

芯片操作系统(COS)	4
COS的发展过程	5
COS的基本特点	6
COS的基本任务	7
COS要解决的三个问题	8
文件操作	8
鉴别与核实	7
安全体系	7
安全状态	9
安全属性	10
文件安全属性	11
命令安全属性	12
内部认证	13
外部认证	14
MAC/TAC校验	15
COS的四个模块	16
COS程序结构	18
COS文件系统	20
COS数据传输	29
物理层	30
异步传输的ATR	31
协议参数选择	36
T=0 异步半双工字符传输协议	43
T=1异步半双工分组传输协议	44
COS命令集	45
COS实现举例介绍	46
文件的逻辑结构	47
文件描述块(文件头16B)	51
文件体	68
与文件操作相关的命令	79
与生命周期维护相关的命令	81

芯片操作系统COS



芯片操作系统COS

- ◆ 芯片操作系统(COS)
- ◆ COS文件系统
- ◆ COS数据传输
- ◆ COS命令集

芯片操作系统(COS)

COS—Chip Operating System

- ◆ COS的发展过程
- ◆ COS的基本特点
- ◆ COS的基本任务
- ◆ COS要解决的三个问题
- ◆ COS的四个模块
- ◆ COS的程序结构

COS的发展过程

- ◆ 早期(上世纪80年代初),专用监控程序
- ◆ 掩膜贵,慢,不能更改----结构化,通用化
- ◆ 通用化COS修改----专用COS
- ◆ 易于使用和二次开发----JAVA COS
- ◆ 标准化

COS的基本特点

- ◆ 原因:硬件性能有限,ROM,EEPROM
- ◆ 快(执行时间,加/解密时间,修改数据时间)
- ◆ 省(程序空间,数据空间,内存)
- ◆ 安全
- ◆ 防数据撕裂
- ◆ 存储器管理(寿命,编程时间,页面管理)



COS的基本任务

- ◆ 控制 卡与外界的数据交换(IN/OUT)
- ◆ 命令的解释与执行
- ◆ 文件的管理和数据安全
- ◆ 加/解密算法的管理

7



COS要解决的三个问题

- ◆ 文件操作
- ◆ 鉴别与核实(鉴别设备,核实持卡人)
- ◆ 安全体系(安全状态,属性,机制)

8



安全状态

安全状态是卡片当前所处的安全级别。

- (1) **卡片复位**: 卡片处于最低级别的安全状态
- (2) **执行鉴别命令**: 鉴别命令包括对**用户密码(PIN)的校验、对卡内密钥的校验**等。
- (3) **安全报文校验**: 对于包含安全报文的命令, 在执行命令前需要对安全报文进行校验。

存在不同的安全状态来记录不同层次的安全级别:

1. **全局安全状态**: 在执行与MF有关的鉴别命令后修改;
2. **特定文件的安全状态**: 当前文件(应用)的安全状态;
3. **特定命令的安全状态**: 只在执行一条包含有安全报文的命令时才存在, 命令执行完毕以后自动失效。

9



安全属性

- ◆ 文件安全属性
- ◆ 命令安全属性

10



文件安全属性

文件访问的安全属性包括了两个层次的内容:

- (1) **允许的操作类型**, 例如对于普通文件允许的读写操作, 对PIN、KEY等文件读操作禁止, 特殊文件只能通过应用命令来维护等。
 - (2) 进行操作所需要**满足的安全条件**, 也就是要求的安全状态。
- ◆ 两者结合就是文件的安全属性, 所以安全属性也可以看作是对文件所能进行的操作及其需要满足的安全条件。

11



命令安全属性

为保证信息传输的安全性、真实性和完整性, 除了以明文方式传递数据外, COS还提供安全报文传送方式。

数据的安全性和完整性通过使用消息认证码MAC(Message Authentication Code)来实现(命令全部报文的安全控制)。数据的可靠性通过对数据域的加密得到保证(命令数据域的安全控制)。

安全报文传送方式有**认证传输**、**加密传输**和**加密认证传输**三种方式。其中认证传输方式是在命令的数据域中添加MAC校验保证命令的真实性; 加密传输方式是将命令的数据域进行加密, 以保证数据的安全性; 而加密认证方式则是既保证数据的安全性, 又保证命令的真实。

12

内部认证

- 1、内部认证是**终端对卡的认证**；
- 2、由终端产生一个随机数，然后经智能卡加密后再传回到终端解密。因为每个卡有唯一的密钥，所以，如果结果和最初产生的随机数相同则说明该卡是合法的；
- 3、内部认证命令是终端认证卡片的过程，不同的应用可能会有不同的规定。
- 4、**注意认证频度**；

13

外部认证

- 1、外部认证是**卡对终端的认证**；
- 2、由智能卡产生随机数发送给终端，终端加密并回送给智能卡，智能卡在卡内判断终端的合法性；
- 3、外部认证成功以后，将修改对应的安全状态，并且复位卡片内的外部认证**密钥的尝试计数器**到初值。如果验证失败，将外部认证密钥的尝试计数器减一，直至减为0，将密钥锁定不能再进行外部认证操作为止。

14

MAC/TAC校验

MAC：安全报文，在需要安全报文的命令中使用，通过对计算MAC所用密钥的认证，完成卡对外部系统的认证，同时也保证了命令数据在传递过程中没有发生错误或者数据被替换

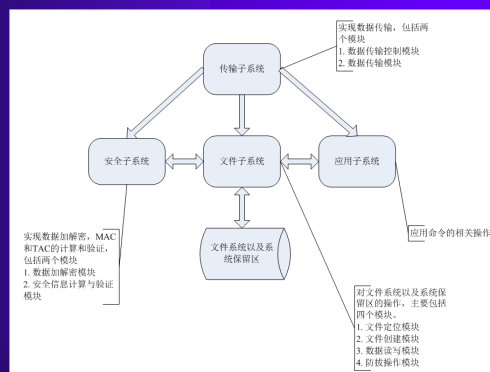
TAC：交易验证码(Transaction Authorization Cryptogram)，是卡片对交易的确认信息，在脱机消费交易TAC正确即表示发卡机构认可这笔交易。

15

COS的四个模块

- ◆ 1.传递管理器TM—传输协议
- ◆ 2.安全管理器SM—安全检查,防窃听侵入
- ◆ 3.应用管理器AM—命令执行的可能性
- ◆ 4.文件管理器FM—通过权限完成任务

16

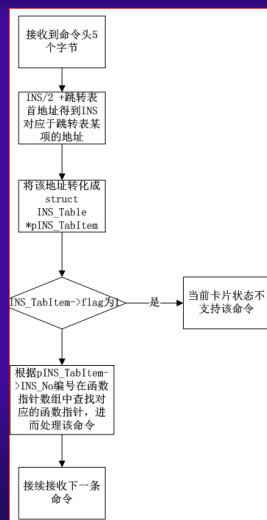


17

COS程序结构

- ◆ 完工操作
- ◆ COS的安全存放(ROM,EEPROM)
- ◆ 结构:ROM代码+EEPROM跳转表
- ◆ 硬件识别(序列号,自适应)
- ◆ 自检(ROM+EEPROM)
- ◆ 掩膜与软掩膜

18



19

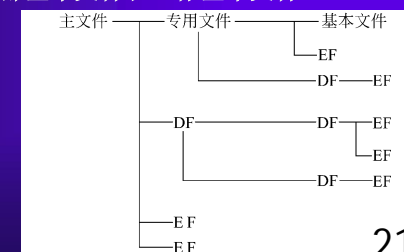
COS文件系统

- ◆ 文件系统
- ◆ 文件结构
- ◆ 文件访问条件
- ◆ 原子进程
- ◆ 文件属性
- ◆ 文件管理
- ◆ 程序下载

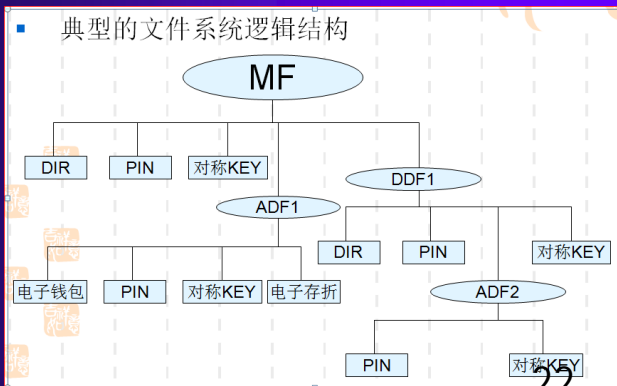
20

文件系统

- ◆ 主文件MF(根目录): 必有
 - ◆ 专用文件DF(子目录): 可选 DDF、ADF
 - ◆ 基本文件EF(文件): 可选
- 基本文件有内部基本文件和工作基本文件



21



22

文件结构

- ◆ 透明结构(二进制文件,执行文件)
- ◆ 线性定长结构(数据库文件结构)
- ◆ 线性变长结构(数据对象文件结构)
- ◆ 定长循环结构(进程控制文件结构)

23

文件访问条件

- ◆ 文件创建时确定,以后不能改动
- ◆ 面向状态的访问条件(灵活,易改)
- ◆ 面向命令的访问条件(鉴别,识别)

24



原子进程（防拔、防数据撕裂）

- ◆ 要么不执行, 要么完整执行的进程(防撕裂)
- ◆ 实现: 数据防拔的主要方法就是数据备份。
- 备份: 1. 备份 2. 标记 3. 改数据 4. 取消标记
- 修复: 在上电ATR前检查若有标记, 则用备份修复后取消标记。
- 实现要点: 标记区、备份区寿命（可用循环结构, 操作时间长, 重要数据才用此进程）。

25



文件属性

- ◆ WORM属性(一次写多次读)
- ◆ 多重存储属性(多备份, 取多数)
- ◆ EDC利用属性(差错检测, 提高可靠性)
- ◆ 写入访问属性(写入操作原子性)
- ◆ 并发访问属性(共享—同步, 优先问题)
- ◆ 数据传输选择属性(接触/非接触通道)

26



文件管理

- ◆ 文件头(不变)
(名, 类型, 结构, 大小, 存取条件, 属性, 链接指针)
- ◆ 文件体(可变)
- ◆ 页面管理(文件头, 文件体分页防撕裂)
- ◆ DF分割(一卡多用)
- ◆ 数据完整性检验
- ◆ 文件名(ISO/IEC7816-4,5), AID申请

27



程序下载

- ◆ 执行代码下载(太开放, 不安全, 界限寄存器)
- ◆ 解释型代码下载(JAVA)

28



COS数据传输

- ◆ 物理层
- ◆ 异步传输的ATR
- ◆ 协议参数选择
- ◆ 通信协议(T=)
- ◆ T=0
- ◆ T=1

29



物理层

- ◆ 半双工(RST, ATR, PPS请求及应答, 命令应答)
- ◆ 正向逻辑(约定) H=1, L=0, 低位先
- ◆ 负向逻辑(约定) H=0, L=1, 高位先
- ◆ 起始位, 停止位(保护时间), 偶校验
- ◆ ETU-基本时间单位(误差0.2ETU)
每一位在I/O线的持续时间定义为基本时间单元 etu, ATR期间 1etu=372个时钟周期, 即
1etu=372/f;
(3.5712MHz/372=9600bps)
(4.9152MHz/512=9600bps)

30

异步传输的ATR

- ◆ 最多33B
- ◆ RST后400-40000个时钟周期后开始传
- ◆ 相邻字节间间隔时间:12-9600ETU
- ◆ 复位应答信息的内容
 - 初始字符TS
 - 格式字符TO
 - 协议参数接口字节TA_i、TB_i、TC_i、TD_i (i=1,2,3,...)
 - 历史字节T1,T2~TK: 发行商与芯片序列号、OS版本
 - 校验字节TCK

31

ATR结构

- ◆ 起始字符:TS
- ◆ 格式字节:TO
- ◆ 参数:TA_i TB_i TC_i
- ◆ TD_i:
 - ◆ 3BH反向,3FH正向
 - ◆ D0-D3,历史字节长度
 - D4-D7 决定后继 TA_i TB_i TC_i TD_i
 - D0-D3,协议类型T
 - D4-D7 决定后继 TA_i TB_i TC_i TD_i
- ◆ 历史字节:T1-TK
- ◆ 校验字节TCK:异或=0

32

ATR参数

- ◆ 接口字节TA1 TB1 TC1 TA2 TB2的含义 (给接口设备用以计算的参数)
 - 时钟频率转换因子F
 - 位速率调整因子D
 - 操作模式-由TA2确定
 - 最大编程电流因子I
 - 编程电压因子P
 - 额外保护时间N
 - 时钟停止指示符X
 - 类别指示符U

33

ATR参数

- ◆ TA1:高四位F (时钟频率转换因子)
低四位D (位速率调整因子)

$$\text{工作时钟周期} = \frac{F}{D} \times \frac{1}{f_s} \text{ s}$$

- ◆ TB1:高二位 编程因子
- ◆ TC1:额外保护时间
- ◆ 当TD_{i-1} (i>2) 指出T=15后
 - TA_i的b8b7为时钟停止指示符X;
 - TA_i的b6~b1为类别指示符U;

34

ATR参数

- ◆ 有两种操作模式:
- ◆ TA2存在时是专用模式; TA2不存在时是协商模式。
- ◆ 专用模式中:
 - 当TA2的b5=0时, 使用由TA1指定的F值和D值;
 - 当TA2的b5=1时, 使用默认值。
- ◆ 协商模式中:
 - 如复位应答后无PPS请求, 则F和D使用默认值;
 - 如复位应答后有PPS请求, 则由IFD发送带有F和D的PPS请求, 并使卡转到新模式。

35

协议参数选择

- 在复位应答之后, 如果处于协商模式, 则允许接口设备向卡发送PPS请求。
- ◆ 只能在ATR后第一条命令
- ◆ 禁止多次,实际少用

36

PPS请求过程

- ◆ 接口设备允许发出PPS请求，其过程如下：
 - 接口设备向卡发送PPS请求；
 - 若卡收到正确的PPS请求，则发出PPS确认信号来应答，否则将超出初始等待时间；
 - 若成功地交换PPS请求和PPS应答，就选择好了新的协议类型和传送参数，然后按规定将数据从接口设备送到卡中；
 - 若卡收到错误的PPS请求，则不发回PPS应答信号；
 - 若初始等待时间超时，接口设备将卡复位或予以拒绝；
 - 若接口设备收到错误的PPS应答信号，将卡复位或予以拒绝；

37

PPS请求与PPS应答信号组成

- ◆ PPS请求与PPS应答信号的组成：
 - ◆ 初始字符PPSS
 - ◆ 格式字符PPS0
 - ◆ 任选字符PPS1, PPS2, PPS3
 - ◆ 校验字符PCK
 - ◆ 一般情况 PPS应答=PPS请求
 - ◆ PPS0的作用与T0相似，其中b8保留；
 - b5、b6、b7表示字符PPS1、PPS2、PPS3是否存在；
 - b1~b4选择协议类型。
 - ◆ PPS1给出F和D的参数值；PPS2给出N值，PPS3未定。

38

协议类型

- ◆ T=0 异步半双工字符传输协议
- ◆ T=1 异步半双工分组传输协议
- ◆ T=2,3 保留用于全双工传输协议
- ◆ T=4 ,增强型异步半双工字符传输协议
- ◆ T=5-13保留
- ◆ T=14 用于ISO非标准协议
- ◆ T=15,不属于传输协议,表示参数

39

应用协议数据单元（APDU）信息结构

- ◆ 应用协议的操作步骤：
 - 接口设备发送一个命令（command）、卡进行处理回送一个应答。
- ◆ 特点：命令—应答 成对
 - 接口设备—卡间的互传

40

命令APDU

- ◆ 命令APDU包含一个必备的命令头（4字节）和一个可选的可变长度的命令体。
CLA INS P1 P2 Lc Data Le
- ◆ 命令头：CLA INS P1 P2
 - CLA—类别字节
 - INS—指令字节
 - P1—参数字节
 - P2—参数字节
- ◆ 命令体：Lc Data Le
 - Lc为体内数据长度，
 - Data 为发送的数据，
 - Le为期望应答数据字段的长度。

41

命令APDU

- ◆ 命令APDU的四种结构
- 命令头（命令无数据，应答无数据）；
- 命令头 Le（命令无数据，应答有数据）；
- 命令头Lc Data（命令有数据，应答无数据）；
- 命令头Lc Data Le（命令有数据，应答有数据）。

42

T=0 异步半双工字符传输协议

- ◆ 命令格式:
- ◆ 命令序列
- ◆ 协议成因:应答
- ◆ 差错控制:
- ◆ 优点:单字节纠错,平均传输效率高,实现代价小,广泛的市场基础
- ◆ 缺点:必须软件实现(半位问题),只能纠一位错,若丢数据会死锁,无层次,不能加密命令头标

43

T=1异步半双工分组传输协议

- ◆ 命令格式:
- ◆ 分组帧:
- ◆ 链接
- ◆ 优点:可纠多位错,可链接,层次好,安全好
- ◆ 缺点:传输效率稍低,对硬件要求高,处理复杂,速度低

44

COS命令集

- ◆ 文件操作:选择、搜索、读、写、修改、运算、建立、封锁、删除;
- ◆ 传输:取应答、信封、ATR等;
- ◆ 安全:认证、鉴别、加解密、随机数、密钥交换
- ◆ 数据库:用户管理、库管理
- ◆ 测试:硬件、COS
- ◆ 专门应用:支付、通信
- ◆ 生产:完工、初始化
- ◆ 具体命令:

45

COS实现举例介绍

- ◆ 文件的逻辑结构
- ◆ 文件描述块(文件头)
- ◆ 文件体
- ◆ 与文件操作相关的命令
- ◆ 与安全操作相关的命令
- ◆ 与生命周期维护相关的命令

46

文件的逻辑结构

1. 主文件MF
 - 根文件, 存在且唯一;
 - 文件标识符FID为0x3F00;
2. 专用文件DF
 - 目录文件: MF是特殊的DF; 由于存储容量的限制, 一般在MF下目录文件不多于两层;
 - 其文件标识符FID在同级DF中或任意路径中是唯一的: 两字节, 如0X4F00等;
 - 卡内全局唯一的应用标识符AID, 5~16字节;
 - ①目录专用文件DDF
 - 包含子DF的专用文件, MF即为DDF;
 - 每个DDF下有一个系统文件DIR, 管理子DF; 唯一;
 - ②应用专用文件ADF
 - 不包含子DF的专用文件; 无DIR系统文件;
3. 基本文件EF

47

文件的逻辑结构

基本文件EF

- 文件标识符FID, 两字节; 高字节和父DF的FID的高字节相同, 低字节为扩展短文件标识符, 其低5位称短文件标识符SFI; 同级EF的SFI唯一;
- EF类型, 特殊文件的类型要求唯一, 如DIR

按数据结构分类:

- ①透明文件: 文件无内部结构;
- ②定长记录文件: 以记录为单位处理数据; 一个记录是定长的字节串; 编号0X01~0XFE, 0XFF保留;
- ③变长记录文件, 以记录为单位处理数据; 记录是变长的字节串; 编号0X01~0XFE, 0XFF保留
- ④循环定长记录文件, 以记录为单位处理数据; 记录是定长的字节串; 若文件体已满, 则新记录会顺序覆盖最老的记录

48

文件的逻辑结构

基本文件EF

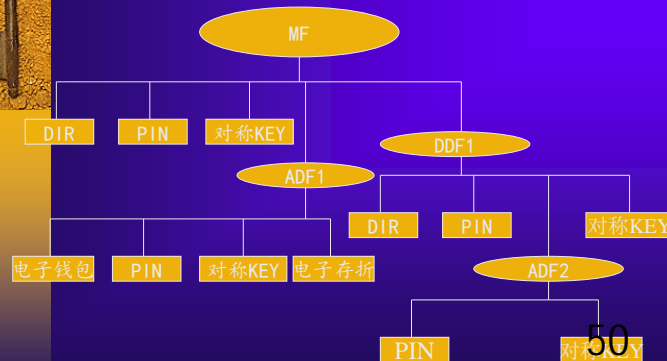
按文件用途分类:

- ① DIR文件, 通常是变长记录文件; 每一项对应一个子DF, 一般包括DF的AID等信息; 隐式操作; 每个DDF中均存在且唯一
- ② PIN文件, 保存和DF相关的用户个人密码信息; 若存在, 则唯一; 变长或定长记录文件; 每一项对应一条PIN记录信息; 可含多个PIN; 不允许读操作; 隐式操作
- ③ 对称KEY文件, 保存和DF相关的各种KEY信息; 若存在, 则唯一; 每一项对应一条KEY记录信息; 可含多个KEY记录; 变长或定长记录文件; 不允许读操作; 隐式操作
- ④ 应用自定义解释文件, 自定义特殊的文件类型, 如电子钱包、电子存折

49

文件的逻辑结构

典型的文件系统逻辑结构



50

文件描述块(文件头16B)

- ◆ 文件标识符(FID)[2B]
- ◆ 文件类型描述符(FDB)[1B]
- ◆ 文件状态符(STAT)1B
- ◆ 文件长度标识符(FSIZE)[2B]
- ◆ 文件自由区长度(FFREE)[2B]
- ◆ 安全控制字SC1,SC2[2B]
- ◆ 安全控制托管标识符(SCIND) [1B]
- ◆ 私有字段B1-B5 [5B]

51

文件类型描述符(FDB)

B8B7高二位为00,其它保留

B6	B5	B4	含义
0	0	0	应用EF
0	0	1	COS系统EF
0	1	0	PIN文件
0	1	1	对称密钥文件
1	0	0	非对称密钥文件
1	0	1	电子钱包文件
1	1	0	电子存折文件
1	1	1	DF文件

52

文件类型描述符(FDB)

◆ EF结构

B3	B2	B1	含义
0	0	0	不确定的EF结构
0	0	1	透明二进制文件
0	1	0	定长记录文件
1	0	0	变长记录文件
1	1	1	循环记录文件
			其他保留

53

不同文件类型描述符(FDB)

- ◆ 38H: DF
- ◆ 01H: 应用透明二进制文件EF
- ◆ 02H: 应用定长记录文件EF
- ◆ 04H: 应用变长记录文件EF
- ◆ 06H: 应用循环记录文件EF
- ◆ 10H: PIN文件
- ◆ 18H: 对称密钥文件
- ◆ 20H: 非对称密钥文件
- ◆ 28H: 电子钱包文件
- ◆ 30H: 电子存折文件

54



文件状态符(STAT)

- ◆ 文件的生命周期状态
- ◆ 01H:建立状态
- ◆ 04H:使用状态的正常子状态
- ◆ 05H:使用状态的临时锁定子状态
- ◆ 08H:终止状态
- ◆ 80H:删除状态

55



文件长度标识符(FSIZE)

- ◆ 通过文件头的地址指针和文件长度标识符可找到下一个文件

56



文件自由区长度(FFREE)

- ◆ 对于DF文件和变长记录文件表示文件体中剩余空间大小
- ◆ 对于其它文件保留

57



安全控制字SC1,SC2

- ◆ 对DF文件: SC1为创建子文件的安全控制
SC2为删除子文件的安全控制
- ◆ 对普通EF文件: SC1为读文件的安全控制
SC2为修改文件的安全控制
- ◆ 对电子钱包和电子存折文件:
SC1为圈存的安全控制
SC2为圈提的安全控制

58



安全控制字SC

- ◆ SC分为高半字节SCH,低半字节SCL,从0-F共16种状态
- ◆ S为卡的安全状态,由安全控制托管标识符(SCIND) 决定, SCIND=0,S=当前安全状态, SCIND=1, S=全局安全状态
- ◆ IF $SCH \leq S \leq SCL$,则可操作,否则禁止操作
- ◆ IF $SCH=0, SCL=F$,则操作开放
- ◆ IF $SCH > SCL$,则禁止操作

59



私有字段B1-B5

- ◆ DF文件的私有字段
- ◆ EF文件的私有字段(除了非对称密钥文件,电子钱包和电子存折文件)
- ◆ 非对称密钥文件的私有字段
- ◆ 电子钱包和电子存折文件的私有字段

60



DF文件的私有字段

- ◆ B1: DF下的DIR文件的SFI
- ◆ B2:应用类型
 - 一般应用:00H
 - 金融应用:01H
 - 社保应用:02H
 - 加油应用:03H
 - 公钥应用:04H
 - 公交应用:05H
 - 市政应用:06H
 - 校园应用:07H
 - 保留扩展:其他值

61



DF文件的私有字段

- ◆ B3:00H:为DDF,DF下可建新DF
01H:为ADF,DF下不可建新DF
其他:保留
- B4,B5:保留

62



EF文件的私有字段

- B1:记录文件存储状态标识符
 - 对于定长记录文件,表示以写入的记录数
 - 对于循环记录文件,表示最后写入记录位置
 - 对于其他文件,保留
- B2:记录数目标识符
 - 对于定长记录和循环记录文件,为记录总条数
 - 对于其他文件,保留
- B3, B4, B5: 保留

63



非对称密钥文件的私有字段

- ◆ B1:密钥文件用途
- ◆ 位1:数字签名计算
- ◆ 位2:数字签名验证
- ◆ 位3:数据加密
- ◆ 位4:数据解密
- ◆ 其他:保留

64



非对称密钥文件的私有字段

- ◆ B2:算法标识符
 - 01H:普通RSA算法
 - 02H:特殊RSA算法
 - 03H:DSA算法
 - 其他:保留


65



非对称密钥文件的私有字段

- ◆ B3:非对称密钥的模长
- ◆ 08H:512位
- ◆ 10H:1024位
- ◆ 20H:2048位
- ◆ 其他:保留
- ◆ B4, B5:保留

66



电子钱包和电子存折文件的私有字段

- ◆ B1:查询交易余额的安全控制,类似SC
- ◆ B2:取现交易余额的安全控制,类似SC
- ◆ B3:修改透支限额的安全控制,类似SC
- ◆ B4,B5:保留

67



文件体

- ◆ 不同数据类型EF文件体
- ◆ 不同用途类型EF文件体

68



不同数据类型EF文件体

- ◆ 透明二进制文件体:全部为数据
- ◆ 定长记录文件体:一个记录=记录数据+记录ID号
- ◆ 变长记录文件体:一个记录=记录长度+上一条记录长度+记录数据
- ◆ 循环记录文件体:同定长记录文件体

69



不同用途类型EF文件体

- ◆ DIR文件体
- ◆ PIN文件体
- ◆ 对称密钥文件体
- ◆ 非对称密钥文件体
- ◆ 电子钱包文件体
- ◆ 电子存折文件体

70



DIR文件体(定长记录)

- ◆ L:1B AID的长度
- ◆ AID:LB DF的应用标识符
- ◆ DFADD:2B对应DF文件描述块的起始地址

71



PIN文件体(变长记录)

- ◆ ID:1B PIN记录的ID号
- ◆ SC:1B安全控制
- ◆ STAT:1B PIN验证后的安全状态
- ◆ MinLen:1B PIN的最小长度
- ◆ INIC:1B PIN尝试计数器
- ◆ DATA: PIN的内容

72



对称密钥文件体(变长记录)

- ◆ Type:1B密钥类别
- ◆ Version:1B密钥版本号
- ◆ Index:1B密钥索引号
- ◆ Alg:1B密钥对应算法
- ◆ SC:1B密钥使用条件
- ◆ STAT:1B密钥认证后的安全状态
- ◆ INIC:1B密钥尝试计数器
- ◆ DATA:密钥内容

73



对称密钥文件体密钥类别(TYPE)

- ◆ 00H:主控密钥
- ◆ 01H:PSAM卡维护密钥
- ◆ 02H:消费密钥DPK
- ◆ 03H:PIN解锁密钥DPUK
- ◆ 04H:重装PIN密钥DRPK
- ◆ 05H:应用维护密钥DAMK
- ◆ 06H:MAC计算密钥
- ◆ 07H:DES加/解密密钥
- ◆ 08H: MAC 和DES加/解密密钥

74



对称密钥文件体密钥类别(TYPE)

- ◆ 09H:保留
- ◆ 0AH:圈存密钥DLK
- ◆ 0BH:圈提密钥DULK
- ◆ 0CH:TAC密钥DTK
- ◆ 0DH:修改透支限额密钥DUK
- ◆ 1EH:内部认证密钥
- ◆ 1FH:外部认证密钥
- ◆ 其他: 保留

75



非对称密钥文件体

- ◆ T:1B数据项类型
- ◆ L:2B长度
- ◆ V:L B内容

76



电子钱包文件体(透明二进制)

- ◆ BAL:3B钱包余额
- ◆ DC:2B脱机交易计数器
- ◆ CC:2B联机交易计数器
- ◆ MAX:3B钱包可存入最大金额

77



电子存折文件体

- ◆ BAL:4B存折余额
- ◆ DC:2B脱机交易计数器
- ◆ CC:2B联机交易计数器
- ◆ OL:3B存折可透支的限额
- ◆ MAX:4B存折可存入最大金额

78



与文件操作相关的命令

- ◆ 创建文件(CREATE FILE)命令
- ◆ 删除文件(DELETE FILE)命令
- ◆ 选择文件(SELECT)命令
- ◆ 读二进制(READ BINARY)命令
- ◆ 修改二进制(UPDATE BINARY)命令
- ◆ 读记录(READ RECORD)命令
- ◆ 修改记录(UPDATE RECORD)命令

79



与安全操作相关的命令

- ◆ 取随机数(GET CHALLENGE)命令
- ◆ 给随机数(PUT CHALLENGE)命令
- ◆ 内部认证(INTERNAL AUTHENTICATION)命令
- ◆ 外部认证(EXTERNAL AUTHENTICATION)命令
- ◆ 添加密码(APPEND PIN)命令
- ◆ 修改密码(CHANGE PIN)命令
- ◆ 验证密码(VERIFY)命令
- ◆ 密码解锁(PIN UNLOCK)命令
- ◆ 重装密码(RELOAD PIN)命令
- ◆ 写密钥(WRITE KEY)命令
- ◆ 数据加密(ENCRYPT)命令
- ◆ 数据解密(DECRYPT)命令

80



与生命周期维护相关的命令

- ◆ 应用锁定(APPLICATION BLOCK)命令
- ◆ 应用解锁(APPLICATION UNBLOCK)命令
- ◆ 卡片锁定(CARD BLOCK)命令
- ◆ 屏蔽文件(DEACTIVATE FILE)命令
- ◆ 激活文件(ACTIVE FILE)命令

81