TimeCOS/PBOC 专用技术

参考手册

(V2.8)

握奇数据系统有限公司

二零零二年九月

重要声明：

随着 TimeCOS/PBOC 卡片产品的升级，本手册内容将会做相应的修改。握奇数据系统有限公司保留对本手册内容进行修改的权利。

手册变化动态

修改日期	新版本序号	主要变化内容描述
2001 年 5 月	2.7	初稿
2002 年 9 月	2.8	修改稿

目 录

图形目录

表格目录

1. 关于本手册

1.1 内容概述

本手册各部分内容概述如下：

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

- TimeCOS/PBOC 文件管理
  本章从文件组织结构、文件格式、文件访问方式及各种类型文件的特点来详细描述了 TimeCOS/PBOC 的文件管理系统。

- 卡片初始化设置
  本章描述了 TimeCOS/PBOC 卡片初始化后的文件结构及使用方法。

- TimeCOS/PBOC 的安全体系
  安全体系是 TimeCOS 的核心部分，它涉及到卡的鉴别与核实，对文件访问时的权限控制机制。本章从安全状态、安全属性、安全机制和密码算法四个方面详细描述了 TimeCOS/PBOC 的安全体系。

- 命令与应答
  本章描述了命令与应答结构及命令返回状态码 SW1SW2 的意义。

- TimeCOS/PBOC 发卡命令

- 附录一 TimeCOS/PBOC 的复位应答
- 附录二 TimeCOS/PBOC 金融 IC 卡应用举例
- 附录三 TimeCOS/PBOC 技术性能指标
- 附录四 TimeCOS/PBOC 可定制的功能

注：有关“安全报文传送”、“TimeCOS/PBOC 基本命令”和“中国金融 IC 卡专用命令”见《TimeCOS/PBOC 通用技术参考手册》。

1.2 参考文献

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

[2] 《TimeCOS/PSAM 技术参考手册》，1999 年 5 月，握奇数据系统有限公司。

[3] ISO/IEC 7816 PART 3：识别卡，带触点的集成电路卡：电气特性和传输协议。

[4] ISO/IEC 7816 PART 4：识别卡，带触点的集成电路卡：行业间交换用命令。

1.3 定义

- 接口设备
  终端上插入 IC 卡的部分，包括其中的机械和电气部分。

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

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

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

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

- 集成电路
  设计用于完成处理和/或存储功能的电子器件。

- 集成电路卡(IC 卡)Integrated Circuit(s) Card
  内部封装一个或多个集成电路的 ID-1 型卡（如 ISO 7810、ISO 7811 第 1 至 5 部分、ISO 7812 和 ISO 7813 中描述的）。

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

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

- 明文 Plaintext
  没有加密的信息。

- 密文 Ciphertext
  通过密码系统产生的不可理解的文字或信号。

- 密钥 Key
  控制加密转换操作的符号序列。

- 保密密钥 Secret Key
  对称加密技术中仅供指定实体所用的密钥。

- 加密算法 Cryptographic Algorithm
  为了隐藏或揭露信息内容而变换数据的算法。

- 对称加密技术 Symmetric Cryptographic Technique
  发送方和接收方使用相同保密密钥进行数据变换的加密技术。在不掌握保密密钥的情况下，不可能推导出发送方或接收方的数据变换。

- 数据完整性 Data Integrity
  数据不受未经许可的方法变更或破坏的属性。

- T=0
  面向字符的异步半双工传输协议。

- T=1
  面向块的异步半双工传输协议。

- 金融交易
  持卡者、商户和收单行之间基于收、付款方式的商品或服务交换行为。

- 电子存折 Electronic Deposit
  一种为持卡人进行消费、取现等交易而设计的使用个人密码（PIN）保护的金融 IC 卡应用。它支持圈存、圈提、消费、取现、修改透支限额及查询余额交易。

- 电子钱包 Electronic Purse
  一种为持卡人小额消费而设计的金融 IC 卡应用。它支持圈存、消费和查询余额交易。除圈存交易外，使用电子钱包进行的其他交易均不记录明细，且均无需提交个人密码（PIN）。

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

- 圈提 Unload
  持卡人将电子存折中的部分或全部资金划回到其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。

- 消费 Puchase
  消费交易允许持卡人使用电子存折或电子钱包的余额进行购物或获取服务。此交易可以在销

售点终端（POS）上脱机进行。使用电子存折进行的消费交易必须提交个人密码（PIN），使用电子钱包则不需要。

- 取现 Cash Withdraw

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

- 透支限额 Overdraw Limit

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

1.4 缩略语和符号表示

以下缩略语和符号表示适用于本手册：

AID ： 应用标识符（Application Identifier）
APDU ： 应用协议数据单元（Application Protocol Data Unit）
ATR ： 复位应答（Answer to Reset）
b ： 二进制（Binary）
BER ： 基本编码规则（Basic Encoding Rules）
BWI ： 块等待时间整数（Block Waiting Time Integer）
CLA ： 命令报文的类别字节（Class Byte of the Command Message）
CWI ： 字符等待时间整数（Character Waiting Time Integer）
DEA ： 数据加密算法（Data Encryption Algorithm）
DES ： 数据加密标准（Data Encryption Satandard）
DF ： 专用文件（Dedicated File）
DIR ： 目录（Directory）
ED ： 电子存折（Electronic Deposit）
EDC ： 错误检测代码（Error Detection Code）
EF ： 基本文件（Elementary File）
EMV ： Europay、Mastercard、VISA
EP ： 电子钱包（Electronic Purse）
Etu ： 基本时间单元（Elementary Time Unit）
FCI ： 文件控制信息（File Control Information）
FID ： 文件标识（File Identifier）
GND ： 地（Ground）
Hex. ： 十六进制数（Hexadecimal）
IC ： 集成电路（Integrated Circuit）
ICC ： 集成电路卡（Integrated Circuit Card）
IEC ： 国际电工委员会（International Electrotechnical Commission）
INS ： 命令的指令字节（Instruction Byte of Command Message）
ISO ： 国际标准化组织（International Standardization Organization）
Lc ： 终端发出的命令数据域的实际长度

Le : 响应数据的最大期望长度
LEN : 长度（Length）
MAC : 报文鉴别代码（Message Authentication Code）
MF : 主控文件（Master File）
P1 : 参数 1（Parameter 1）
P2 : 参数 2（Parameter 2）
PBOC : 中国人民银行
PIN : 个人密码（Personal Identification Number）
PIX : 专用应用标识符扩展码（Proprietary Application Identifier Extension）
PSA : 支付系统应用（Payment System Application）
PSAM : 消费安全存取模块（Purchase Secure Access Module）
PSE : 支付系统环境（Payment System Environment）
RFU : 保留为将来使用（Reserved for Future Use）
RID : 已注册的应用提供者标识（Registered Application Provider Identify）
RST : 复位（Reset）
SAM : 安全存取模块（Secure Access Module）
SFI : 短文件标识符（Short File Identifier）
SW1 : 状态码 1（Status Word One）
SW2 : 状态码 2（Status Word Two）
TAC : 交易认证码（Transaction Authorization Crypogram）
TCK : 校验字符（Check Character）
TLV : 标签、长度、值（Tag Length Value）
VCC : 电源电压（Supply Voltage）
VPP : 编程电压（Programming Voltage）

‘0’～‘9’和‘A’ ～‘F’ : 十六进制数
0x00～0x0F ：十六进制数
XX : 1 个字节 16 进制数
XXXX : 2 个字节 16 进制数
XX…XX : 未知个字节 16 进制数

2. TimeCOS/PBOC 简介

2.1 关于 TimeCOS/PBOC

TimeCOS/PBOC(Time Card Operating System)是由握奇数据系统有限公司自行开发的智能卡（SmartCard）操作系统，完全符合以下国际、国内标准：

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

TimeCOS/PBOC具有以下主要特征：

- 支持一卡多应用，各应用之间相互独立（多应用、防火墙功能）。
- 支持多种不同的文件组织形式（文件组织系统）。
- 在通讯过程中支持多种安全保护机制（信息的机密性和完整性保护）。
- 支持多种安全访问方式和权限（认证功能和口令保护）。
- 支持中国人民银行认可的Single DES、Triple DES算法。
- 支持中国人民银行规定的电子钱包和电子存折功能。
- 支持多种通讯协议：接触界面支持T=0（字符传送）和T=1（块传送）通讯协议。

2.2 TimeCOS 体系结构

2.2.1 卡片内部逻辑结构

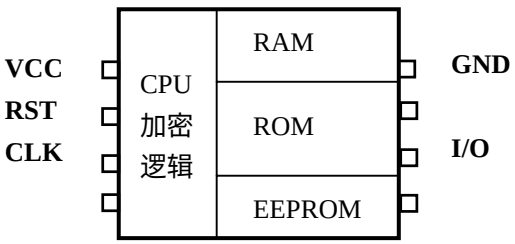


图 2-1 卡片内部逻辑结构

TimeCOS 卡片芯片由以下四部分硬件模块组成：(见图 2-1)

- CPU及加密逻辑
  保证 EEPROM 中数据安全，使外界不能用任何非法手段获取 EEPROM 中的数据。

- RAM
  TimeCOS 工作时存放命令参数、返回结果、安全状态及临时工作密钥的区域。
- ROM
  存放 TimeCOS 程序的区域。
- EEPROM
  存放用户应用数据区域，TimeCOS 将用户数据以文件形式保存在 EEPROM 中，在满足用户规定的安全条件时，可进行读或写。

2.2.2 TimeCOS 功能模块划分

TimeCOS 由传输管理、文件管理、安全体系、命令解释四个功能模块组成：

- 传输管理
  按 ISO7816-3 标准监督卡与终端之间的通信，保证数据正确地传输，防止卡与终端之间通讯数据被非法窃取和篡改。
- 文件管理
  将用户数据以文件形式存储在 EEPROM 中，保证访问文件时快速性和数据安全性。
- 安全体系
  安全体系是 TimeCOS 的核心部分，它涉及到卡的鉴别与核实，对文件访问时的权限控制机制。
- 命令解释
  根据接收到的命令检查各项参数是否正确，执行相应的操作。

2.2.3 TimeCOS/PBOC 命令集

表 2.1 TimeCOS/PBOC 命令集

编号	命令名称	CLA	INS	功能描述	兼容性
1	Append Reocrd	00/04	E2	增加记录	ISO
2	Verify PIN	00/04	20	验证口令	ISO&PBOC
3	External Authentication	00	82	外部认证	ISO&PBOC
4	Get Challenge	00	84	取随机数	ISO&PBOC
5	Internal Authentication	00	88	内部认证	ISO&PBOC
6	Select File	00	A4	选择文件	ISO&PBOC
7	Read Binary	00/04	B0	读二进制文件	ISO&PBOC
8	Read Record	00/04	B2	读记录文件	ISO&PBOC
9	Get Response	00	C0	取响应数据	ISO&PBOC
10	Update Binary	00/04	D6	写二进制文件	ISO&PBOC
11	Update Record	00/04	DC	写记录文件	ISO&PBOC
12	Card Block	84	16	卡片锁定	PBOC
13	Application Unblock	84	18	应用解锁	PBOC
14	Application Block	84	1E	应用锁定	PBOC
15	PIN Unblock	80/84	24	个人密码解锁	PBOC
16	Initialize	80	50	初始化交易	PBOC
17	Credit For Load	80	52	圈存	PBOC
18	Debit For Purchase /Cash Withdraw	80	54	消费/取现/圈提	PBOC
19	Update Overdraw Limit	80	58	修改透支限额	PBOC
20	Get Transaction Proof	80	5A	取交易认证	PBOC
21	Get Balance	80	5C	读余额	PBOC
22	Reload/Change PIN	80	5E	重装/修改个人密码	PBOC
22	Erase MF	80	0E	擦除 MF	专有
23	Erase EF/DF	00	E4	擦除 EF/DF	专有
24	Set Protocol	80	14	设置卡片通信参数	专有
25	Unblock	80	2C	解锁被锁住口令	专有
26	Decrease	80/84	30	扣款	专有
27	Increase	80/84	32	存款	专有
28	Write Key	80/84	D4	增加或修改密钥	专有
29	Create File	80	E0	建立文件	专有

3. 文件管理

本章介绍 TimeCOS/PBOC 的文件系统，包括文件组织结构、文件结构、文件的访问方式及文件空间计算。其中文件结构与文件的访问方式是以文件类型为索引来叙述的。

3.1 文件组织结构

TimeCOS/PBOC 的文件系统是由专用文件 DF（Dedicated File）和基本文件 EF（Elementary File）组成的。

卡内数据的逻辑组织结构由专用文件（DF）的结构化分级组成。

- 在根处的 DF 称作主文件（MF）。该 MF 是必备的。
- 其他 DF 是任选的。

TimeCOS/PBOC 的文件组织结构如图 3-1 所示，MF（第 1 级）为根 DF，是必须有的，所有其他的文件都是她的分支。在 MF 的下一级可以由 DF 和 EF 组成，在 DF 的下一级亦可由 DF 和 EF 组成，即卡片最多支持三级目录结构（MF-DF-DF）。我们将不包含子 DF 的 DF 称为 ADF，包含子 DF 的 DF 称为 DDF。

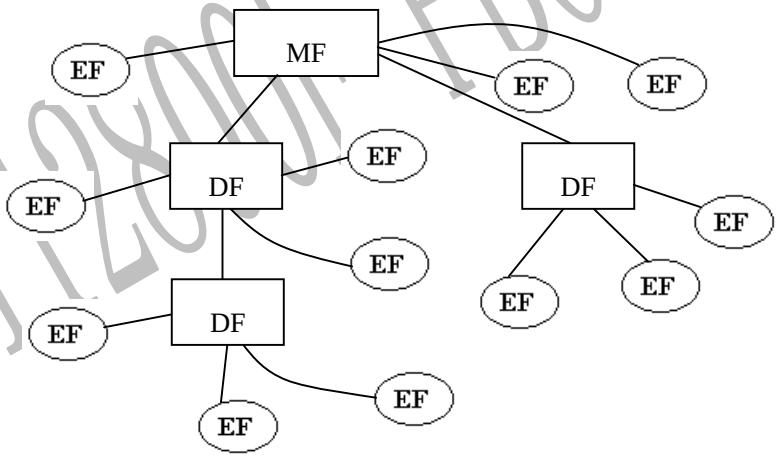


图 3-1 TimeCOS/PBOC 文件组织树结构

图 3-2 给出了一个卡片内部结构示例，该卡片支持电子存折、电子钱包、磁条卡功能应用（Easy Entry）以及一个没有定义的发卡方应用。

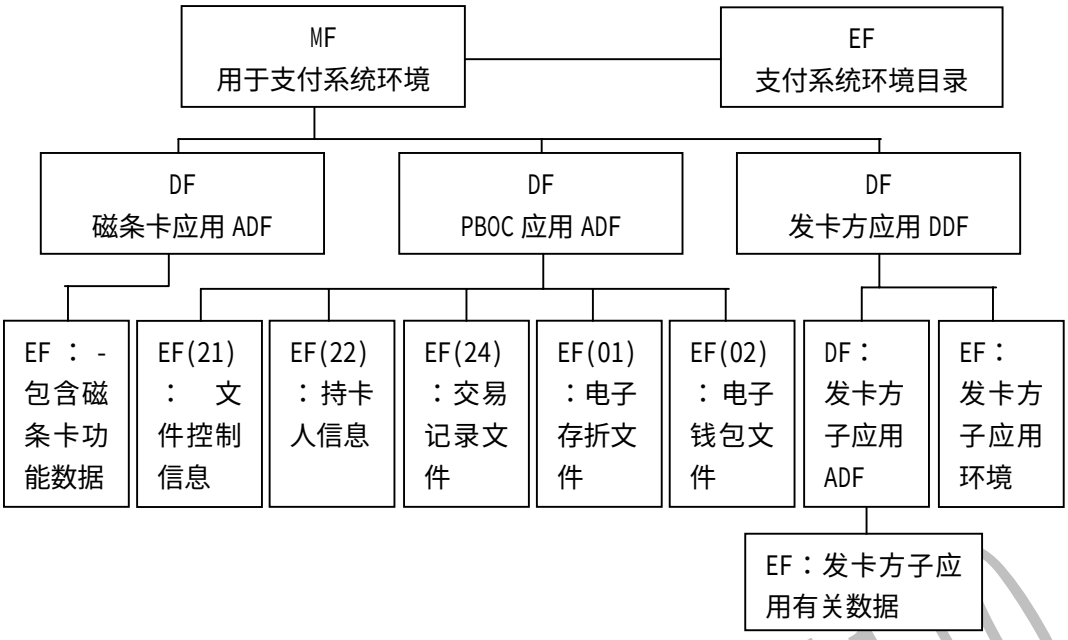


图 3-2 卡片内部结构示例

3.2 文件格式

3.2.1 概述

- TimeCOS/PBOC 中的所有文件都是由文件头和文件体组成（如图 3-3 所示）。文件头长度是 12 个字节，TimeCOS/PBOC 用这些信息来管理文件。

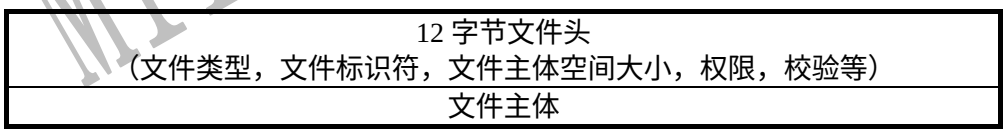


图 3-3 文件在 EEPROM 中存放的格式

- 文件头用于存储文件类型、文件标识、文件大小和访问权限等内容（见表 3.1）。文件体是存放数据的区域。

表 3.1 文件头定义

描述	字节（Byte）
文件类型	1
文件标识(FID)	2
文件大小	2
访问权限 1	1
访问权限 2	1
RFU	1
RFU	1
校验和（由 COS 计算）	1

注：表 3.1 中两个 RFU 字节对于不同类型的文件有不同的定义。对于文件头的详细描述见“7.1 Create File 命令”。校验和由 COS 计算。

◆ ***注意：文件格式是在建立文件时唯一确定的，所使用的命令是 Create File.***

3.2.2 文件类型

- TimeCOS/PBOC 支持下列两种文件：
  ——专用文件(DF)。
  ——基本文件(EF)。
- 在根处的 DF 称作主文件(MF)。该 MF 是必备的。
- 定义了以下两种基本文件（EF）：
  1、工作基本文件
  用于存储不由卡所解释的数据（即用户数据），包括二进制文件、定长记录文件、循环文件、钱包文件和变长记录文件。
  2、内部基本文件
  用于存储由卡所解释的数据，指为了管理和控制目的由卡分析和使用的数据，包括密钥文件。
- EF 支持的文件类型及相应的文件结构如表 3.2 所示。

表 3.2 文件类型字节的定义

类型字（HEX）	文件描述	文件结构
38	MF 或 DF	
28	二进制文件	透明文件
2A	定长记录文件	定长线性文件
2E	循环文件	循环文件
2F	钱包文件	循环文件
2C	变长记录文件	变长线性文件
3F	密钥文件（存放密钥和 PIN，不允许外部访问）	变长线性文件

3.2.3 文件标识和文件名称

TimeCOS/PBOC 是通过逻辑寻址而非物理寻址方式来管理文件的，支持通过文件名称和文件标识两种方式来访问文件。

3.2.3.1 文件标识（FID）

文件标识符（File Indentifier）是文件的标识代码，用2个字节来表示，在选择文件时只要指出文件标识符，TimeCOS/PBOC就可以找到相应文件（KEY文件除外），同一目录下的文件标识符必须是唯一的。

◆ *注意： MF 的文件标识均为'3F00'， KEY 文件标识均为‘0000’;‘FFFF’保留将来使用。同一目录下的文件标识符必须是唯一的。*

3.2.3.2 短文件标识符 SFI

短文件标识符由 5 个二进制位组成，可选择的最大文件标识符为 31。若文件需要用短文件标识符进行选择，则建立文件时就需将文件标识符取在 1-31（00001-11111）之间。

3.2.3.3 文件名称

文件名称是指 DF 名称，用于标识 DF，卡中任何 ADF 或 DDF 可通过其 DF 名称进行选择。

ADF 的 DF 名称对应其应用标识（AID），应用标识的格式可参考 ISO/IEC 7816-5 的有关规定。应用标识的长度为 5～16 字节，分为 2 部分（见图 3-4）：第一部分内容叫注册 ID（Registered ID），长度为 5 字节，由注册机构分配，包含国家代码、应用类别和应用提供商的标识号；第二部分（PIX）是可选的，由应用提供商定义，长度为 0～11 字节。

AID	
RID	PIX
5 Byte	0...11 Byte

图 3-4 应用标识编码

3.3 文件访问方式

- 通过文件标识符（FID ）进行访问
  在选择文件（Select File）时只要指出文件标识符，TimeCOS/PBOC 就可以找到相应文件。（KEY 文件不能通过文件标识进行选择）

- 通过短文件标识符（SFI）进行访问

短文件标识符选择可以通过Read Binary、Update Binary命令的参数P1来实现文件的选择：

P1	b7	b6	b5	b4	b3	b2	b1	b0
	1	0	0	短文件标识符				

若参数P1的高三位为100，则低5位为短的文件标识符。

[例] 若P1为81H即10000001，其中高三位为100，则所选的文件标识符为0001。

短文件标识符选择还可以通过Read Record、Update Record、Append Record、Decrease、Increase命令的参数P2来实现文件的选择：

P2	B7	b6	b5	b4	b3	b2	b1	b0
	短文件标识符					1	0	0

若P2的高五位不全为0，低三位为100，则高五位为短的文件标识符。

[例] 若P2为0CH即00001100，其中低三位为100，所选的文件标识符为0001。

- 通过 DF 文件名称进行访问
  在选择文件（Select File）时只要指出该 DF 的文件名称，TimeCOS/PBOC 就可以找到相应的 DF。

3.4 专用文件（DF）

3.4.1 主文件（MF）

3.4.1.1 定义

在 TimeCOS/PBOC 中，在根处的 DF 称作主文件(MF)。该 MF 是必备的。它相当于 DOS 的根目录。

- IC 卡复位后，卡片自动选择 MF 为当前文件。
- 在金融应用中，MF 与 MF 下的目录文件（DIR 文件，一个记录型文件）一起构成支付系统环境（PSE），MF 的文件名称是 1PAY.SYS.DDF01.

3.4.1.2 文件头定义

表 3.3 MF 文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘ 3F ’
文件标识(FID)	2	‘ 3F00 ’
文件大小	2	‘ FFFF ’，指自动将 MF 空间建立为最大值
访问权限 1	1	建立权限：在 MF 下建立文件的权限
访问权限 2	1	擦除权限：擦除 MF 下所有文件的权限
RFU	1	‘ FF ’
RFU	1	‘ FF ’
RFU	1	‘ FF ’
RFU	1	‘ FF ’

3.4.1.3 文件操作命令

- 建立文件命令(Create File)
  在卡片无 MF 时，必须首先建立 MF 才能对卡片进行其它操作。
- 选择文件命令（Select MF）
  可以用 Select File 命令通过文件标识符‘ 3F00 ’或文件名称 1PAY.SYS.DDF01 来选择文件。
- 擦除 DF 命令（Erase DF）
  在满足当前 MF 的擦除权限时，可以用此命令擦除 MF 下的所有文件(包括 DF 或 EF)，但 MF 当前的访问权限、空间等信息并没有改变（即不能擦除 MF 的文件头信息）。

> ◆ ***注：若 MF 下无任何文件，则在该目录下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开 MF 再进入 MF 时，将遵循文件的访问权限。***

3.4.2 专用文件（DF）

3.4.2.1 定义

在 TimeCOS/PBOC 中，专用文件 DF 相当于 DOS 的目录。每一个 DF 下可以存放多个 EF 和多个下级 DF。

- 卡片可支持 3 级目录（MF-DF-DF）。我们称包含下级目录的专用文件（DF）为 DDF，不包含下级目录的专用文件为 ADF.
- 任何一个 DF 在物理上和逻辑上都保持独立，都有自己的安全机制和应用数据。
- DF 的个数仅受 EEPROM 空间的限制。

3.4.2.2 文件头定义

表 3.4 DF 文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘ 3F ’
文件标识(FID)	2	见“ 3.2.3.1 文件标识（FID）”
文件大小	2	表示 DF 文件体大小
访问权限 1	1	建立权限：在 DF 下建立文件的权限
访问权限 2	1	擦除权限：擦除 DF 下所有文件的权限
RFU	1	‘ FF ’
RFU	1	‘ FF ’

3.4.2.3 文件名称

见“ 3.2.3.3 文件名称 ”。

3.4.2.4 文件操作命令

- 建立文件命令(Create File)
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 选择文件命令（Select MF）
  可以用 Select File 命令通过文件标识符或 DF 名称来选择文件。
- 擦除 DF 命令（Erase DF）
  在满足当前 DF 的擦除权限时，可以用此命令擦除 DF 下的所有文件(包括 DF、EF)，但 DF 当前的访问权限、空间等信息并没有改变（即不能擦除当前 DF 的文件头信息），且 DF 的文件名称也不能被擦除。

> ◆ ***注：若当前 DF 下无任何文件，则在该 DF 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开该 DF 再进入此 DF 时，将遵循文件的访问权限。***

3.5 工作基本文件

工作基本文件用于存储不由卡所解释的数据（即用户数据），包括二进制文件、定长记录文件、循环文件、钱包文件和变长记录文件。

3.5.1 二进制文件

3.5.1.1 定义

二进制文件为一个数据单元序列，数据以二进制为单位进行读写。

3.5.1.2 文件体结构—透明文件

透明文件通常又叫二进制文件或流文件，即透明文件不处理任何内部结构。存储在文件中的数据通过使用地址偏移量访问（文件逻辑地址从 0 开始）。

透明文件的结构如下图所示：

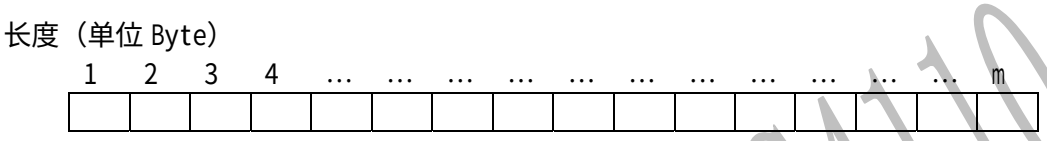
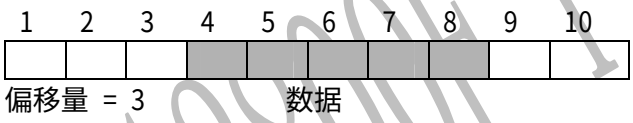


图 3-5 透明结构

[例] 从一个 10 字节的文件中读取偏移量为 3 的 5 个字节：



3.5.1.3 文件头定义

表 3.5 二进制文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘ 28 ’，安全报文模式的设置见“ 7.1 Create File ”
文件标识(FID)	2	见“ 3.2.3.1 文件标识（FID）”
文件大小	2	文件体长度
访问权限 1	1	读权限
访问权限 2	1	写权限
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘ FF ’

3.5.1.4 文件操作命令

- 建立文件命令（Create File ）

  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。

- 选择文件命令（Select File）
  可以用 Select File 命令通过文件标识符来选择文件。
- 读二进制文件（Read Binary）
  当满足文件的读权限时，可以用 Read Binary 命令读取文件信息。
- 写二进制文件（Update Binary）
  当满足文件的写权限时，可以用 Update Binary 命令写入文件信息。

3.5.2 定长记录文件

3.5.2.1 定义

定长记录文件为具有固定长度记录的文件。

3.5.2.2 文件体结构—定长线性文件

定长线性文件又叫定长记录文件，它的结构是相同长度的记录。不同的记录通过顺序号来区分访问。记录只能整条访问，不允许访问记录的部分数据。

定长记录文件的结构如下图所示：

图 3-6 定长线性记录文件结构

3.5.2.3 文件头定义

表 3.6 定长记录文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘2A’，安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”
文件大小	2	字节 1 表示记录总个数(2-254) 字节 2 表示记录长度(≤178)
访问权限 1	1	读权限
访问权限 2	1	写权限
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘FF’

3.5.2.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用 Select File 命令通过文件标识符来选择文件。
- 读记录文件（Read Record）
  当满足文件的读权限时，可以用 Read Record 命令读取一条记录。
- 写记录文件（Update Record）
  当满足文件的写权限时，可以用 Update Record 命令写（或更新）一条记录。

3.5.3 循环文件

3.5.3.1 定义

循环文件为具有固定长度记录的环行文件。

3.5.3.2 文件体结构—循环文件

循环文件又叫循环记录文件。循环文件的每条记录都只有一个数据域，数据以记录为单位进行存储，记录长度最大为 178 个字节。不同的记录通过顺序号来区分访问，应用时只能顺序增加记录。当写记录时，当前写入的为第一条记录，则上一次写入的记录为第二条，依此类推，滚动写入。记录只能在文件头中所规定的范围内滚动写入，当写完最后一条记录时将覆盖最先写入的记录。

循环记录文件的结构如下图所示：

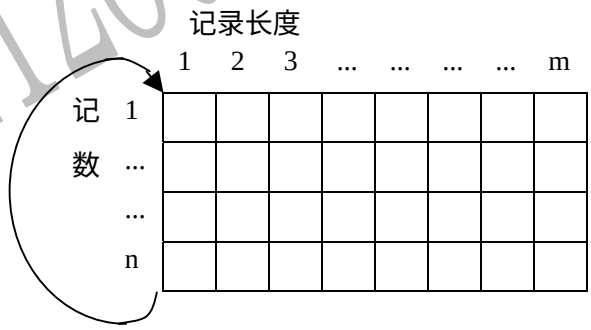


图 3-7 循环记录文件结构

3.5.3.3 文件头定义

表 3.7 循环文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘2E’，安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”：
文件大小	2	字节 1 表示记录总个数(2-254) 字节 2 表示记录长度(≤178)
访问权限 1	1	读权限
访问权限 2	1	添加权限
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘FF’

3.5.3.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用 Select File 命令通过文件标识符来选择文件。
- 读记录文件（Read Record）
  当满足文件的读权限时，可以用 Read Record 命令读取一条记录。
- 增加记录（Append Record）
  当满足文件的添加权限时，可以用 Append Record 命令增加一条新记录。
- 写记录文件（Update Record）
  当满足文件的添加权限时，可以用 Update Record 命令增加一条新记录。

3.5.4 普通钱包文件

3.5.4.1 定义

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

3.5.4.2 文件体结构—循环文件

见“3.5.4.2 文件体结构—循环文件”。

- 记录个数必须大于或等于 2，记录长度必须小于 8 字节。
- 钱包文件中的金额是以二进制形式进行运算的，新建立的钱包文件余额为 00。
- 存款/扣款时用第一条记录（此记录号为 1）的数值加上/减去交易金额，然后将新写的记录作为第一条记录。

3.5.4.3 文件头定义

表 3.8 普通钱包文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘2F’， 安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）“
文件大小	2	字节 1 表示记录总个数（2-254） 字节 2 表示记录长度（<8）
访问权限 1	1	扣款权限/读权限
访问权限 2	1	存款权限
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘FF’

- 读权限
  指使用 Read Record 命令读出指定记录的权限。
- 扣款权限
  指使用 Decrease 命令减少钱包余额的权限。
- 存款权限
  指使用 Increase 命令增加钱包余额的权限。

3.5.4.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用 Select File 命令通过文件标识符来选择文件。
- 存款命令（Increase）
  当满足存款权限时，可以用 Increase 命令增加钱包余额。
- 扣款命令（Decrease）
  当满足扣款权限时，可以用 Decrease 命令减少钱包余额。
- 读记录文件（Read Record）
  当满足读权限时，可以用 Read Record 命令读出指定记录。

3.5.5 电子存折/电子钱包文件

3.5.5.1 定义

- 电子存折（ED）
  一种为持卡人进行消费、取现等交易而设计的使用个人密码（PIN）保护的金融 IC 卡应用。它支持圈存、圈提、消费、取现、修改透支限额及查询余额交易。
- 电子钱包（EP）

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、消费以及查询余额交易。除圈存交易外，使用电子钱包进行的任何交易均不记录交易明细，且无需验证口令（PIN）。

3.5.5.2 文件体结构—循环文件

请参看 3.4.5.2 文件体结构—循环文件。
每条记录的数据项如下表所示:

表 3.9 电子存折/电子钱包的文件结构

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

注：对于 EP，余额有效长度是 3 个字节。

3.5.5.3 文件头定义

表 3.10 电子存折/电子钱包文件头定义

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

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

3.5.5.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用 Select File 命令通过文件标识符来选择文件。
- 中国金融 IC 卡专用命令，见“《TimeCOS/PBOC 通用技术参考手册》之 7.中国金融 IC 卡专

用命令”。

3.5.6 变长记录文件

3.5.6.1 定义

变长记录文件为具有可变长度记录的文件。

3.5.6.2 文件体结构—变长线性文件

变长线性文件又叫变长记录文件。变长记录文件的数据以记录为单位进行存储，通过记录号或记录标识来选择每条记录。更新记录时，新的记录长度必须与卡中原有记录长度相同，否则本次更新无效。

一个文件中的记录数为 2～254，不同的操作系统所支持的记录长度最大值不一样，TimeCOS/PBOC 支持的记录长度最大值为 178 字节。

通常，变长记录以 TLV（Tag-Length-Value）格式存在。在 TimeCOS/PBOC 中，变长记录文件和密钥文件都采用变长记录格式。

变长记录文件的结构如下图所示：

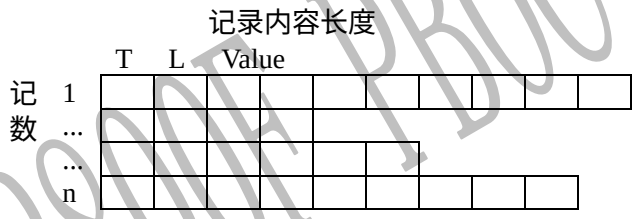


图 3-8 变长记录文件结构

3.5.6.3 文件头定义

表 3.11 变长记录文件头格式

文件头	字节（Byte）	描述
文件类型	1	‘2C’， 安全报文模式的设置见“7.1 Create File”
文件标识(FID)	2	见“3.2.3.1 文件标识（FID）”
文件大小	2	文件主体空间
访问权限 1	1	读权限
访问权限 2	1	追加权限/写权限
维护密钥标识	1	计算安全报文的密钥标识
RFU	1	‘FF’

说明：

- 文件主体空间=所有记录长度和；
  每条记录长度=1 字节记录标识符(T)+1 字节记录长度（L）+L 字节数据+1 字节校验码

（由 COS 计算）
每条记录长度的最大为 178 个字节。

3.5.6.4 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 选择文件命令（Select File）
  可以用 Select File 命令通过文件标识符来选择文件。
- 读记录文件（Read Record）
  当满足文件的读权限时，可以用 Read Record 命令文件中的记录。
- 增加记录（Append Record）
  当满足文件的追加权限时，可以用 Append Record 命令增加一条新记录。
- 写记录文件（Update Record）
  当满足文件的写权限时，可以用 Update Record 命令写（或更新）一条记录。

3.6 内部基本文件

用于存储由卡所解释的数据，指为了管理和控制目的由卡分析和使用的数据，包括密钥文件。

3.6.1 密钥文件（KEY 文件）

3.6.1.1 定义

存放密钥的文件，不可由外界读出。当满足文件的增加密钥权限时可以向文件中写入一条密钥；当满足密钥的使用权限时可在卡内进行相应的密码运算；当满足某条密钥的更改权限时可以修改此密钥。

- ***注：***
  - ***每个 DF 下只能有一个 KEY 文件，且必须最先被建立。在任何情况下密钥数据均无法读出。***
  - ***若当前 DF 下无任何文件，则在该 DF 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开该 DF 再进入此 DF 时，将遵循文件的访问权限。***

3.6.1.2 文件体结构—变长记录格式

一个 KEY 文件中可以包含多种密钥，每种密钥可以有多个。在 TimeCOS/PBOC 中，密钥文件采用变长记录格式，数据项定义如下表所示，记录中的 T、L 字节由 COS 维护。

表 3.12 KEY 文件记录格式

数据元		长度
T（由 COS 维护）		1
L（由 COS 维护）		1
Value	密钥头	5
	密钥值	不同的密钥类型长度不同

说明：

- 每条记录长度=1 字节 TAG+1 字节的长度+5 字节的密钥头+密钥值的长度。
- 密钥头和密钥值的设置见“ 7.4 Write Key 命令 ”。

- ***注：在 DF 下的 KEY 文件中增加一条连接 MF 下密钥的 KEY 记录，则记录长度=1 字节 TAG+1 字节的长度+1 字节密钥类型。见“3.6.3 全局密钥”。***

3.6.1.3 密钥头—密钥类型

表 3.13 密钥类型

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

3.6.1.4 文件头定义

表 3.14 KEY 文件头定义

文件头	字节（Byte）	描述
文件类型	1	‘ 3F ’
文件标识(FID)	2	‘ 0000 ’
文件大小	2	所有密钥记录长度之和+5 字节保留空间
DF 短文件标识符	1	见表 3.14
访问权限 2	1	增加密钥权限
RFU	1	‘ FF ’
RFU	1	‘ FF ’

说明：

- DF 短文件标识符

表 3.15 DF 短文件标识符

b7	b6	b5	b4	b3	b2	b1	b0	描述
0	0	0	X	X	X	X	X	当前 DF 为 DDF，低 5 位为 DDF 下目录基本文件的短文件标识符。
1	0	0	X	X	X	X	X	当前 DF 为 ADF，低 5 位为发卡方专用数据文件的短文件标识符。
1	1	0	X	X	X	X	X	包含当前 DF 的 A5 模板的短文件标识符
1	1	1	1	1	1	1	1	保留值

注：‘ A5 ’为文件控制信息专用模板的记录标识。

3.6.1.5 文件操作命令

- 建立文件命令（Create File ）
  当满足卡片当前 DF 的建立权限时，可以用 Create File 命令创建文件。
- 增加或修改密钥命令（Write Key）
  在满足密钥文件的增加密钥的权限时，可以用 Write Key 命令向密钥文件中写入一条密钥（设置密钥头和密钥值）；在满足密钥的更改权限时可以用 Write Key 命令更改密钥数据（不能更改密钥头数据）。
  注：不能用 Write Key 命令修改口令密钥。
- 对于不同的密钥类型，有其相应的命令，见“ 3.6.2. 密钥（KEY）和表 3.15 密钥类型及命令”。
  在满足密钥使用权限时才可使用相应的密钥进行认证或密码运算。

3.6.2 密钥（KEY）

3.6.2.1 DES 加密密钥

DES 加密密钥是用于进行 DES 加密运算的密钥。
DES 加密密钥所涉及的命令如下：

- 内部认证命令（Internal Authenticate）

3.6.2.2 DES 解密密钥

DES 解密密钥是用于进行 DES 解密运算的密钥。
DES 解密密钥所涉及的命令如下：

- 内部认证命令（Internal Authenticate）

3.6.2.3 DES&MAC 密钥

DES&MAC 密钥是用于进行 MAC 运算的密钥。
DES&MAC 密钥所涉及的命令如下：

- 内部认证命令（Internal Authenticate）

3.6.2.4 内部密钥

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

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

3.6.2.5 维护密钥

在以安全报文方式访问文件时，维护密钥是用于产生安全报文的密钥。见“《TimeCOS/PBOC 通用技术参考手册》之 4.安全报文传送”。
维护密钥所涉及的命令如下：

- 读二进制文件（Read Binary）
- 写二进制文件（Update Binary）
- 读记录文件（Read Record）
- 写记录文件（Update Record）
- 增加记录（Append Record）
- 存款（Increase）
- 扣款（Decrease）
- 卡片锁定（Card Block）
- 应用锁定（Application Block）
- 应用解锁（Application Unblock）

3.6.2.6 主控密钥

在以安全报方式装载或更改密钥时，主控密钥是用于产生安全报文的密钥。见“《TimeCOS/PBOC 通用技术参考手册》之 4.安全报文传送 ”。

主控密钥所涉及的命令如下：

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

3.6.2.7 口令解锁密钥

在以安全报文方式访问口令时，口令解锁密钥是用于产生安全报文的密钥。见“《TimeCOS/PBOC 通用技术参考手册》之 4.安全报文传送 ”。

- 口令密钥解锁命令（PIN Unblock），适用于标识为 00、长度为 2 到 6 字节的口令密钥。
- 口令认证命令（Verify PIN）
  验证并修改口令（Verify&Change PIN）,使用于长度为 8 字节的口令密钥。

3.6.2.8 口令重装密钥

口令重装密钥用来产生重装 PIN 命令的 MAC。

口令重装密钥所涉及的命令如下：

- 重装/修改口令密钥（Reload/Change PIN），适用于标识为 00、长度为 2 到 6 字节的口令密钥。

3.6.2.9 外部认证密钥

外部认证主要用于外部认证过程（卡对机具进行认证）中认证鉴别数据。

外部认证密钥如果被锁死将无法被解锁。

外部认证密钥所涉及的命令如下：

- 外部认证命令（External Authenticate）
  在满足密钥的使用权限时，可以用 External Authentication 命令验证终端的合法性。

3.6.2.10 修改透支限额密钥

修改透支限额密钥用来产生修改透支限额交易中使用的过程密钥 SK，在修改透支限额交易中计算 MAC 和 TAC。

修改透支限额密钥所涉及的命令如下：

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

3.6.2.11 圈提密钥

圈提密钥用来产生圈提交易中使用的过程密钥 SK，在圈提交易中计算 MAC。

圈提密钥所涉及的命令如下：

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

3.6.2.12 消费密钥

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

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

3.6.2.13 圈存密钥

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

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

3.6.2.14 口令密钥（PIN）

- PIN 也是密钥的一种，只有卡片持有者知道此 PIN 值，用以实现卡片对持有者的鉴别。
- 口令长度是 2 到 8 字节。
- 正确核对口令后可使卡片达到指定的安全状态，以执行某个操作（如读文件等）。
- 每次核对口令失败时错误计数器自动减一，当正确核对口令后，错误次数计数器复位（恢复原值）。当错误数达到 0 时，口令密钥自动被锁死。可以用相应的命令对被锁定口令进行口令解锁操作。
  错误计数器的取值范围是 1 到 15。

口令密钥所涉及的命令如下：

- 验证口令（Verify PIN）
- 验证并修改口令（Verify & Change PIN），适用于长度为 8 字节的口令密钥。
- 解锁口令（Unblock PIN），适用于长度为 8 字节的口令密钥。
- 重装/修改口令密钥（Reload/Change PIN），适用于标识为 00、长度为 2 到 6 字节的口令密钥。
- 口令密钥解锁（PIN Unblock），适用于标识为 00、长度为 2 到 6 字节的口令密钥。

全局 PIN

如果某口令密钥被装载在 MF 下，且此口令密钥可以在指定的 DF 下使用，则该密钥为全局 PIN。
在 DF 下，当满足全局 PIN 的使用权限时，可以核对该全局 PIN，以改变当前安全状态寄存器的值；也可使用其它相关命令对全局 PIN 进行操作，如验证并修改口令（Verify & Change PIN）等。
全局 PIN 的实现方法见“ 3.6.3 全局密钥 ”。

3.6.2.15 解锁口令密钥

解锁口令密钥用于解锁被锁定的 8 字节口令密钥。
解锁密钥解锁后无法被解锁。
解锁口令密钥所涉及的命令如下：

- 解锁口令（Unblock）

3.6.3 全局密钥

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

- 实现方法
  在 DF 下的 KEY 文件中增加一条连接 MF 下某一密钥的 KEY 记录，即 Write Key 命令中仅指明与 MF 下密钥相同的密钥标识和密钥类型，其真正的密钥属性和内容为 MF 下相对应的密钥类型和标识的密钥属性和内容。
- 应用方法
  在 DF 下，当满足全局密钥的使用权限时，可以进行相应的操作；当满足全局密钥的修改权限时，可以使用 Write Key 命令更改密钥（口令密钥除外）。

[例] 为了在卡片各个应用中使用一个口令，我们引入了全局 PIN 的概念（见“全局 PIN”）。

3.6.4 主密钥与密钥分散

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

对于 Single DES 主密钥，分散方法见图 3-8。

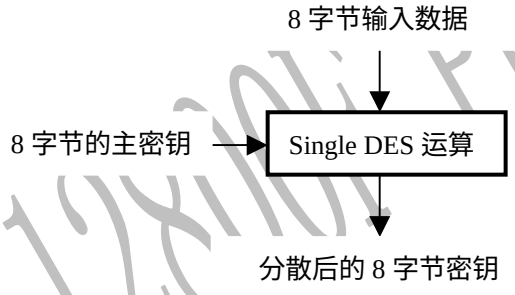


图 3-9 Single DES 密钥分散

对于 Triple DES 主密钥，分散方法见图 3-9。

左边的 8 字节输入数据=特定数据；

右边的 8 字节输入数据=特定数据按位求反。

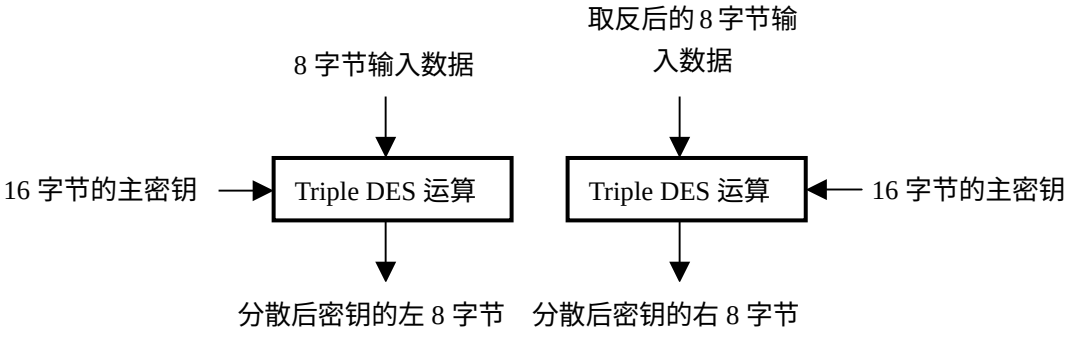


图 3-10 Triple DES 密钥分散

如此，终端必须知道此主密钥（MK）。

3.6.5 过程密钥

过程密钥是由指定密钥对可变数据加密产生的单倍长密钥。过程密钥产生后只能在某一（消费、取现等）过程中有效。图 3-10 描述了产生过程密钥的机制，其中输入数据是 8 字节。

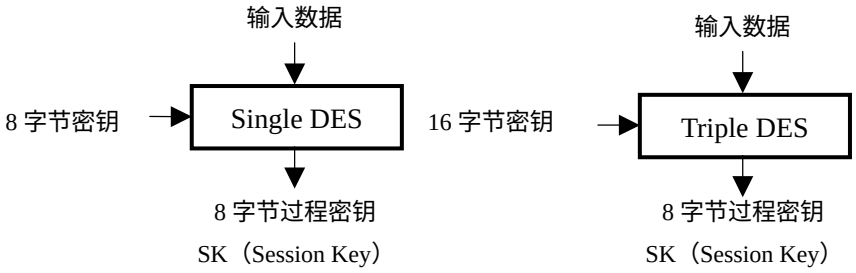


图 3-11 过程密钥的产生

3.6.6 密钥类型及命令集

表 3.15 密钥类型及命令集

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

说明：

表格中V表示命令可用于对应的密钥类型。

密钥类型用一个字节表示，如某个密钥类型为‘30’则表示该密钥为DES加密密钥。密钥类型在装载KEY文件时确定。

3.7 文件类型及命令集

下表为TimeCOS/PBOC命令适用的文件类型及命令集，水平方向表示TimeCOS的文件类型， 垂直方向表示TimeCOS/PBOC命令集：

表 3.16 文件类型及命令集

文件类型（HEX） / 命令	MF 38	DF 38	二进制 28	定长记录 2A	循环 2E	钱包 2F	变长记录 2C	KEY 文件 3F
Append Record					V		V	
Create	V	V	V	V	V	V	V	V
Credit For Load						V		
Debit For Purchase/Cash Withdraw						V		
Debit For Unload						V		
Decrease						V		
Erase DF	V	V						
Get Balance						V		
Get Transaction Proof						V		
Increase						V		
Initialize For Cash Withdraw						V		
Initialize For Load						V		
Initialize For Purchase						V		
Initialize For Unload						V		
Initialize For Update						V		
Read Binary			V					
Read Record				V	V	V	V	
Select File	V	V	V	V	V	V	V	
Update Binary			V					
Update Overdraw Limit						V		
Update Record				V	V		V	
Write Key								V

说明：

表格中V表示命令可用于对应的文件类型。

文件类型表示文件内部结构组织形式，用一个字节来表示，如某个文件类型为28H则表示该文件为二进制文件。文件类型在建立文件时规定。

3.8 TimeCOS/PBOC 文件结构举例

TimeCOS/PBOC 文件结构如下图所示：

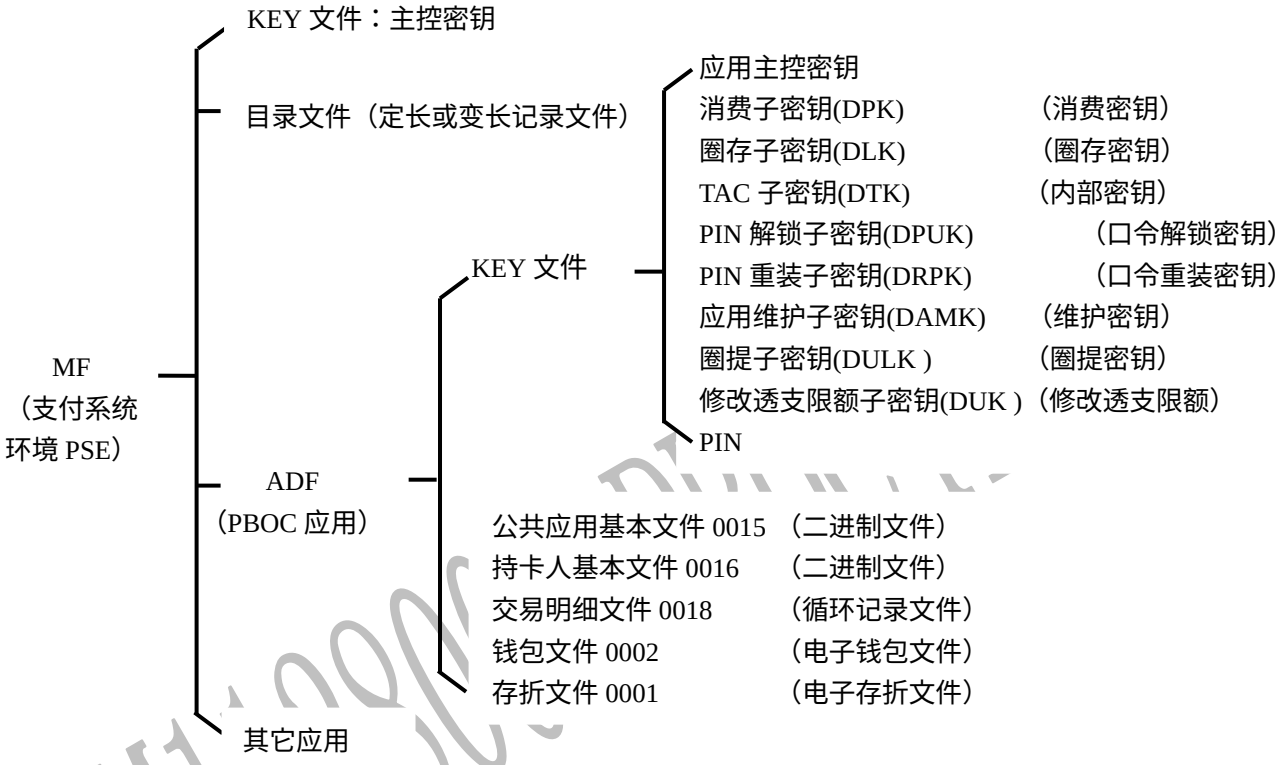


图 3-12 TimeCOS/PBOC 文件结构举例（简要）

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

3.9 文件空间计算

如前所述，每个文件在 EEPROM 中存放的格式如下：

12 字节文件头 （文件类型，文件标识符，文件主题空大小，权限，校验等）
文件主体

- 每个基本文件所占的 EEPROM 空间=文件头+文件主体空间
- 定长、钱包和循环文件的主体空间=记录个数*（记录长度+1）
- 每个 DF 所占的 EEPROM 空间=DF 头 12 字节+DF 下所有文件的空间和+DF 名称长度
- MF 的空间=MF 头 12 字节+MF 下所有文件空间之和

4. 卡片初始化设置

4.1 卡片初始化

卡片初始化完成以下两个功能：

- TimeCOS/PBOC的参数设置
- 安装传输密钥

卡片初始化是在卡片制造厂家完成。在卡片初始化之前，只能使用卡片初始化指令。

4.2 卡片传输协议

卡片传输协议 T=0.

4.3 卡片初始化后的文件结构

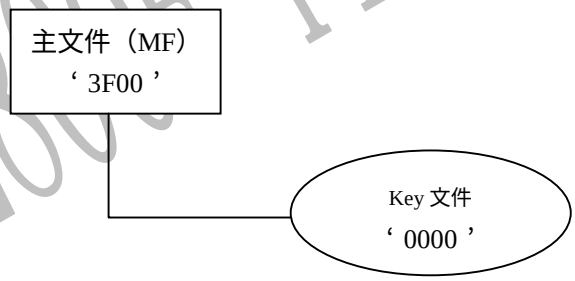


图 4-1 卡片初始化文件结构

4.4 主文件（MF）

- MF 是卡片文件系统的根。
- 文件参数

  文件类型：‘ 38 ’
  文件标识符：‘ 3F00 ’
  文件大小：卡片已根据芯片最大空间建立 MF
  MF 建立权：‘ AA ’
  MF 擦除权：‘ AA ’
  文件名称：1PAY.SYS.DDF01

4.5 KEY 文件

- KEY 文件里仅包含一条卡片传输密钥，以保证卡片运输过程中的安全。只有认证此密钥后才能进行发卡操作。
- 文件参数
  文件类型：‘ 3F ’
  文件标识符：‘ 0000 ’
  文件大小：‘ 1C ’
  MF 的短文件标识符：‘ 01 ’
  密钥增加权限：‘ EF ’

4.6 卡片传输密钥

- 只有认证卡片传输密钥后才能进行发卡操作。
- 密钥参数
  密钥标识：00
  密钥类型：‘ F9 ’
  使用权限：‘ F0 ’
  更改权限：‘ AA ’
  后续状态：‘ 0A ’
  错误计数器：‘ 33 ’
- 密钥值
  密钥长度：16 字节
  默认密钥值：‘ WATCHDATATimeCOS ’的 ASC 码，
  即 57415443484441544154696D65434F53.

> ◆ ***注：如果您需要专用的卡片传输密钥，必须在批量订货时声明。由我公司代为生成唯一的专用卡片传输密钥。***

4.7 使用说明

如前所述，卡片中 MF 的建立和擦除权限已经预置为 AA 且不可更改。只有卡片传输密钥认证通过后，安全状态寄存器达到状态‘ 0A ’时，才能进行发卡操作。

卡片传输密钥认证通过后，有以下两种操作方式：

1）擦除 MF 下的文件，重新建立卡片结构。

2）替换传输密钥值，后建立卡片结构。

有关外部认证的方法见“《TimeCOS/PBOC 通用技术参考手册》之 6.3 外部认证（External Authentication）”。

5. TimeCOS/PBOC 的安全体系

TimeCOS/PBOC 的安全体系从概念上可以分为安全状态、安全属性、安全机制和密码算法。

5.1 安全状态

安全状态是指卡在当前所处的一种安全级别。TimeCOS/PBOC的MF和DF分别具有16种不同的安全状态。

TimeCOS/PBOC在卡内部用两个4位寄存器来表示安全状态，每个寄存器的值可以是0至F之间的某一值。两个寄存器如下：

- MF安全状态寄存器

  它表示整个卡所处的安全级别。

- DF安全状态寄存器

  它表示当前应用所处的安全级别。

5.1.1 MF 安全状态寄存器

- 在以下几种情况下，MF 安全寄存器将被复位为 0：
  [1] 卡片复位后；
  [2] 当在 MF 下的核对口令或外部认证命令返回的错误状态为 63CX.
- 应用目录的改变不会影响该寄存器的值。
- 只有 MF 下的口令核对或外部认证通过后 MF 的安全状态寄存器值才发生变化。

5.1.2 DF 安全状态寄存器

- 在以下几种情况下，DF 安全寄存器将被复位为 0：
  [1] 卡片复位后。
  [2] 选择 DF 后（如选择下级子目录或同级目录等）。
  [3] 当前 DF 下的核对口令或外部认证命令返回的错误状态为 63CX.
- 只有当前目录下的口令核对或外部认证通过后 DF 的安全状态寄存器值才发生变化。

若当前目录为MF，则当前目录的DF安全状态寄存器的值等于MF的安全状态寄存器值。

5.2 安全属性

安全属性是指对某个文件/密钥进行某种操作时所必须满足的条件，也就是在进行某种操作时要求安全状态寄存器的值是什么。

安全属性又称访问权限，如下表所示：

表 5.1 访问权限

文件类型	访问权限
MF/DF	建立/擦除
KEY 文件	增加
——KEY 文件中的密钥	使用/更改
二进制文件	读/写
定长记录文件	读/写
循环文件	读/写
普通钱包文件	读&扣款/存款
电子存折/电子钱包文件	使用
变长记录文件	读/写

每种文件访问权限在***建立该文件（Create File）***时用一个字节指定；每种密钥访问权限在***增加密钥(Write Key)***时用一个字节指定。

TimeCOS的访问权限有别于其它任何操作系统的访问权限，它用一个区间来严格限制其他非法访问者。

假设当前安全状态寄存器的值用V来表示。

- 访问权限为‘0Y’时表示要求MF的安全状态寄存器的值大于等于Y。

  即：访问权限=‘0Y’ V>=Y

  [例] 如某文件读的权限为‘05’表示在对该文件进行读之前必须使MF的安全状态寄存器的值大于等于5. 即：文件的读权限=‘05’ V>=5

- 访问权限为‘XY’时（X不为0）表示要求当前目录的安全状态寄存器的值大于等于Y且小于等于X.

  [1] 当X>Y时

  即访问权限=‘XY’，且X>Y， 如此 Y≤V≤X

  [2] 当X=Y时,当前安全状态寄存器必须等于X.

  即访问权限=‘XY’，且X=Y， 如此 V=X=Y

  [3] 当X<Y时，表示禁止相应的操作。

  [例1] 如某文件写的权限为53表示对该文件进行写之前必须使当前目录的安全状态寄存器的值为3、4或5.

  [例2] 某文件读的权限为F0，写的权限为F1，代表可任意读取，写时必须满足当前目录的安全状态寄存器的值大于等于1.

5.3 安全机制

安全机制是指某种安全状态转移为另一种安全状态所采用的方法和手段。

为改变安全状态寄存器的值，必须通过某个密钥的口令或外部认证认证来实现；在密钥装载时，它的后续状态字（8bit）已经规定好了相应的安全状态，认证通过后，密钥的后续状态字节低4位将被置入安全状态寄存器。

- 在MF下认证通过后，将同时改变MF和当前目录的安全状态寄存器的值；

  在非MF下认证通过后，将只改变当前目录的安全状态寄存器值。

为更好的理解 TimeCOS 的安全机制，下面举一例说明：

设卡中某目录下有一个二进制文件，参数定义如下：

读权限=‘F1’；

写权限=‘F2’；

该目录下有一个口令密钥，口令核对通过之后的后续状态为1；

该目录下有一外部认证密钥，使用权限为11，外部认证通过之后后续状态为2。

请看下面的操作及当前目录的状态寄存器的变化情况：

卡终端操作	方向	当前目录安全状态寄存器的值
选择 DF	⇒	0
	⇐	送返回信息
读二进制文件	⇒	0
	⇐	读的权限不满足，不允许读
验证口令	⇒	1
	⇐	口令核对正确
读二进制文件	⇒	1
	⇐	送出读出的数据
写二进制文件	⇒	1
	⇐	写的权限不满足，不允许写
外部认证	⇒	2
	⇐	外部认证正确
写二进制文件	⇒	2
	⇐	写成功
读二进制文件	⇒	2
	⇐	送出读出的数据

图 5-1 访问权限控制

5.4 密码算法

TimeCOS/PBOC支持Single DES、Triple DES密码算法，密钥长度分别是8和16个字节。DES属于对称算法，加密和解密密钥相同。

Single DES算法

Single DES 算法是指使用单长度（8 字节）密钥 K 对 8 字节块的输入数据 X_1，X_2，X_3…加密，得到 8 字节块的输出数据 Y_1，Y_2，Y_3…。其中，

$$Y_I = DES\ (K)\ [\ X_I\ ]$$

解密方式如下：

$$X_I = DES^{-1}\ (K)\ [\ Y_I\ ]$$

3DES 算法（Triple DES 算法）

3DES 算法是指使用双长度（16 字节）密钥 K＝（$K_L||K_R$）将 8 字节明文数据块加密成密文数据块， 如下所示：

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

解密的方式如下：

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

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

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

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

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

6. 命令与应答

6.1 命令与响应格式

从终端发出的命令和卡片响应的信息必须遵从以下 4 种格式。

情形 1:

命令：

CLA	INS	P1	P2	00

响应：

SW1	SW2

情形 2：

命令:

CLA	INS	P1	P2	Le

响应:

Le 字节的 DATA	SW1	SW2

情形 3：

命令:

CLA	INS	P1	P2	Lc	DATA

响应：

SW1	SW2

情形 4：

命令:

CLA	INS	P1	P2	Lc	DATA	Le

响应:

Le 字节的 DATA	SW1	SW2

6.2 命令格式

TimeCOS 命令由 4 字节的命令头和命令体组成，见图 6-1。

命令头				命令体		
CLA	INS	P1	P2	Lc	DATA	Le

图 6-1 命令格式

6.2.1 命令头域

命令头定义板报文的内容如下表所示：

表 6.1 命令头域

代码	长度 (byte)	值 (Hex)	描述
CLA	1	X0	不带安全报文的命令
		X4	带安全报文的命令
INS	1	XX	指令代码
P1	1	XX	参数 1
P2	1	XX	参数 2

6.2.2 命令体

命令体中各项是可选的。

Lc 命令数据域中 DATA 的长度，该长度不可超过 178 字节。
Data 命令和响应中的数据域。
Le 响应数据域中期望数据的长度。
Le=00，表示需要最大字节数， 该长度不可超过 178 字节。

XX ⇒ 1 个字节 16 进制数
XXXX ⇒ 2 个字节 16 进制数
XX...XX ⇒ 未知个字节 16 进制数

6.3 响应数据格式

TimeCOS 命令的应答由数据和状态字组成，见图 6-2。

数据	状态字	
响应中接收的数据位串	SW1	SW2

图 6-2 响应数据格式

6.3.1 返回数据

返回数据域是可选项。

6.3.2 返回状态字（SW1SW2）

SW1 SW2 是卡片执行命令的返回代码，任何命令的返回信息都至少由一个状态字组成。

6.4 状态字 SW1SW2 意义

状态字说明了命令处理的情况，即命令是否被正确执行，如果未被正确执行，原因是什么。

状态字由2部分组成：

SW1（status word1）：表示命令处理状态；

SW2（status word1）：表示命令处理限定。

表 6.2 状态字 SW1SW2

SW1	SW2	Description
90	**00**	正确执行
61	**XX**	正确执行 XX 表示响应数据长度。可用 Get Response 命令取回响应数据。（仅用于 T=0）
62	**81**	回送的数据可能错误
62	**83**	选择文件无效，文件或密钥校验错误
63	**Cx**	X 表示还可再试次数
64	**00**	状态标志未改变
65	**81**	写 EEPROM 不成功
67	**00**	错误的长度
69	**00**	CLA 与线路保护要求不匹配
69	**01**	无效的状态
69	**81**	命令与文件结构不相容
69	**82**	不满足安全状态
69	**83**	密钥被锁死
69	**85**	使用条件不满足
69	**87**	无安全报文
69	**88**	安全报文数据项不正确
6A	**80**	数据域参数错误

6A	**81**	功能不支持或卡中无 MF 或卡片已锁定
6A	**82**	文件未找到
6A	**83**	记录未找到
6A	**84**	文件无足够空间
6A	**86**	参数 P1 P2 错误
6B	**00**	在达到 Le/Lc 字节之前文件结束，偏移量错误
6C	**xx**	Le 错误
6E	**00**	无效的 CLA
6F	**00**	数据无效
93	**02**	MAC 错误
93	**03**	应用已被锁定
94	**01**	金额不足
94	**03**	密钥未找到
94	**06**	所需的 MAC 不可用

注意：

- 当 SW1 的高半字节为‘9’，且低半字节不为‘0’时，其含义依赖于相关应用。
- 当 SW1 的高半字节为‘6’，且低半字节不为‘0’时，其含义与应用无关。

7. TimeCOS/PBOC 发卡命令

- 此部分描述了 TimeCOS/PBOC 的发卡命令，以下各节将详细描述这些命令。
- 有关安全报文的操作见 “《TimeCOS/PBOC 通用技术参考手册》之 4. 安全报文传送 ”。

表 7.1 列出了 TimeCOS/PBOC 发卡命令。

表 7.1 TimeCOS/PBOC 发卡命令

序号	命令	CLA	INS	功能描述	兼容性
1	**Create File**	80	E0	建立文件（DF、EF）	专有
2	**Erase MF**	80	0E	擦除 MF	专有
3	**Erase EF/DF**	00	E4	擦除 EF/DF	专有
4	**Set Protocol**	80	14	设置卡片通讯协议	专有
5	**Write Key**	80/84	D4	增加或改密钥	专有

7.1 Create File（建立文件）

7.1.1 定义与范围

Create File 命令用于建立文件系统。请参见“ 3.4 专用文件、3.5 工作基本文件和 3.6 内部基本文件 ”。

7.1.2 注意事项

- 在满足当前 DF 的建立权限时，可用此命令建立 DF 或 EF。
- 每个 DF 下只能有一个 KEY 文件，且必须最先被建立。
- 当前 DF 被擦除后，则在该 DF 下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开当前 DF 再进入 DF 时，将遵循文件的访问权限。
- 目录文件建立后不能自动被选择（MF 除外），需使用 Select File 命令选择。

7.1.3 命令报文

表 7.2 Create File 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	80	-
INS	1	E0	-
P1P2	1	XXXX	文件标识（FileID）
Lc	1	XX	-
DATA	XX	XX…XX	文件控制信息（和 DF 名称）
Le	-	-	不存在

注：MF 的文件标识符必须是‘3F00’；
KEY 文件的文件标识符必须是‘0000’；
电子存折的文件标识符必须是‘0001’； 电子钱包的文件标识符必须是‘0002’。

7.1.4 命令报文数据域

命令数据域中的所有权限设置请参见“ 5. TimeCOS/PBOC 的安全体系 ”。

7.1.4.1 主文件（MF）

- P1 P2 参数固定为‘ 3F 00 ’

表 7.3 MF 的文件控制信息

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

7.1.4.2 专用文件（DF）

表 7.4 DF 的文件控制信息

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

7.1.4.3 基本文件（EF）

基本文件控制信息内容如下表所示。

表 7.5 EF 的文件控制信息

数据域 / 文件类型	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
二进制文件	‘ 28 ’	文件空间		读权限	写权限	‘ FF ’	见说明[2]
定长记录文件	‘ 2A ’	2≤记录数≤254	记录长度≤178	读权限	写权限	‘ FF ’	见说明[2]
循环文件	‘ 2E ’	2≤记录数≤254	记录长度≤178	读权限	写权限	‘ FF ’	见说明[2]
普通钱包文件	‘ 2F ’	2≤记录数≤254	记录长度<8	读/扣款权限	存款权限	‘ FF ’	见说明[2]
电子存折/电子钱包	‘ 2F ’	记录数=2	记录长度=8	使用权限	TAC 密钥标识符 见说明[3]	‘ FF ’	交易明细文件短标识 见说明[3]
变长记录文件	‘ 2C ’	文件空间=所有记录长度和 每条记录=记录长度+1 字节校验码（由 COS 计算）		读权限	写权限	‘ FF ’	见说明[2]
密钥文件	‘ 3F ’	文件空间=所有密钥记录长度之和+5 字节保留空间 每条记录的计算方法见说明[4]		当前 DF 文件短标识符 见说明[4]	增加权限	‘ FF ’	‘ FF ’

说明：

[1] 二进制文件、定长记录文件、变长记录文件、循环文件、普通钱包文件（密钥文件、电子存折/电子钱包文件除外）都可以采用安全报文传送。

如对上述文件进行安全报文传送，只需在建立文件时改变文件类型字节高两位即可。

基本文件数据域Byte1（文件类型）定义如下：

b7	b6	b5	b4	b3	b2	b1	b0	线路保护方式
0	0	文件类型						无
1	0	文件类型						MAC
1	1	文件类型						DES&MAC

[例] 建立文件时若需进行线路保护则将文件类型最高位置 1，如二进制类型由 28 变为 A8。

◆ ***注意：具有线路保护属性的文件，在进行写操作时必须使用相应的线路保护模式，在进行读操作时必须按"说明[2]"中的规定使用明文方式或相应的线路保护模式。***

[2] 对文件进行线路保护时所使用的*维护密钥标识设置*

基本文件数据域 Byte7 定义如下：

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

1) b7=1，表示该文件不支持带线路保护读,b3b2=11；
b7=0,表示该文件必须带线路保护读。
2) b6-b4 位保留为 1。
3) b3b2=11,表示用标识 00 的维护密钥；
b3b2=10，表示用标识 01 的维护密钥；
b3b2=01，表示用标识 02 的维护密钥；
b3b2=00，表示用标识 03 的维护密钥。
4) b1b0 的设置方法与 b3b2 相同。

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

[3] 电子存折/电子钱包文件

1) TAC 密钥标识符：Byte6 为该钱包文件进行交易时用于生成交易验证码 TAC 的密钥标识。
2) 交易明细文件短标识：Byte7 的低 5 位为交易明细文件的短文件标识符。

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

[4] KEY 文件

注：KEY 文件标识符必须是‘0000’。

1) 每条记录长度=1 字节 TAG+1 字节的长度+5 字节的密钥头+密钥值的长度。
记录中的 T、L 字节由 COS 维护。
注：对于连接 MF 下密钥的 KEY 记录，则
记录长度=1 字节 TAG+1 字节的长度+1 字节密钥类型。
记录中的 T、L 字节由 COS 维护。
2) DF 文件短标识符
DF 文件短标识符如下表所示。

表 7.6 DF 文件短标识符

b7	b6	b5	b4	b3	b2	b1	b0	描述
0	0	0	X	X	X	X	X	当前 DF 为 DDF，低 5 位为 DDF 下目录基本文件的短文件标识符。
1	0	0	X	X	X	X	X	当前 DF 为 ADF，低 5 位为发卡方专用数据文件的短文件标识符。
1	1	0	X	X	X	X	X	包含当前 DF 的 A5 模板的短文件标识符
1	1	1	1	1	1	1	1	保留值

注：‘ A5 ’为文件控制信息专用模板的记录标识。

7.1.5 响应报文数据域

响应报文数据域不存在。

7.1.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.7 Create File 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
67	00	错误的长度
69	82	建立权限不满足
6A	80	记录个数小于 2 或目录级数超过三级
6A	84	文件无足够空间
6A	86	文件已存在

7.2 Erase MF（擦除主文件 MF）

7.2.1 定义与范围

Erase MF 命令用于擦除 MF，该指令仅对 MF 有效。

7.2.2 注意事项

- 在满足 MF 的擦除权限时，可以用此命令擦除 MF 下的所有文件(DF、EF)，但 MF 当前的访问权限、空间等信息并没有改变（即不能擦除当前 MF 的文件头信息），且 MF 的文件名称也不能被擦除。
- 当前 MF 下无任何文件时，则在该目录下可任意擦空 MF 而不受擦除权限控制。
- 当前 MF 被擦除后，则在该目录下可任意建立文件和读写文件而不受文件访问权限的限制，一旦离开 MF 再进入 MF 时，将遵循文件的访问权限。

7.2.3 命令报文

表 7.8 Erase MF 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	80	-
INS	1	0E	-
P1	1	00	-
P2	1	00	-
Lc	1	00	-
DATA	-	-	不存在
Le	-	-	不存在

7.2.4 命令报文数据域

命令报文数据域不存在。

7.2.5 响应报文数据域

响应报文数据域不存在。

7.2.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.9 Erase MF 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
65	81	写 EEPROM 不成功
69	82	擦除权限不满足
6A	81	用此命令擦除 DF 时回送的错误信息

7.3 Erase EF/DF（擦除目录文件 EF/DF）

7.3.1 定义与范围

Erase EF/DF 命令用于擦除 MF 下与 P1P2 匹配的 EF/DF，并且该文件的访问权限、空间等信息（即头文件，包括文件名称）也都被擦除。擦除所带来的剩余空间也重新任意分配。。(**P1P2 指 MF 下某一 EF/DF 的 文件标识)**

7.3.2 注意事项

- 擦除任何文件（EF/DF）均必须在其父 DF 下进行，且必须满足父 DF 的擦除权限。
- 在满足其父 DF 的擦除权限时，可以用此命令擦除 MF 下与 P1P2 匹配的 EF/DF，并且该文件的访问权限、空间等信息（即头文件，包括文件名称）也都被擦除。擦除所带来的剩余空间也重新任意分配。
- 擦除与 P1P2 匹配 EF/DF 时，不对别的 EF/DF 产生任何影响。

7.3.3 命令报文

表 7.10 Erase EF/DF 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	00	-
INS	1	E4	-
P1	1	00	-
P2	1	00	-
Lc	1	02	-
DATA	-	-	见说明
Le	-	-	不存在

说明：数据域中为 MF 下的某一 DF/EF 的文件标识号，长度 2 字节。

7.3.4 命令报文数据域

命令报文数据域不存在。

7.3.5 响应报文数据域

响应报文数据域不存在。

7.3.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.11 Erase EF/DF 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
65	81	写 EEPROM 不成功
69	82	擦除权限不满足

7.4 Set Protocol（设置通讯协议）

7.4.1 定义与范围

Set Protocol 命令用于设置通讯协议。

7.4.2 注意事项

- 当前目录必须是 MF 且必须满足 MF 的擦除权限时才可用此命令设置卡片通讯协议。
- 若当前 MF 下无任何文件，则设置卡片通讯协议不受任何权限的限制。

7.4.3 命令报文

表 7.12 Set Protocol 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	80	-
INS	1	14	-
P1	1	00	-
P2	1	00	-
Lc	1	01	-
DATA	1	XX	协议参数，见表 7.13
Le	-	-	不存在

7.4.4 命令报文数据域

命令报文数据域为 1 字节的协议参数，如下表所示：

表 7.13 协议参数设置

b7	b6	b5	b4	b3	b2	b1	b0
1	1	1	1	1	1	1	通讯协议

说明：

b0=0，表示卡片采用 T=0 通讯协议；

b0=1，表示卡片采用 T=1 通讯协议；

卡片的缺省值为 FE，即使用 3.57MHz 晶振，9600bps 通讯速率，T=0 通讯协议。

◆ ***注意：在正常情况下，通讯协议只能从 T=0 改为 T=1。若要求自由改变或希望支持其它通讯速率，批量定卡时必须特殊申明。***

7.4.5 响应报文数据域

响应报文数据域不存在

7.4.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.14 Set Protocol 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
67	00	长度错误
69	82	权限（MF 擦除权限）不满足
6A	81	当前目录不是 MF 或无 MF

7.4.7 应用举例

[1] 操作：将通讯协议由 T=0 改为 T=1.
命令：80 14 00 00 01 FF
说明：参数为 FF(11111111)表示使用 3.57MHZ 晶振,9600bps 通讯速率，T=1 通讯协议。

7.5 Write Key（增加或修改密钥）

7.5.1 定义与范围

Write Key 命令可向卡中装载密钥（向 KEY 文件写入密钥），或更新卡片已存在密钥（口令密钥除外）。请参见“ 3.6 内部基本文件 ”。

7.5.2 注意事项

- 在满足当前 DF 下 KEY 文件的增加权限时时，可用 Write Key 命令向 KEY 文件中写入密钥。
- 当满足密钥的修改权限时，可以对密钥值进行修改（口令密钥除外）。

7.5.3 命令报文

表 7.15 Write Key 命令报文编码

代码	长度 (byte)	值 (Hex)	描述
CLA	1	80/84	-
INS	1	D4	-
P1	1	01	用于密钥装载
		3X	密钥类型，用于密钥更新
P2	1	XX	密钥标识
Lc	1	XX	数据长度
DATA	XX	XX…XX	密钥头+密钥值
Le	-	-	不存在

说明：P2 的设置见“ 7.4.4.1 密钥装载 之说明[3] ”

7.5.4 命令报文数据域

命令数据域中的所有权限设置请参见“ 5. TimeCOS/PBOC 的安全体系 ”。

7.5.4.1 密钥装载

命令报文数据=密钥头（5 字节）+密钥值。

若为线路加密保护则由被加过密的数据附上 4 字节 MAC 码组成。（见说明[2]）

表 7.16 Write Key 之密钥装载命令报文数据域

数据域 / 密钥类型	Byte 1	Byte2	Byte3	Byte 4	Byte 5	密钥值长度（byte）
DES 加密密钥	‘ 30 ’	使用权限	更改权限	密钥版本号	算法标识	8/16
DES 解密密钥	‘ 31 ’	使用权限	更改权限	密钥版本号	算法标识	8/16
DESMAC 密钥	‘ 32 ’	使用权限	更改权限	密钥版本号	算法标识	8/16
内部密钥	‘ 34 ’	使用权限	更改权限	密钥版本号	算法标识	8/16
维护密钥	‘ 36 ’	使用权限	更改权限	‘ FF ’	错误计数器	8/16
主控密钥	即密钥标识为 00 的外部认证密钥，其命令报文数据域同外部认证密钥。					
外部认证密钥	‘ 39 ’	使用权限	更改权限	后续状态	错误计数器	16
口令解锁密钥	‘ 37 ’	使用权限	更改权限	‘ FF ’	错误计数器	8/16
口令重装密钥	‘ 38 ’	使用权限	更改权限	‘ FF ’	错误计数器	8/16
修改透支限额密钥	‘ 3C ’	使用权限	更改权限	密钥版本号	算法标识	8/16
圈提密钥	‘ 3D ’	使用权限	更改权限	密钥版本号	算法标识	8/16
消费密钥	‘ 3E ’	使用权限	更改权限	密钥版本号	算法标识	8/16
圈存密钥	‘ 3F ’	使用权限	更改权限	密钥版本号	算法标识	8/16
口令密钥	‘ 3A ’	使用权限	‘ EF ’	后续状态	错误计数器	2～8（对于金融目录下的口令，如果口令长度不足 6 个字节，后补‘ FF ’）
解锁口令密钥	‘ 3B ’	使用权限	更改权限	指定需解锁的口令密钥标识	错误计数器	8
连接 MF 下的密钥	‘ 3X ’	此密钥数据域只有密钥类型 1 字节。 采用此种方法装载的密钥，其真正的密钥属性和内容为 MF 下相对应的密钥类型和标识的密钥属性和内容（见 3.6.3 全局密钥）				

注：表中密钥版本号、后续状态等见说明[4]。

说明：

[1] 对于密钥也可以采用安全报文传送。

如对密钥进行安全报文传送（使用Write Key、Verify等），只需在安装密钥时改变Byte1(密钥类型)字节高两位即可。

密钥数据域Byte1（密钥类型）字节定义如下：

b7	b6	b5	b4	b3	b2	b1	b0	线路保护方式
0	0	密钥类型						无
0	1	密钥类型						DES
1	1	密钥类型						DES&MAC

例：对密钥若需进行线路加密保护（DES&MAC）则将密钥类型最高位及次高位均置1，如外部认证密钥类型由‘ 39 ’变为‘ F9 ’.

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

[2] 以安全报文方式装载或修改密钥时所使用的密钥如下：

- 当装载 MF 下的主控密钥时，分以下两种情况：
  i. 由厂家在卡片 MF 的 KEY 文件中已预先装入一条主控密钥(即卡片传输密钥，见“4.卡片初始化设置”)，其密钥带有线路保护属性。用户可以在发卡中先认证或替换此密钥，后继续对卡片进行发卡操作。
  ii. 在用户擦除 MF 后，MF 下的主控密钥必须以明文方式装入，但可以设置密钥类型为线路保护方式，此后可以使用线路保护方式更新此密钥。

  当修改 MF 下的主控密钥时，用 MF 下的主控密钥加密数据和计算 MAC。
- 当装载应用目录（MF 除外）下的主控密钥时，用上一级应用目录下的主控密钥加密数据和计算 MAC。

  当修改应用目录（MF 除外）下的主控密钥时，用当前应用目录下的主控密钥加密数据和计算 MAC。
- 当装载/更新应用目录（MF 或 DF）下的密钥（主控密钥除外）时，用当前应用下的主控密钥加密数据和计算 MAC。

MAC 计算方法见“《TimeCOS/PBOC 通用技术参考手册》之 4.安全报文传送”。

[3] 若应用目录下某类型密钥只有一个，则其密钥标识是‘00’，否则，应从‘01’顺序开始。在一个应用下：

- 只能有一个主控密钥、口令解锁密钥、一个重装口令密钥，它们的密钥标识必须是 00。
- 维护密钥最多可以有 4 个，密钥标识为 00～03。
- 对于金融应用下的口令，密钥标识为 00。
- 密钥标识不能是‘FF’。

[4] 术语解释：

- 使用权限

  指该密钥在使用时如核对、认证、运算时所需满足的条件。

  例如：使用权为 41 表示在使用该密钥时当前目录安全状态寄存器值必须大于等于 1 且小于等于 4。
- 更改权限

  指用 WRITE KEY 更改密钥内容的权限,在满足该条件时可使用 Write Key 更改密钥内容，但不能改变错误计数器的值。
- 错误计数器

  高半字节指出密钥可以连续错误的最多次数，低半字节指出还可以再试的次数。如果连续错误错超过规定的次数，密钥自动被锁死。

  例如：错误计数器的值为 33，表示该密钥最多可以连续错误 3 次，若输错一次则其值变为 32，再错一次之后变为 31，若下次核对或认证正确则该值变为 33。使用解锁口令时，解锁口令正确后错误次数低半字节被设置成高半字节值，同时口令被修改。

解锁口令若错误，解锁口令允许再试次数减一，解锁口令和外部认证密钥锁死后无法被解锁。

- 后续状态
  当口令核对成功或外部认证成功后，置安全状态寄存器值为后续状态的低半字。
- 解锁 KID(指定需解锁的口令标识)
  当解锁口令核对成功后，想要解开的口令密钥的密钥标识，即要解锁哪个口令密钥。
- 密钥版本号和算法标识由用户自己定义。

7.5.4.2 密钥更改

命令报文数据=新密钥值。
若为线路加密保护则由被加过密的数据附上 4 字节 MAC 码组成。（见说明[2]）

- 在满足密钥更改权限时可使用 Write Key 更改密钥内容，但不能改变错误计数器的值。
- 口令密钥不允许使用此命令进行修改。
- 密钥被锁死不能使用该命令修改密钥。

7.5.5 响应报文数据域

响应报文数据域不存在

7.5.6 响应报文状态码

IC 卡可能回送的状态码如下所示：

表 7.17 Write Key 命令响应状态码

SW1	SW2	意义
90	00	命令成功执行
67	00	密钥长度错误
69	82	增加或修改权限不满足
69	83	密钥被锁死
6A	82	KEY 文件未找到
6A	83	密钥未找到
6A	84	KEY 文件空间已满
93	02	修改密钥时线路保护错误

7.5.7 举例说明

例如：某 ADF 下的主控密钥为 KActl，在该应用下以 DES&MAC 方式写入一维护密钥 K（16 字节），则命令报文如下（该命令的前一条命令为取 4 字节的随机数 Rnd4）：

84 D4 00 01 00 1C Encrypt(KActl， DATA)[24Bytes]+MAC(Rnd4+00000000， KActl， 84 D4 …Encrypt(KActl，DATA)[24Bytes]))[4Bytes]
响应状态为 9000。

附录 1 TimeCOS/PBOC 复位应答

- 在由终端发出复位信号以后，IC 卡以一串字节作为应答（即复位应答）。卡片通讯速率默认为 9600bps.
- 这些传输到终端的字节规定了卡和终端之间即将建立的通信特性。
- TimeCOS/PBOC 的复位信息完全符合 ISO 7816 规范。
- 客户可以定制特殊的复位信息。

对于 T=0 通讯协议的卡，复位应答信息如下表所示：

表附录 11.1 T=0 协议

符号	值 (Hex)	说明	长度（byte）
TS	3B	正向约定，首先传送的是字符最低有效位	1
T0	6D	TB1 和 TC1 存在，历史字符为 13 个	1
TB1	00	无需额外编程电压 VPP	1
TC1	00	无需额外的保护时间	1
T1 ~ TD	XX	历史字符	13

说明：

- TS=‘ 3B ’，它表示从 I/O 口传送数据时先传低位再传高位。
- T0=‘ 6D ’，它的低半字节D表明有13个历史字符，高半字节6（0110）表示TB1、TC1存在，由于TD1不存在所以为T=0的通讯协议。

历史字符如下表所示：

表附录 11.4 复位信息中的历史字符

符号	值 (Hex)	意义
T1	‘ W ’（‘ 57 ’）	芯片厂商注册代码：WATCHDATA 的缩写
T2	‘ D ’（‘ 44 ’）	
T3-T5	XX…XX	由 TimeCOS 定义
T6-T7	XXXX	卡片制造机构注册标识号
T8	XX	OS 用途定义
T9~TD	XX…XX	卡序号，每卡该序号唯一

附录 2 卡片的空间说明

1、建立 DF 时，Body Size 字节不存在任何意义，建立文件受建立权限和卡片空间限制，不受 DF 空间限制（因为其已经无意义）。

2、2.8 版中，开始支持 64K 卡片。对于 TimeCOS 而言，前 32K 和后 32K 是独立管理的。每个文件都由文件头和文件体组成，卡片中，所有文件的文件头都在前 32K 空间。而文件体要么全部位于前 32K，要么全部位于后 32K，不能跨越。且后 32K 仅能建立二进制文件/定长记录文件/变长记录文件。在计算空间的时候要注意该特点。

64K 卡片建立文件的指令具体描述如下：

对于 64K 的管理如下表所示：

	前 32K	**后 32K**
描述	1、Lc=7，即原定义的 Create File 命令，该文件体将位于此 2、所有文件的文件头均位于此	1、Lc=8，且最后一个字节必须为 FF 2、仅能建立二进制文件／定长记录文件／变长记录文件

附录 3 TimeCOS/PBOC 金融 IC 卡应用举例

1. 主密钥内容

PBOC 应用密钥索引为 0x01,0x02
密钥版本为 0x01

PBOC 应用（AID=A00000000386980701）下的主密钥如下表所示：

表附录 2.1 PBOC 应用下的主密钥

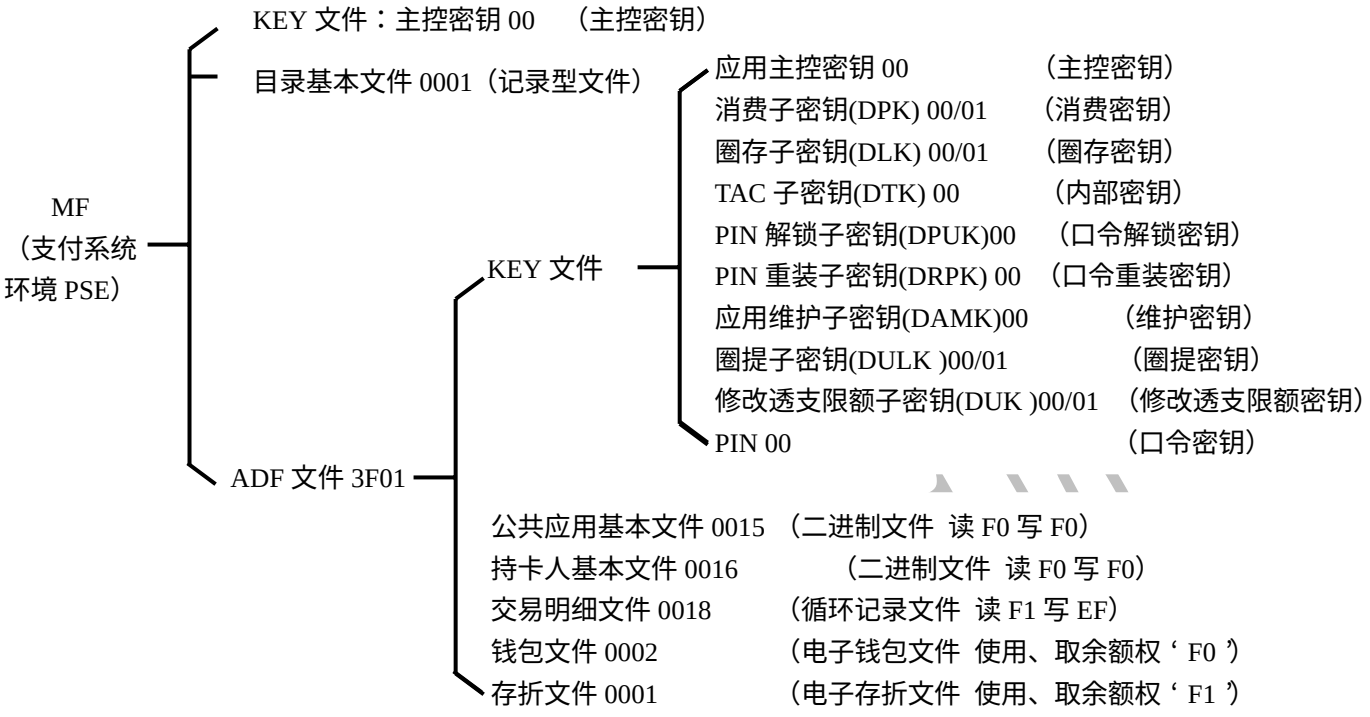
序号	密钥名称	默认值
1	消费主密钥 MPK_01	70E9BEA697723DF83605EBBCB7C2C7C4
1.	消费主密钥 MPK_02	6F153B35A97E1B56A1F8A3CE7AC5DAE2
2.	圈存主密钥 MLK_01	D3D6E8836832FDD4706D0671BB8BD28B
3.	圈存主密钥 MLK_02	B117DE007E79E786634B73A483AE9746
4.	TAC 主密钥 MTK	138D34F84B2031FF479E71BEFF107A76
5.	口令解锁主密钥 MPUK	07C3EAA0997CE026B8629A77CCB5AC9A
6.	口令重装主密钥 MRPK	48396B19B5E9765FDA25EC5C394058A0
7.	应用维护主密钥 MAMK	0F6FF9CC72204371093916F9E8BBF062
8.	圈提主密钥 MULK_01	E938FDDAAE9E5C8CE6A137B7F162E57E
9.	圈提主密钥 MULK_02	EFFA773C95533A0371BBA0B2D545734A
10.	修改透支限额主密钥 MUK_01	38B4BE8A7D9949440A868C68A6459216
11.	修改透支限额主密钥 MUK_02	B06FC85C7522F1D83A708844F33CACFD

2. 消费 SAM 卡

消费 SAM 卡文件结构请参见《TimeCOS/PSAM 技术参考手册》。PSAM 卡内有消费主密钥（算法级别为 01）。

3. 用户卡

1）用户卡文件结构如下图所示：



图附录 2-1 TimeCOS/PBOC 文件结构举例（详细）

2） 命令序列如下表所示。

表附录 2.2 TimeCOS/PBOC 卡发卡命令序列

命令描述	命令代码	安全报文传送方式
认证传输密钥	见“4.卡片初始化设置”	无
擦除 MF	800e000000	无
建立 KEY 文件	80E00000073F001C01EFFFFF	无
安装主控密钥	80D4010015F9F0AA0A335741544348444415441546 96D65434F53	无
建立目录基本文件(DIR)	80E00001072C0018F0AAFFFF	无
写目录基本文件	00DC000A15701361114F09A00000000386980701500450424F43	无
建立 ADF	80E03F01113802F4EFEFFFFFFFA00000000386980701	无
选择 ADF	00A4040009A00000000386980701	无
建立 KEY 文件	80E00000073F013D95EFFFFF	无
安装应用主控密钥	80D4010015F9F0AA0A335741544348444415441546 96D65434F53	DES&MAC
安装消费子密钥01（DPK_01）	80D4010115FEF0AA0100C8F0AA9765F6755FC1784BB1F3559F89	DES&MAC
安装消费子密钥02DPK_02	80D4010215FEF0AA0100C4091BBA14DB1476DE20282CBF6B4DCA	DES&MAC
安装圈存子密钥01（DLK_01）	80D4010115FFF0AA0100AAB15E015AD3AD2DC520583AAD8562C4	DES&MAC
安装圈存子密钥02（DLK_02）	80D4010215FFF0AA0100F04E391BACCDECE9909EAD7892151217	DES&MAC
安装 TAC 子密钥（DTK）	80D4010015F4F0AA01007D4CC5201758A960645361DFC293674E	DES&MAC
安装口令解锁子密钥（DPUK）	80D4010015F7F0AAFF33EC7CB73FA456435C79B44311FEEF45B1	DES&MAC
安装口令重装子密钥（DRPK）	80D4010015F8F0AAFF33BD98E4AA4E65615869B8C3BA5CEDFA9F	DES&MAC
安装应用维护子密钥（DAMK）	80D4010015F6F0AAFF33140DAE0916A9B16B5C64F22F6CE5378F	DES&MAC
安装圈提子密钥 1（DULK_01）	80D4010115FDF0AA01003C3D46BD7D7A6198985D8F454B12BBCF	DES&MAC
安装圈提子密钥 2（DULK_02）	80D4010215FDF0AA0100A386FADEDED1541CEE82BAD0BD688FC5	DES&MAC
安装修改透支限额子密钥 1（DUK_01）	80D4010115FCF0AA01007671A10411820448D7FDF4242C4AFCAD	DES&MAC
安装修改透支限额子密钥 2（DUK_01）	80D4010215FCF0AA01003311C442A3275BDBF3F75040D0FEC7B0	DES&MAC
安装 PIN	80D401000B3AF0EF01331234FFFFFFFF	无
建立公共应用基本文件	80E0001507A8001EF0F0FFFF	无
写基本应用文件	00D695001E1111222233330006030100061998081700000030199808151 9812155566	MAC
建立持卡人基本文件	80E0001607A80027F0F0FFFF	无
写持卡人基本应用文件	00D6960027000053414D504C4520434152442041444631000000000313130313032393831323138303031300 5	MAC
建立交易明细文件	80E00018072E0B17F1EFFFFF	无
建立电子存折文件	80E00001072F0208F100FF18	无
建立电子钱包文件	80E00002072F0208F000FF18	无

3） 说明

- ♦ 主文件（MF）
  - 文件标识符：‘ 3F00 ’
  - 文件名称是 1PAY.SYS.DDF01
  - 正确选择 MF 后，卡片返回相应的文件控制信息（FCI）如下：
    6F 15 84 0E 31 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 03 88 01 01
    有关 FCI 的的详细描述见 “《TimeCOS/PBOC 通用技术参考手册》之 6.10 选择文件（Select File) ”。
- ♦ MF 下的目录基本文件
  - 目录基本文件定义
    目录基本文件是一个记录型文件，用 1 到 10 的短文件标识符（SFI）标识。该目录基本文件附属于 DDF，目录的 SFI 包含在 DDF 文件控制信息中。目录可以使用 Read Record 命令进行读取。目录中一个记录可以包含几个入口地址，但一个入口地址不能跨越多个记录存储。
  - 本例中目录文件的短文件识符=01
  - 本例中目录基本文件有一条记录：70 13 61 11 4F 09 A0 00 00 00 03 86 98 07 01 50 04 50 42 4F 43，各部分意义见“《TimeCOS/PBOC 通用技术参考手册》之 6.10 选择文件（Select File) 应用举例[2] ”。

- ♦ PBOC 应用
  文件标识：‘ 3F01 ’
  文件名称：A00000000386980701
  正确选择此 ADF 后，卡片返回相应的文件控制信息（FCI）如下：
  6F 2E 84 09 A0 00 00 00 03 86 98 07 01 A5 21 9F 0C 1E 11 11 22 22 33 33 00 06 03 01 00 06 19 98 08 17 00 00 00 30 19 98 08 15 19 98 12 15 55 66
  有关 FCI 的的详细描述见“《TimeCOS/PBOC 通用技术参考手册》之 6.10 选择文件（Select File) ”。
- ♦ 电子存折/电子钱包应用的基本数据文件

表附录 2.4 电子存折和电子钱包应用的应用基本数据文件

文件标识符	‘ 0015 ’
文件类型	‘ A8 ’（线路保护的二进制文件）
文件主体空间	‘ 1E ’
读权限	‘ F0 ’（自由读取）
写权限	‘ F0 ’（写二进制时必须使用 DAMK 进行线路保护，如连续三次执行此命令失败，IC 卡回送‘ 9303 ’即应用永久锁定）

字节	数据元	长度
1-8	发卡方标识	8
9	应用类型标识	1
10	应用版本	1
11-20	应用序列号	10
21-24	应用启动日期	4
25-28	应用有效日期	4
29-30	发卡方自定义文件控制信息数据	2

- 电子存折和电子钱包应用的持卡人基本数据文件

表附录 2.5 电子存折和电子钱包应用的持卡人基本数据文件

文件标识符	‘ 0016 ’
文件类型	‘ A8 ’（线路保护的二进制文件）
文件主体空间	‘ 27 ’
读权限	‘ F0 ’（自由读取）
写权限	‘ F0 ’（写二进制时必须使用 DAMK 进行线路保护，如连续三次执行此命令失败，IC 卡回送‘ 9303 ’即应用永久锁定）

字节	数据元	长度
1	卡类型标识	1
2	本行职工标识	1
3-22	持卡人姓名	20
23-38	持卡人证件号码	16
39	持卡人证件类型	1

- 电子存折和电子钱包应用的交易明细文件

表附录 2.6 电子存折和电子钱包应用的交易明细文件

文件标识符	‘0018’
文件类型	‘2E’（循环文件）
记录个数	‘0B’（该循环文件必须能够容纳至少十条消费、取现、圈存、圈提交易 记录）
记录长度	‘17’
读权限	‘F1’（必须先验证口令）
写权限	‘EF’（交易明细由 IC 卡维护，不允许外部对其修改）

字节	数据元	长度
1-2	电子存折/电子钱包联机或脱机交易序号	2
3-5	透支限额	3
6-9	交易金额	4
10	交易类型标识	1
11-16	终端机编号	6
17-20	交易日期	4
21-23	交易时间	3

- 子密钥推导方法

以生成16字节的消费子密钥为例，在银行应用目录下，子密钥的生成均可参考此例。

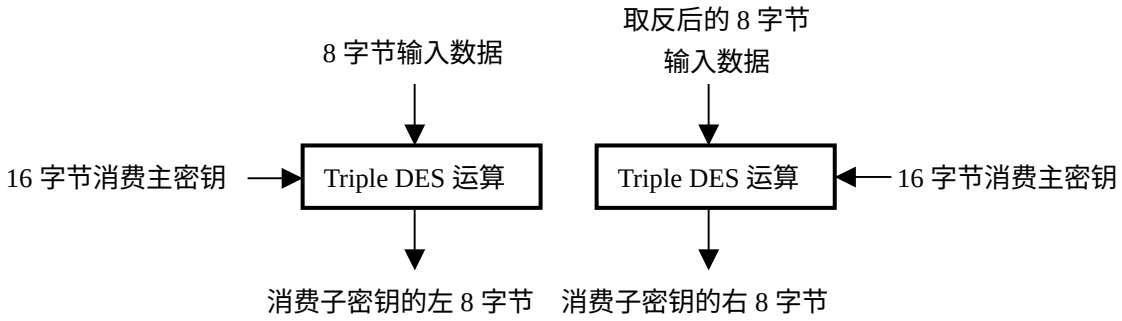
消费子密钥(DPK)左半部分的推导方法

1．将本张用户卡的应用序列号的最右 8 个字节作为输入数据。
2．将 16 个字节的消费主密钥(MPK)作为加密密钥。
3．用消费主密钥(MPK)对输入数据进行 Triple DES 运算。

消费子密钥(DPK)右半部分的推导方法

1．将本张用户卡的应用序列号的最右 8 个字节的求反作为输入数据。
2．将 16 个字节的消费主密钥(MPK)作为加密密钥。
3．用消费主密钥(MPK)对输入数据进行 Triple DES 运算。

如下图所示：



图附录 2-2 推导 16 字节消费子密钥的方法

附录 3 TimeCOS/PBOC 技术性能指标

一、 硬件技术性能参数

TimeCOS/PBOC 已经在很多种类型的芯片上实现，部分芯片的硬件性能参数如下表所示。随着技术的发展日新月异，这些指标将有变动，对于这些变动，本公司不再另行通知。

表附录 3.1 硬件技术性能参数

	技术指标
芯片类型	**SLE44C 系列/P83W86 系列**
微处理器	8 位保密控制器
程序空间 ROM	17K/20K
RAM	256 字节
EEPROM	512 字节/1K/2K/4K/8K/16K
时钟频率	1 ～ 5MHZ 可选，缺省为 3.57MHZ
EEPROM 寿命	500,000 次
擦写时间	擦写 1/2/4/8/16 字节时需 5.28/5.31/5.38/5.52/5.8 毫秒
数据保存时间	10 年
工作电压	2.7 ～ 5.5 V,缺省为 5 V
工作电流	小于 10 mA
省电模式	当 TimeCOS 等待接收命令时处于休眠状态，最大电流 100 微安
温度	-25 ～ +70 摄氏度
通讯速率	支持 9600bps,19200bps,38400bps 可选,缺省为 9600bps
通讯协议	支持 T = 0,T = 1 可选,缺省为 T = 0
APDU 长度	APDU 的最大长度为 183 字节

二、 TimeCOS 技术性能参数

TimeCOS/PBOC 在执行某些指令或运算是所需的时间参数如下表所示，仅供参考，这些参数的测试条件如无特别注明为：接触模式、工作时钟 3.57MHz、T = 0 协议、波特率 9600bps。参数本身如无特别注明只包括命令或运算的执行时间，而不包括通讯时间。时间单位为 mS。

表附录 3.2 TimeCOS/PBOC 技术性能参数

	技术指标
芯片类型	P83W86 系列/SLE44C 系列
TripleDES 时间	37
SHA 算法时间	147ms/64 Bytes
圈存（存折）	130
圈提	125
修改透支限额	127
消费（存折）	178
消费（钱包）	146
解锁应用	58
应用锁定	53
重装 PIN	46
解锁 PIN	106

附录 4 TimeCOS/PBOC 可定制的功能

TimeCOS/PBOC 可定制的功能如下所示:

- 通讯速率
- 复位信息
- COS 扩充功能

> - ***注：以上所示 TimeCOS/PBOC 可定制的功能必须在卡片初始化时进行设置，所以您必须在订货时指明所需的特征。***

通讯速率

通讯速率是指卡片与读写器之间的通讯速率。TimeCOS/PBOC 卡可支持以下两种通讯速率：

- 9600bps (标准产品配置)
- 38400bps
- 56K bps

复位信息

您可以定制特殊的历史字节以满足应用的特殊需求。

COS 扩充功能

我们可以在 TimeCOS/PBOC 卡中开发并加入 COS 扩充功能，以满足特殊用户的需求。

> - ***注：如果您需要以下定制功能：***
> - ***通讯速率***
> - ***复位信息***
> - ***COS 扩充功能***
>
> ***必须在订卡时特殊申明。***
>
> ***TimeCOS/PBOC 标准卡片产品不包括以上定制功能。***