证通过，则将交易金额加到余额上，更新交易明细记录，并用内部密钥前后 8 字节异或对新余额、联机交易序号、交易金额、交易类型标识、终端机编号、主机交易日期和时间进行 TAC 计算，产生 4 字节的 TAC 码、卡片联机交易序号加 1。	←	终端接收主机交易日期和时间以及 MAC2，将其作为圈存命令的 DATA 域，发送圈存命令 Credit for load 给 IC 卡	←	如果 MAC1 校验正确，则主机联机交易序号加 1，并用 SK 对金额、交易类型标识、终端号、交易日期和时间进行 MAC 计算得到 MAC2，送至终端，否则，交易终止。
6	将 TAC 码回送给终端。	→	终端接收到 TAC 码，确认交易成功。		

图 **错误！未找到引用源。**-1 圈存交易流程

7.3 Initialize For Unload圈提初始化

7.3.1 定义和范围

Initialize For Unload命令用于初始化圈提交易。

7.3.2 命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘05’

P2	‘01’用于 ED 圈提交易。其他值保留。
L_c	‘0B’
Data	见说明
L_e	‘10’

表 7-9 Initialize For Unload 命令报文

7.3.3 命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

表 7-10 Initialize For Unload 命令报文数据域

7.3.4 响应报文数据域

说明	长度（字节）
ED 余额	4
ED 联机交易序号	2
密钥版本号（DULK）	1
算法标识（DULK）	1
伪随机数（IC 卡）	4
MAC1	4

表 7-11 Initialize For Unload 响应报文数据域

MAC1 计算如下：

1) 生成 8 字节过程密钥 SK：由 Initialize For Unload 命令指定下的密钥对下表的数据加密生成 8 字节过程密钥 SK。

数据	长度（字节）
伪随机数	4
电子存折联机交易序号	2
‘8000’	2

2) 生成 MAC1：采用步骤 1 中的过程密钥 SK 对下表的数据按照 4.3.4MAC 中的 MAC 计算方法生成 MAC1。

数据	长度（字节）
电子存折或电子钱包旧余额	4
交易金额	4
交易类型标识（参考附录 3）	1
终端机编号	6

7.3.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1、P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持

表 7-12 Initialize For Unload 响应报文状态码

7.4 Debit For Unload圈提

7.4.1 定义和范围

Debit For Unload命令用于圈提交易。该命令只有在成功执行Initialize For Unload之后才能执行。通过圈提交易，持卡人可以把电子存折中的部分或全部资金划回其在银行的相应帐户上。

此交易必须在金融终端机上联机进行并要求验证口令。

7.4.2 命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘03’
P2	‘00’
L_c	‘0B’
Data	见说明
L_e	‘04’

表 7-13 Debit For Unload 命令报文

7.4.3 命令报文数据域

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

表 7-14 Debit For Unload 命令报文数据域

MAC2 的计算如下：

采用 Initialize For Unload 圈提初始化时生成的过程密钥 SK 对下表达数据按 MAC 计算方法生成的。

数据	长度（字节）
交易金额	4
交易类型标识（参考附录 3）	1

终端机编号	6
主机交易日期	4
主机交易时间	3

7.4.4 响应报文数据域

说明	长度（字节）
MAC3	4

表 7-15 Debit For Unload 响应报文数据域

MAC3 的计算如下：

MAC3 由 Initialize For Unload 圈提初始化时生成的过程密钥 SK 对下表达数据按 MAC 计算方法生成的。

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

7.4.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

Debit For Unload**错误状态**

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘01’	命令不接受（无效状态）
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效

表 7-16 Debit For Unload 响应报文状态码

注：完成圈提后，UranusPay ED/EP 将做如下操作：

- 从电子存折余额中扣减交易金额；
- 将电子存折联机交易序号加 1；
- 用数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。交易明细文件由哪些数据组成具体请参考章节 3 的文件结构。

7.4.6 圈提交易流程

序号	IC 卡	方向	终端	方向	主机

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

图 **错误！未找到引用源。**-2 圈提交易流程

7.5 Initialize For Purchase消费初始化

7.5.1 定义和范围

Initialize For Purchase命令用于初始化消费交易。

7.5.2 命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘01’
P2	‘01’用于 ED ‘02’用于 EP

	其他值保留
L_c	‘0B’
Data	见说明
L_e	‘0F’

表 7-17 Initialize For Purchase 命令报文

7.5.3 命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

表 7-18 Initialize For Purchase 命令报文数据域

7.5.4 响应报文数据域

说明	长度（字节）
ED 或 EP 余额	4
ED 脱机交易序号或 EP 脱机交易序号	2
透支限额	3
密钥版本号（DPK）	1
算法标识（DPK）	1
伪随机数（IC 卡）	4

表 7-19 Initialize For Purchase 响应报文数据域

7.5.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

Initialize For Purchase错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持
‘67’	‘00’	Lc 长度错
‘69’	‘82’	不满足安全状态
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘93’	‘03’	应用被永久锁定

表 7-20 Initialize For Purchase 响应报文状态码

7.6 Initialize For Cash Withdraw取现初始化

7.6.1 定义和范围

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

7.6.2 命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘02’
P2	‘01’用于 ED 取现交易；其他值保留。
L_c	‘0B’
Data	见说明
L_e	‘0F’

表 7-21 Initialize For Cash Withdraw 命令报文

7.6.3 命令报文数据域

说明	长度（字节）
密钥索引号	1
交易金额	4
终端机编号	6

表 7-22 Initialize For Cash Withdraw 命令报文数据域

7.6.4 响应报文数据域

说明	长度（字节）
ED 余额	4
ED 脱机交易序号（IC 卡）	2
透支限额	3
密钥版本号（DPK）	1
算法标识（DPK）	1
伪随机数（IC 卡）	4

表 7-23 Initialize For Cash Withdraw 响应报文数据域

7.6.5 响应报文的状态码

此命令执行成功的状态码是'9000'。

Initialize For Cash Withdraw错误状态

SW1	SW2	说明
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误
'94'	'01'	金额不足
'94'	'03'	密钥索引不支持

表 7-24 Initialize For Cash Withdraw 响应报文状态码

7.7 Debit For Purchase/Cash Withdra消费/取现

7.7.1 定义和范围

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

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

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

7.7.2 命令报文

代码	值
CLA	'80'
INS	'54'
P1	'01'
P2	'00'
L_c	'0F'
Data	见说明
L_e	'08'

表 7-25 Debit For Purchase/Cash Withdraw 命令报文

7.7.3 命令报文数据域

说明	长度（字节）
终端交易序号	4
交易日期（终端）	4

交易时间（终端）	3
MAC1	4

表 7-26 Debit For Purchase/Cash Withdraw 命令报文数据域

MAC1 计算如下：

1) 生成 8 字节过程密钥 SK：由 Debit For Purchase/Cash Withdraw 命令指定下的密钥对下表的数据加密生成 8 字节过程密钥 SK。

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

2) 生成 MAC1：采用步骤 1 中的过程密钥 SK 对下表的数据按照 4.3.4MAC 中的 MAC 计算方法生成 MAC1。

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

7.7.4 响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

表 7-27 Debit For Purchase/Cash Withdraw 响应报文数据域

TAC 的计算如下：

TAC 由内部密钥 DTK 左右 8 字节异或运算的结果对下表的数据按 MAC 计算方法生成的。

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

MAC2 的计算如下：

MAC2 由卡中过程密钥 SK 对（4 字节交易金额）按 MAC 计算方法生成的。

7.7.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

Debit For Purchase/Cash Withdraw错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误

‘69’	‘01’	命令不接受（无效状态）
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘02’	MAC 无效
‘93’	‘03’	应用被永久锁定
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确

表 7-28 Debit For Purchase/Cash Withdraw 响应报文状态码

7.7.6 消费交易流程

消费交易可以脱机进行，取现交易必须联机进行，且只有电子存折上具有取现交易。
下图为消费脱机交易流程。

序号	**IC 卡**	方向	**终端**	方向	**PSAM 卡**
1	设置当前应用标识	←	选择银行应用		
2	并送出应用序列号	→	接收应用序列号并保存	→	主机保留该卡片应用序列号
3	卡片产生过程密钥 SK。	←	发送消费初始化命令 Initialize For Purchase		
4	将原余额、联机交易序号、透支限额、密钥版本号、算法标识、4 字节伪随机数送卡外	→	将收到的有关数据作为 MAC1 计算命令的 DATA 域，送 MAC1 计算命令给 PSAM 卡	→	PSAM 卡按指定的密钥版本号，使用相应的消费主密钥对应用序列号分散得到消费子密钥。按卡片相同方法产生相同的过程密钥 SK，并计算产生 MAC1。
5	IC 卡用过程密钥 SK 验证 MAC1 的正确性，若验证通过，则将从余额上扣除消费的金额，将卡片脱机交易序号加 1，更新交易明细记录。 用 SK 对相应数据计算得到 4 字节的 MAC2；用内部密钥左右 8 字节异运算的结果对相应数据计算得到 4 字节的 TAC 码。	←	终端将终端号、交易日期和时间以及 MAC1，将其作为消费命令的 DATA 域，发送消费命令 Debit For Purchase 给 IC 卡	←	将 MAC1 回送给终端。
6	将 MAC2 和 TAC 码回送给终端。	→	终端接收到 TAC 码，确认交易成功，并将 MAC2 送 PSAM 卡校验。		如果 MAC2 校验成功，则终端应记录该笔交易并发送确认信息给终端，否则，PSAM 卡应用错误计数器减 1，当计数器值为 0 时，PSAM 卡将

					锁死。

图 **错误！未找到引用源。**-3 消费交易流程

7.8 Initialize For Update修改透支限额初始化

7.8.1 定义和范围

Initialize For Update命令用于初始化修改透支限额交易。

7.8.2 命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘04’
P2	‘01’（用于电子存折 ED，只有电子存折支持修改透支限额交易）
L_c	‘07’
Data	见说明
L_e	‘13’

表 7-29 Initialize For Update 命令报文

7.8.3 命令报文数据域

说明	长度（字节）
密钥索引号（修改透支限额密钥）	1
终端机编号	6

表 7-30 Initialize For Update 命令报文数据域

7.8.4 响应报文数据域

说明	长度（字节）
ED 余额	4
ED 联机交易序号	2
旧透支限额	3
密钥版本号（DUK）	1
算法标识（DUK）	1
伪随机数（IC 卡）	4
MAC1	4

表 7-31 Initialize For Update 响应报文数据域

MAC1 计算如下：

1) 生成 8 字节过程密钥 SK：由 Initialize For Update 命令指定下的密钥对下表的数据加密生成 8

字节过程密钥 SK。

数据	长度（字节）
伪随机数	4
电子存折联机交易序号	2
‘8000’	2

2) 生成 MAC1：采用步骤 1 中的过程密钥 SK 对下表的数据按照 4.3.4MAC 中的 MAC 计算方法生成 MAC1。

WOAI	长度（字节）
电子存折余额	4
旧透支限额	3
交易类型标识（参考附录 3）	1
终端机编号	6

7.8.5 响应报文的状态码

此命令执行成功的状态码是’9000’。

错误状态

SW1	SW2	说明
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘6A’	‘86’	P1、P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘03’	密钥索引不支持

表 7-32 Initialize For Update 响应报文状态码

7.9 Update Overdraw Limit修改透支限额

7.9.1 定义和范围

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

- 当电子存折中的实际金额不足时，“透支”功能为持卡人提供了一种在发卡方所允许的透支额度内继续进行交易的方便性。
- 修改透支限额交易必须在金融终端上联机进行。
- 只有电子存折应用支持修改透支限额交易。

7.9.2 命令报文

代码	值
CLA	‘80’

INS	‘58’
P1	‘00’
P2	‘00’
L_C	‘0E’
Data	见说明
L_e	‘04’

表 7-33 Update Overdraw Limit 命令报文

7.9.3 命令报文数据域

说明	长度（字节）
新透支限额	3
交易日期（发卡方）	4
交易时间（发卡方）	3
MAC2	4

表 7-34 Update Overdraw Limit 命令报文数据域

MAC2 的计算如下：

采用 Initialize For Update 修改透支限额初始化时生成的过程密钥 SK 对下表达数据按 MAC 计算方法生成的。

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

7.9.4 响应报文数据域

说明	长度（字节）
交易验证码 TAC	4

表 7-35 Update Overdraw Limit 响应报文数据域

TAC 的计算如下：

TAC 由内部密钥 DTK 左右 8 字节异或运算的结果对下表的数据按 MAC 计算方法生成的。

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

7.9.5 响应报文的状态码

此命令执行成功的状态码是'9000'。
错误状态

SW1	SW2	说明
'65'	'81'	内存错误
'67'	'00'	长度错误
'69'	'00'	不能处理
'69'	'01'	命令不接受（无效状态）
'69'	'85'	使用条件不满足
'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误
'93'	'02'	MAC 无效

表 7-36 Update Overdraw Limit 响应报文状态码

注：完成圈存后，UranusPay ED/EP 将作如下操作：

- 将当前电子存折透支限额置为新的电子存折余额；
- 将电子存折联机交易序号加 1；
- 用数据组成一个记录，保存在电子存折所指定记录长度为 23 个字节的交易明细文件中。交易明细文件由哪些数据组成具体请参考章节 3 各应用的文件结构。

7.9.6 修改透支限额交易流程

序号	IC 卡	方向	终端	方向	主机
1	设置当前应用标识	←	选择银行应用		
2	并送出应用序列号	→	将应用序列号送主机	→	主机保留该卡片应用序列号
3	卡片产生过程密钥 SK,并利用 SK 计算得到 MAC1	←	发送圈存初始化命令 Initialize For Update		主机按终端指定的密钥标识，使用相应的修改透支限额主密钥对应用序列号分散得到修改透支限额子密钥。
4	将原透支限额、联机交易序号、密钥版本号、算法标识、4 字节伪随机数和 MAC1 送卡外	→	将收到的所有响应数据传送给银行主机	→	按卡片相同方法产生相同的过程密钥 SK，校验 MAC1 的正确性
5	IC 卡用过程密钥 SK 验证 MAC2 的正确性，若验证通过，则更新透支限额，卡片联机交易序号加 1。更新交易明细记录。并用内部密钥左右 8 字节异或对电子存折余额、联机交易序号、电子存折新透支限额、交易类型标识、终	←	终端接收主机交易日期和时间以及 MAC2，将其作为修改透支限额命令的 DATA 域，发送修改透支限额命令 Update Overdraw Limit 给 IC 卡。	←	如果 MAC1 校验正确，则主机联机交易序号加 1，并用 SK 对新透支限额、交易类型标识、终端号、交易日期和时间进行 MAC 计算得到 MAC2，送至终端，否则，交易终止。

	端机编号、主机交易日期和时间进行 TAC 计算，产生 4 字节的 TAC 码。				
6	将 TAC 码回送给终端。	⟶	终端接收到 TAC 码，确认交易成功。		

图 **错误！未找到引用源。**-4 修改透支限额交易流程

7.10 Get Balance读余额

7.10.1 定义和范围

Get Balance命令用于读取电子存折或电子钱包余额，实现查询余额交易。
读取电子存折余额需验证个人密码（PIN）。

7.10.2 命令报文

代码	值
CLA	‘80’
INS	‘5C’
P1	‘00’
P2	‘01’用于 ED ‘02’用于 EP 其他值保留
L_C	不存在
Data	不存在
L_e	‘04’

表 7-37 Get Balance 命令报文

7.10.3 命令报文数据域

无

7.10.4 响应报文数据域

说明	长度（字节）
ED 余额或 EP 余额	4

表 7-38 Get Balance 响应报文数据域

7.10.5 响应报文的状态码

此命令执行成功的状态码是'9000'。

Get Balance错误状态

SW1	SW2	说明
'65'	'81'	内存错误
'69'	'85'	使用条件不满足
'69'	'82'	安全条件不满足
'6A'	'86'	P1、P2 参数不正确
'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误
'6A'	'81'	功能不被支持
'93'	'03'	应用被永久锁定

表 7-39 Get Balance 响应报文状态码

7.11 Get Transaction Proof取交易认证

7.11.1 定义和范围

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

7.11.2 命令报文

代码	值
CLA	'80'
INS	'5A'
P1	'00'
P2	要取的 MAC 或/和 TAC 所对应的交易类型标识。
Lc	'02'
Data	见说明
Le	'08'

表 7-40 Get Transaction Proof 命令报文

7.11.3 命令报文数据域

说明	长度（字节）
要取的 MAC 或/和 TAC 所对应的 ED/EP 联机或脱机交易序号	2

表 7-41 Get Transaction Proof 命令报文数据域

7.11.4响应报文数据域

如果命令中指定的交易类型标识和ED/EP联机或脱机交易序号对应的MAC或TAC可用，则响应报文数据域见表

说明	长度
MAC	4
交易验证码 TAC	4

表 7-42 Get Transaction Proof 响应报文数据域

7.11.5响应报文的状态码

此命令执行成功的状态码是’9000’。
错误状态

SW1	SW2	含义
‘65’	‘81’	内存错误(社保应用不存在此项)
‘69’	‘85’	使用条件不满足
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘94’	‘06’	所需 MAC 不可用
‘67’	‘00’	Le 长度错
‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1、P2 不正确
‘93’	‘03’	应用被永久锁定

表 7-43 Get Transaction Proof 响应报文状态码

7.12Reload PIN重装个人密码

7.12.1定义和范围

Reload PIN 命令用于发卡方重新给持卡人产生一个新的PIN（可以与原PIN相同）。
Reload PIN只能在拥有或能访问到重装PIN子密钥（DRPK）的发卡方终端（例如发卡方银行终端）上执行。
在成功执行Reload PIN命令后，IC卡必须完成以下操作：
———PIN错误尝试计数器复位。
———IC卡的原PIN必须设置为新的PIN值。
命令中的PIN数据以明文传送。
Reload PIN 命令连续执行三次失败后，应用将永久锁定。

7.12.2命令报文

代码	值

CLA	‘80’
INS	‘5E’
P1	‘00’
P2	‘00’
L_c	‘06’ ～ ‘0A’
Data	见说明
L_e	不存在

表 7-44 Reload PIN 命令报文

注：在重装口令密钥命令报文中并不能指定口令密钥的密钥标识符，系统将自动对密钥文件标识为 00 的口令密钥进行重装。

7.12.3命令报文数据域

说明	长度（字节）
重装的 PIN 值	2-6
MAC	4

表 7-45 Reload PIN 命令报文数据域

用DRPK左右8位字节进行异或运算后的结果与新PIN值计算MAC。

7.12.4响应报文数据域

响应报文的数据域不存在。

7.12.5响应报文的状态码

此命令执行成功的状态码是’9000’。

错误状态

SW1	SW2	含义
‘65’	‘81’	内存错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘69’	‘88’	安全信息数据对象不正确
‘6A’	‘86’	P1、P2 参数不正确
‘6A’	‘88’	引用数据找不到
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用永久锁住

表 7-46 Reload PIN 响应报文状态码

7.13PIN Unblock 解锁个人密码

7.13.1定义和范围

PIN Unblock 命令为发卡方提供了解锁个人密码的功能。
当 PIN Unblock 命令成功完成后，卡将重置个人密码尝试计数器的值；
命令中个人密码的传递采用加密方式。

7.13.2命令报文

代码	值
CLA	‘84’
INS	‘24’
P1	‘00’
P2	‘01’：表示解锁个人密码。此时应重置尝试计数器，但不更改个人密码。数据域中的 PIN 为旧 PIN。
Lc	‘0C’
Data	加密的个人密码数据元和报文认证码(MAC)数据元；
Le	不存在

表 7-47 PIN Unblock 命令报文

7.13.3命令报文数据域

命令报文数据域中个人密码数据元(如果存在)和其后的 MAC 数据元组成。

7.13.4响应报文数据域

响应报文数据域不存在。

7.13.5响应报文状态码

IC 卡可能回送的错误状态码如下表所示：

SW1	SW2	含　　义
‘65’	‘81’	内存失败
‘67’	‘00’	Lc 不正确
‘69’	‘82’	不满足安全状态
‘69’	‘84’	引用数据无效
‘69’	‘85’	使用条件不满足（PIN 未锁定）
‘69’	‘88’	安全报文数据项不正确

‘6A’	‘81’	功能不被支持
‘6A’	‘86’	参数 P1 P2 不正确
‘6A’	‘88’	未找到引用数据
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误
‘93’	‘03’	应用被永久锁定

表 7-48 Reload PIN 响应报文状态码

7.14Application Block 应用锁定

7.14.1定义和范围

Application Block 命令使当前选择的应用失效。

当 Application Block 命令成功地完成应用临时锁定后，用 Select 命令选择已临时锁定的应用，将回送状态码“不支持此功能”(SW1 SW2=’6A81’)。同时回送 FCI（对于 T=0 卡片，需要用 GET RESPONSE 指令取回）。

当 Application Block 命令成功完成应用永久锁定后，此后执行所有命令，卡片将回送状态码“应用永久锁定”（SW1 SW2 = ‘9303’）。

7.14.2命令报文

代码	值
CLA	‘84’
INS	‘1E’
P1	‘00’，其他值保留为将来使用
P2	‘00’或’01’，社保应用为‘00’
Lc	数据字节数，社保应用为‘04’
Data	报文认证码(MAC)数据元
Le	不存在

表 7-49 Application Block 命令报文

P2=’00’：此命令执行成功后可锁定应用，但该应用可以用 APPLICATION UNBLOCK 命令解锁。

P2=’01’：此命令执行成功后将永久锁定应用。

7.14.3命令报文数据域

命令报文数据域的内容为报文认证码(MAC)数据元。

7.14.4响应报文数据域

响应报文数据域不存在。

7.14.5 响应报文状态码

无论应用是否已经失效，此命令执行成功的状态码是'9000'。
IC 卡可能回送的状态码如下表所示：

SW1	SW2	含　义
'65'	'81'	内存失败
'67'	'00'	Lc 长度错误
'69'	'82'	不满足安全状态
'69'	'84'	引用数据无效
'69'	'85'	使用条件不满足
'69'	'88'	安全报文数据项不正确
'6A'	'86'	参数 P1 P2 不正确
'6A'	'88'	未找到引用数据
'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误

表 7-50 Application Block 响应报文状态码

7.15 Application Unblock 应用解锁

7.15.1 定义和范围

Application Unblock 命令用于恢复当前应用。
当 Application Unblock 命令成功地完成后，由 Application Block 命令产生的对应用命令响应的限制将被取消。

7.15.2 命令报文

代码	值
CLA	'84'
INS	'18'
P1	'00'，其他值保留为将来使用
P2	'00'，其他值保留为将来使用
Lc	数据字节数
Data	报文认证码(MAC)数据元；
Le	不存在

表 7-51 Application Unblock 命令报文

7.15.3 命令报文数据域

命令报文数据域的内容为报文认证码(MAC)数据元。

7.15.4响应报文数据域

响应报文数据域不存在。

7.15.5响应报文状态码

当应用被临时锁定时，此命令执行成功的状态码是'9000'。
当应用未被临时锁定，此命令执行返回的状态码是使用条件不满足（SW1 SW2 = '6985'）。
IC 卡可能回送的状态码如下表所示:

SW1	SW2	含　义
'65'	'81'	内存失败
'67'	'00'	Lc 错误
'69'	'82'	不满足安全状态
'69'	'84'	未取随机数
'69'	'85'	使用条件不满足
'69'	'88'	安全报文数据项不正确
'6A'	'82'	文件未找到
'6A'	'86'	P1，P2 错误
'6D'	'00'	INS 不支持或错误
'6E'	'00'	CLA 不支持或错误
'93'	'03'	应用已被永久锁定

表 7-52 Application Unblock 响应报文状态码

7.16Card Block

7.16.1定义与范围

代码	值
CLA	84
INS	16
P1	00
P2	00
L_c	04(MAC 码长度)
Data	MAC
L_e	不存在

表 7-53 Card Block 命令报文

7.16.2命令报文数据域

包括报文鉴别代码（MAC）数据元。
用密钥标识为 00 的 16 字节维护密钥计算 MAC，方法见 4.3.4 MAC

7.16.3响应报文数据域

无

7.16.4响应报文状态码

SW1	SW2	说明
90	00	执行成功
65	81	内存错误
6A	88	未找到引用数据
67	00	Lc 长度错误
69	82	不满足安全状态
69	84	引用数据无效
69	85	使用条件不满足
69	88	安全报文数据项不正确
6A	86	参数 P1、P2 错误

表 7-54 Card Block 响应报文状态码

7.17Change PIN修改个人密码

7.17.1定义和范围

Change PIN允许持卡人将当前个人密码修改为新的密码。
当Change PIN命令成功完成后，卡片要进行以下操作：
— 密码尝试计数器复位至密码尝试次数的上限；
— 将原个人密码置为新的个人密码。

7.17.2注意事项

此命令中的个人密码（PIN）值以明文方式传送。命令数据中个人密码（PIN）是以 ’cn’格式存放的，它不需要整字节的填充，只有最低有效字节的低半字节可能需要填充，且填以’F’。

7.17.3命令报文

代码	值
CLA	‘80’
INS	‘5E’
P1	‘01’
P2	‘00’
L_c	‘05’ - ‘0D’；

Data	当前 PIN ‖ ‘FF’ ‖ 新的 PIN
L_e	不用

表 7-55 Change PIN 命令报文

7.17.4命令报文数据域

当前 PIN ‖ ‘FF’ ‖ 新的 PIN

7.17.5响应报文数据域

响应报文的数据域不存在。

7.17.6响应报文的状态码

IC 卡可能回送的警告状态码如下表所示：

SW1	SW2	含　义
‘63’	‘Cx’	鉴别失败，‘x’表示允许继续尝试的次数（‘0’-‘F’）

此命令执行成功的状态码是’9000’。

Change PIN错误状态

SW1	SW2	含义
‘65’	‘81’	内存错误
‘67’	‘00’	Lc 不正确
‘69’	‘83’	验证方法锁定
‘69’	‘85’	使用条件不满足
‘6A’	‘80’	数据域参数不正确
‘6A’	‘86’	P1、P2 参数不正确
‘6D’	‘00’	INS 不支持或错误
‘6E’	‘00’	CLA 不支持或错误

表 7-56 Change PIN 响应报文状态码

7.18Get Message取安全认证码

7.18.1定义和范围

Get Message 命令为建设部应用专用，用于获取建设部专用安全认证码。

7.18.2注意事项

- 如果该命令执行成功，在建设部应用下消费 MAC1 计算将采用建设部 MAC1 计算方法。

7.18.3命令报文

代码	值
CLA	‘80’
INS	‘CA’
P1	‘00’
P2	‘00’
L_c	‘00’
Data	安全认证码
L_e	‘09’

表 7-57 Get Message 命令报文

7.18.4命令报文数据域

无

7.18.5响应报文数据域

9 字节安全认证码

7.18.6响应报文的状态码

错误状态

SW1	SW2	说明
‘90’	‘00’	状态标志位未改变
‘6A’	‘86’	参数错误
‘67’	‘00’	长度错误

表 7-58 Get Message 响应报文状态码

7.19Initialize For Capp Purchase复合消费初始化

7.19.1定义和范围

复合消费初始化，在完成本初始化后方能进行复合交易。

7.19.2命令报文

代码	值
CLA	‘80’
INS	‘50’
P1	‘03’
P2	‘02’
L_c	‘0B’
Data	见下表
L_e	‘0F’

表 7-59 Initialize For Capp Purchase 命令报文

7.19.3命令报文数据域

说明	长度（字节）
密钥索引	1
交易金额	4
终端机编号	6

表 7-60 Initialize For Capp Purchase 命令报文数据域

7.19.4响应报文数据域

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

表 7-61 Initialize For Capp Purchase 响应报文数据域

7.19.5响应报文的状态码

成功执行返回代码为“9000”
错误状态

SW1	SW2	说明
‘61’	‘xx’	命令执行成功，有 xx 数据返回
‘6A’	‘86’	参数错误
‘67’	‘00’	长度错误
‘69’	‘85’	使用条件不满足
‘94’	‘01’	金额不足
‘94’	‘03’	密钥索引不支持
‘94’	‘08’	已灰锁（仅 ETC 应用与建设部应用返回此状态码）

表 7-62 Initialize For Capp Purchase 响应报文状态码

7.20Debit For Capp Purchase复合消费

7.20.1定义和范围

复合应用消费交易允许持卡人使用电子钱包的余额进行购物或获取服务。此交易可以在终端设备或其它读卡设备上脱机进行。此交易无需提交个人密码（PIN）。

复合应用消费交易允许消费金额为 0。

Debit For Capp Purchase 命令用于复合应用消费交易。

7.20.2注意事项

本指令执行前必须成功执行 Update Capp Data Cache

7.20.3命令报文

代码	值
CLA	‘80’
INS	‘54’
P1	‘01’
P2	‘00’
L_c	‘0F’
Data	见数据域说明
L_e	8

表 7-63 Debit For Capp Purchase 命令报文

7.20.4命令报文数据域

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

表 7-64 Debit For Capp Purchase 命令报文数据域

MAC1 计算如下：

1) 生成 8 字节过程密钥 SESPK：由 DPK 密钥对下表的数据加密生成 8 字节过程密钥 SESPK。

数据	长度（字节）
伪随机数	4
电子钱包交易序号	2
终端交易序号	2（终端交易序号最右的 2 个字节）

2) 生成 MAC1：采用步骤 1 中的过程密钥 SESPK 对下表的数据按照 4.3.4MAC 中的 MAC 计算方法生成 MAC1。

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

7.20.5 响应报文数据域

说明	长度（字节）
交易验证码 TAC	4
MAC2	4

表 7-65 Debit For Capp Purchase 响应报文数据域

TAC 的计算如下：

采用密钥 DTK 产生 TAC。TAC 将被写入终端交易明细，以便于主机进行交易验证。下面是用来生成 TAC 的数据，它们以明文形式通过 Debit For Capp Purchase 命令的响应报文从 IC 卡传送到终端：

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

MAC2 的计算如下：

采用 Initialize For Capp Purchase 复合消费初始化生成的 SESPK 对以下数据进行加密产生 MAC2：

数据	长度（字节）
交易金额	4

7.20.6 响应报文的状态码

此命令可能返回的状态吗如下

SW1	SW2	说明
‘61’	‘08’	命令执行成功
‘6A’	‘86’	参数错误
‘93’	‘02’	MAC 错
‘69’	‘01’	执行条件不满足
‘6A’	‘83’	指定交易记录不存在
‘6A’	‘82’	文件未找到
‘94’	‘03’	密钥没有找到

表 7-66Debit For Capp Purchase 响应报文状态码

注：完成复合消费交易后，UranusPay DI 将作如下操作：

- IC 卡从电子钱包余额中扣减消费的金额
- 电子钱包交易序号加 1
- 更新复合应用专用文件
- 用数据组成一个记录，保存在电子钱包所指定记录长度为 23 个字节的交易明细文件中。交易明细文件由哪些数据组成具体请参考章节 3 各应用的文件结构。

7.20.7复合消费交易流程

消费交易可以脱机进行，取现交易必须联机进行，且只有电子存折上具有取现交易。
下图为复合消费脱机交易流程。

序号	**IC 卡**	方向	**终端**	方向	**PSAM 卡**
1	设置当前应用标识	←	选择银行应用		
2	并送出应用序列号	→	接收应用序列号并保存	→	主机保留该卡片应用序列号
3	卡片产生过程密钥 SESPK。	←	发送复合消费初始化命令 Initialize For Capp Purchase		
4	将钱包余额、电子钱包交易序号、透支限额、算法版本、密钥版本号、4 字节伪随机数送卡外	→	将收到的有关数据作为 MAC1 计算命令的 DATA 域，送 MAC1 计算命令给 PSAM 卡	→	PSAM 卡按指定的密钥版本号，使用相应的消费主密钥对应用序列号分散得到消费子密钥。按卡片相同方法产生相同的过程密钥 SESPK，并计算产生 MAC1。
	IC 卡暂存命令中的 SFI、记录号、复合应用类型标识符和数据域	←	发送复合消费缓存命令 Update Capp Data Cache		
5	IC 卡用过程密钥 SESPK 验证 MAC1 的正确性，若验证通过，则将从余额上扣除复合消费的金额，将卡片脱机交易序号加 1，更新交易明细记录。 用 SESPK 对相应数据计算得到 4 字节的 MAC2；用内部密钥左右 8 字节异运算的结果对相应数据计算得到 4 字节的 TAC 码。	←	终端将终端号、交易日期和时间以及 MAC1，将其作为消费命令的 DATA 域，发送消费命令 Debit For Capp Purchase 给 IC 卡	←	将 MAC1 回送给终端。
6	将 MAC2 和 TAC 码回送给终端。	→	终端接收到 TAC 码，确认交易成功，并将 MAC2 送 PSAM 卡校验。	→	如果 MAC2 校验成功，则终端应记录该笔交易并发送确认信息给终端，否则，PSAM 卡应用错误计数器减 1，当计数器值

					为 0 时，PSAM 卡将锁死。

图 7-5 消费交易流程

注：在建设部应用下，在消费过程中需获取建设部专用安全认证码，可通过终端发送 Get Message 获得。

7.21Update Capp Data Cach复合消费缓存

7.21.1定义和范围

Update Capp Data Cache 命令用于复合应用消费交易中更新复合应用数据缓存，缓存数据将被 Debit For Capp Purchase 命令用于改写复合应用专用文件中相关记录。

7.21.2注意事项

- 本指令执行前必须成功进行 Initialize For Capp Purchase 复合交易初始化，同时本指令也是执行复合交易的前提；

7.21.3命令报文

代码	值
CLA	‘80’
INS	‘DC’
P1	‘复合应用类型标识’
P2	‘见说明’
L_c	‘xx’ 后续数据域的长度
Data	由更新原有记录的新记录组成
L_e	无

表 7-67 Update Capp Data Cache 命令报文

P2 参数说明

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

7.21.4命令报文数据域

此命令报文数据域由更新原有记录的新记录组成。

7.21.5响应报文数据域

响应报文数据域不存在

7.21.6响应报文的状态码

此命令可能返回的状态吗如下

SW1	SW2	说明
‘90’	‘00’	命令执行成功
‘6A’	‘86’	参数错误
‘67’	‘00’	长度错误
‘69’	‘01’	未进行初始化
‘6A’	‘83’	指定交易记录不存在
‘94’	‘07’	应用锁定
‘6A’	‘84’	长度超限

表 7-68 Update Capp Data Cache 响应报文数据域

8 命令执行成功后的卡片交易状态变化

以下是金融交易命令执行成功后的卡片交易状态变化的总表，各种不同的应用下不完全适用。需要注意：某应用下不支持的交易指令仍然会将交易状态变为空闲状态。

状态 命令	空闲	圈存	消费/取现	圈提	修改
Credit For Load	N/A	空闲	N/A	N/A	N/A
Debit For Purchase/ Cash Withdraw	N/A	N/A	空闲	N/A	N/A
Debit For Unload	N/A	N/A	N/A	空闲	N/A
Get Balance	空闲	圈存	消费/取现	圈提	修改
Get Lock Proof	空闲	圈存	消费/取现	圈提	修改
Get Transaction Prove	空闲	圈存	消费/取现	圈提	修改
Initialize For Load	圈存	圈存	圈存	圈存	圈存
Initialize For Purchase	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现
Initialize For Withdraw	消费/取现	消费/取现	消费/取现	消费/取现	消费/取现
Initialize For Unload	圈提	圈提	圈提	圈提	圈提
Initialize For Update	修改	修改	修改	修改	修改
Update Overdraw Limit	N/A	N/A	N/A	N/A	空闲

表 8-1 命令执行成功后的状态变化

附录 1：接触式接口复位应答ATR

在复位之后，UranusPay ED/EP 卡片接触式接口默认使用 T=0 协议，返回的 ATR 信息定义如下：

字符	内容	解释
TS	3B	正向约定
T0	9F	TA1 和 TD1 存在，历史字符为 15 个
TA1	11	通讯速率，默认 9600bps
TD1	80	T＝0 通信协议，存在 TD2
TD2	1F	全局接口字节，存在 TA3
TA3	C3	时钟停止支持（无论高低电平），支持 3/5V
T1-T15	XX..XX	历史字符定义（参考下表）
TCK	XX	校验字符

表 附录 1-1 T=0 协议返回的 ATR

历史字符定义如下：

字符	内容	解释
T1	80	历史字节，符合 7816-4 格式
T2	65	卡片数据服务 TAG
T3	XX	芯片参考
T4	XX	COS 版本（高 4 位：主版本；低 4 位：次版本）
T5	XX	应用版本
T6	86	发行商代码 1
T7	53	发行商代码 2
T8	73	卡片能力 TAG
T9	B6	卡片能力
T10	21	数据编码字节
T11	00	一个逻辑通道
T12	83	3 字节状态信息
T13	XX	卡状态信息（生命周期字节 CLCB）
T14	XX	卡片支持的应用
T15	XX	卡片当前的安全模式： 0 位模式； 1 ：区间模式

表 附录 1-2 历史字符定义

例如：3B 9F 00 80 1F C3 ….

UranusPay ED/EP 卡片选择 T＝1 协议时，返回的 ATR 信息定义如下。

字符	内容	解释
TS	3B	正向约定
T0	9F	TA1 和 TD1 存在，历史字符为 15 个
TA1	11	通讯速率，默认 9600bps
TD1	81	T＝1 通信协议，存在 TD2
TD2	31	全局接口字节，存在 TA3 和 TB3，使用 T=1 协议
TA3	FE	返回 IFSI，表示 IC 卡信息域大小的初始值且具有 16～254 字节的 IFSC
TB3	45	BWI=4；CWI=5

T1-T15	XX..XX	历史字符定义（同上表历史字符描述）
TCK	XX	校验字符

表 附录 1-3 T=1 协议，返回的 ATR

附录 2：非接触式接口选择应答ATS

ATS 由 PICC（非接触卡）按 T=CL 协议返回，完全符合 ISO14443 规范，各字节的值如下：

字符	内容	解释
TL	14	长度字节，表示 ATS（不包括 CRC）共有 20 个字节
T0	78	表示 TA1，TB1，TC1 存在，卡片接收缓冲区最大值 FSCI＝256 字节
TA1	91	卡片通信速率默认为‘91’（212kbps）。
TB1	D0	帧等待时间（FWT）＝0D（命令最多等 2.4S），帧保护时间 SFGI＝0
TC1	02	支持 CID，不支持 NAD
T1-T15	XX..XX	历史字符定义（同接触式卡片 ATR）
CRC1-CRC2	XXXX	校验字符

表 附录 2-1 T=CL 协议，返回的 ATS

附录 3：交易类型标识TTI

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

表 附录 3-0-1 交易类型标识 TTI