凌科芯安 LKCOS V2.1

参考手册

凌科芯安科技（北京）有限公司

目　录

声明

1. 引言

1.1. 编写目的

凌科芯安 CPU 卡配合凌科芯安自主开发的 LKCOS，支持金融环境，适用于金融领域中的应用。通过此用户手册可以帮助用户了解凌科芯安 CPU 卡的性能，熟悉使用凌科芯安 CPU 卡，配合应用的开发。

此用户手册适用于利用凌科芯安 CPU 卡进行应用设计与开发的人员使用。

1.2. 内容概述

本手册各部分内容包括：

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

1.3. 定义

- 接口设备　Interface Device
  终端上插入 IC 卡的部分，包括其中的机械和电气部分。
- 终端　Terminal
  为完成交易而在交易点安装的设备，用于同 IC 卡的连接。
- 命令　Command
  终端向 IC 卡发出的一条信息，该信息启动一个操作或一个应答。
- 响应　Response

IC 卡处理完成收到的命令报文后，返回给终端的报文。

- 报文　Message
  由终端向卡或卡向终端发出的，不含传输控制字符的字节串。
- 明文　Plaintext
  没有加密的信息。
- 密文　Ciphertext
  通过密码系统产生的不可理解的文字或信号。
- 密钥　Key
  控制加密转换操作的符号序列。
- 加密算法　Cryptographic Algorithm
  为了隐藏或揭露信息内容而变换数据的算法。
- 认证机构　Certification Authority
  利用公开密钥和其他相关数据为所有者提供可靠校验的第三方机构。
- 对称加密技术　Symmetric Cryptographic Technique
  发送方和接收方使用相同保密密钥进行数据变换的加密技术。
- DES 算法
  DES 是一个对称算法，加密和解密用的是同一算法。DES 的安全性依赖于所用的密钥。
- 保密密钥　Secret Key
  对称加密技术中仅供指定实体所用的密钥。
- 数据完整性　Data Integrity
  数据不受未经许可的方法变更或破坏的属性。
- 电子钱包　Electronic Purse
  一种为方便持卡人进行小额消费而设计的 IC 卡应用，它支持圈存、消费等交易。除圈存外，使用电子钱包进行的其他交易均不记录明细，且均无需提交个人密码（PIN）。
- 电子存折　Electronic Deposit
  一种为持卡人进行消费、取现等交易而设计的使用个人密码（PIN）保护的金融 IC 卡应用，它支持圈存、圈提、消费、取现等交易。
- 圈存　Load
  持卡人将其在银行相应账户上的资金划转到电子存折或电子钱包中。
- 圈提　Unload
  持卡人将其在电子存折中的部分或全部资金划回到其在银行的相应账户上。

1.4. 缩略语与符号

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

ans	字母数字及特殊字符型（Alphanumeric Special）
APDU	应用协议数据单元（Application Protocol Data Unit）
ATR	复位应答（Answer to Reset）
b	二进制（Binary）
CLA	命令类别（Chip Card Payment Service）
CLK	时钟（Clock）
cn	压缩数字（Compressed Numeric）
DDF	目录数据文件（Directory Definition File）
DF	专用文件（Dedicated File）
DIR	目录（Directory）
EF	基本文件（Elementary File）
FCI	文件控制信息（File Control Information）
f	频率（Frequency）
GND	地(Ground)
IFS	信息域（Information Field）
INS	命令报文的指令字节（Instruction Byte of Command Message）
I/O	输入/输出（Input/Output）
Lc	终端发出的命令数据的实际长度（Exatct Length of Data Sent）
Le	响应数据中的最大期望长度（Maximum Length of Data Expected）
MAC	报文鉴别代码（Message Authentication Code）
MF	主控文件（Mater File）
N	数字型（Numeric）
O	可选型（Optional）
P1	参数 1（Parameter 1）
P2	参数 2（Parameter 2）
P3	参数 3（Parameter 3）
PIN	个人密码（Personal Identification Number）
RFU	保留为将来所用（Reserved for Future Use）
SW1	状态码 1（Status Word One）
SW2	状态码 2（Status Word Two）
TLV	标签、长度、值（Tag Length Value）
TAC	交易验证码（Transaction Authorization Cryptogram）
VCC	电源电压（Supply Voltage）
V_{PP}	Vpp 触点上的测量电压（Programming Voltage Message VCC Contact）

1.5. 参考资料

- ISO 7816-1: Identification cards - Integrated circuit(s) cards with contacts – Physical characteristics-1987/07/01
- ISO 7816-2: Identification cards - Integrated circuit(s) cards with contacts – Dimensions and location of the contacts-1998/05/15
- ISO 7816-3: Identification cards - Integrated circuit(s) cards with contacts – Electronic signals and transmission protocols-1989
- ISO 7816-4: Identification cards - Integrated circuit(s) cards with contacts – Inter-industry commands for interchange-1994/07/08
- ISO 7816-5: Identification cards - Integrated circuit(s) cards with contacts – Numbering system and registration procedure for application identifiers-1992/09/24
- ISO 7816-6: Identification cards - Integrated circuit(s) cards with contacts – Inter-industry data elements-1994/07/08
- EMV2000 Integrated Circuit Card Specification for Payment System
- EMV2000 Integrated Circuit Card Application Specification for Payment System
- 《中国金融集成电路（IC）卡规范 2.0》

2. 功能介绍

LKCOS 是智能卡的操作系统，主要功能是控制智能卡和外界的信息交换，管理智能卡内的存储器并在卡内部完成各种命令的处理。根据接口设备与卡之间的命令处理过程，LKCOS 大致可分为四个功能模块：即传输管理器、安全管理器、应用管理器和文件管理器。

2.1. 传输管理

LKCOS 支持 ISO7816 中规定的 T=0 传输协议。T=0 通讯协议是异步半双工字符传输协议，数据以字符的形式按照规定的时间周期进行传输。负责终端和卡片之间的数据传输。

2.2. 安全管理

安全管理是对 CPU 卡中的数据进行安全控制及管理，它具体可分为两种功能：一是安

全传输功能，二是对内部安全数据的控制管理。

（1）在卡与外界进行数据传输时，若以明文方式传输，数据有可能被劫获或篡改。为防止这种情况，提供了线路保护功能，主要通过以下两种方式实现：一是对传输的数据进行加密，数据以密文方式传输。二是对传输的数据附加安全报文 MAC 码，接收方首先对传输的数据进行 MAC 码校验，以此来确认数据在传输过程中的完整性并对发送方进行认证。

LKCOS 具有线路保护功能。写入或修改密钥时，可采用密文方式；写入或修改二进制文件，可采用安全报文方式。用户可以根据应用的具体要求，灵活地使用线路保护功能。

（2）内部安全数据的控制管理包括对卡中文件访问权限的控制和密钥的管理二方面。考虑到密钥的绝对安全性能，LKCOS 对于内部用于安全认证和数据加密的各种密钥实行安全控制管理。一旦密钥在卡中建立，只有在授权的情况下，才允许内部使用，CPU 卡之外绝不会被泄露出来。

2.3. 应用管理

应用管理对外部而言是指卡片如何管理不同的应用，也就是说，卡片是多应用卡片还是单应用卡片。单应用卡片相对比较简单，内部只提供单个 DF 文件，并且只有一套安全管理系统和应用数据。而多应用卡片就比较复杂，卡中可以存在多个 DF 文件，每个 DF 文件都有自己的专有 EF 数据文件和密钥系统，每个应用之间相互独立，具有“防火墙”功能。LKCOS 支持一卡多应用，可以建立一个 DF 文件当作一个应用，也可以将多个 DF 文件组合在一起看作一个应用。用户在使用的时候，可以根据情况来规划。应用管理对卡片内部来说指的是卡片是如何管理 DF 文件及其下属的 EF 数据文件，并且负责解释执行命令。命令是卡片提供给外部环境用来访问卡片数据的手段，外部只有通过命令才能访问卡片中的数据或对卡片进行相应的操作，通过卡片提供的命令就能判断卡片具有的功能。

2.4. 文件管理

在 CPU 卡中，数据都是以各种文件的形式进行存储，以目录的方式进行管理。文件管理器负责对所有文件的操作和访问，因此文件管理系统设计的好坏直接影响着卡片的使用效率和功能。

LKCOS 的文件管理遵循以下原则：

- 文件系统分三层结构即 MF-DF-EF。在选择某个文件之前必须先选择它的上一层文件，不允许跨层选择。卡片上电后自动选择 MF 文件。

- MF 建立之后，LKCOS 自动将整个 EEPROM 空间都分配给了它。只要 EEPROM 空间允许且满足增加权限要求，MF 下可任意增加新应用；只要 EEPROM 空间允许且满足增加权限要求，DF 下可任意增加基本文件。

- 对某个文件操作之前，必须先选择该文件；对于基本文件操作，可在命令中直接用短文件标识符指定该文件。

- 每个文件都有可以设置访问权限；文件的访问权限受该文件安全属性的控制。在 MF 和 DF 建立正常结束之前，安全条件不起作用。

3. 文件系统

本章介绍 LKCOS 的文件系统，包括文件组织结构、文件类型及文件的访问方式。

3.1. 文件名称和文件标识

3.1.1. 文件名称

文件名称是 DF 的名称，用于标识 DF，长度为 5-16 字节，卡中的 DF 可以用名称进行选择。对于 ADF 来说，ADF 的 DF 名称对应其应用标识。应用标识的长度为 5-16 字节，一般分为两部分，头 5 字节称为 RID(Registed ID)，RID 的设置必须由注册机构分配，包含国家代码、应用类别、应用提供商的标识号。后面的部分称为 PIX，长度为 0-11 字节，由应用提供商自行定义。

3.1.2. 文件标识 FID

文件标识符是文件的标识代码，为 2 字节长度，COS 可以通过 FID 来对应到相应的文件，同一目录下的文件标识符必须是唯一的。

3.1.3. 短文件标识符 SFI

短文件标识符由 5 个二进制位组成，可选择的最大短文件标识符为 31。如果文件需要用 SFI 进行选择，则建立文件的时候，需要为文件分配短文件标识符，取值范围为 1-31 之间。

3.2. 文件组织结构

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

文件系统分两个层次级别，分别是专有文件 DF 和基本文件 EF，最上层的 DF 又称为 MF，组成一个类似于 DOS 的层次结构。若要对文件系统中的某文件进行读、写操作，应先使用选择命令指定相应的 MF、DF 和 EF。

3.2.1. 主控文件(Master File , MF)

主控文件是整个文件系统的根，每张卡有且只有一个主控文件。它是在卡的个人化过程中首先被建立起来的，在卡的整个生命周期内一直存在并保持有效，可存储卡的公共数据信息并为各种应用服务。在物理上，主控文件占有的存储空间包括 MF 文件头的大小以及 MF 所管理的 EF 和 DF 的存储空间。

- IC 卡复位后，卡片自动选择 MF 为当前文件。
- 在金融环境下，MF 的文件名称是 1PAY.SYS.DDF01。

MF 文件头定义

数据域	*类型*	*FID*	*大小*	*建立权限*	*擦除权限*	*FCI-SFI*	*RFU*	*文件名*
长度	1	2	2	1	1	1	2	5-16
值	38	3F00	FFFF	XX	XX	XX	FFFF	“PAY.SYS.DDF01”

文件大小 FFFF，表示 MF 将会根据用户空间自动计算大小；

FCI-SFI，表示返回 FCI 的 EF 短文件标识符；

3.2.2. 专用文件(Dedicated File，DF)

在 MF 下针对不同的应用建立起来的一种文件，是位于 MF 之下的含有 EF 的一种文件结构（可看做文件目录），它存储了某个应用的全部数据以及与应用操作相关的安全数据，LKCOS 采用多级目录结构，即 MF 下只能有 DF，DF 下面也可以建立子 DF。

DF 文件头定义

数据域	*类型*	*FID*	*大小*	*建立权限*	*擦除权限*	*FCI-SFI*	*RFU*	*文件名*
长度	1	2	2	1	1	1	2	5-16
值	38	XXXX	XXXX	XX	XX	XX	FFFF	“PAY.SYS.DDF01”

FCI-SFI，表示返回 FCI 的 EF 短文件标识符；

3.2.3. 基本文件(Elementary File，EF)

基本文件存储了各种应用的数据和管理信息，它存在于 MF 或 DF 下。EF 从存储内容上分为两类：安全基本文件和工作基本文件。

安全基本文件(Key File)的内容包含用于用户识别和与加密有关的密钥数据(个人识别码、密钥等)，卡将利用这些数据进行安全管理。在每个 MF 或 DF 下，都必须存在一个 Key 文件，而且 Key 文件在 DF 建立之后应该首先被建立，安全基本文件的内容不可被读出，但可使用专门的指令来写入和修改。在 MF 和每个 DF 下只能建立一个安全基本文件，但 KEY 和 PIN 的类型须由用户写入密钥时指出。

工作基本文件(Elementary File)包含了应用的实际数据，其内容不被卡解释。在符合读、修改安全属性时，可对其内容进行读取、修改。工作文件的个数和大小受到 MF 或 DF 所拥有空间的限制。

工作基本文件包括 4 种基本结构：透明结构的二进制文件、线性结构的定长记录文件、变长记录文件、循环记录文件。

3.2.3.1. KEY 文件（密钥文件）

KEY 文件是存放密钥的文件，是一种变长记录结构的内部文件。KEY 文件头定义如下：

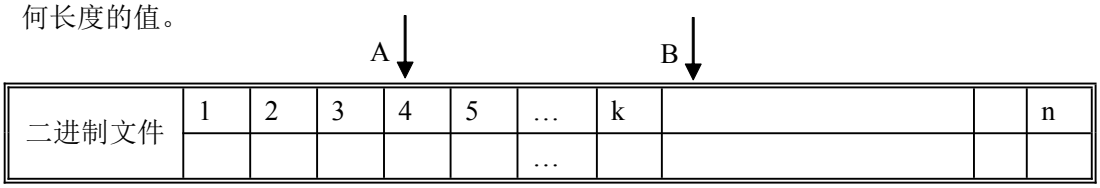
域	长度	描述
文件类型	1	3F
文件标识 FID	2	0000
文件大小	2	KEY 文件的大小
访问权限 1	1	保留 RFU
访问权限 2	1	增加密钥的权限
SFI	1	‘SFI
安全机制 KID	1	XX，用以增加加密钥时所使用的安全机制

KEY 文件具有以下特点：

- 每个 DF 下必须存在一个 KEY 文件；
- KEY 文件在每个 DF 先必须首先被建立；
- KEY 文件的 FID 固定为 0000；
- KEY 文件不可被选择，也不能被读出。

3.2.3.2. 二进制文件

二进制文件是普通以字节为单位访问的文件。可以从文件范围内任何一个字节开始访问任何长度的值。



可以文件内容范围内任意调整地址 A、B，访问 AB 区间(例如 4…k)的数据。

二进制文件头定义：

域	长度	描述

文件类型	1	28
文件标识 FID	2	XXXX
文件大小	2	定义文件体能够存储的字节数
访问权限 1	1	读权限
访问权限 2	1	写权限
SFI	1	‘XX’，指定当前文件的 SFI
安全机制 KID	1	XX

SFI 用以设定文件的短文件标识符

KID 标识文件的安全属性字节，具体定义如下：

	b7	b6	b5	b4	b3	b2	b1	b0	意义
安全属性	0	0							RFU
			MAC						MAC=1 表示写需要 MAC
				DES					DES=1 表示写需要加密
					X	X			读文件返回数据加密时使用的密钥标识符；KID 取反
							X	X	写文件返回数据加密时使用的密钥标识符；KID 取反

3.2.3.3. 定长记录文件

记录文件是以记录为访问单位的文件，可由多条记录组成，每条记录的长度是固定一致的。

记 录 号	记录内容
1	XX…XX

2	XX…XX
3	XX…XX
…	XX…XX
N	XX…XX

记录访问指定记录号，一次读出整条记录内容。

定长记录文件头定义如下：

域	长度	描述
文件类型	1	2A
文件标识 FID	2	XXXX
文件大小	2	字节 1：记录个数 字节 2：记录长度
访问权限 1	1	读权限
访问权限 2	1	写权限
SFI	1	‘XX’，指定当前文件的 SFI
安全机制 KID	1	XX

3.2.3.4. 变长记录文件

变长记录文件是以记录为访问单位的文件，可由多条记录组成，每条记录的长度可以是不一致的,每条记录是都是 TLV 结构。

记录号	记录内容
1	
…	
…	
N	

记录访问指定记录号，一次读出整条记录内容。

修改记录时，只能按照原有的记录长度修改。

域	长度	描述
文件类型	1	2C
文件标识 FID	2	XXXX
文件大小	2	XXXX
访问权限 1	1	读权限
访问权限 2	1	写权限
SFI	1	‘XX’，指定当前文件的 SFI
安全机制 KID	1	XX

3.2.3.5. 循环记录文件

循环记录文件是以记录为访问单位的文件，可由多条记录组成，每条记录的长度是固定一致的。记录访问指定记录号，一次读出整条记录内容。
最近写入的记录号为永远为记录 1
当记录写满后，又写入一条记录，则最旧的记录将被覆盖。

循环记录文件头定义：

域	长度	描述
文件类型	1	2E
文件标识 FID	2	XXXX
文件大小	2	字节 1：记录个数 字节 2：记录长度
访问权限 1	1	读权限
访问权限 2	1	写权限
SFI	1	‘XX’，指定当前文件的 SFI
安全机制 KID	1	XX

3.3. 文件的访问方式

3.3.1. 通过文件标识符（FID）访问

在选择文件时，只要指出 FID，COS 就可以找到相应的文件。

注：KEY 文件不能被选择

3.3.2. 通过短文件标识符（SFI）访问

在读写文件的时候，也可以直接在参数中输入 SFI 来选定文件，用这种方法操作文件的时候，不需要先选择再读写。

3.3.3. 通过 DF 文件名称进行访问

在选择 DF 文件的时候，可以直接输入 5-16 字节长度的文件名称来选择相应的 DF 文件。

4. 安全机制

4.1. 安全状态

安全状态是指卡当前所处的一种安全级别，有 16 种不同的安全级别。在卡内用一个 4 位的二进制来表示，值为 0-15，初始状态为 0。只有在当前目录下检验口令或外部认证成功后，安全状态寄存器的值才发生变化。

在以下情况下，DF 的安全状态寄存器复位为 0：

- 卡片复位后
- 选择 DF 后
- 当前 DF 下核对口令，或者外部认证命令失败后

4.2. 权限

在本文中提到的各种权限：建立权限、删除权限、读权限、写权限、增加权限等均属于权限的概念。

权限指对某个文件/密钥操作时，对应的安全状态寄存器的值必须符合某个条件才能进行操作。

COS 对于不同的文件/密钥涉及到的权限如下：

对象	权限
DF(MF)	建立/删除
安全文件	增加
二进制文件	读/写
定长记录文件	读/写
不定长记录文件	读/写
循环文件	读/写
密钥	使用/更改

文件的访问权限是在 Create File 时的文件参数中指定了；密钥的权限是在 Write Key 命令中 Key 的属性中指定的。

权限为一个字节，分为两部分：高 4 位 X 和低 4 位 Y 部分。

权限 ＝‘XY’：

X＞0 表示 DF 安全状态机 Z 必须满足 X ≥ Z ≥ Y

X＜Y ，表示没有此权限，禁止操作的意思。

例如：在创建 DF 时，设置 DF 的建立权限字节值为：

‘31’，表示 DF（局部）安全状态机 Z 必须满足 3 ≥ Z ≥ 1

也就是 Z＝1，2，3 均符合要求

‘33’， 表示 DF（局部）安全状态机 Z 必须满足 3 ≥ Z ≥ 3

也就是 Z＝3 才符合要求

‘13’， 表示没有权限，也就是不能在 DF 下建立文件

4.3. 数据交换模式

4.3.1. 明文模式

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

4.3.2. 加密模式

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

4.3.3. 校验模式

如果侧重于数据在传输中的完整性和对数据发送方进行认证，可以采用校验模式。校验模式就是对命令报文的所有内容或响应报文的所有内容使用一个算法进行加密得到一个 4 字节的校验码（MAC），然后把它放在命令报文或响应报文的数据域中发送。有关校验码的计算，请看下面 MAC 的计算一节。

4.3.4. 加密校验模式

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

4.4. 安全计算

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

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

4.4.1. DES 算法

4.4.1.1. DES 在金融环境中的安全管理

4.4.1.1.1. 密钥分散的计算方法

密钥分散通过分散因子产生子密钥。

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

推导 DK 左半部分的方法是：

第一步：将分散因子作为输入数据；

第二步：将 MK 作为加密密钥；

第三步：用 MK 对输入数据进行 3DEA 运算。

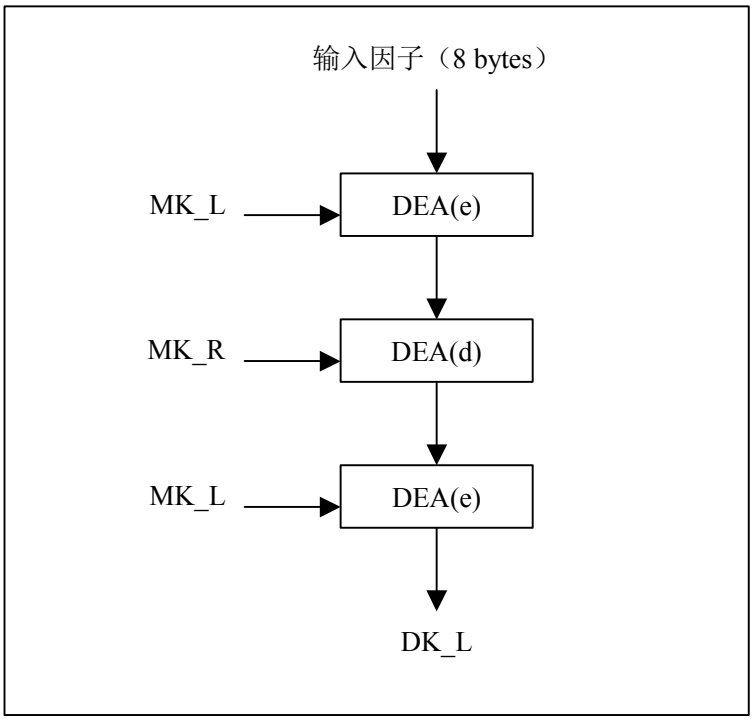


图 1 1 推导 DK 左半部分

推导 DK 右半部分的方法是：

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

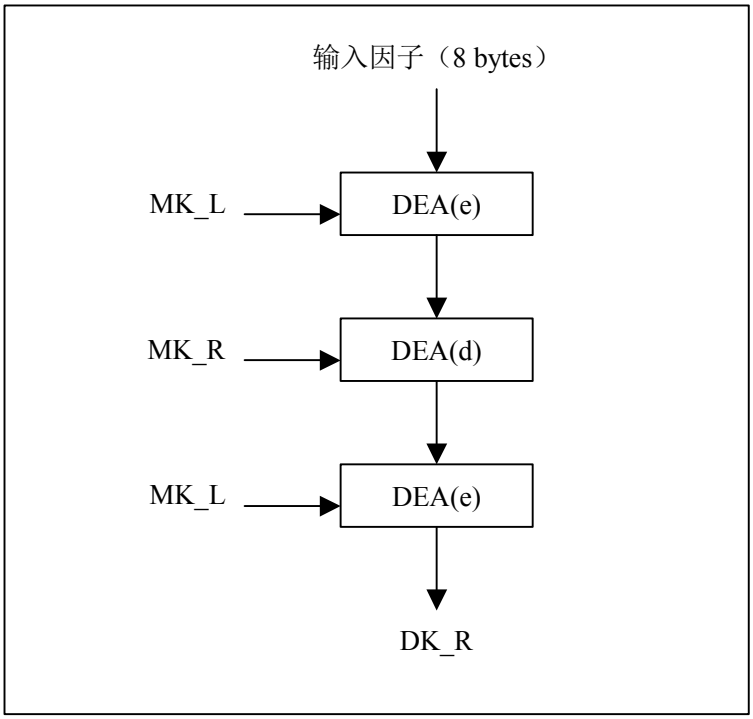


图 1 2　推导 DK 右半部分

4.4.1.1.2.　过程密钥的计算方法

4.4.1.1.2.1.　过程密钥的计算方法 1

该方法来源于 PBOC。

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

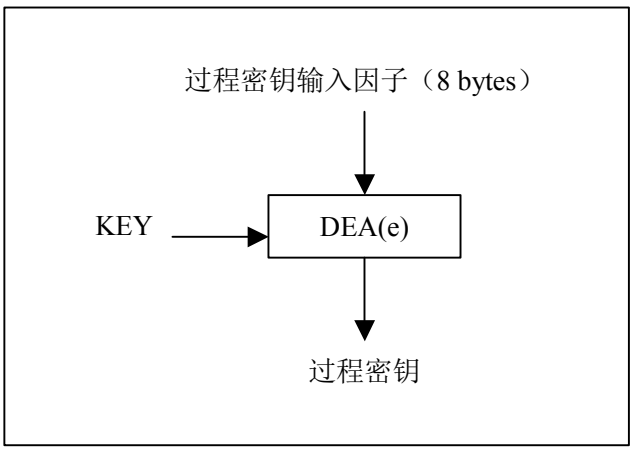


图 1 3 单倍长密钥产生过程密钥

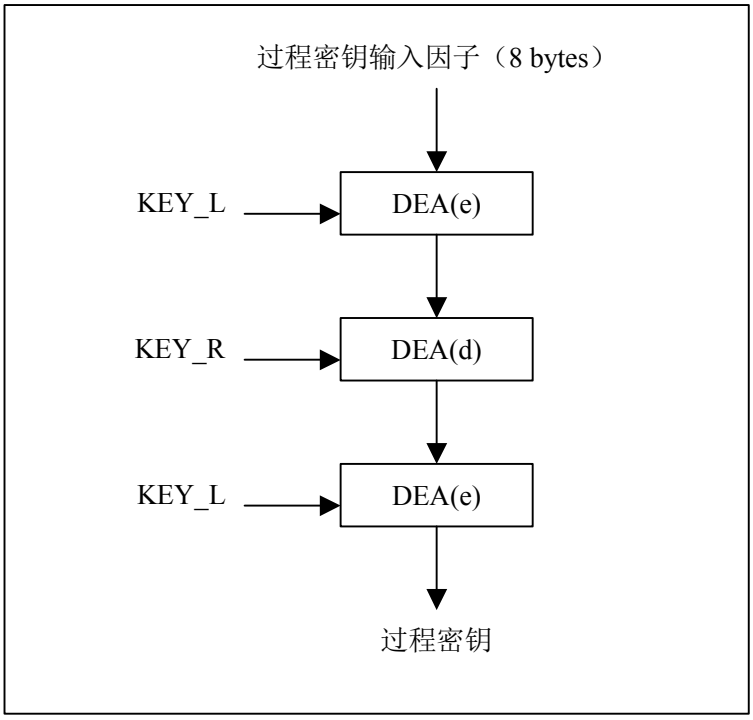


图 1 4 双倍长密钥产生过程密钥

4.4.1.1.2.2. 过程密钥的计算方法 2

该方法来源于 PBOC 标准。

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

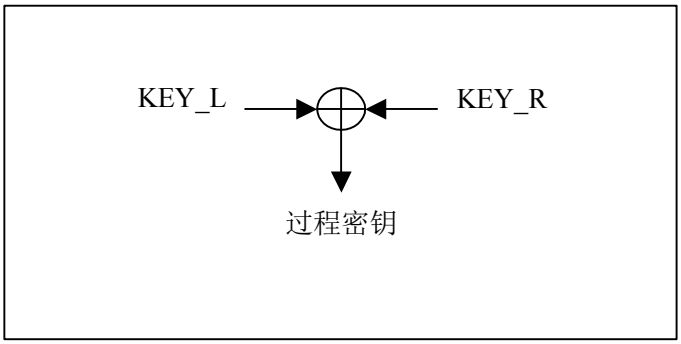


图 1 5　过程密钥产生

4.4.1.1.3.　鉴别数据的计算方法

该方法来源于 PBOC 标准。

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

按照如下方式使用 DEA 加密方式产生 MAC：

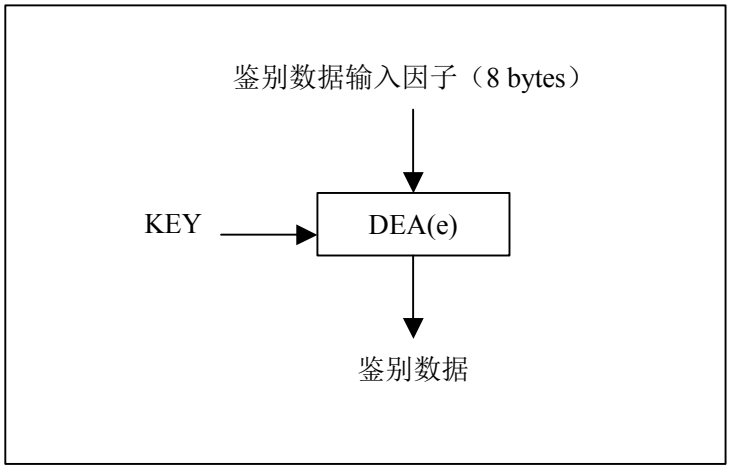


图 1 6　单倍长密钥的鉴别数据的计算

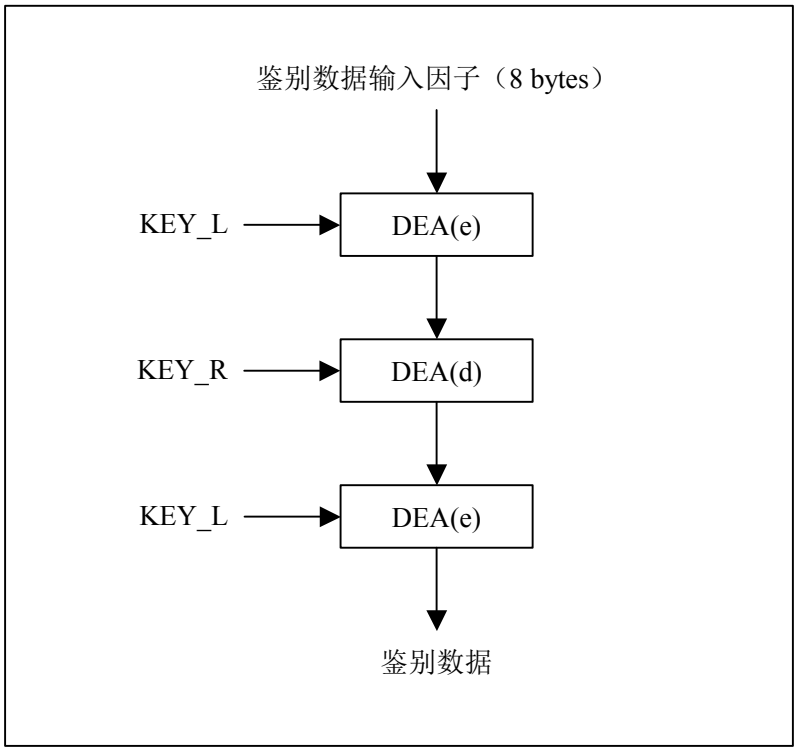


图 1-7　双倍长密钥的鉴别数据的计算

4.4.1.1.4.　MAC 的计算方法

4.4.1.1.4.1.　命令安全报文中的 MAC

该方法来源于 PBOC 标准。

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

按照如下方式使用 DEA 加密方式产生 MAC：

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

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

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

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

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

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

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

第六步： 最终取计算结果（高 4 字节）作为 MAC。

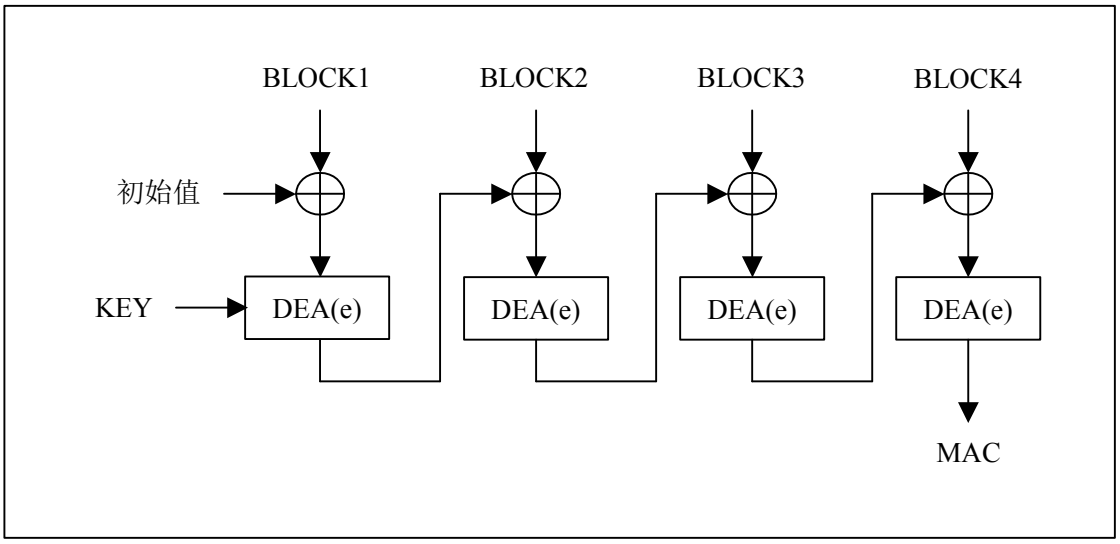


图 1 8 安全报文中单倍长密钥 MAC 计算

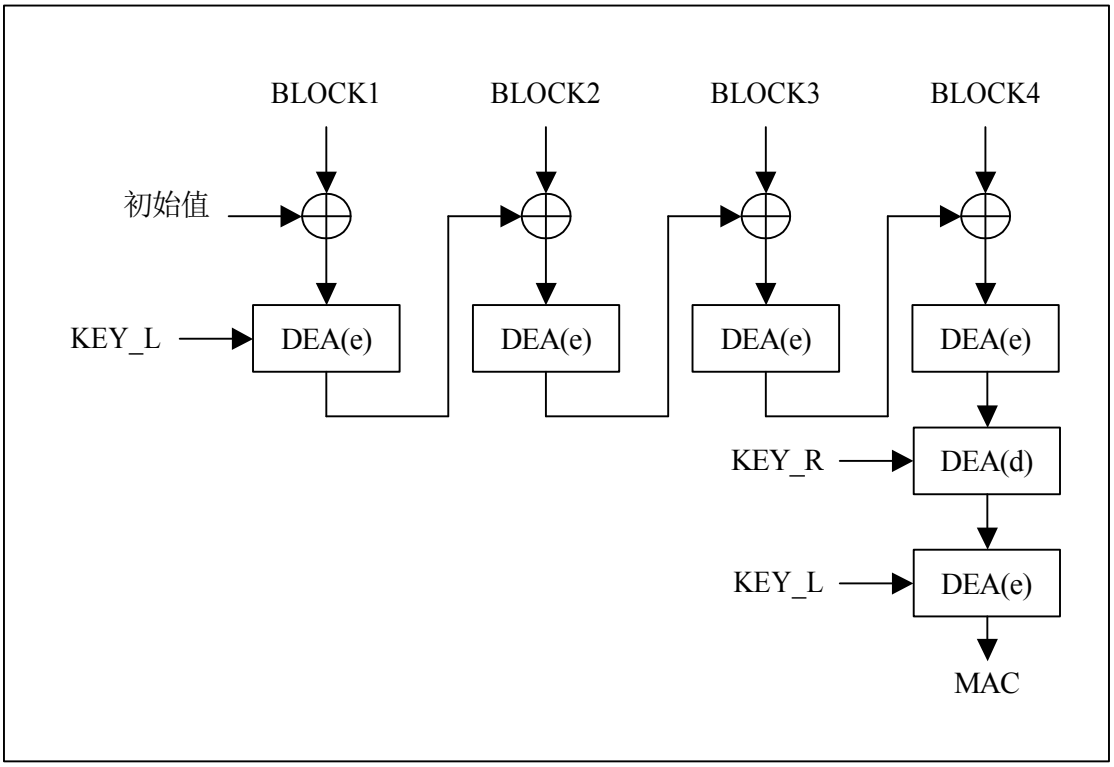


图 1 9 安全报文中双倍长密钥 MAC 算法

4.4.1.1.4.2. 交易中的 MAC

交易中的 MAC 计算使用此方法。计算方法分二步完成。先用指定密钥产生过程密钥（请参看过程密钥计算），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 1-10 所述的算法对这些数据块使用过程密钥（单倍长度）进行加密来产生 MAC。

第六步： 最终取计算结果（高 4 字节）作为 MAC。

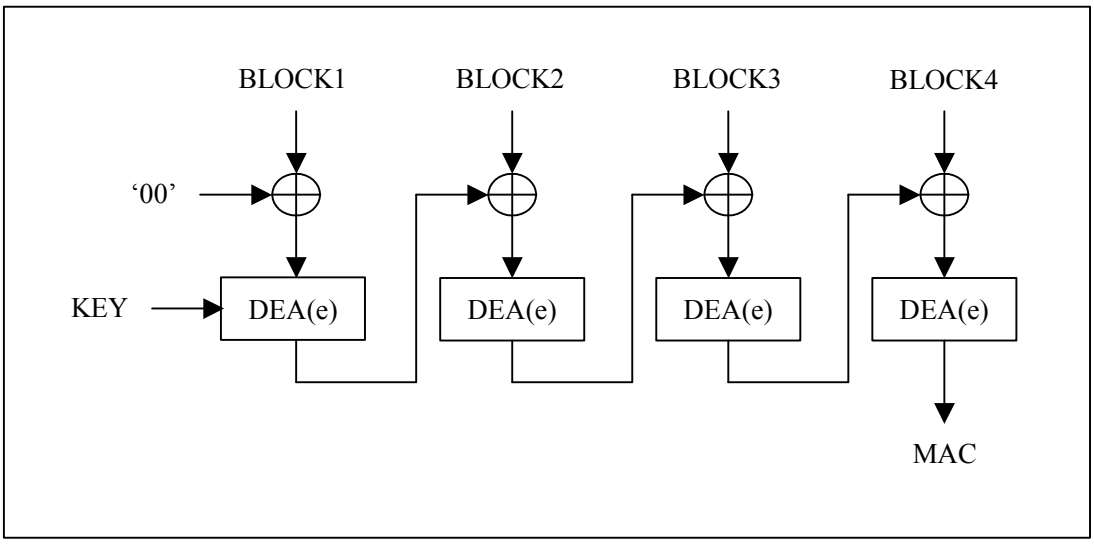


图 1 10 ED/EP 交易中的 MAC 算法

4.4.1.1.5. 数据加密的计算方法

按照如下方式对数据进行加密：

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

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

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

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

第五步： 计算结束后，所有加密后的数据块依照原顺序连接在一起。

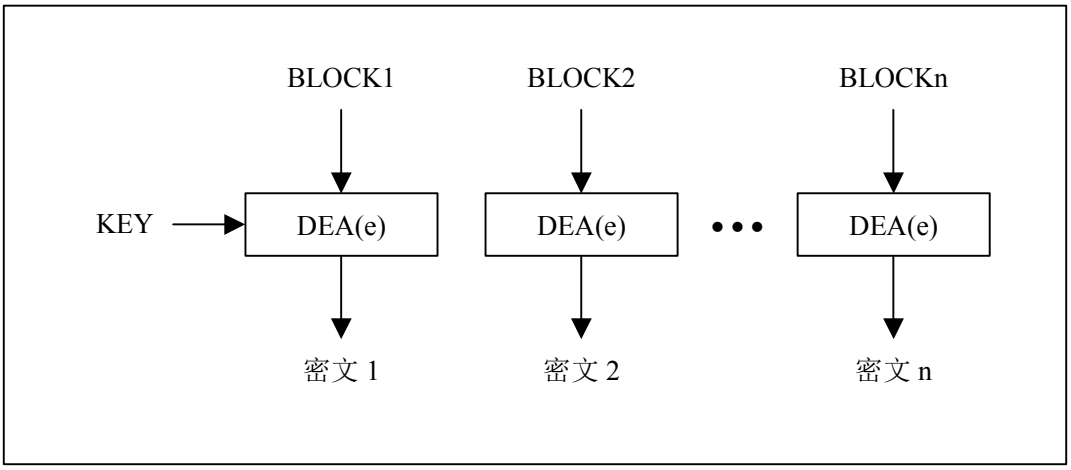


图 1 11 单倍长密钥 DEA 数据加密算法

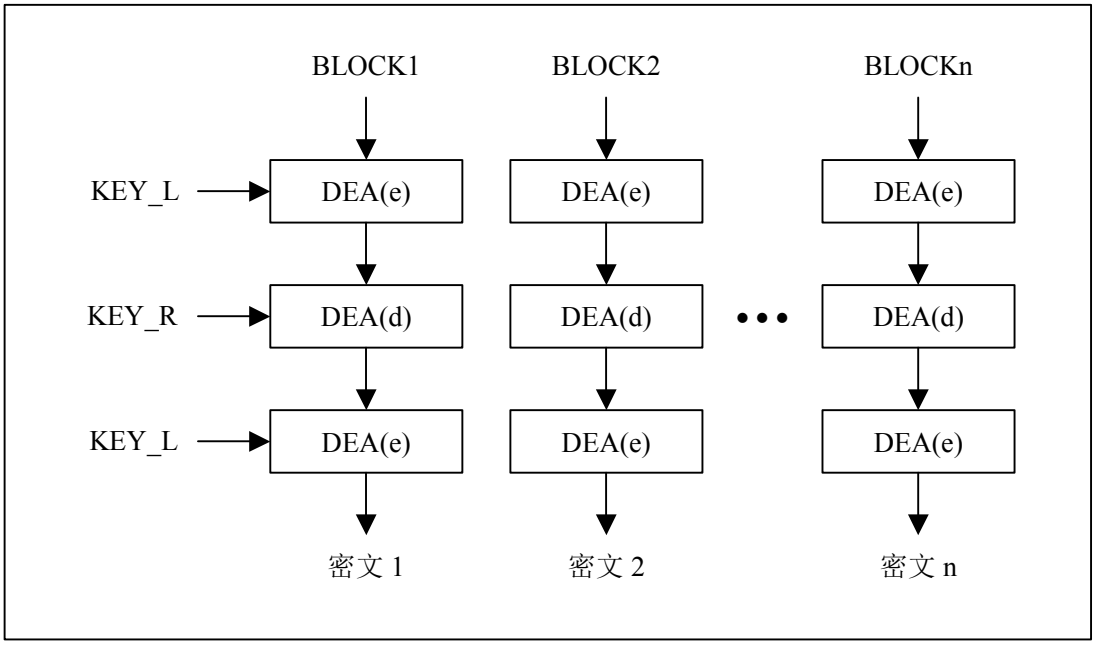


图 1 12 双倍长密钥 DEA 数据加密算法

4.4.1.1.6. 数据解密的计算方法

数据解密则采用相反的过程，如图 1-13 和图 1-14。

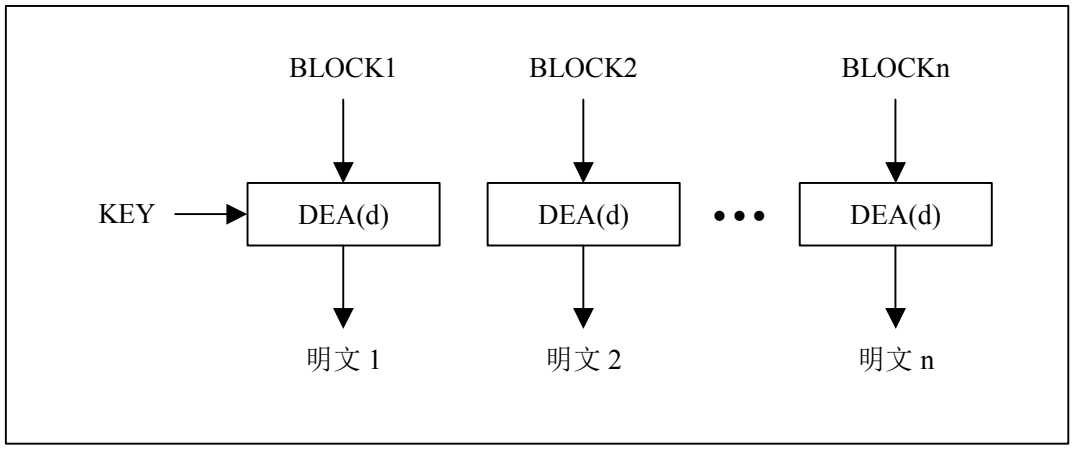


图 3-1 13 单倍长密钥 DEA 数据解密算法

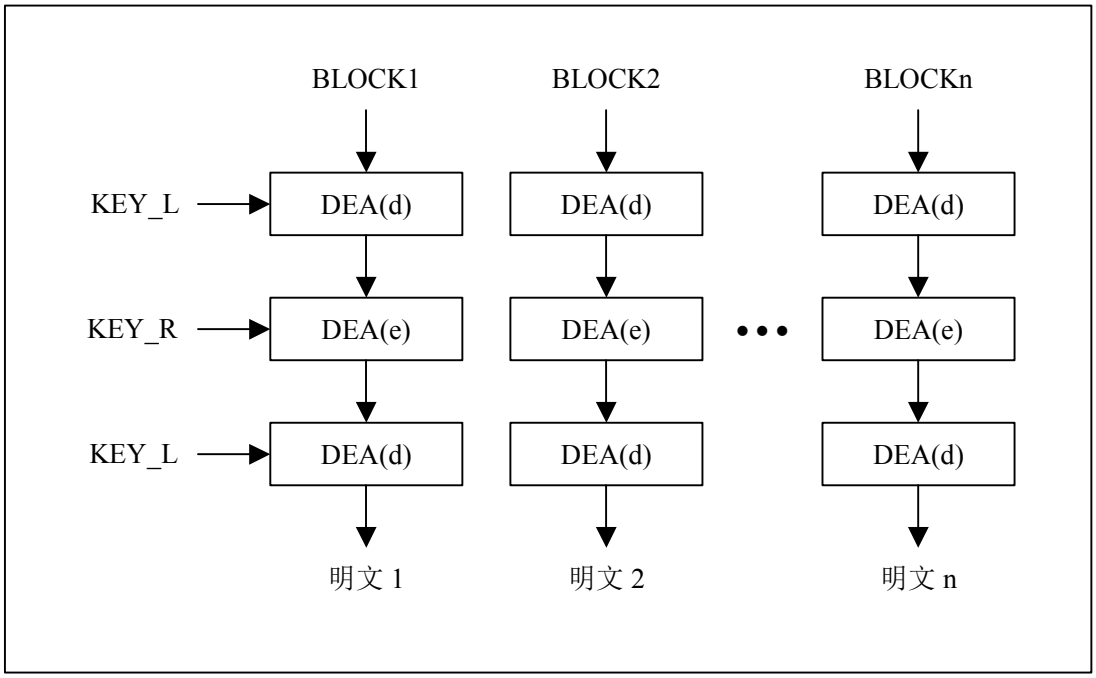


图 1 14 双倍长密钥 DEA 数据解密算法

4.5. 安全报文传送的命令情况

4.5.1. CASE 1

这种情况时，命令中没有数据送到卡（Lc）中，也没有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2

含安全报文的命令：

CLA	INS	P1	P2	Lc	MAC

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = MAC 的长度，4 字节。

4.5.2. CASE 2

这种情况时，命令中没有数据送到卡（Lc）中，有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2	Le

含安全报文的命令：

CLA	INS	P1	P2	Lc	MAC	Le

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = MAC 的长度，4 字节。

4.5.3. CASE 3

这种情况时，命令中有数据送到卡（Lc）中，没有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA

含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA	MAC

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = 数据的长度 + MAC 的长度（4 字节）。

4.5.4. CASE 4

这种情况时，命令中既有数据送到卡（Lc）中，也有数据从卡中返回（Le）。

不含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA	Le

含安全报文的命令：

CLA	INS	P1	P2	Lc	DATA	MAC	Le

传送要求：

CLA 字节的低四位必须为十六进制数‘4’；

Lc = 数据的长度 + MAC 的长度（4 字节）。

5. APDU 命令集

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

5.1. 命令与响应的格式

5.1.1. 命令格式

命令由“命令头”和“命令体”组成

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

命令可分为四种情况：

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

5.1.2. 响应格式

响应的格式：

数据	状态字	
DATA	SW1	SW2

DATA ：响应数据

SW1、SW2：卡片执行命令的返回值

5.2. 发卡专有命令

5.2.1. Create File 命令

5.2.1.1. 命令描述

Create File 用于建立文件系统。卡中的各种类型的文件，都必须通过 Create File 来建立。建立文件时必须满足下列规则：

- 满足当前 DF 建立权限的时候，可以用此命令建立 DF 或 EF。
- KEY 文件必须是但前 DF 下第一个被建立的文件，建立 KEY 文件的时候不不要满足建立权限。
- 目录文件 DF 在建立后，不能被自动选择，需要 Select File 命令来选择。

5.2.1.2. 命令报文

代码	值	描述
CLA	80	-
INS	E0	-
P1P2	XXXX	文件标识符 FID
Lc	XX	数据域的长度
DATA	XX…X	文件控制信息（详见下表）
	X	

注：MF 的文件标识符必须是“3F00”,KEY 文件的文件标识符必须是“0000”

MF 的文件控制信息：

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

DF 的文件控制信息：

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

文件控制信息;

	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
KEY 文件	3F	空间大小		RFU	增加权	FF	FF
二进制文件	28	空间大小		读权限	写权限	FF	KID
定长记录文件	2A	记录数	记录长度	读权限	写权限	FF	KID
变长记录文件	2C	空间大小		读权限	写权限	FF	KID
循环记录文件	2E	记录数	记录长度	读权限	写权限	FF	KID
钱包文件	2F	记录数	钱包长度	读/扣权限	加权限	FF	KID
…	…	…	…	…	…	…	…

对 KID 的说明：

b7	1
b6	1
b5	1
b4	1
b3	读文件返回数据加密时使用的密钥标识符；
b2	KID 取反
b1	写文件返回数据加密时使用的密钥标识符；
b0	KID 取反

5.2.1.3. 响应信息

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

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

5.2.2. Write Key 命令

5.2.2.1. 命令描述

Write Key 命令可向卡中增加密钥(向 KEY 文件中写入密钥),或更新卡中已经存在的密钥。

- 增加密钥时需要满足 KEY 文件的增加密钥的权限
- 修改密钥的时候需要满足密钥的修改权限

5.2.2.2. 命令报文

代码	值	描述
CLA	80 / 84	-
INS	D4	-
P1	01，	01：表示增加密钥
	3X	3X：密钥类型，用于密钥更新
P2	XX	密钥标识
Lc	XX	数据域的长度
DATA	XX…X	➢ 如果是增加密钥，则数据域为密钥信息（详见下表），包括密钥头和密钥值
	X	➢ 如果是修改密钥，则数据域为新的密钥值

密钥信息：

	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	密钥值
DES 加密密钥	30	使用权	修改权	密钥版本	算法标识	8 或 16 字节
DES 解密密钥	31	使用权	修改权	密钥版本	算法标识	8 或 16 字节
DESMAC 密钥	32	使用权	修改权	密钥版本	算法标识	8 或 16 字节
过程密钥	35	使用权	修改权	密钥版本	算法标识	8 或 16 字节
维护密钥	36	使用权	修改权	FF	错误计数器	8 或 16 字节
外部认证密钥	39	使用权	修改权	后续状态	错误计数器	8 或 16 字节
主控密钥	即密钥标识符为‘00’的外部认证密钥，其命令报文数据域同外部认证密钥。					
口令密钥	3A	使用权	EF	后续状态	错误计数器	2-8 字节

说明：

对于密钥也可以采用安全报文传送，只需在增加密钥的时候改变密钥类型的高两位即可，使用线路保护方式增加或修改密钥的时候，所使用的线路保护密钥为当前 DF 下的主控密钥。

b7	b6	b5	B4	b3	b2	b1	b0	线路保护方式
0	0	密钥类型						无
1	0	密钥类型						MAC
1	1	密钥类型						DES & MAC

例：如果增加密钥时的密钥类型为 F0（30 的最高两位变成了二进制 11），则表示此密钥在修改的时候必须用密文带 MAC 的方式。

5.2.2.3. 命令响应

SW1	SW2	说　明
90	00	命令执行成功
65	81	写 FLASH 或 FLASH 或 EEPROM 失败
67	00	Lc 长度错误
69	82	不满足安全状态
69	83	认证密钥锁定
69	84	引用数据无效（未申请随机数）
69	85	使用条件不满足

69	88	安全信息（MAC 和密文）数据错误
6A	80	数据域参数错误
6A	81	功能不支持
6A	82	未找到文件
6A	83	未找到密钥数据
6A	84	文件空间已满
6A	86	P1、P2 参数错
6A	88	未找到密钥数据
6D	00	命令不存在
6E	00	CLA 错
93	03	应用永久锁定

5.2.3. Erase DF 命令

5.2.3.1. 命令描述

Erase DF 命令用于擦除当前 DF 下的所有文件，包括 KEY 文件，但是当前 DF 的文件头不被擦除。擦除后所带来的剩余空间可以用来重新分配。

Erase DF 命令的成功执行，必须要满足当前 DF 的擦除权限。

5.2.3.2. 命令报文

代码	值	描述
CLA	80	-
INS	0E	-
P1	00	-
P2	00	-
Lc	00	-

5.2.3.3. 响应信息

SW1	SW2	说　明
90	00	命令执行成功

67	00	Lc 长度错误
69	82	不满足安全状态
6A	86	P1、P2 参数错
6D	00	命令不存在
6E	00	CLA 错

5.3. 基本命令

5.3.1. APPEND RECORD

5.3.1.1. 功能描述：

Append Record命令用于对变长记录文件、循环文件增加记录。

注意事项：

- Append Record命令适用于变长记录文件和循环文件。
- 若循环文件记录已满则覆盖最早写入的记录，且新增加记录的记录号总为1。

5.3.1.2. 命令格式：

数据	描述
CLA	00
INS	E2
P1	00
P2	见下表
LC	增加记录的长度
DATA	增加记录的数据

LE	无

P2 内容：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	描述
0	0	0	0	0	0	0	0	使用当前 EF 文件
X	X	X	X	X	0	0	0	b4-b8 为短文件标识符

5.3.1.3. 响应状态码：

SW1SW2	描述
9000	执行成功
6581	写 EEPROM 失败
6700	LC 错误
6981	命令与文件结构不相容
6982	安全状态不满足
6986	没有当前 EF 文件
6A81	功能不支持
6A82	没有找到文件
6A84	空间不够

5.3.2. APPLICATION BLOCK

5.3.2.1. 功能描述：

此命令使当前选择的应用失效。

执行条件和处理过程：

--当前应用必须存在

--使用的密钥为密钥类型=01，密钥标识=00。

--执行此命令需要满足所使用的 MAC 密钥的使用权限

--如果当前应用已经临时锁定，那么只能执行永久锁定命令

--在应用锁定（临时或者永久锁定）后，只有以下命令可以执行：

- SELECT
- GET CHALLENGE
- APPLICATION UNBLOCK (*)

- CARD BLOCK
- GET RESPONSE（*）

执行其他命令则返回 6A81。

（*）为永久锁定后不能再执行的命令。

5.3.2.2. 命令格式：

数据	描述
CLA	84
INS	1E
P1	00
P2	00：临时锁定，可用 APPLICATION UNBLOCK 解锁 01：永久锁定，不可解锁
LC	04
DATA	MAC 码
LE	无

5.3.2.3. 响应状态码：

SW1SW2	**描述**
9000	执行成功
6283	选择文件无效
6400	状态标志位未变
6581	写 EEPROM 失败
6984	引用数据无效
6987	SM 数据项丢失
6988	SM 数据项不正确
6A86	P1，P2 错误
6A88	没有找到引用数据
9303	应用已经永久锁定

5.3.3. APPLICATION UNBLOCK

5.3.3.1. 功能描述：

此命令用于恢复当前应用为锁定前状态。

执行条件和处理过程：

--当前应用必须存在

--使用的密钥为密钥类型=01，密钥标识=00。

--执行此命令需要满足所使用的 MAC 密钥的使用权限

--如果当前应用已经永久锁定，那么不能执行此命令

--此命令可以重复执行

--如果连续 3 次解锁失败，将当前应用永久锁定

5.3.3.2. 命令格式：

数据	描述
CLA	84
INS	18
P1	00
P2	00
LC	04
DATA	MAC 码
LE	无

5.3.3.3. 响应状态码：

SW1SW2	描述
9000	执行成功
6400	状态标志位未变
6581	写 EEPROM 失败
6982	安全状态不满足
6987	SM 数据项丢失
6988	SM 数据项不正确

9303	应用已被永久锁定

5.3.4. CARD BLOCK

5.3.4.1. 功能描述：

此命令是卡片中的所有应用失效（无法恢复）。

执行条件和处理过程：

--使用的密钥为密钥类型=01，密钥标识=00。

--执行此命令需要满足所使用的 MAC 密钥的使用权限

说明：如果此命令执行成功，那么对于所有后续命令，卡片都回送 6A81

5.3.4.2. 命令格式：

数据	描述
CLA	84
INS	16
P1	00
P2	00
LC	04
DATA	MAC 码
LE	无

5.3.4.3. 响应状态码：

SW1SW2	描述
9000	执行成功
6400	状态标志位未变
6581	写 EEPROM 失败
6982	安全状态不满足
6987	SM 数据项丢失
6988	SM 数据项不正确

5.3.5. EXTERNAL AUTHENTICATION

5.3.5.1. 功能描述：

要求卡片验证数据。

执行条件和处理过程：

--如果此命令在 MF 下执行，成功后设置 MF 状态；如果此命令在 DF 下执行，成功后设置 DF 状态；

--执行此命令需要满足所使用的认证密钥使用权限

--前一条命令必须是 GET CHALLENGE

--如果比较认证数据不正确，将密钥的错误计数器减 1，当错误计数器减为 0 时，密钥即被锁定，即使再发送正确的认证数据也不会再执行此命令；当错误计数器不为 0 时，如果再成功地执行此命令，则恢复密钥的错误计数器为最大允许值。

5.3.5.2. 命令格式：

数据	描述
CLA	00
INS	82
P1	00
P2	密钥标识
LC	08

DATA	8 字节加密后的随机数
LE	无

5.3.5.3. 响应状态码：

SW1SW2	描述
9000	执行成功
63CX	认证失败，可重试次数为 X
6700	LC 错误
6982	安全状态不满足
6A86	P1，P2 不正确
6F00	数据无效

5.3.6. GET CHALLENGE

5.3.6.1. 功能描述：

从卡片取得一个随机数。

执行条件和处理过程：

--不需要任何访问权限

--在以下情况下，生成的随机数会丢失：

- 卡片复位
- 选择新的 DF
- 成功执行了新的 GET CHALLENGE 命令
- 成功执行完使用随机数的以下条命令：
  - ✓ EXTERNAL AUTHENTICATION

5.3.6.2. 命令格式：

数据	描述
CLA	00
INS	84
P1	00
P2	00
LE	04 或 08

5.3.6.3. 响应报文：

卡片生成的随机数。

5.3.6.4. 响应状态码：

SW1SW2	描述
9000	执行成功
6700	LC 错误
6A86	P1，P2 不正确

5.3.7. GET RESPONSE

5.3.7.1. 功能描述：

从卡片中取前一条命令执行成功后等待返回的数据。

5.3.7.2. 命令格式：

数据	描述
CLA	00

INS	C0
P1	00
P2	00
LE	所取全部数据的长度

5.3.7.3. 响应报文：

卡片准备返回的全部数据

5.3.7.4. 响应状态码：

SW1SW2	描述
9000	执行成功
6281	回送的数据可能出错
6700	LC 错误
6A86	P1，P2 参数不正确
6CXX	长度错误，XX 为正确长度
6F00	数据无效

5.3.8. INTERNAL AUTHENTICATION

5.3.8.1. 功能描述：

使用命令中的数据和卡片的密钥进行运算认证码。

执行条件和处理过程：

--执行此命令需要满足所用密钥的使用权限

--返回数据通过下一条 GET RESPONSE 指令取回。

5.3.8.2. 命令格式：

数据	描述	
CLA	00	
INS	88	
P1	00	加密
	01	解密
	02	计算 MSC
P2	密钥标识	
LC	08	
DATA	认证数据的内容	
LE	00	

说明：

- P1=00，表示进行加密运算，密钥类型是DES加密密钥
- P1=01，表示进行解密运算，密钥类型是DES解密密钥
- P1=02，表示进行MAC运算， 密钥类型是DES&MAC密钥

5.3.8.3. 响应状态码：

SW1SW2	描述
61XX	有 XX 字节数据等待返回
6281	回送数据可能有错
6700	LC 错误
6882	不支持安全报文
6985	不满足使用条件
6A80	数据域参数不正确
6A86	P1，P2 不正确

5.3.9. READ BINARY

5.3.9.1. 功能描述：

用于读取透明二进制文件的内容。

执行条件和处理过程：

--必须满足二进制文件的读权限才能执行此命令。

--如果 LC=00，那么卡片回送 6CXX，XX 表示以下 2 个值中的最小值：

- ✓ 从起始地址开始到文件结束的长度
- ✓ 卡片数据缓冲区的长度

--此命令只能读取二进制文件，如果用来读取记录文件，则返回错误。

5.3.9.2. 命令格式：

数据	描述
CLA	00
INS	B0
P1	见下表
P2	见下描述
LC	无
DATA	无
LE	所读数据的长度

说明：

◆ 若 P1 的高三位为 100，则低 5 位为短的文件标识符，P2 为读的偏移量。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
1	0	0	短文件标识符					文件的偏移量

◆ 若 P1 的最高位不为 1，则 P1 P2 为欲读文件的偏移量，所读的文件为当前文件。

P1								P2
b7	b6	b5	b4	b3	b2	b1	b0	
0	文件的偏移量							

5.3.9.3. 响应报文：

读取的二进制文件内容

5.3.9.4. 响应状态码：

SW1SW2	描述
9000	执行成功
6700	LC 长度错误
6981	命令与文件结构不相容
6982	不满足安全状态
6986	没有当前 EF
6A81	不支持此功能
6A82	没有找到文件
6A86	P1，P2 参数错误
6B00	偏移地址超出 EF
6CXX	长度错误，实际长度=XX
9303	应用被永久锁定

5.3.10. READ RECORD

5.3.10.1. 功能描述：

用于读取记录文件的内容。

执行条件和处理过程：

--必须满足记录文件的读权限才能执行此命令。

--如果 LC=00，那么卡片回送 6CXX，XX 表示记录长度。

--此命令只能读取记录文件，如果用来读取二进制文件，则返回错误。

5.3.10.2. 命令格式：

数据	描述
CLA	00
INS	B2
P1	记录号
P2	见下表
LC	无
DATA	无
LE	所读记录的长度

P1 说明：

类型	P1 义
定长记录文件	记录号，若该文件有 N 条记录，则记录号可以是 1-N。
变长记录文件	记录号，若该文件有 N 条记录，则记录号可以是 1-N。 记录标识，如按记录标识来读，则 P2 的低 3 位必须为'000'。
循环文件	记录号最新写入的记录号为 01,上 1 条记录的记录号为 02，依次类推…

P2 说明

b7	b6	b5	b4	b3	b2	b1	b0	描述
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
-	-	-	-	-	1	0	0	按记录号，读 P1 指定的记录
-	-	-	-	-	1	0	1	按记录号，从 P1 指定的记录读到最后一条记录
-	-	-	-	-	1	1	0	按记录号，从最后一条记录读到 P1 指定的记录
-	-	-	-	-	0	0	0	读 P1 指定记录标识符的第一个记录
-	-	-	-	-	0	0	1	读 P1 指定记录标识符的最后一个记录
-	-	-	-	-	0	1	0	读 P1 指定记录标识符的下一个记录
-	-	-	-	-	0	1	1	读 P1 指定记录标识符的上一个记录

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

5.3.10.3. 响应报文：

记录文件的某条记录内容

5.3.10.4. 响应状态码：

SW1SW2	描述
9000	执行成功
6700	LC 长度错误
6981	命令与文件结构不相容
6982	安全状态不满足
6986	没有当前 EF
6A81	不支持此功能
6A82	没有找到文件
6A83	没有找到记录
6A86	P1，P2 错误

5.3.11. SELECT

5.3.11.1. 功能描述：

用于通过文件标识（FID）或者文件名（AID）来选择 MF、DDF，ADF、EF。

执行条件和处理过程：

--执行此命令不需要任何权限。

--如果选择的是 DF，并且是与当前 DF 不相同的 DF，则当前 DF 的安全状态丢失，否则安全状态不变。

--返回数据通过下一条 GET RESPONSE 指令取回。

--如果当前应用已经临时锁定，那么执行此命令后返回 6A81，但是 FCI 信息仍然可以使用 GET RESPONSE 命令取得。

5.3.11.2. 命令格式：

数据	描述
CLA	00
INS	A4
P1	见下表
P2	见下表
LC	见下表
DATA	FID 或者 AID

LE	无

P1：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	描述
0	0	0	0	0	0	0	0	选兄弟 DF 或 EF
0	0	0	0	0	0	0	1	选择子 DF
0	0	0	0	0	0	1	0	选择当前 DF 下的 EF
0	0	0	0	0	1	0	0	通过文件名（AID）选择 DF，具体方式见 P2

P2：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	描述
0	0	0	0	0	0	0	0	选择第一个
0	0	0	0	0	0	1	1	选择下一个

LC：

LC=02，DATA 为文件标识（FID）。

LC=05-10，DATA 为 DF 的全部文件名或部分文件名。

5.3.11.3. 响应状态码：

SW1SW2	描述
61XX	回送数据 XX 字节等待返回
6700	LC 长度错误
6A81	不支持此功能
6A82	没有找到文件
6A86	P1，P2 参数不正确

5.3.12. UPDATE BINARY

5.3.12.1. 功能描述：

用于写内容到二进制文件。

执行条件和处理过程：

--必须满足二进制文件的更新权限才能执行此命令。

--此命令只能更新二进制文件，如果用来更新记录文件，则返回错误。

--本命令支持明文+MAC 方式更新数据，二进制文件头的最后一个字节为使用的 MAC 密钥索引，不使用时将其置为‘FF’。如果设置了 MAC 密钥索引，则只能使用带 MAC 方式更新文件数据。如果连续 3 次执行此命令失败，则将应用永久锁定。

5.3.12.2. 命令格式：

数据	描述
CLA	00
INS	D6
P1	见下表
P2	见下面描述
LC	更新数据的长度
DATA	更新数据的内容
LE	无

P1：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	描述
0	0	0	0	0	0	0	0	使用当前 EF
1	0	0	X	X	X	X	X	使用低 5 位的 SFI 选择 EF

P2：

当 P1 的 bit7=1 时，只使用 P2 作为数据的起始偏移地址。

当 P1 的 bit7=0 时，使用 P1 和 P2 的 2 个字节作为数据的起始偏移地址。

5.3.12.3. 响应状态码：

SW1SW2	描述
9000	执行成功
6581	写 EEPROM 失败
6700	LC 长度错误
6981	命令与文件结构不相容
6982	安全状态不满足
6986	没有当前 EF
6A81	不支持此功能
6A82	没有找到文件
6B00	偏移地址超出 EF 空间

5.3.13. UPDATE RECORD

5.3.13.1. 功能描述：

用于写整条记录内容到记录文件。

执行条件和处理过程：

--必须满足记录件的更新权限才能执行此命令。

--此命令只能更新记录文件，如果用来更新二进制文件，则返回错误。

--当更新记录（P1=00）时，在修改记录成功后重新设定内存记录指针

5.3.13.2. 命令格式：

数据	描述
CLA	00
INS	DC
P1	见下面描述
P2	见下表
LC	更新记录的长度
DATA	更新记录的内容
LE	无

P1：

P1=00，更新当前记录

P1≠00，更新 P1 指定的记录

P2：

Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	描述
X	**X**	**X**	**X**	**X**	-	-	-	使用 SFI 选择 EF
-	-	-	-	-	**0**	**0**	**0**	第一个记录
-	-	-	-	-	**0**	**0**	**1**	最后一个记录
-	-	-	-	-	**0**	**1**	**0**	下一个记录
-	-	-	-	-	**0**	**1**	**1**	上一个记录
-	-	-	-	-	**1**	**0**	**0**	更新 P1 指定的记录

说明：

- 当 P1≠00 时，P2 只能等于 04，表示更新 P1 指定的记录，更新成功后不修改内存记录指针。

5.3.13.3. 响应状态码：

SW1SW2	描述
9000	执行成功
6581	写 EEPROM 失败
6700	LC 长度错误
6981	命令与文件结构不相容
6982	安全状态不满足
6986	没有当前 EF
6A81	不支持此功能
6A82	没有找到文件
6A83	没有找到记录
6A84	文件空间不够

5.3.14. VERIFY

5.3.14.1. 功能描述：

用于校验用户 PIN。

执行条件和处理过程：

--如果此命令在 MF 下执行，成功后设置 MF 状态；如果此命令在 DF 下执行，成功后设置 DF 状态；

--此命令首先在当前应用下搜寻指定的 PIN ，如果 PIN 为空记录，则搜寻 MF 下密钥文件中的满足要求的 PIN。

-- 如果连续 3 次输入错误的 PIN，则 PIN 被锁定；如果输入了正确的 PIN，则不论目前剩余的可重试次数是多少，都将恢复为最大允许次数。

5.3.14.2. 命令格式：

数据	描述
CLA	00
INS	20
P1	00
P2	PIN 的标识
LC	02-06
DATA	PIN 值
LE	无

5.3.14.3. 响应状态码：

SW1SW2	描述
9000	执行成功
63CX	比较不成功，X 为剩余可重试次数，如果 X=0，表示 PIN 已经锁定。
6700	LC 长度错误
6983	密钥锁定

6984	引用数据无效
6985	不满足使用条件
6A81	不支持此功能
6A86	参数 P1，P2 错误
6A88	没有找到引用数据