



山东华翼 PBOC ED/EP COS 用户手册

日期：2010-11-16

版本：1.2

山东华翼微电子技术有限责任公司 系统应用部



1 前言

1.1 声明

本手册详细说明了使用嵌入了 HYCOS/PBOC 2.0 的智能卡开发应用所必需的资料以及 HYCOS/PBOC 2.0 的命令。

嵌入 HYCOS/PBOC 2.0 智能卡操作系统的智能卡是为达到最佳的性能价格比而对硬件和软件功能进行过优化的通用微处理器卡。在单片集成电路中所使用的 CMOS 技术保证了超大规模的集成度和低功耗，增强了卡片本身的可靠性。这种智能卡符合 ISO 14443-1,2,3,4、ISO7816 标准，可以在支持这些标准的终端设备上使用。

本手册由山东华翼微电子技术有限责任公司编制和发行。未经山东华翼微电子技术有限责任公司的书面许可，本手册的任何部分不得以任何形式或手段复制或传播。

本手册适用于 HYM4616 32K 卡片。

1.2 内容

系统介绍

- ✧ 系统特性。
- ✧ 系统文件结构组织。
- ✧ 通讯选择。
- ✧ 复位应答。

指令描述

- ✧ 基本指令。
- ✧ 专有指令。
- ✧ 发卡指令。

应用流程

- ✧ 包括卡片个人化流程。
- ✧ 包括 PBOC ED/EP 交易流程。



✎ 安全特性

- ✧ 安全状态。
- ✧ 权限设置。
- ✧ 数据传输模式。
- ✧ 加密算法。

1.3 定义

✎ 复位应答文件 Answer-to Reset file

表示卡操作特性的基本文件。

✎ 命令响应对 Command-response pair

两种报文的集合:命令后面紧跟着响应。

✎ 数据单元 data unit

可以无二义性地被引用的最少位集合。

✎ 数据元 data element

在接口处所看到的信息, 为它定义了名称、逻辑内容描述、格式和编码。

✎ 数据对象 data object

在接口处所看到的信息, 它由标签、长度和值(即, 数据元)组成。在本部分规范中, 数据对象称之为 BER—TLV、压缩 TLV 和简单 TLV 数据单元。

✎ 专用文件 dedicated file

包含文件控制信息和任选地供分配用的存储器的文件。它可以是 EFs 和/或 DFs 的父辈。

✎ DF 名称 DF name

唯一地标识了卡内专用文件的字节串。

✎ 目录文件 directory file

ISO/IEC7816 第 5 部分定义的基本文件。

✎ 基本文件 elementary file

共享同一文件标识符的数据单元或记录的集合。它不可能是另一文件的父辈。

✎ 文件控制参数 file control parameters

文件的逻辑、结构和安全的属性。



✎ 文件标识符 file identifier

用来寻址文件的 2 字节二进制值。

✎ 文件管理数据 file management data

除文件控制参数(例如, 有效日期, 应用标号)外, 关于文件的任何信息。

✎ 内部基本文件 internal elementary file

用来存储由卡所解释数据的基本文件。

✎ 主文件 master file

表示文件结构根的强制性唯一专用文件。

✎ 报文 message

由接口设备向卡所发送的字节串, 反之亦然, 但不包括在 ISO/IEC7816 第 3 部分定义的面向传输的字符。

✎ 父辈文件 parent file

在分级结构范围内, 直接在某一给定文件之前的专用文件。

✎ 口令 password

应用可以要求的数据, 通过其用户将它呈现给卡。

✎ 路径 path

文件标识符的并置, 而无需定界。如果路径以主文件的标识符开始, 则它是一条绝对的路径。

✎ 提供者 provider

具有或曾获得在卡内建立专用文件权利的管理机构。

✎ 记录 record

可以由卡处理为一整体的并且可由记录号或记录标识符所引用的字节串。

✎ 记录标识符 record identifier

与记录相关的值, 可用来引用那个记录。在一个基本文件内几个记录可以具有的相同标识符。

✎ 记录号 record number

分配给每个记录的顺序号, 它唯一地标识其基本文件内的记录。

✎ 工作的基本文件 working elementary file

用来存储不由卡所解释数据的基本文件。

✎ 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。

✎ 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。

✎ SSF33 算法

SSF33 算法采用国家密码管理部门批准的分组密码算法（简称BCEA），其分组长度和密钥长度均为128 比特。

✎ 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。

✎ 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。

✎ 传输密钥 TK（Transmit Key）

MF 或 DF 注册后会把控制权限交给 TK 来控制。

✎ 主控密钥 MK（Main Key）





KEY 文件追加的第一条密钥；其追加受 TK 的控制，然后 TK 失去作用；MK 成为追加 KEY 文件其它密钥的控制密钥。

1.4 缩略语

以下缩略语和符号表示适用于本手册。

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)
ASN	抽象语法表示(Abstract Syntax Notation)
ATR	复位应答(Answer to Reset)
b	二进制(Binary)
BER	基本编码规则(Basic Encoding Rules)
C-APDU	命令 APDU(Command APDU)
CCYYMMDD	年、月、日(Year, Month, Day)
C _{IN}	输入电容(Input Capacitance)
C _{OUT}	输出电容(Output Capacitance)
CLA	命令报文的类别字节(Class Byte of the Command Message)
CLK	时钟(Clock)
cn	压缩数字(Compressed Numeric)
C-TPDU	命令 TPDU(Command TPDU)
CWI	字符等待时间整数(Character Waiting Time Integer)
CWT	字符等待时间(Character Waiting Time)
DDF	目录定义文件(Directory Definition File)
DEA	数据密码算法 (Data Encryption Algorithm)
DF	专用文件(Dedicated File)
DIR	目录(Directory)



EF	基本文件(Elementary File)
etu	基本时间单元(Elementary Time Unit)
FCI	文件控制信息(File Control Information)
f	频率(Frequency)
GND	地(Ground)
hex	十六进制数(Hexadecimal)
HHMM	时、分(Hours, Minutes)
HHMMSS	时、分、秒(Hours, Minutes, Seconds)
IC	集成电路(Integrated Circuit)
ICC	集成电路卡(Integrated Circuit Card)
I _{CC}	VCC 上的电流(Current at VCC)
IEC	国际电工委员会(International Electrotechnical Commission)
IFD	接口设备(Interface Device)
I _{IH}	高电平输入电流(High Level Input Current)
I _{IL}	低电平输入电流(Low Level Input Current)
INS	命令报文的指令字节(Instruction Byte of Command Message)
I/O	输入/输出(Input/Output)
I _{OH}	高电平输出电流(High Level Output Current)
I _{OL}	低电平输出电流(Low Level Output Current)
ISO	国际标准化组织(International Organization for Standardization)
K _M	主控密钥(Master Key)
KS	过程密钥(Session Key)
Lc	终端发出的命令数据的实际长度(Exact Length of Data Sent by the TAL in a Case 3 or 4 Command)
Le	响应数据的最大期望长度(Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command)
Licc	IC 卡回送的可用数据的实际长度(Exact Length of Data Available in the ICC to be Returned in Response to the Case 2 or 4 Command Received by the ICC)
LEN	长度(Length)



L _{Key}	密码算法块长度(Block Length of Cryptographic Algorithm)
L _r	响应数据域的长度(Length of Response Data Field)
M	必备型(Mandatory)
MAC	报文鉴别代码(Message Authentication Code)
MF	主控文件(Master 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)
PIX	用应用标识符扩展码(Proprietary Application Identifier Extension)
PTS	协议类型选择(Protocol Type Selection)
R-APDU	响应 APDU(Response APDU)
RFU	保留为将来使用(Reserved for Future Use)
RID Identifier)	注册的应用提供者标识 (Registered Application Provider
RST	复位(Reset)
R-TPDU	响应 TPDU(Response TPDU)
SAM	安全存取模块(Secure Access Module)
SFI	短文件标识符(Short File Identifier)
SSA	社会保障应用(Social Security Application)
SSSE	社会保障系统环境(Social Security System Environment)
SW1	状态码 1(Status Word One)
SW2	状态码 2(Status Word Two)
TAL	终端应用层(Terminal Application Layer)
t _F	信号幅度从 90%下降到 10%的时间(Fall Time Between 90% and 10% of Signal Amplitude)
TLV	标签、长度、值(Tag Length Value)
TPDU	传输协议数据单元(Transport Protocol Data Unit)



t_R	信号幅度从 10%上升到 90%的时间(Rise Time Between 10% and 90% of Signal Amplitude)
TTL	终端传输层(Terminal Transport Layer)
V _{CC}	VCC 触点上测量到的电压(Voltage Measured on VCC Contact)
VCC	电源电压(Supply Voltage)
V _{IH}	高电平输入电压(High Level Input Voltage)
V _{IL}	低电平输入电压(Low Level Input Voltage)
VOH	高电平输出电压(High Level Output Voltage)
VOL	低电平输出电压(Low Level Output Voltage)
V _{PP}	VPP 触点上测量到的编程电压(Programming Voltage Measured on VPP Contact)
VPP	编程电压(Programming Voltage)
WI	等待时间整数(Waiting Time Integer)
'0'-'9' 'A'-'F'	十六进制数字
A=B	A 等于 B
xx	任意值

2 HYCOS/PBOC 2.0 介绍

2.1 特性

山东华翼微电子技术有限责任公司研制开发并拥有版权的 HYCOS/PBOC 2.0 COS 智能卡操作系统, 控制智能卡上的微处理器, 实现数据传送、数据存储和信息处理, 并且提供必要的运算和多应用管理功能。

HYCOS/PBOC 2.0 COS 实现的功能包括:

- 多层物理文件管理;
- 多类型密钥管理;
- SINGLE DES、TRIPLE DES、国密 33 和 SM1 加密算法;
- MAC 生成;
- 数据镜像和保护;



- 高安全度的电子帐户功能；
- 随机数生成。

上述功能保证了嵌入 HYCOS/PBOC 2.0 COS 的智能卡具有以下主要特点：

- 支持一卡多用途，每个应用项目都有自己独立的管理条件；
- 支持《8—中国金融集成电路（IC）卡规范-与应用无关的非接触式规范》；
- 支持《1—中国金融集成电路（IC）卡电子钱包电子存折卡片规范》；
- 支持《2—中国金融集成电路（IC）卡电子钱包电子存折应用规范》；
- 具有多层次的文件结构，支持 ISO/IEC 7816-4 所定义的数据文件格式；
- 在通信过程中，支持多层次的保密通信；
- 每个文件都有各自的访问控制条件。

应用项目的具体数目仅受 EEPROM 容量的限制。用户可根据自定义的保密层次，创建应用文件并在这些文件中写入应用数据。应用项目设计者能够定义自己的保密措施和应用文件结构。

2.2 复位应答

当 IC 卡非接触界面上电时，HYCOS/PBOC 2.0 向卡外发送“复位应答”序列，包括如下所列的 16 个字节：

107880D002	00 9D	48 59	12 08	20	XX XX XX XX XX XX
固定标识	芯片制造 商标标识符	COS 厂商 代码	COS 名称	操作系 统版本	卡片序列号

当 IC 卡接触上电时，HYCOS/PBOC 2.0 向卡外发送“复位应答”序列，包括如下所列的 15 个字节：

3B 6D 00 00	00 9D	12	08	20	46 16	XX XX XX XX XX XX
固定标识	芯片制造 商标标识符	卡内测试 系统版本	芯片 版本	操作系 统版本	卡片制造 商标标识符	卡片序列号

说明：

- 这个序列总是以 3B 6D 00 00 打头。
- 芯片制造商标识符 = 00 9D。
- 卡内测试系统版本 = 12，表示卡内测试系统版本为 1.2。



- 芯片版本 = 08，表示芯片版本为 08H。
- 卡操作系统版本 = 20，表示卡操作系统版本为 2.0。
- 卡片制造商标识符 = 46 16。
- 卡片序列号共 6 字节

3 指令

3.1 基本指令

3.1.1 APPLICATION BLOCK

3.1.1.1 定义

该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'）。

对其他命令的影响根据不同应用而定。

3.1.1.2 命令报文

代码	值
CLA	84
INS	1E
P1	00
P2	00/01
Lc	04
Data	报文鉴别代码（MAC）数据元
Le	无

说明：

- ✧ P2=00：此命令执行成功后可临时锁定应用，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。

3.1.1.3 命令报文数据域

使用索引号为 01 的应用维护密钥来计算 MAC。

3.1.1.4 响应报文数据域

无。

3.1.1.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
63	Cx	X 指出剩余的错误计数值
69	84	引用数据无效
69	85	使用条件不满足
65	81	内存失败
93	03	应用被永久锁定
6D	00	指令不支持

3.1.2 APPLICATION UNBLOCK

3.1.2.1 定义

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。



3.1.2.2 命令报文

代码	值
CLA	84
INS	18
P1	00
P2	00
Lc	04
Data	报文鉴别代码（MAC）数据元
Le	无

3.1.2.3 命令报文数据域

使用索引号为 01 的应用维护密钥来计算 MAC。

3.1.2.4 响应报文数据域

无。

3.1.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
63	Cx	X 指出剩余的错误计数值
69	83	Key、pin 锁定
69	84	引用数据无效
69	85	使用条件不满足
93	03	应用被永久锁定
6D	00	指令不支持



3.1.3 CARD BLOCK

3.1.3.1 定义

该命令使卡中所有应用永久失效。

当该命令成功地完成后，所有后续的命令都将回送状态码“6A81”（不支持此功能），且不执行任何其它操作。

3.1.3.2 命令报文

代码	值
CLA	84
INS	16
P1	00
P2	00
Lc	04
Data	报文鉴别代码（MAC）
Le	无

3.1.3.3 命令报文数据域

使用索引号为 01 的应用维护密钥来计算 MAC；MAC 计算使用随机数。

3.1.3.4 响应报文数据域

无。

3.1.3.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
69	88	安全报文数据项不正确
69	84	引用数据无效



69	85	使用条件不满足
65	81	内存失败
69	83	Key、pin 锁定
93	03	应用被永久锁定
6D	00	指令不支持

3.1.4 EXTERNAL AUTHENTICATION

3.1.4.1 定义

该命令用于 IC 卡中的应用验证接口设备中保密模块的有效性,以使接口设备获得某种授权。

- 在下面三种情况下认证卡片传输密钥 (CTK): ①当只注册 MF, 没有创建 MF; ②创建了 MF, 但没有创建 MF 下 KEY 文件时; ③创建了 MF 下 KEY 文件, 但没有创建主控密钥时。
- 在下面三种情况下认证 DF 传输密钥: ①当注册 DF, 没有创建 DF 时; ②创建了 DF, 但没有创建 DF 下 KEY 文件时; ③创建了 DF 下的 KEY 文件, 但没有创建主控密钥时。
- 其它情况下认证当前或上一层文件的相应外部认证密钥。

3.1.4.2 命令报文

代码	值
CLA	00
INS	82
P1	00
P2	密钥标识符或 00
Lc	08'
Data	鉴别用数据
Le	无

说明:

暂时只支持 p2=00

3.1.4.3 命令报文数据域

——第 1 至第 8 个字节为随机数加密数据。

3.1.4.4 响应报文数据域

无。



3.1.4.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
63	Cx	X 指出剩余的错误计数值
6A	88	未找到引用数据
69	83	Key、pin 锁定
69	84	引用数据无效
69	85	使用条件不满足
93	03	应用被永久锁定
6D	00	指令不支持

3.1.5 GET CHALLENGE

3.1.5.1 定义

该命令请求一个用于与安全相关的过程（如安全报文）的随机数。

3.1.5.2 命令报文

代码	值
CLA	00
INS	84
P1	00
P2	00
Lc	无
Data	无
Le	04/08/10H

3.1.5.3 命令报文数据域

无。



3.1.5.4 响应报文数据域

返回 Le 指定长度的随机数。

3.1.5.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
6D	00	指令不支持

3.1.6 GET RESPONSE

3.1.6.1 定义

当 APDU 不能使用现有的协议传输时，“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。

3.1.6.2 命令报文

代码	值
CLA	00
INS	C0
P1	00
P2	00
Lc	无
Data	无
Le	响应的期望数据最大长度

3.1.6.3 命令报文数据域

无。



3.1.6.4 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 0，在附加数据有效时，卡片必须回送 ‘6Cxx’，否则回送状态码 ‘6F00’。

3.1.6.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
6A	81	功能不支持
61	Xx	SW2 指出仍然有效的应答字节数
6F	00	没有可用的响应数据
6C	Xx	Le 长度错
93	03	应用被永久锁定
6D	00	指令不支持

3.1.7 INTERNAL AUTHENTICATION

3.1.7.1 定义

该命令提供了利用接口设备发来的随机数和自身存储的相关密钥进行数据鉴别的功能。

当有关的密钥位于 MF 层时，该命令可以用来鉴别整个卡片；当有关的密钥位于 DF 时，该命令可以用来鉴别此 DF。

3.1.7.2 命令报文

代码	值
CLA	00
INS	88
P1	00
P2	00
Lc	08'
Data	鉴别用数据
Le	无



3.1.7.3 命令报文数据域

——第 1 至第 8 个字节为随机数加密数据。

3.1.7.4 响应报文数据域

返回鉴别数据。

3.1.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
61	Xx	SW2 指出仍然有效的应答字节数
6A	88	未找到引用数据
93	03	应用被永久锁定
6D	00	指令不支持

3.1.8 PIN CHANGE/UNBLOCK

3.1.8.1 定义

该命令让发卡方解锁个人密码（即，重置个人密码尝试计数器的值为应用设定的最大次数），或者更改个人密码。

命令中个人密码的传递采用加密的方式。

3.1.8.2 命令报文

代码	值
CLA	84
INS	24
P1	00



P2	控制参数
Lc	数据域长度
Data	个人密码数据域和报文鉴别 (MAC) 数据元。
Le	无

说明：

P2 控制参数

b7	b6	b5	b4	b3	b2	b1	b0	意义
0	0	0	0	0	0	0	0	解锁个人密码。仅重置尝试计数器，并不更改个人密码。
0	0	0	0	0	0	0	1	更改个人密码。重置尝试计数器并以新 PIN 取代原 PIN。

3.1.8.3 命令报文数据域

操作	Lc 值	数据域内容
解锁个人密码	04	Lc 应包括 MAC 数据元的长度
更改个人密码	‘0C’ ~ ‘14’	Lc 应同时包括被加密的个人密码数据元和 MAC 数据元的长度

数据加密和 MAC 计算都采用 DPUK 密钥；MAC 计算不使用随机数。

3.1.8.4 响应报文数据域

无。

3.1.8.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
69	84	引用数据无效
69	88	安全报文数据项不正确
6A	88	未找到引用数据
93	03	应用被永久锁定
6D	00	指令不支持



3.1.9 READ BINARY

3.1.9.1 定义

该命令从透明文件中读取全部或部分数据。

- 如命令包含有效基本文件标识符，它所对应的文件即被设置为当前文件。
- 该命令只对当前所选择的文件（即当前文件）进行操作。
- 只有在满足当前文件读操作的权限的情况下，该命令才会被执行。
- 如当前文件的运行模式规定了读需要保密通信的方式，则回送的数据会采用。

3.1.9.2 命令报文

代码	值
CLA	00
INS	B0
P1	见 P1 和 P2 控制参数
P2	见 P1 和 P2 控制参数
Lc	无
Data	无
Le	‘00’ 或要读出的数据的长度

说明：

P1 和 P2 控制参数：

P1								P2								含义
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0	x	x	x	x	x	y	y	y	y	y	y	y	y	Xxxxx 表示 SFI (取值范围 ‘05’ ~ ‘1E’), yyyyyyyy 为要读的首字节距离文件首字节的偏移量
0	x	x	x	x	x	x	x	y	y	y	y	y	y	y	y	P1 × ‘100’ + P2 为要读的首字节距离文件首字节的偏移量



3.1.9.3 命令报文数据域

无。

3.1.9.4 响应报文数据域

- 当 Le 为 0 时，读出自首字节起的 255 个字节；如果在读出 255 个字节前已得到文件最后一个字节，则自要读的首字节起的全部字节将被读出。
- 读出的数据是否加密或线路保护取决于创建文件时所指定的属性；如文件规定使用加密或 MAC 方式，则使用相应的应用维护密钥进行计算。

3.1.9.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
94	03	密钥索引不支持
61	Xx	SW2 指出仍然有效的应答字节数
6C	Xx	LE 长度错
69	82	不满足安全状态
69	81	命令与文件组织不匹配
6A	82	没有找到文件
6B	00	参数越界
93	03	应用被永久锁定
6D	00	指令不支持

3.1.10 READ RECORD

3.1.10.1 定义

该命令从记录结构的基本文件中读取一些指定的记录或一个记录起始部分的数据。



3.1.10.2 命令报文

代码	值
CLA	00
INS	B2
P1	记录号或记录标识符
P2	P2 控制参数
Lc	无
Data	无
Le	‘00’ 或要读出的数据的长度

说明：

记录号的取值范围为 ‘01’ ~ ‘FE’，‘00’ 标识当前记录。

P2 控制参数

B8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	-	-	-	对当前文件进行操作
X	X	X	X	X	-	-	-	基本文件标识符(值为 05-1EH)
-	-	-	-	-	1	0	0	读 P1 指定的记录
-	-	-	-	-	1	0	1	从 P1 指定的记录开始读到最后一个记录
-	-	-	-	-	1	1	0	从最后一个记录开始读到 P1 指定的记录
-	-	-	-	-	0	0	0	读具有 P1 指定的记录标识符的第一个实例
-	-	-	-	-	0	0	1	读具有 P1 指定的记录标识符的最后一个实例
-	-	-	-	-	0	1	0	读具有 P1 指定的记录标识符的下一个实例
-	-	-	-	-	0	1	1	读具有 P1 指定的记录标识符的上一个实例

3.1.10.3 命令报文数据域

无。

3.1.10.4 响应报文数据域

读出的数据是否加密或线路保护取决于创建文件时所指定的属性；由回送的响应记录组成；如文件规定使用加密或 MAC 方式，则使用相应的应用维护密钥进行计算。

3.1.10.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回



6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
94	03	密钥索引不支持
6C	Xx	LE 长度错
61	Xx	SW2 指出仍然有效的应答字节数
69	82	不满足安全状态
69	81	命令与文件组织不匹配
69	86	不允许的命令（无当前 EF）
6A	82	没有找到文件
6A	83	没有找到记录
93	03	应用被永久锁定
6D	00	指令不支持

3.1.11 SELECT

3.1.11.1 定义

该命令通过文件名或应用标识符来选择 IC 卡中的 MF、DF 或 EF。

该命令设置当前文件。此命令执行以后，紧接着的所有命令都隐含地对此文件进行操作。

对一个专用文件(DF)的选择操作将该专用文件设置为当前文件，此后即可对它所包含的文件进行进一步的选择。

在复位应答后，主控文件(MF)被默认为当前文件。

3.1.11.2 命令报文

代码	值
CLA	00
INS	A4
P1	命令选项
P2	命令选项
Lc	数据域长度
Data	XX
Le	所希望的返回信息的最大长度

说明：

P1 命令选项：

b8	b7	b6	b5	b4	b3	b2	b1	说明
0	0	0	0	0	0	0	0	用文件标识符选择MF、DF或EF(XX=文件标识符或为空)



0	0	0	0	0	0	1	0	用文件标识符在当前 DF 下选择 EF(XX=EF 的文件标识符)
0	0	0	0	0	1	0	0	用 DF 文件名直接选择 DF(XX=DF 的文件名)
0	0	0	0	0	0	1	1	选当前 DF 的父 DF (Data 为空)

✎ 如果 P1=00H 并且数据域为空或等于 3F00H, 就选择 MF。

✎ P2 命令选项:

b8	b7	b6	b5	b4	b3	b2	b1	说明
0	0	0	0	-	-	0	0	第一个或唯一的文件实例
0	0	0	0	-	-	1	0	下一个文件实例

✎ Lc=05~10 或 00 或 02。

3.1.11.3 命令报文数据域

文件名、AID、文件标识符或不存在。

3.1.11.4 响应报文数据域

除选择 AEF 外, 响应报文数据域应包括所选择的 SSSE、DDF 或 ADF 的 FCI。

3.1.11.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
61	Xx	SW2 指出仍然有效的应答字节数
6A	82	没有找到文件
65	81	内存失败
93	03	应用被永久锁定
6D	00	指令不支持

3.1.12 UPDATE BINARY

3.1.12.1 定义

该命令写入或修改透明文件的全部或部分数据。



使用条件:

- ✎ 命令包含有效基本文件标识符，它所对应的文件即被设置为当前文件。
- ✎ 命令只对当前所选择的文件（即当前文件）进行操作。
- ✎ 只有在满足写入或修改当前文件的安全要求时，该命令才会被执行。
- ✎ 当前文件的安全属性规定了保密通信的方式，则只有用保密级别不低于这种方式的通信方式命令才会被接受。

3.1.12.2 命令报文

代码	值
CLA	00 或 04
INS	D6
P1	命令选项
P2	命令选项
Lc	数据域长度
Data	XX
Le	无

说明：

- ✎ P1 和 P2 命令选项：

P1								P2								含义
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0	x	x	x	x	x	y	y	y	y	y	y	y	y	xxxxx 表示 SFI (取值范围 ‘05’ ~ ‘1E’), yyyyyyyyy 为要写的首字节距离文件首字节的偏移量
0	x	x	x	x	x	x	x	y	y	y	y	y	y	y	y	P1 × ‘100’ + P2 为要写的首字节距离文件首字节的偏移量

3.1.12.3 命令报文数据域

- 要写入的数据（明文、明文+MAC 方式、加密+MAC 方式）。
- 加密或 MAC 计算使用的 key 为相应的应用维护密钥；MAC 计算使用随机数。



3.1.12.4 响应报文数据域

无。

3.1.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
69	81	命令与文件组织不匹配
69	86	不允许的命令（无当前 EF）
6A	82	没有找到文件
69	88	安全报文数据项不正确
6B	00	参数越界
69	85	使用条件不满足
6A	84	空间不足
93	03	应用被永久锁定
6D	00	指令不支持

3.1.13 UPDATE RECORD

3.1.13.1 定义

该命令用命令中给出的数据更新记录文件中指定记录的内容。

使用条件：

- ✎ 命令包含有效基本文件短标识符，它所对应的文件即被设置为当前文件，同时将当前记录指针复位。
- ✎ 该命令只对当前所选择的文件（即当前文件）进行操作。
- ✎ 只有在满足修改当前文件的权限要求时，该命令才会被执行。
- ✎ 如当前文件的运行模式规定了保密通信的方式，则只有用保密级别不低于这种方式的通信方式命令才会被接受。
- ✎ 对于线性结构文件，当指定的记录号不存在时，可按记录号的顺序添加记录。
- ✎ 按记录标识符访问记录不存在时，也应视为添加新的记录。
- ✎ 定长或环形结构的基本文件，命令中所用的记录长度必须与记录创建时所确定的记



录长度一致，否则命令将被拒绝执行。

✎ 该命令仅对记录结构的文件有效。

3.1.13.2 命令报文

代码	值
CLA	00 或 04
INS	DC
P1	命令选项
P2	命令选项
Lc	数据域长度
Data	XX
Le	无

说明：

✎ P1 命令选项说明：

——记录号的取值范围为 01-FEH，00H 表示当前记录。

✎ P2 命令选项说明：

——访问控制字节的具体含义如下表所述。

B8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	-	-	-	对当前文件进行操作
X	X	X	X	X	-	-	-	基本文件标识符(值为 05-1EH)
-	-	-	-	-	1	X	X	利用 P1 中的记录号
-	-	-	-	-	1	0	0	写 P1 指定的记录
-	-	-	-	-	0	X	X	利用 P1 中的记录标识符
-	-	-	-	-	0	0	0	写具有 P1 指定的记录标识符的第一个实例
-	-	-	-	-	0	0	1	写具有 P1 指定的记录标识符的最后一个实例
-	-	-	-	-	0	1	0	写具有 P1 指定的记录标识符的下一个实例
-	-	-	-	-	0	1	1	写具有 P1 指定的记录标识符的上一个实例
其他值							RFU	

——当记录为简单 TLV 数据对象时，命令中数据域的格式如下：

记录标识符(1 个字节)	记录长度 Ln(1 个字节)	该记录全部(Ln 个)数据字节
--------------	----------------	-----------------

3.1.13.3 命令报文数据域

- 要写入的数据（明文、明文+MAC 方式、加密+MAC 方式）。
- 加密或 MAC 计算使用的 key 为相应的应用维护密钥；MAC 计算使用随机数。



3.1.13.4 响应报文数据域

无。

3.1.13.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
69	81	命令与文件组织不匹配
69	86	不允许的命令（无当前 EF）
6A	82	没有找到文件
69	88	安全报文数据项不正确
69	85	使用条件不满足
6A	83	没有找到记录
6A	84	空间不足
93	03	应用被永久锁定
6D	00	指令不支持

3.1.14 VERIFY

3.1.14.1 定义

该命令用于校验命令数据域中的个人密码的正确性或返回允许继续尝试校验的次数。

✎ 此命令的执行结果将影响卡片的保密状态。当前的应用选择中，命令数据域中外部输入的个人密码与卡中存放的个人密码校验失败时，IC 卡将回送“63Cx”，x 表示个人密码允许重试的次数；当卡回送“63C0”时，表示不能重试个人密码，即个人密码被锁定。此时再使用该命令时，将回送失败状态码“6983”。如果校验成功，出错计数器的值将被置为 0。

✎ 对被锁定的个人密码进行校验，无论结果如何都不影响出错计数器值。

✎ 一旦 PIN 被锁定，所有需要校验 PIN 后才能执行的操作均不能执行。



3.1.14.2 命令报文

代码	值
CLA	00
INS	20
P1	00
P2	00
Lc	02~06
Data	输入的个人密码
Le	无

说明：

——如果 Lc=00H，则命令返回”63Cx”，X 指示允许继续尝试校验的次数(0-15)。

3.1.14.3 命令报文数据域

个人密码数据。

3.1.14.4 响应报文数据域

无。

3.1.14.5 响应报文状态码

此命令执行成功的状态码是‘9000’。
IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
63	Cx	X 指出剩余的错误计数值
69	83	Key、pin 锁定
6A	88	未找到引用数据
93	03	应用被永久锁定
6D	00	指令不支持



3.2 PBOC指令

3.2.1 CHANGE PIN

3.2.1.1 定义

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。

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。

使用条件：

- ✧ ——此命令的执行结果将影响卡片的保密状态。当前的应用选择中，命令数据域中外部输入的个人密码与卡中存放的个人密码校验失败时，IC 卡将回送“63Cx”，x 表示个人密码允许重试的次数；当卡回送“63C0”时，表示不能重试个人密码，即个人密码被锁定。此时再使用该命令时，将回送失败状态码“6983”。如果校验成功，出错计数器的值将被置为 0。
- ✧ ——对被锁定的个人密码进行校验，无论结果如何都不影响出错计数器值。
- ✧ ——一旦 PIN 被锁定，所有需要校验 PIN 后才能执行的操作均不能执行。

3.2.1.2 命令报文

代码	值
CLA	80
INS	5E
P1	01
P2	00
Lc	05-0D
Data	当前 PIN FF 新的 PIN
Le	无



3.2.1.3 命令报文数据域

见命令报文说明。

3.2.1.4 响应报文数据域

无。

3.2.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CEA 错
6A	86	P1、P2 错
67	00	LC 错
63	Cx	X 指出剩余的错误计数值
6A	81	功能不支持
93	03	应用被永久锁定
69	85	使用条件不满足
6A	80	数据域参数错
6D	00	指令不支持

3.2.2 RELOAD PIN

3.2.2.1 定义

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。



MAC 是用 DRPK 左右 8 个字节进行异或运算的结果，对新 PIN 值计算而得。

命令中的 MAC 仅对新 PIN 部分进行计算；MAC 计算不使用随机数。

3.2.2.2 命令报文

代码	值
CLA	80
INS	5E
P1	00
P2	00
Lc	06~0A
Data	新 PIN(2~6)+MAC(4)
Le	无

3.2.2.3 命令报文数据域

说明	长度（字节）
重装的新 PIN	2~6
MAC	4

✧ MAC 的计算是使用 DRPK 左右 8 字节进行异或运算的结果对新 PIN 值进行计算。

3.2.2.4 响应报文数据域

3.2.2.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	85	使用条件不满足 ➤ 存折溢出



		➤ 只有在金融应用的 ADF 下才可以 run。
6A	88	未找到引用数据
6D	00	指令不支持

3.2.3 INITIALIZE FOR LOAD

3.2.3.1 定义

INITIALIZE FOR LOAD 命令用于初始化圈存交易。

✧ --此命令的执行后卡片处于圈存状态中。

✧ --此命令的执行需经过 PIN 验证。

3.2.3.2 命令报文

代码	值
CLA	80
INS	50
P1	00
P2	01(ED) 02(EP)
Lc	0B
Data	密钥标识(1)+交易金额(4)+终端机编号(6)
Le	10

3.2.3.3 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

3.2.3.4 响应报文数据域

说明	长度（字节）
ED/EP（旧）余额	4
ED/DP 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

3.2.3.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	85	使用条件不满足 ➤ 存折溢出 ➤ 只有在金融应用的 ADF 下才可以 run。
94	02	交易计数器达到最大值
94	03	密钥索引不支持
69	82	不满足安全状态
6D	00	指令不支持

3.2.4 CREDIT FOR LOAD

3.2.4.1 定义

CREDIT FOR LOAD 命令用于圈存交易，将持卡人在银行相应帐户上的资金划入电子存折或电子钱包中。

使用条件：此命令的执行必须在卡片处于圈存状态中。

3.2.4.2 命令报文

代码	值
CLA	80
INS	52



P1	00
P2	00
Lc	0B
Data	交易日期(4)+交易时间(3)+MAC2(4)
Le	04

3.2.4.3 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

3.2.4.4 响应报文数据域

说明	长度（字节）
TAC	4

3.2.4.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	01	命令不接收（无效状态）
69	85	使用条件不满足
93	02	MAC 无效
93	03	应用被永久锁定
6D	00	指令不支持



3.2.5 INITIALIZE FOR UNLOAD

3.2.5.1 定义

INITIALIZE FOR UNLOAD 命令用于初始化圈提交易。

- ✧ ——此命令的执行后卡片处于圈提状态中。
- ✧ ——此命令的执行需经过 PIN 验证。

3.2.5.2 命令报文

代码	值
CLA	80
INS	50
P1	05
P2	01(ED)
Lc	0B
Data	密钥标识(1)+交易金额(4)+终端机编号(6)
Le	10

3.2.5.3 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

3.2.5.4 响应报文数据域

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



3.2.5.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	85	使用条件不满足 ➤ 只有在金融应用的 ADF 下才可以 run。
94	02	交易计数器达到最大值
94	01	金额不足
94	03	密钥索引不支持
69	82	不满足安全状态
6D	00	指令不支持

3.2.6 DEBIT FOR UNLOAD

3.2.6.1 定义

DEBIT FOR Unload 命令用于圈提交易，可以将持卡人在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。

使用条件：

- ✧ ——此命令的执行必须在卡片处于圈提状态中。

3.2.6.2 命令报文

代码	值
CLA	80
INS	54
P1	03
P2	00
Lc	0B
Data	交易日期(4)+交易时间(3)+MAC2(4)



Le	04
----	----

3.2.6.3 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

3.2.6.4 响应报文数据域

说明	长度（字节）
MAC3	4

3.2.6.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	01	命令不接收（无效状态）
69	85	使用条件不满足
93	02	MAC 无效
6D	00	指令不支持

3.2.7 INITIALIZE FOR PURCHASE/CASH WITHDRAW

3.2.7.1 定义

INITIALIZE FOR PURCHASE 命令用于初始化消费交易。

✧ --此命令的执行后卡片处于消费/取现状态中。

✧ --使用电子存折进行交易，则此命令的执行需经过 PIN 验证；而电子钱包不需要。



3.2.7.2 命令报文

代码	值
CLA	80
INS	50
P1	01/02
P2	01(ED) 02(EP)(不用于 P1=02)
Lc	0B
Data	密钥标识(1)+交易金额(4)+终端机编号(6)
Le	0F

说明：

- ✧ --P1 等于 01，执行消费操作。
- ✧ --P1 等于 02，执行取现操作。

3.2.7.3 命令报文数据域

说明	长度（字节）
密钥标识（索引号）	1
交易金额	4
终端机编号	6

3.2.7.4 响应报文数据域

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

3.2.7.5 响应报文状态码

此命令执行成功的状态码是‘9000’。



IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	85	使用条件不满足 ➤ 只有在金融应用的 ADF 下才可以 run。
94	02	交易计数器达到最大值
94	01	金额不足
94	03	密钥索引不支持
69	82	不满足安全状态
6D	00	指令不支持

3.2.8 DEBIT FOR PURCHASE/CASH WITHDRAW

3.2.8.1 定义

DEBIT FOR PURCHASE/CASH WITHDRAW 命令用于消费取现交易，使用持卡人在电子存折或电子钱包中的余额进行消费。

使用条件：

- ✧ ——此命令的执行必须在卡片处于消费/取现状态中。

3.2.8.2 命令报文

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



3.2.8.3 命令报文数据域

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

3.2.8.4 响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

3.2.8.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	01	命令不接收（无效状态）
69	85	使用条件不满足
93	02	MAC 无效
6D	00	指令不支持

3.2.9 INITIALIZE FOR CAPP PURCHASE

3.2.9.1 定义

INITIALIZE FOR CAPP PURCHASE 命令用于初始化复合消费交易。此命令成功执行后卡片处于 CAPP1 状态中。



3.2.9.2 命令报文

代码	值
CLA	80
INS	50
P1	03
P2	02
Lc	0B
Data	密钥标识(1)+交易金额(4)+终端机编号(6)
Le	0F

3.2.9.3 命令报文数据域

说明	长度（字节）
密钥标识（索引号）	1
交易金额	4
终端机编号	6

3.2.9.4 响应报文数据域

说明	长度（字节）
EP 旧余额	4
脱机交易序号	2
透支限额	3
密钥版本（DPK）	1
算法标识（返回密钥版本）(DPK)	1
伪随机数	4

3.2.9.5 响应报文状态域

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
62	83	选择文件无效，文件或密钥校验错误
65	81	EEPROM 错误
69	82	不满足安全状态
69	85	使用条件不满足



6A	81	不支持此功能（未创 MF 或卡片锁定）
6A	82	文件未找到
94	01	金额不足
94	03	密钥索引不支持

3.2.10 UPDATE CAPP CACHE

3.2.10.1 定义

INITIALIZE FOR CAPP PURCHASE 命令用于复合消费交易中更新复合应用数据缓存，此命令成功执行后卡片处于 CAPP2 状态。

允许在同一次复合消费流程中多次更新不同的复合应用数据缓存，若多次更新同一复合应用数据缓存，则在 DEBIT 中以最后一次更新的数据为实际更新数据。

3.2.10.2 命令报文

代码	值
CLA	80
INS	DC
P1	复合应用标志符/记录号(记录号仅限上海公交应用)
P2	见下表
Lc	更新记录的长度
Data	更新的记录内容

此命令报文中的引用控制参数 P2 定义见下表：

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

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



3.2.10.3 命令报文数据域

此命令报文数据域由更新原有记录的新记录组成。

3.2.10.4 响应报文数据域

响应报文数据域不存在。

3.2.10.5 响应报文状态域

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

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

3.2.11 DEBIT FOR CAPP PURCHASE

3.2.11.1 定义

DEBIT FOR CAPP PURCHASE 命令用于复合应用消费交易。

3.2.11.2 命令报文

代码	值
CLA	80
INS	54



P1	01
P2	00
Lc	0F
Data	终端交易序号(4)+交易日期(4)+交易时间(3)+MAC1(4)
Le	08

3.2.11.3 命令报文数据域

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

3.2.11.4 响应报文数据域

说明	长度（字节）
TAC	4
MAC2	4

3.2.11.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

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
‘93’	‘01’	金额不足
‘93’	‘02’	MAC 无效



3.2.12 UPDATE OVERDRAW LIMIT

3.2.12.1 定义

UPDATE OVERDRAW LIMIT 命令用于修改透支限额交易。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。

✧ ——此命令的执行必须在卡片处于修改状态中。

3.2.12.2 命令报文

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

3.2.12.3 命令报文数据域

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

3.2.12.4 响应报文数据域

说明	长度（字节）
TAC	4

3.2.12.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。



SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	01	命令不接收（无效状态）
69	85	使用条件不满足
93	02	MAC 无效
93	03	应用被永久锁定
6D	00	指令不支持

3.2.13 GET BALANCE

3.2.13.1 定义

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。

使用条件：

- ✧ ——此命令的执行 P1 等于 01 时，需经过 PIN 验证。

3.2.13.2 命令报文

代码	值
CLA	80
INS	5C
P1	00
P2	01(ED)/02(EP)
Lc	无
Data	无
Le	04

说明：

- ✧ ——如果透支限额存在时，则电子存折的余额是实际圈存余额与透支限额之和。

3.2.13.3 命令报文数据域

无。



3.2.13.4 响应报文数据域

说明	长度（字节）
ED 余额/EP 余额	4

3.2.13.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	82	不满足安全状态
69	85	使用条件不满足
6D	00	指令不支持

3.2.14 GET TRANSACTION PROOF

3.2.14.1 定义

GET TRANSACTION PROOF 命令提供了一种在交易过程中拔出并重插卡后卡片的恢复机制。

3.2.14.2 命令报文

代码	值
CLA	80
INS	5A
P1	00
P2	XX 交易类型标识
Lc	02



Data	对应的联机/脱机交易序号
Le	08

说明：

✧ P2 交易类型对应的参数值如下：

- ◆ 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

3.2.14.3 命令报文数据域

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

3.2.14.4 响应报文数据域

说明	长度（字节）
MAC	4
TAC	4

3.2.14.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
94	06	所需 MAC 不可用



69	85	使用条件不满足
6D	00	指令不支持

3.2.15 GET MESSAGE

3.2.15.1 定义

GET MESSAGE命令用于消费/取现交易。读取CPU卡中的认证识别信息，即MID _UID0UID1UID2UID3_ 四字节安全认证识别码，将安全认证识别码发送给PSAM卡进行认证。该命令在应在任意目录下都可以执行。

3.2.15.2 命令报文

代码	值
CLA	80
INS	CA
P1	00
P2	00
Le	09
Data	不存在

3.2.15.3 命令报文数据域

命令报文数据域不存在。

3.2.15.4 响应报文数据域

响应报文数据域为 9 字节建设部认证码。

3.2.15.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
67	00	长度错误
6A	86	P1 P2 错误
6E	00	CLA 字节错误



3.3 发卡指令

3.3.1 Write Key/Pin (创建、修改KEY、PIN指令)

3.3.1.1 定义

该命令创建、修改或重新激活各种密钥或个人识别码。

使用条件：只有在密钥/密码文件所对应的写操作控制密钥得到成功认证后，该命令才能执行。

3.3.1.2 命令报文

代码	值
CLA	80/84
INS	D4
P1	01：表示添加密钥 密钥类型：表示更新密钥
P2	Key/Pin 记录索引号
Lc	见命令报文数据域
Data	
Le	无

说明：

- ✧ 指令根据 KEY/PIN 文件的文件属性定义来判断是用明文、MAC 或加密+MAC 三种方式来追加 KEY/PIN。
- ✧ 密钥文件下的第一条密钥无权限保护。
- ✧ 第一个追加的 KEY 应为主控密钥 (MK) (使用加密、加密+MAC 方式追加密钥的流程如下：追加 MF 下的 MK 使用 MF 的 TK(传输密钥)；追加 MF 下的其它 KEY 使用 MF 下的 MK；追加 DF 下的 MK 使用 MF 的 MK；追加 DF 下的其它密钥使用 DF 下的 MK；MF 下或 DF 下追加的第一个密钥应为 MK)

3.3.1.3 命令报文数据域

- ✧ 增加消费，圈提，圈存，修改透支限额密钥

CLA	INS	P1	P2	LC	数据域					
80/84	D4	01	密钥索引	XX	类型	RFU(FF)	RFU(FF)	密钥版本号	算法标识	密钥值



◇ 增加外部认证密钥

CLA	INS	P1	P2	LC	数据域					
80/84	D4	01	密钥索引	XX	39	版本号	RFU	后续状态	错误计数器	密钥值

◇ 增加内部认证密钥

CLA	INS	P1	P2	LC	数据域					
80/84	D4	01	密钥索引	XX	30	版本号	RFU	RFU	错误计数器	密钥值

◇ 增加应用维护密钥

CLA	INS	P1	P2	LC	数据域					
80/84	D4	01	密钥索引	XX	36	RFU	RFU	RFU	错误计数器	密钥值

◇ 增加 PIN

CLA	INS	P1	P2	LC	数据域					
80/84	D4	01	密钥索引	XX	3A	RFU	RFU	后续状态	错误计数器	PIN 值

◇ 增加解锁口令密钥，重装口令密钥

CLA	INS	P1	P2	LC	数据域					
80/84	D4	01	密钥索引	XX	37/38	RFU	RFU	RFU	错误计数器	密钥值

密钥类型	意义
30	内部认证密钥
36	应用维护密钥
37	解锁 PIN 密钥
38	重装 PIN 密钥
39	外部认证密钥
3A	PIN
3C	修改透支限额密钥
3D	圈提密钥
3E	消费密钥
3F	圈存密钥
34	TAC 密钥

➤ 密钥类型的高 2 bit 定义了采用的算法类型：

- 00—表示使用 3DES 算法
- 01—表示使用 DES 算法
- 10—表示使用 SSF33 算法
- 11—表示使用 SM1 算法



- 后续状态可以设为一个点或者一个区间，且高四位 \geq 低四位，如 F0 表示认证后的权限区间在 0~F 之间，FF 表示认证后只达到 F 这一点的权限
- 错误计数器的高四位=低四位，以便认证正确后恢复计数器
- PIN 值的长度的范围为 2~6 个字节，不允许 16 进制中的 A~E，允许最后一个半字节为 F，如 1234AB 不正确，12349F 正确

3.3.1.4 响应报文数据域

无。

3.3.1.5 响应报文状态码

此命令执行成功的状态码是 ‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
6A	82	没有找到文件
63	Cx	X 指出剩余的错误计数值
69	83	Key、pin 锁定
6A	84	空间不足
93	03	应用被永久锁定
6D	00	指令不支持

3.3.2 Create File (创建文件)

3.3.2.1 定义

该命令为要创建的文件分配存储空间，写入所创文件的属性定义，并根据需要写入传输密钥等信息。

3.3.2.2 命令报文

代码	值
CLA	80/84
INS	E0



P1	文件 ID (FID)
P2	
Lc	xx(DF/MF)/0B(EF)
Data	数据
Le	无

3.3.2.3 命令报文数据域

数据域的构成如下表所示：

◇ 创建 MF

字节	01	02~03	04	05	06	07	08	
值	38	XX XX	XX	XX	XX	XX	XX	XX...XX
含义	文件类型	文件空间	建立/擦除权限	锁定权限	应用文件 ID	MF 文件属性	FF (RFU)	文件名

- 当文件空间设置超出卡容量（如 FFFF），则默认设置为最大允许空间。
- 建立/擦除权限字节中，建立权限表示 MF 下建立文件的权限；擦除权限表示擦除 MF 的权限。
- 权限字节定义请见章节 5.2。
- MF 属性字节
 - Bit 7 ~ Bit 5: RFU
 - Bit 4: 1—mf 可被删除
0—mf 不可被删除
 - Bit 3: 1—表示使用建设部认证码
0—表示不使用建设部认证码
 - Bit 2: 1—表示创建目录下文件需用 MAC 方式
0—表示创建目录下文件不需 MAC 方式
 - Bit 1: 默认=1，表示 pboc 应用
 - Bit 0: RFU

◇ 创建 DF

字节	01	02~03	04	05	06	07	08		后 0x14 字节
值	38	XX XX	XX	XX	XX	XX	XX	XX...XX	XX...XX
含义	文件类型	文件空间	建立/擦除权限	锁定权限	应用文件 ID	DF 文件属性	FF	文件名	DF 传输密钥

- 建立/擦除权限字节中，建立权限表示 DF 下建立文件的权限；擦除权限表示擦除 DF 的权限。
- 权限字节定义请见章节 5.2。
- DF 属性字节
 - Bit 7~6:默认 = 01
 - Bit 5: RFU
 - Bit 4: 1—表示该 df 能被删除
0—表示该 df 不能被删除
 - Bit 3: 1—表示使用建设部认证码



0—表示不使用建设部认证码

Bit 2: 1—表示创建目录下文件需用 MAC 方式

0—表示创建目录下文件不需 MAC 方式

Bit 1: 默认=1, 表示 pboc 应用

Bit 0: 1—表示创建目录下文件无 DF 传输密钥

0—表示创建目录下文件有 DF 传输密钥

➤ 传输密钥 TK 结构:

Rfu	Rfu	Rfu	错误计数器	Tk 密钥
-----	-----	-----	-------	-------

◇ 创建 EF

◇ 电子存折需要验证 pin

Byte 文件类型	01	02~03		04	05	06	07
二进制文件	28	文件空间		读权限	写权限	FF (RFU)	文件属性
定长记录文件	2A	文件空间 (记录数* 记录长度)		读权限	写权限	FF (RFU)	文件属性
循环文件	2E	文件空间 (记录数* 记录长度)		读权限	写权限	FF (RFU)	文件属性
PBOC ED/EP 文件	2F	读起 始日 期权 限	更新 起始 日期 权限	读余额权 限	充值权 限	消费 权限	交易记 录 SFI
变长记录	2C	文件空间		读权限	写权限	FF (RFU)	文件属性
密钥文件	3F	文件空间		FF	增加权 限	FF (RFU)	PIN 更新 /解锁权 限

➤ 若需采用 MAC 更新方式, 则须将文件类型字节最高 bit 置 1, 如将 28 改为 A8。

➤ 若需采用密文更新方式, 则须将密钥类型字节次高 bit 置 1, 如将 28 改为 68。

➤ 定长记录文件空间, 第一个字节为记录个数, 第二个字节为每条记录的长度。

➤ 若需采用 MAC 方式更新或者添加密钥, 则须将文件类型字节最高 bit 置 1, 将 3F 改为 AF

➤ 若需采用 MAC+加密方式更新或者添加密钥, 则须将文件类型字节次高 bit 置 1, 将 3F 改为 FF

➤ 权限字节定义请见章节 5.2。

➤ EF 属性字节

Bit 7: 1—表示读文件不需要 MAC

0—表示读文件需要 MAC

Bit 6: 1—表示读文件不需采用加密方式



0—表示读文件必须采用加密方式

Bit 5 ~ Bit 4: RFU, 保留为 1

Bit 3 ~ Bit 2: 读操作时使用的密钥标识

11—标识为 00 的密钥

10—标识为 01 的密钥

01—标识为 02 的密钥

00—标识为 03 的密钥

Bit 1 ~ Bit 0: 写操作时使用的密钥标识

11—标识为 00 的密钥

10—标识为 01 的密钥

01—标识为 02 的密钥

00—标识为 03 的密钥

3.3.2.4 响应报文数据域

无。

3.3.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	82	不满足安全状态
63	Cx	X 指出剩余的错误计数值
69	83	Key、pin 锁定
93	03	应用被永久锁定
69	85	使用条件不满足
6D	00	指令不支持

3.3.3 Register MF (注册主控文件)

3.3.3.1 定义

该命令为卡片进行预个人化。预个人化操作包括：构造主控文件的结构、写入复位应答中与卡片制造有关的历史字节、在卡片中写入传输密钥等。



3.3.3.2 命令报文

代码	值
CLA	00
INS	EE
P1	00
P2	38
Lc	1A/22
Data	数据域
Le	无

3.3.3.3 命令报文数据域

数据域的构成如下表所示：

字节	01~02	03	04~05	06~07	08~0D
值	3F 00	38	FF FF	XX XX	XX XX XX XX XX XX
含义	文件标识	文件类型	RFU	制造厂商代码	卡片序列号

字节	0E	0F	10	11	12	13~23
值	FF	XX	XX	FF	XX	XX.....XX
含义	RFU	TK 标识	注册标识	RUF	TK 计数器	传输密钥 TK

➤ TK 标识字节

高两 Bit 定义所使用的算法：

00—表示使用 3DES 算法

01—表示使用 DES 算法

10—表示使用 SSF33 算法

11—表示使用 SM1 算法

➤ 注册标识字节

Bit 7: RFU

Bit 6: 默认设为 1，表示非接通道下创建 MF 时认证 TK 使用 PBOC 方式

Bit 5: 1—表示非接通道下创建 MF 需用 MAC 方式

0—表示非接通道下创建 MF 不需 MAC 方式

Bit 4: 1—表示非接通道下创建 MF 需要认证 TK

0—表示非接通道下创建 MF 不需要认证 TK

Bit 3: RFU

Bit 2: 默认设为 1，表示非接通道下创建 MF 时认证 TK 使用 PBOC 方式

Bit 1: 1—表示接通道下创建 MF 需用 MAC 方式

0—表示接通道下创建 MF 不需 MAC 方式

Bit 0: 1—表示接通道下创建 MF 需要认证 TK

0—表示接通道下创建 MF 不需要认证 TK



3.3.3.4 响应报文数据域

无。

3.3.3.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
69	85	使用条件不满足
6A	84	空间不足
6D	00	指令不支持

3.4 其他指令

3.4.1 Erase DF（删除DF指令）

3.4.1.1 定义

删除当前应用（MF 或 DF）。

- ✧ 删除 MF 后，回到卡片的注册状态。
- ✧ 删除 DF 后，可以回到 DF 的注册状态或删除 DF 本身。

使用条件：

- ✧ 需使用 MF 或当前应用下的 MK 或 TK 进行线路保护，进行权限的认证；同时判断 FLAG_OF_ERASE_DF（创建 MF 或 DF 时写入）标志是否有效。

3.4.1.2 命令报文

代码	值
CLA	84



INS	0E
P1	00
P2	00
Lc	04/10/18
Data	TRANSMIT KEY _{DATA} +MAC
Le	无

说明：

- ✧ TRANSMIT KEYDATA 为传输密钥（参见 change key/pin 的密钥格式）。
- ✧ FLAG_OF_ERASE_DF 在文件创建时写入（参见 create file 指令）。

3.4.1.3 命令报文数据域

- ✧ 删除 MF 时，COS 回到注册状态，数据域中 TRANSMIT KEYDATA 是可选的。
- ✧ 删除 DF 时，数据域中如有 TRANSMIT KEYDATA，则删除 DF 后，回到 DF 的注册状态；如只有 MAC，则删除整个 DF。
- ✧ MAC 计算使用主控密钥；且不使用随机数。

3.4.1.4 响应报文数据域

3.4.1.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	82	不满足安全状态
63	Cx	X 指出剩余的错误计数值
69	83	Key、pin 锁定
6D	00	指令不支持



3.4.2 Modify ATR (修改ATR指令)

3.4.2.1 定义

修改 ATR 客户代码和序列号。

使用条件：

- ✧ 需使用 MF 下的主控密钥进行线路保护，进行权限的认证；同时判别 FLAG_OF_MODIFY_SID 和 FLAG_OF_MODIFY_CID (COS 的配置信息，需在测试模式下写入) 是否有效。

3.4.2.2 命令报文

代码	值
CLA	84
INS	E6
P1	00
P2	01/02/FF/11/12
Lc	XX(04~0E)
Data	DATA+MAC
Le	无

说明：

MAC 计算使用主控密钥；且不使用随机数。

P2 参数说明：

- ✧ P2 为 01，修改 ATR 的序列号；P2 为 02，修改客户代码。
- ✧ P2 为 FF，关闭所有修改特性；P2 为 11，关闭修改 ATR 的历史字符功能；P2 为 12，关闭修改客户代码功能；修改功能关闭后不可以再开启。

3.4.2.3 命令报文数据域

要修改的数据+MAC。

3.4.2.4 响应报文数据域

无。



3.4.2.5 响应报文状态码

此命令执行成功的状态码是‘9000’。

IC 卡可能返回的错误状态码如下表。

SW1	SW2	含义
90	00	正确返回
6E	00	CLA 错
6A	86	P1、P2 错
67	00	LC 错
6A	81	功能不支持
93	03	应用被永久锁定
69	82	不满足安全状态
63	Cx	X 指出剩余的错误计数值
69	83	Key、pin 锁定
6D	00	指令不支持

4 应用流程

4.1 卡片个人化流程

卡片的个人化过程包括以下步骤：

- ✧ REGISTER MF。
- ✧ 认证 MF 的传输密钥。
- ✧ 创建 MF（线路保护模式）。
- ✧ 选择 MF。
- ✧ 认证 MF 的传输密钥。
- ✧ 创建 MF 下的 KEY 文件（线路保护模式）。
- ✧ 追加主控密钥（线路保护模式）。
- ✧ 认证主控密钥。
- ✧ REGISTER ADF。
- ✧ 选择 ADF。
- ✧ 认证 ADF 的传输密钥。
- ✧ 创建 ADF（线路保护模式）。

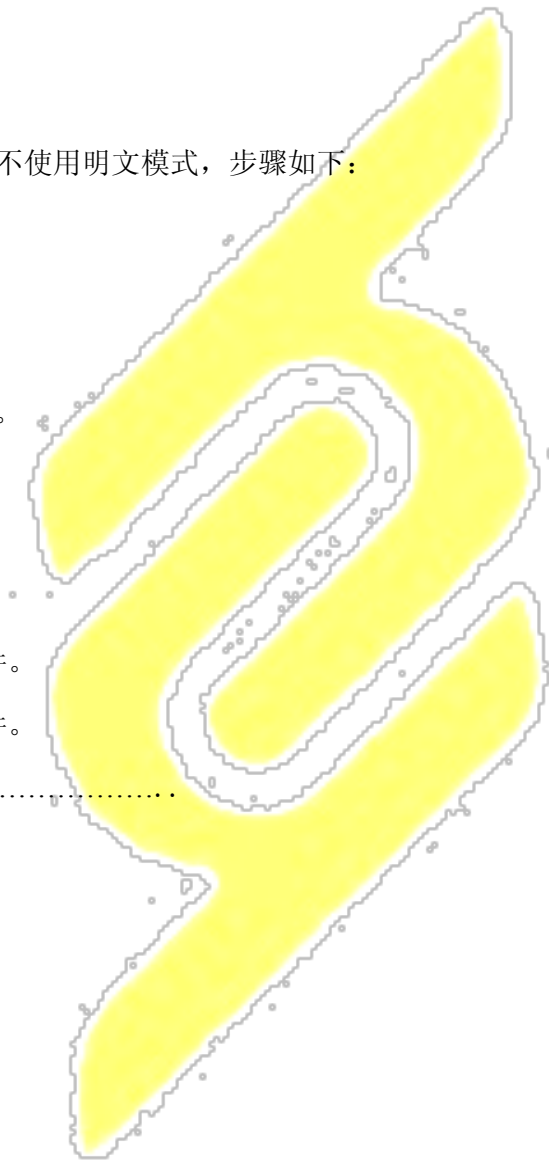


- ✧ 创建 ADF 下的 KEY 文件（线路保护模式）。
- ✧ 追加 ADF 下的主控密钥（线路保护模式）。
- ✧ 认证 ADF 下的主控密钥。
- ✧ 追加 ADF 下的其它文件（线路保护模式）。
- ✧

4.1.1 明文模式

建议卡片的个人化时不使用明文模式，步骤如下：

- ✧ REGISTER MF。
- ✧ 创建 MF。
- ✧ 选择 MF。
- ✧ 创建 MF 下的 KEY 文件。
- ✧ REGISTER ADF。
- ✧ 选择 ADF。
- ✧ 创建 ADF。
- ✧ 创建 ADF 下的 KEY 文件。
- ✧ 追加 ADF 下的其它文件。
- ✧



4.1.2 权限模式

- ✧ 步骤如下：
- ✧ REGISTER MF。
- ✧ 认证 MF 的传输密钥。
- ✧ 创建 MF。
- ✧ 选择 MF。
- ✧ 认证 MF 的传输密钥。
- ✧ 创建 MF 下的 KEY 文件
- ✧ 追加主控密钥



- ✧ 认证主控密钥。
- ✧ REGISTER ADF。
- ✧ 选择 ADF。
- ✧ 认证 ADF 的传输密钥。
- ✧ 创建 ADF。
- ✧ 创建 ADF 下的 KEY 文件。
- ✧ 追加 ADF 下的主控密钥。
- ✧ 认证 ADF 下的主控密钥。
- ✧ 追加 ADF 下的其它文件。

.....

4.1.3 线路保护模式

步骤如下：

- ✧ REGISTER MF。
- ✧ 创建 MF（线路保护模式）。
- ✧ 选择 MF。
- ✧ 创建 MF 下的 KEY 文件（线路保护模式）。
- ✧ 追加主控密钥（线路保护模式）。
- ✧ REGISTER ADF。
- ✧ 选择 ADF。
- ✧ 创建 ADF（线路保护模式）。
- ✧ 创建 ADF 下的 KEY 文件（线路保护模式）。
- ✧ 追加 ADF 下的主控密钥（线路保护模式）。
- ✧ 追加 ADF 下的其它文件（线路保护模式）。
- ✧





4.1.4 混合模式

混合交叉上述模式。

4.2 交易流程

本章描述了电子存折/电子钱包应用的交易流程。该流程描述的是卡片插入终端并与终端相互作用后，所进行的交易处理过程。

消费或取现交易要求终端必须具有安全存取模块（PSAM）。JR/T 0025.2-2004 的本部分假定终端和 PSAM 之间是以安全方式进行通信的，因此不定义任何与 PSAM 通信相关的命令—响应对。

4.2.1 交易预处理

- ✧ 应用选择。
- ✧ IC 卡有效性检查。
- ✧ VERIFY PIN。

4.2.2 交易类型

PBOC ED/EP 交易类型如下：

- ✧ 圈存交易。
- ✧ 圈提交易。
- ✧ 消费交易。
- ✧ 取现交易。
- ✧ 修改透支限额交易。
- ✧ 查询余额交易。
- ✧ 查询明细交易

详细的流程见“1—中国金融集成电路（IC）卡电子钱包电子存折卡片规范”和“2—中国金融集成电路（IC）卡电子钱包电子存折应用规范”



4.2.3 应用维护功能

电子存折/电子钱包应用涉及到的安全机制，应按照《中国金融集成电路(IC)卡规范》第1部分：电子钱包/电子存折卡片规范中“安全机制”部分的规定进行，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（参见《中国金融IC卡规范》第1部分：电子钱包/电子存折卡片规范的“数据元和命令”部分）。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，用以代替《中国金融集成电路(IC)卡规范》第1部分：电子钱包/电子存折卡片规范中定义的初始化值。

不采用过程密钥。除去UNBLOCK PIN 命令外，均使用导出的应用维护密钥(DAMK)来计算MAC。UNBLOCK 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。

4.2.3.1 卡片锁定

终端发出CARD BLOCK 命令来锁定卡片。

此命令参照《中国金融集成电路(IC)卡规范》第1部分：电子钱包/电子存折卡片规范的“数据元和命令”部分。其安全机制在5.5.9.1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）。

4.2.3.2 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《中国金融集成电路(IC)卡规范》第1部分：电子钱包/电子存折卡片规范的“数据元和命令”部分。其安全机制在5.5.9.1中描述。在JR/T 0025.2-2004



的本部分所述的应用中，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 卡回送状态码 ‘6A81’（功能不被支持）和文件控制信息（FCI），在 T=0 协议时，卡片 FCI 需用 GET RESPONSE 命令取回。

—— 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）：

- ✧ 当用 SELECT 命令选择此应用或其他应用时；
- ✧ 当用 GET CHALLENGE 命令为 UNBLOCK PIN 命令产生 MAC 时；
- ✧ APPLICATION BLOCK 命令；
- ✧ CARD BLOCK 命令；
- ✧ APPLICATION UNBLOCK 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。

4.2.3.3 应用解锁

终端发出 APPLICATION UNBLOCK 命令来对应用解锁，详细定义见《中国金融集成电路(IC)卡规范》第 1 部分：电子钱包/电子存折卡片规范，安全机制见 5.5.9.1。

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 ‘9303’（应用永久锁定）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象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。

4.2.3.4 PIN 解锁

终端发出 UNBLOCK PIN 命令对 PIN 解锁，详细描述参见《中国金融集成电路(IC)卡规范》第 1 部分：电子钱包/电子存折卡片规范，有关安全要求见第 2 部分应用规范



5.5.9.1。

在命令报文中，P2 取 ‘01’ 值。使用 DPUK 对 PIN 数据加密（电子钱包/电子存折中国金融集成电路(IC)卡规范》第 1 部分：卡片规范“安全机制”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）。

4.2.3.5 二进制形式修改

终端按照《中国金融集成电路(IC)卡规范》第 1 部分：电子钱包/电子存折卡片规范和第 2 部分应用规范 5.5.9.1 中所描述的安全要求，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）。

4.2.3.6 更改 PIN

更改 PIN 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，它将进行以下操作：

—— 检查 PIN 尝试计数器。如果为 0，表明 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：

- ✧ 将 IC 卡上的 PIN 改为命令中的新 PIN；
- ✧ 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：

- ✧ 将 PIN 尝试计数器减 1；
- ✧ 回送状态码 ‘63Cx’，这里 x 是 PIN 尝试计数器的新值。如达到零，则卡片自动锁定 PIN。

4.2.3.7 重装 PIN

终端按照 5.2.13 节中的描述发出 RELOAD PIN 命令来重装 PIN。

按照附录 B 中描述的机制用密钥 DRPK 来产生一个 MAC。



当此命令失败三次之后，应用被永久锁定。

4.2.4 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，并且在重新加电后自动地触发恢复机制。

在终端发给 IC 卡一个命令以更新电子存折余额或电子钱包余额时，卡片总会回送一个 MAC 或/和 TAC，以证明更新已经发生。这样的情况有圈存 (TAC)，圈提 (MAC3)、消费/取现 (TAC) 和修改透支限额 (TAC)。

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 TRANSACTION PROVE 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 ED 或 EP 余额的命令，如 Debit、Credit 命令时，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 PROVE 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 TRANSACTION PROVE 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 无法回送，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。

5 安全特性

5.1 安全状态

COS 采用鉴别寄存器的权限管理模式，具体如下：

- ✓ COS 仅保存当前层和父层两层的状态。
- ✓ 每一层可以描述 15 个外部认证密钥中某一个密钥状态和单 PIN 的状态。
- ✓ 在当前层，COS 提供了认证上一层外部认证密钥的指令，但并不提供认证父层的 PIN。



5.2 权限设置

- ✓ COS 中操作权限由单字节描述；可以设置受当前层和父层的状态组合控制。
- ✓ 权限字节为 0x00H 时，默认无权限控制，为 0xFFH 时默认为完全禁止，其余单字节的权限定义如下：

b8	b7	b6	b5	b4	b3	b2	b1	说明
x								控制该操作的权限（权限 1、权限 2）关系： ☞ 1=AND ☞ 0=OR
	x							权限 1 的层次描述： ☞ 0=UpLayer ☞ 1=CurrentLayer
		x	x					权限 1 的后续状态要求： ☞ 由于只有 2 个 bit，所以只能描述 4 个状态。 ☞ 如果是指 UpLayer，并且当前值是 00，则表示不受权限控制，所以在此情况下，只能描述 3 个状态；如果是指 CurrentLayer，则 00 也可以是一个后续的状态。
				x	x	x	x	权限 2 的后续状态要求： ☞ 为了描述比较多的状态，所以此处省略了层次的描述，默认就是当前层。 ☞ 有 16 个 bit，所以能描述 16 个状态。

为更好的理解安全机制，下面举一例说明：

权限字节设为 3（上一层），9（当前层），and，满足条件：上一层达到 3，当前层达到 9

权限字节设为 3（当前层），9（当前层），and，满足条件：当前层达到 3 且达到 9

权限字节设为 3（上一层），9（当前层），or，满足条件：当上一层达到 3 或者当前层达到 9

权限字节设为 3（当前层），9（当前层），or，满足条件：当前层达到 3 或者当前层达到 9

5.3 数据传送模式

HYCOS/PBOC 2.0 提供了 4 种数据传输模式，即明文模式、加密模式、MAC 模式和加密 MAC 模式。

数据传送要求应用根据安全级别采用不同模式，目的是保证数据的可靠性、数据完整性和对发送方的鉴别。

在实际应用时，并不是每条命令或应答都必须使用安全数据交换。在满足文件操作方



式所规定的最低保密通信要求的前提下，具体的通信方式将由应用确定。

5.3.1 MAC鉴别方式

MAC 鉴别方式通过多传递一个 4 字节的校验和(MAC)来检查信息是否被篡改。MAC 鉴别方式保密通信的命令信息结构如下图所示。

CLA	INS	P1	P2	L+4	数据	MAC 校验和
					L 字节	4 字节

MAC 鉴别方式的应答信息的结构和 MAC 计算如下图所示。

数据	MAC 校验和	SW1	SW2
4 字节			

5.3.2 密文方式

密文方式通过对所传递的信息进行加密来防止未经授权的信息获取。其命令信息结构和密文计算方式如下图所示。

					密文部分		
CLA	INS	P1	P2	L	明文数据长度	数据	添补的字节
					1 字节	L 字节	

密文方式的应答信息的结构和密文计算方法如下图所示。

明文数据长度字节	数据	SW1	SW2	添补字节
密文				

5.3.3 组合方式

组合方式的实现过程为：先使用密文方式对有关的信息进行加密，然后将再计算密文信息的校验和。具体的命令信息结构和计算方式如下图所示。



					密文部分			
CLA	INS	P1	P2	L	明文数据长度	数据	MAC 校验和	添补的字节
					1 字节	L 字节	4 字节	

CLA	INS	P1	P2	L	数据	添补的字节
					对此部分信息计算 MAC	

CLA	INS	P1	P2	L	明文数据长度	数据	MAC 校验和	添补的字节
					对此部分信息进行加密处理			

组合方式保密通信的应答信息结构和计算方法如下图所示。

发送序列计数器	数据	MAC 校验和	SW1	SW2	添补字节
密文					

发送序列计数器	数据	SW1	SW2	添补字节
此部分信息与密钥的算法变换结果作为 MAC 校验和				

发送序列计数器	数据	MAC 校验和	SW1	SW2	添补字节
这些信息与密钥的算法变换结果作为密文传递					

5.3.4 明文方式

除上述三种安全数据交换的通信方式外，如果应用对数据传输的安全性、完整性以及对发送方的鉴别都没有要求，则可以采用明文通信方式。数据交换中的明文方式就是命令报文的数据域中和响应报文的数据域中是明文数据。



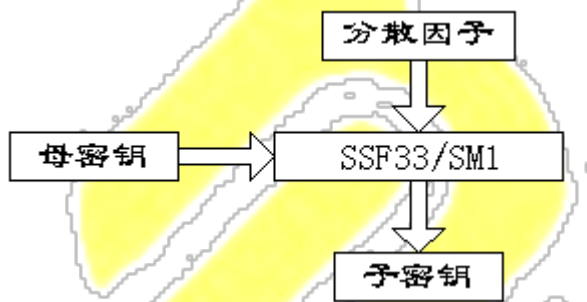
5.4 安全算法

5.4.1 SSF33/SM1 算法

5.4.1.1 算法介绍

SSF33 /SM1算法采用国家密码管理部门批准的分组密码算法（以下简称BCEA），其分组长度和密钥长度均为128 比特。

5.4.1.2 SSF33/SM1 密钥分散



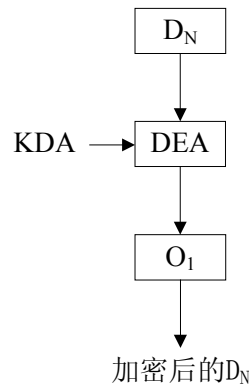
5.4.2 算法流程介绍

5.4.2.1 数据加密计算

数据加密技术如下所述：

第一步：用 L_D 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：将第一步中生成的数据块分解成 L_{Key} 字节数据块，标号为 D_1, D_2, D_3, D_4 等等。最后一个数据块长度有可能不足 L_{Key} 字节。



图例：

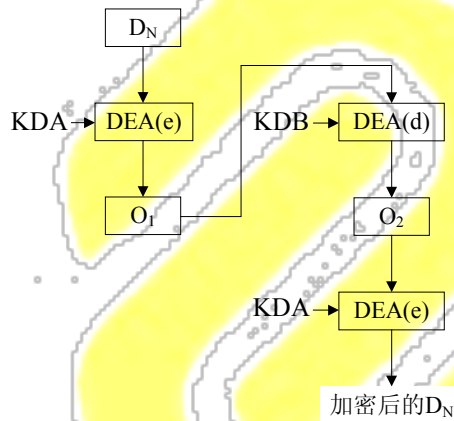
DEA = 数据密码算法（加密模式）

D = 数据块

O = 输出

KDA = 数据加密过程密钥 A

使用单长度数据密码算法密钥的数据加密



图例：

DEA(e) = 数据密码算法（加密模式）

D = 数据块

DEA(d) = 数据密码算法（解密模式）

KDA = 数据加密过程密钥 A

O = 输出

KDB = 数据加密过程密钥 B

使用双长度数据密码算法密钥的数据加密

第三步：如果最后（或唯一）的数据块长度等于 L_{Key} 字节，转入第四步；如果不足 L_{Key} 字节，在右边添加十六进制数字‘80’。如果长度已达 L_{Key} 字节，转入第四步；否则，在其右边添加 1 字节十六进制数字‘0’，直到长度达到 L_{Key} 字节。

第四步：每一个数据块使用中描述的数据加密过程密钥加密。

如果采用单长度数据加密的密码算法密钥，数据块的加密如所示（使用数据加密过程密钥 A 进行加密）。



如果采用双长度数据加密的数据密码算法密钥，则数据块的加密如所示（使用数据加密过程密钥 A 和 B 来进行加密）。

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（加密后的 D1，加密后的 D2，等等），并将结果数据块插入到命令数据域中。

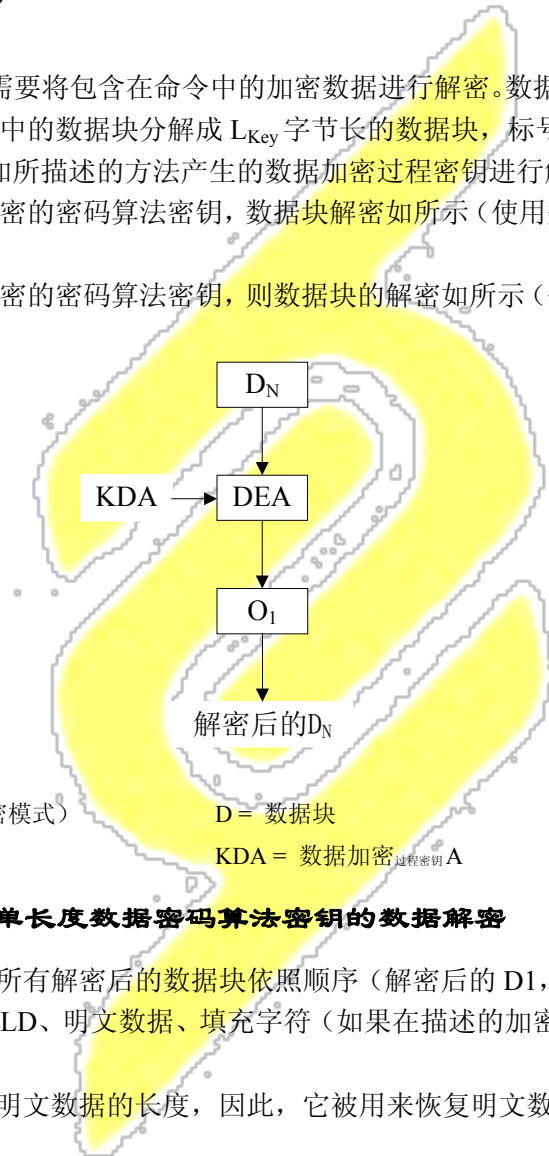
5.4.2.2 数据解密计算

卡片接收到命令之后，需要将包含在命令中的加密数据进行解密。数据解密的技术如下：

第一步：将命令数据域中的数据块分解成 L_{Key} 字节长的数据块，标号为 D1，D2，D3，D4 等等。每个数据块使用如所描述的方法产生的数据加密过程密钥进行解密。

如果采用单长度数据加密的密码算法密钥，数据块解密如所示（使用数据加密过程密钥 A 进行解密）。

如果采用双长度数据加密的密码算法密钥，则数据块的解密如所示（使用数据加密过程密钥 A 和 B 来进行解密）。



图例：

DEA = 数据密码算法（解密模式）

O = 输出

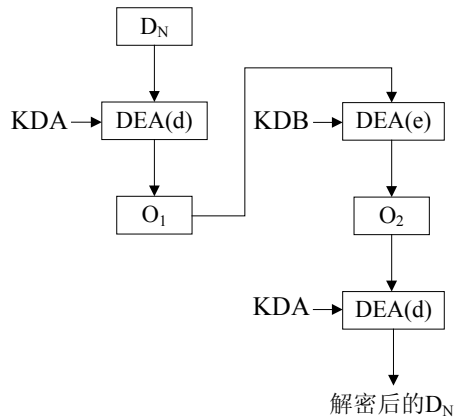
D = 数据块

KDA = 数据加密过程密钥 A

使用单长度数据密码算法密钥的数据解密

第二步：计算结束后，所有解密后的数据块依照顺序（解密后的 D1，解密后的 D2，等等）连接在一起。数据块由 LD、明文数据、填充字符（如果在描述的加密过程中增加的话）组成。

第三步：因为 LD 表示明文数据的长度，因此，它被用来恢复明文数据。



图例:

DEA(e) = 数据密码算法 (加密模式)

D = 数据块

DEA(d) = 数据密码算法 (解密模式)

KDA = 数据加密过程密钥 A

O = 输出

KDB = 数据加密过程密钥 B

使用双长度数据密码算法密钥的数据解密

5.4.2.3 MAC计算

按照如下的方式使用单重或三重 DEA 加密方式产生 MAC:

第一步: 取 L_{Key} 个字节的十六进制数字‘0’作为初始变量。

第二步: 按照顺序将以下数据连接在一起形成数据块:

——CLA, INS, P1, P2, $Lc^{1)}$;

——所有在《社会保障(个人)卡规范》第二部分应用规范中定义的数据;

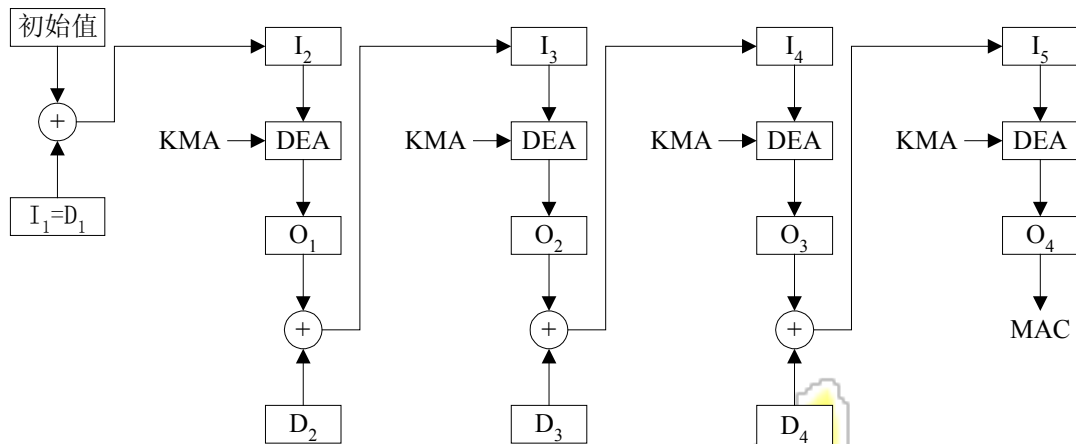
——在命令的数据域中(如果存在)包含明文或加密的数据(例如要更改个人密码,加密后的个人密码数据块放在命令数据域中传输)。

第三步: 将该数据块分成 L_{Key} 字节为单位的数据块, 标号为 D1, D2, D3, D4 等。最后的数据块有可能是 $1-L_{Key}$ 个字节。

第四步: 如果最后的数据块长度是 L_{Key} 字节的话, 则在其后加上十六进制数字‘80’和 $L_{Key}-1$ 个十六进制数字‘00’, 转到第五步。

如果最后的数据块长度不足 L_{Key} 字节, 则在其后加上十六进制数字‘80’, 如果达到 L_{Key} 字节长度, 则转入第五步; 否则在其后加入十六进制数字‘0’直到长度达到 L_{Key} 字节。

¹⁾ Lc 表示命令数据域后面 4 个字节 MAC 数据的长度, 例如: “APPLICATION BLOCK” 命令需要产生一个 MAC, 计算 MAC 的 Lc 的输入值是‘04’-‘FE’, 而不是‘00’, CLA 包括安全报文的标志(‘x4’)。



图例：

I = 输入

DEA = 数据密码算法（加密模式）

O = 输出

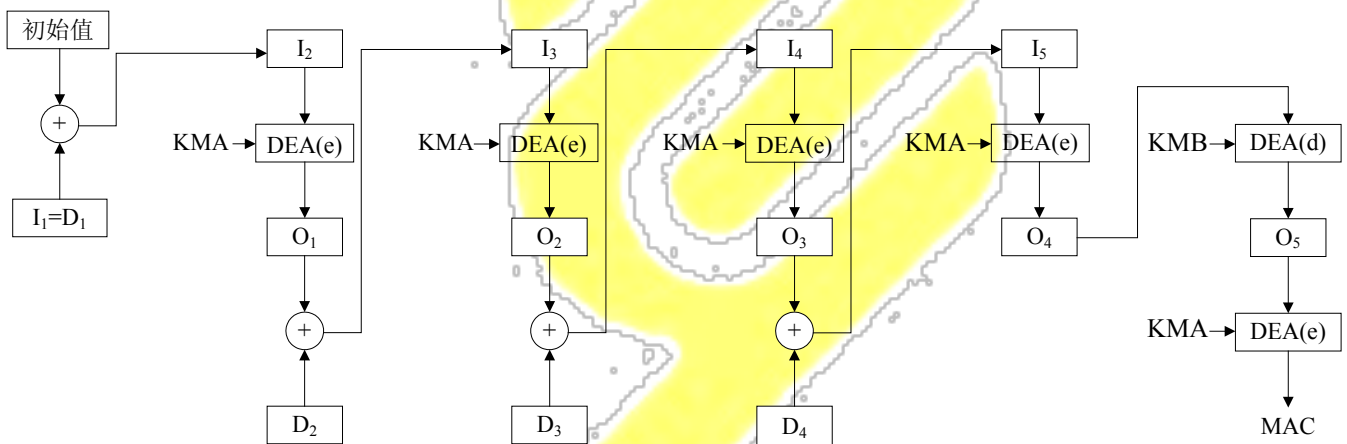
D = 数据块

KMA = MAC 过程密钥 A

+ = 异或运算

单长度数据密码算法密钥的 MAC 算法

第五步：对这些数据块使用 MAC 过程密钥进行加密，过程密钥按照**错误！未找到引用源。**描述的方式产生。如果安全报文传送支持单长度的 MAC 密码算法密钥，则依照**错误！未找到引用源。**的方式使用 MAC 过程密钥来产生 MAC（根据在第二步中产生的数据块长度的不同，有可能在计算中会多于或少于四步）。



图例：

I = 输入

DEA(e) = 数据密码算法（加密模式）

DEA(d) = 数据密码算法（解密模式）

O = 输出

D = 数据块

KMA = MAC 过程密钥 A

KMB = MAC 过程密钥 B

+ = 异或运算

双长度数据密码算法密钥的 MAC 算法

如果安全报文传送的处理支持双长度 MAC 密码算法密钥，则使用 MAC 过程密钥 A 和 B，MAC 的产生如中所示（根据第二步产生的数据块的长度，计算过程有可能多于或少于四步）。

第六步：最终得到从计算结果左侧取得的 4 字节长度的 MAC。



附录A

(规范性附录)

数据元解释

表 A.1 定义 JR/T 0025.2-2004 的本部分本部分所使用的数据元。

数据域	说明	来源	格式	长度 (字节)	值
算法标识 (DLK)	用来标识圈存交易的加密算法。	IC 卡终端	b	1	
算法标识 (DPK)	用来标识消费和取现交易的加密算法。	IC 卡终端	b	1	
算法标识 (DTK)	用来标识在交易中计算 TAC 使用的加密算法。	IC 卡终端	b	1	
算法标识 (DUK)	用来标识在修改透支限额交易中使用的加密算法。	IC 卡终端	b	1	
算法标识 (DULK)	用来标识在圈提交易中使用的加密算法。	IC 卡终端	b	1	
应用有效日期	该日期后卡应用终止。	IC 卡	cn CCYYMM DD	4	
应用标识符	用于标识一个应用，并符合 ISO 7816-5	IC 卡终端	b	5-16	
应用序列号	发卡方分配的一个数字，符合国家标准 GB/T14504-93	IC 卡	cn	10	
应用启用日期	指示应用生效日期。	IC 卡	cn CCYYMM DD	4	
应用类型标识	IC 卡支持的表示卡存在的应用类型 (ED 或 EP) 的标识。	IC 卡	cn	1	值: 01: 只有 ED 02: 只有 EP 03: ED 和 EP 都存在 所有其他值保留为将来使用。
应用版本号	表示 IC 卡当前使用的应用版本的一个数字。	IC 卡	b	1	
发卡方应用版本号	表示发卡方当前使用的应用版本的一个数字。	IC 卡	b	1	
本行职工标识	用来表示持卡人是否银行职员的一个标识。该标识可用来获得某种优惠。	IC 卡	n	1	
卡类型标识		IC 卡	cn	1	值: 00 - 个人卡 10 - 单位卡



山东华翼微电子技术有限责任公司

					所有其他值保留为将来使用
持卡人证件号码	用来标识持卡人。	IC 卡	an	32	

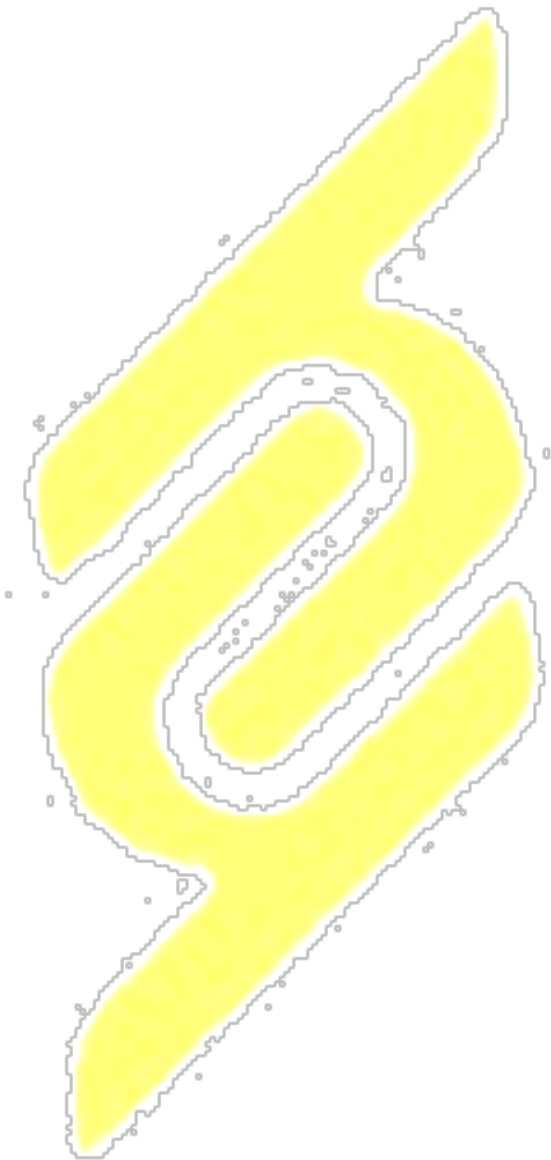




表 A.1(续)

数据域	说明	来源	格式	长度 (字节)	值
持卡人证件类型	用于区分持卡人证件类型而分配的值。	IC 卡	cn	1	值: 00: 身份证 01: 军官证 02: 护照 03: 入境证 (仅限香港/台湾居民使用) 04: 临时身份证 05: 其他
持卡人姓名	根据 ISO 7813 格式, 标识持卡人姓名。	IC 卡	an	20	
ED 余额	IC 卡中 ED 的当前余额。这个 ED 余额是卡上实际余额和透支限额之和。	IC 卡	b	4	
ED 脱机交易计数器	IC 卡中的一个计数器, 每发生一次 ED 消费/取款交易时就增加。	IC 卡	b	2	
ED 联机交易计数器	IC 卡中的一个计数器, 每发生一次 ED 圈存、圈提或修改透支限额交易时就增加。该计数器和主机同步, 并且可以在过程密钥的产生中使用。	IC 卡、	b	2	
EP 余额	IC 卡中 EP 的当前余额。	IC 卡	b	3	
EP 脱机交易计数器	IC 卡中的一个计数器, 每当 EP 消费交易发生就增加。	IC 卡	b	2	
EP 联机交易计数器	IC 卡中的一个计数器, 每次发生 EP 圈存交易时就增加。该计数器和主机同步, 并且可以在过程密钥的产生中使用。	IC 卡、 主机	b	2	
发卡方标识	用来唯一标识发卡方的一个数字	IC 卡	cn	8	
发卡方专用 FCI 数据	发卡方在其自己终端上用于特殊处理的专用数据	IC 卡	b	2	
密钥索引号	为了唯一标识在一个密钥版本中的密钥索	IC 卡 终端	cn	1	



山东华翼微电子技术有限责任公司

	引号而分配的一个数字。				
密钥版本号 (DLK)	用来唯一标识圈存交易的密钥版本。	IC 卡	b	1	
密钥版本号 (DPK)	用来唯一标识一个消费或取现交易的密钥版本。	IC 卡	b	1	
密钥版本号 (DTK)	用来唯一标识计算 TAC 所用的密钥版本。	IC 卡	b	1	

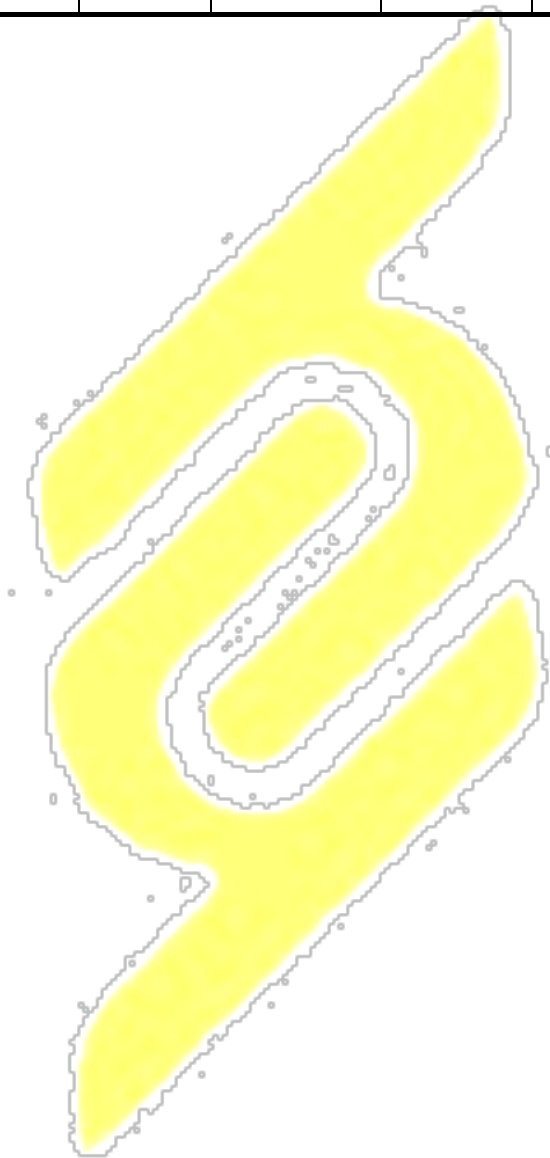




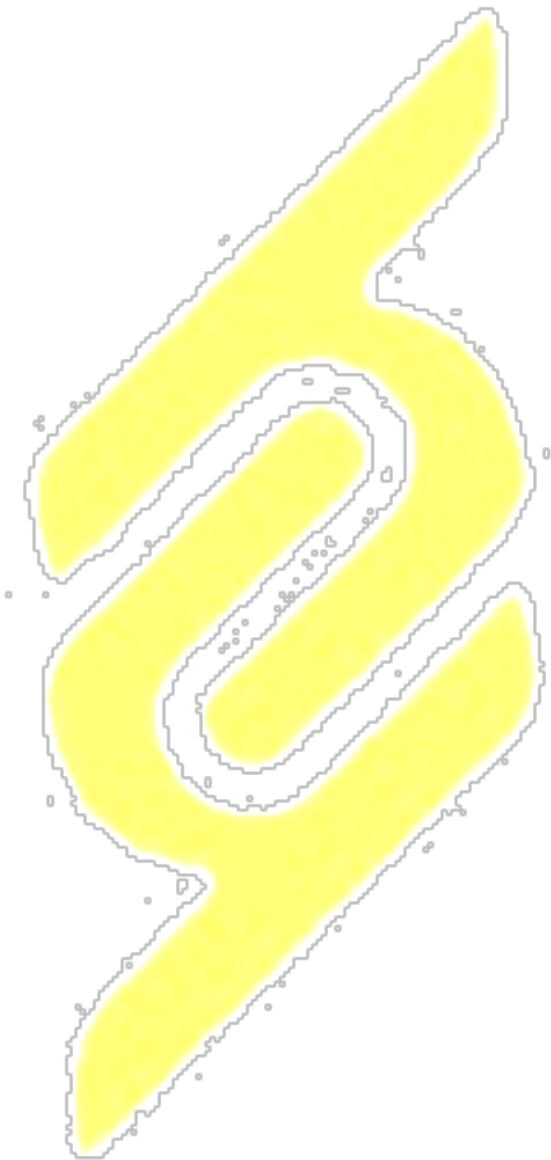
表 A.1(续)

数据域	说明	来源	格式	长度 (字节)	值
密钥版本号 (DUK)	用来唯一标识一个修改透支限额交易的密钥版本。	IC 卡	b	1	
密钥版本号 (DULK)	用来唯一标识一个圈提交易的密钥版本。	IC 卡	b	1	
透支限额	发卡方给持卡人指定的最大透支额度。	IC 卡	b	3	
PIN 尝试计数器	用来记录剩余的 PIN 尝试次数。	IC 卡	b	1	
PIN 尝试上限	发卡方给定的一个应用中允许 PIN 连续错误的最大次数。	IC 卡	b	1	该数据元素必须初始一个值
PSAM 标识符	用来唯一标识安装在终端中的 PSAM 的一个数字。	PSAM	b	4	
伪随机数 (IC 卡)	IC 卡随机产生的一个数字。	IC 卡	b	4	
PIN 参考值	IC 卡中存放的用来与持卡人输入的个人密码的值进行比较的值。	IC 卡	cn	2-6	
终端机编号	用来唯一标识商户终端的一个数字。	终端	cn	6	以下标识由交易确认： 第 1-2 数字：银行 第 3-6 数字：城市 第 7-12 数字：序号
终端交易计数器	终端里的一个计数器，每当交易发生就增加。	终端	b	4	
交易金额	当前交易的金额。	终端	B	4	
交易日期（发卡方）	交易发生日期。	发卡方	cn CCYYMM DD	4	
交易日期（终端）	交易发生日期。	终端	cn CCYYMM DD	4	
数据域	说明	来源	格式	长度 (字节)	值
交易时间	交易发生时间。	终端	cn	3	
交易类型标识 (TTI)	用于标识持卡人选择的交易类型（例如：圈存、圈提、消费等等）而分配的一个值。	终端、 IC 卡	cn	1	值： 01 - ED 圈存 02 - EP 圈存 03 - 圈提 04 - ED 取款



山东华翼微电子技术有限责任公司

					05 - ED 消费 06 - EP 消费 07 - ED 修改透支限额 08 - 信用消费
--	--	--	--	--	---

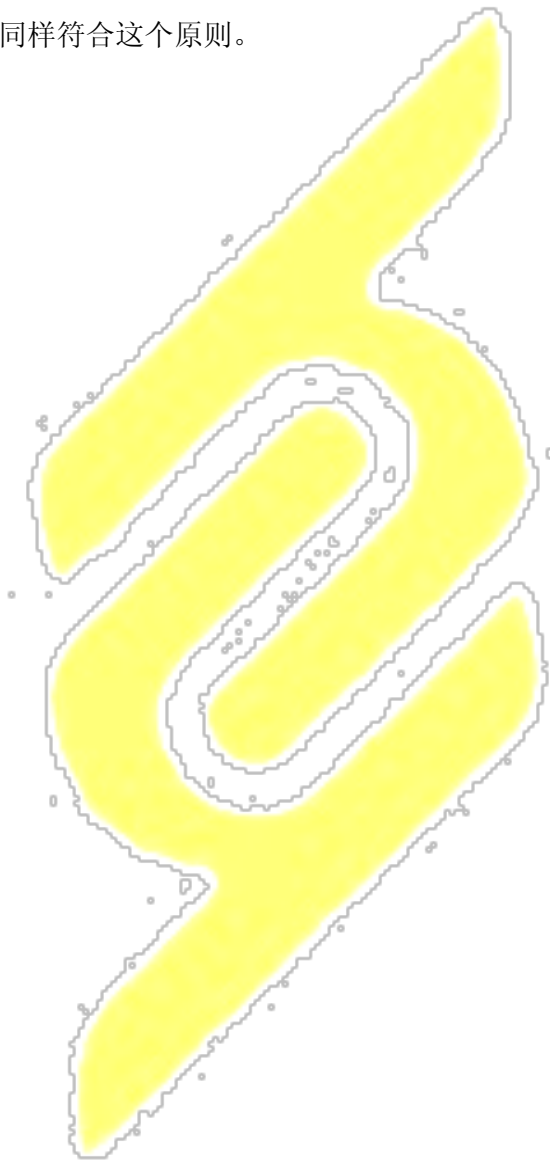




当为数据定义的长度超过实际数据长度，而位数没有占满时，补位规则如下：

- 格式 n 的数据元右靠齐并且左补十六进制 '0' 。
- 格式 cn 的数据元左靠齐并且右补十六进制 'F' 。
- 格式 an 的数据元左靠齐并且右补十六进制 '0' 。
- 格式 ans 的数据元左靠齐并且右补十六进制 '0' 。

当数据从一个实体移动到另一个时（例如：卡到终端），不管其内部如何存放，都是按照由高到低的顺序传送。数据的连接也同样符合这个原则。





附录B


(规范性附录)

ED/EP 应用的密钥关系


本附录描述了与 ED/EP 应用相关的设备实体之间的密钥关系，此处还描述了 IC 卡密钥的推导方法和过程密钥的产生方法

以下描述的所有密钥均为双倍长 DEA 密钥（128 比特长）。为确保密钥的安全，密钥的产生和存放都应由一个专用的安全模块来处理。下表概述了支持 ED 和 EP 应用的主机、IC 卡、POS 设备之间的密钥关系。

B1. 密钥关系表

 IC卡中存储的共用于电子存折和电子钱包应用的密钥

密钥	发卡方	IC 卡	POS (PSAM)
用于消费/取现交易的密钥	消费主密钥 (MPK)	消费子密钥 (DPK)，由 MPK 用应用序列号推导获得。	消费主密钥(MPK)
用于圈存交易的密钥	圈存主密钥 (MLK)	圈存子密钥 (DLK)，由 MLK 用应用序列号推导获得。	N/A
消费/取现交易中用于产生 TAC 的密钥	TAC 主密钥 (MTK)	TAC 子密钥 (DTK)，由 MTK 用应用序列号推导获得。	N/A
用于解锁 PIN 的密钥	PIN 解锁主密钥 (MPUK)	PIN 解锁子密钥(DPUK)，由 MPUK 用应用序列号推导获得。	由发卡方考虑决定
用于重装 PIN 的密钥	PIN 重装主密钥 (MRPK)	PIN 重装子密钥(DRPK)，由 MRPK 用应用序列号推导获得。	N/A
用于应用维护功能的密钥	应用主控密钥 (MAMK)	应用主控子密钥 (DAMK)，由 MAMK 用应用序列号推导获得。	N/A

 IC卡中用于电子存折应用的密钥

密钥	发卡方	IC 卡	POS (PSAM)
用于圈提交交易的密钥	圈提主密钥 (MULK)	圈提子密钥 (DULK)，由 MULK 用应用序列号推导获得。	N/A
用于修改透支限额交易的密钥	修改主密钥 (MUK)	子修改（透支限额）密钥 (DUK)，由 MUK 用应用序列号推导获得。	N/A

B2 子密钥推导方法

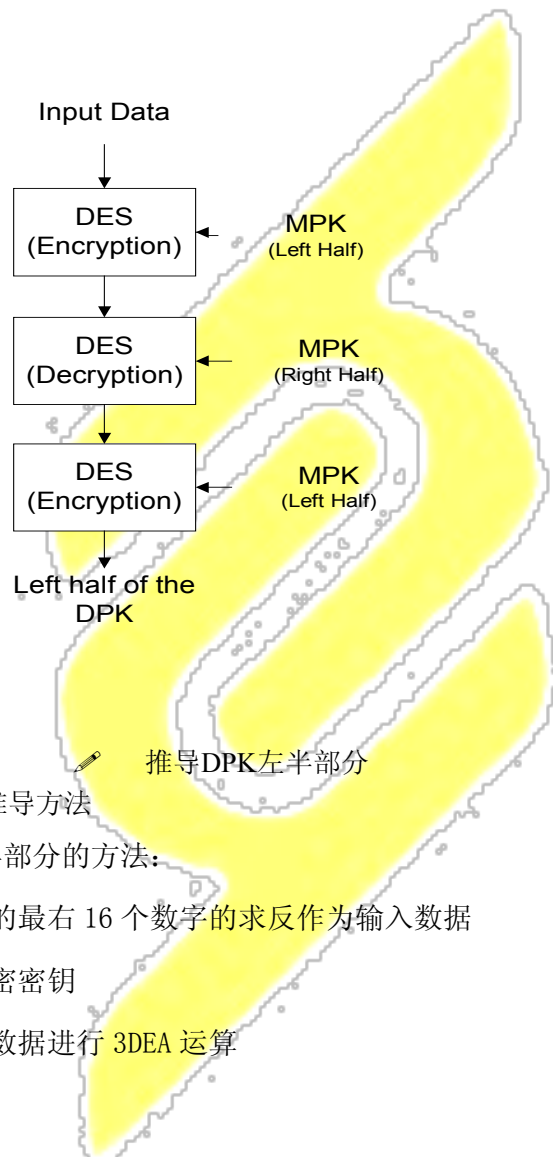


本节描述了 IC 卡中密钥的推导方法。图 B. 1 和图 B. 2 描述了 DPK 推导的过程。

B2.1 DPK左半部分的推导方法

推导双倍长 DPK 左半部分的方法：

- 将应用序列号的最右 16 个数字作为输入数据
- 将 MPK 作为加密密钥
- 用 MPK 对输入数据进行 3DEA 运算

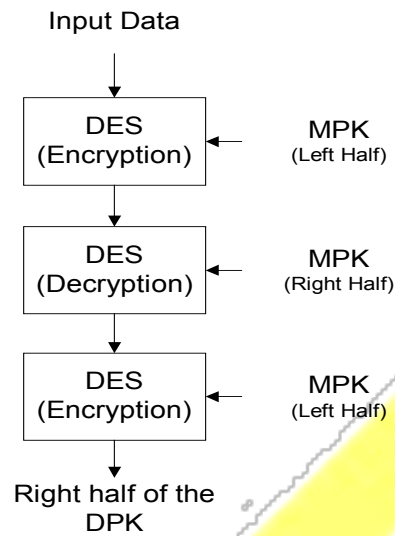


推导DPK左半部分

B2.2 DPK右半部分的推导方法

推导双倍长 DPK 右半部分的方法：

- 将应用序列号的最右 16 个数字的求反作为输入数据
- 将 MPK 作为加密密钥
- 用 MPK 对输入数据进行 3DEA 运算



推导DPK右半部分

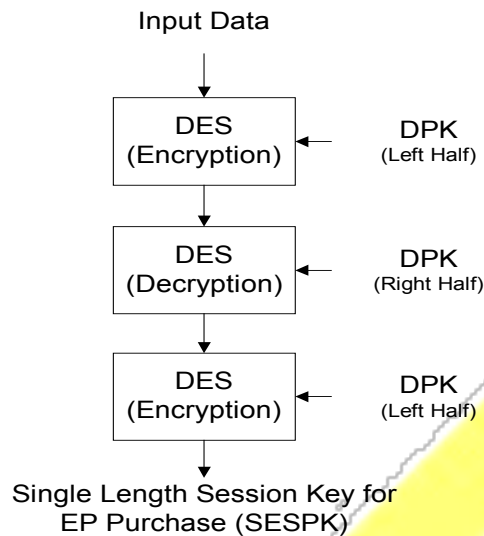
图 B.1 和图 B.2 描述的方法同样适用于 ED 的消费/取现、圈存和圈提、修改等子密钥的推导，及 EP 的消费和圈存子密钥的推导。

B3. 过程密钥的产生

过程密钥是在交易过程中用可变数据产生的单倍长密钥。

过程密钥产生后只能在某过程/交易中使用一次。

图 B.3 描述了 EP 进行消费交易时产生过程密钥的机制。这方法也用于不同交易类型的过程密钥的产生，但输入的数据取决于不同的交易类型。



过程密钥的产生

B4. MAC/TAC的计算

MAC/TAC 的产生使用以下单倍长 DEA 算法：

第一步：将一个 8 个字节长的初始值（Initial Vector）设定为 16 进制的‘0x 00 00 00 00 00 00 00 00’。

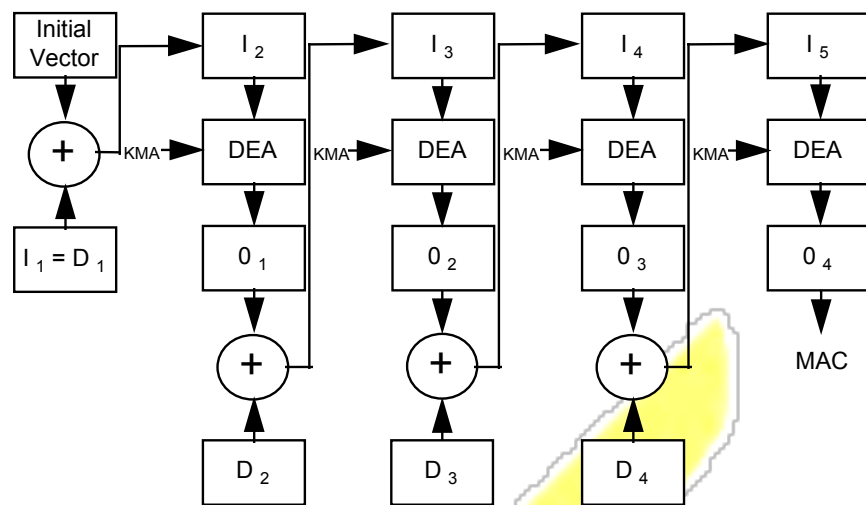
第二步：将所有的输入数据按指定顺序连接成一个数据块。

第三步：将连接成的数据块分割为 8 字节长的数据块组，标识为 D1, D2, D3, D4 等等。分割到最后，余下的字节组成一个长度小于等于 8 字节的最后一块数据块。

第四步：如果最后一个数据块长度为 8 字节，则在此数据块后附加一个 8 字节长的数据块，附加的数据块为：16 进制的‘0x 80 00 00 00 00 00 00 00’。如果最后一个数据块长度小于 8 字节，则该数据块的最后填补一个值为 16 进制 ‘0x80’的字节。如果填补之后的数据块长度等于 8 字节，则跳至第五步。如果填补之后的数据块长度仍小于 8 字节，则在数据块后填补 16 进制‘0x00’的字节至数据块长度为 8 字节。

第五步：MAC 的产生是通过上述方法产生的数据块组，由过程密钥进行加密运算，过程密钥的产生方法见 图 B-3。TAC 的产生是通过上述方法产生的数据块组，由 DTK 密钥左右 8 位字节进行异或运算的结果进行加密运算。MAC 或 TAC 的算法见图 B-4 描述。

第六步：最终值的左 4 字节为 MAC 或 TAC。



Legend:

I = Input

DEA = Data Encryption Algorithm
(encipherment mode)

O = Output

D = Data block

KMA = MAC Session Key A

+ = Exclusive-OR



MAC和TAC的单倍长DEA密钥算法



附录C

Cos基本数据文件及内部数据元

表C.1 ED和EP应用的公共应用基本数据文件

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

表C.2 ED和EP应用的持卡人基本数据文件

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

表C.3 内部数据元

数据元	长度
ED 余额	4
ED 脱机交易序号	2
ED 联机交易序号	2
透支限额	3
EP 余额	3
EP 脱机交易序号	2
EP 联机交易序号	2
密钥版本号 (DPK)	1
密钥版本号 (DTK)	1
密钥版本号 (DLK)	1
密钥版本号 (DULK)	1



密钥版本号 (DUK)	1
算法标识 (DPK)	1
算法标识(DTK)	1
算法标识(DLK)	1
算法标识(DULK)	1
算法标识(DUK)	1

表C.4 IC卡交易明细文件

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 2
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
17-20	交易日期 (终端)	4
21-23	交易时间 (终端)	3

这个文件必须能够容纳至少十条消费、取款、圈存、圈提交易记录。

交易明细必须允许卡对其循环修改。循环文件的结构应符合 ISO/IEC CD7816-4。

对明细中所有数据元的修改必须考虑数据完整性和安全要求。



附录D

类别	SW1 SW2	含义
正常类	90 00	命令正确完成
	61 XX	可发 Get Response 命令从卡获取 xx 个字节的返回数据(xx 作为 Le 参数)
警告类	62 81	数据可能出错
	62 83	选择的文件无效
	62 84	FCI 格式与 P2 指定不符
错误类	63 CX	验证失败, 还可试 X 次
	65 81	写 EEPROM 操作失败
	67 00	Lc/Le 不正确, Lc 域为空
	68 82	不支持安全报文
	69 00	CLA 与 SM 保护规定不符, 不能处理
	69 01	命令不接受(无效状态)
	69 81	命令 与文件结构不相符, 当前文件非所需文件
	69 82	不满足安全条件
	69 83	密钥锁定 (算法锁定) 鉴别方法锁定
	69 84	引用数据无效, 随机数无效
	69 85	不满足使用条件; 应用被锁定; 应用未选择; 余额上溢
	69 86	不满足命令执行的条件, 当前文件不是 EF 文件或不是所需 EF 文件
	69 87	安全报文数据项丢失, MAC 丢失
	69 88	安全报文数据项不正确, MAC 不正确
	6A 80	数据域参数不正确
	6A 81	不支持该功能, 卡中无 MF, 卡被锁定, 应用锁定
	6A 82	未找到文件, 文件标识相重, SFI 不正确
	6A 83	未找到记录
	6A 84	文件空间不足
	6A 85	LC 与 TLV 结构不符
	6A 86	参数 P1 或 P2 不正确
	6A 88	未找到引用数据 密钥未找到
	6B 00	参数错(偏移地址超出了 EF)
	6C XX	Le 不正确, 实际长度应为 xx
	6D 00	INS 不正确
	6E 00	无效的 CLA
	6F 00	数据无效
	93 02	MAC 无效
	93 03	应用已被永久锁定, 卡片锁定



94 01	金额不足
94 02	交易计数器达到最大值
94 03	密钥未找到(索引不支持)
94 06	所需 MAC(或/和 TAC)不可用

