Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS6-SAM

功能规格书

info@acs.com.hk
www.acs.com.hk

目录

图

表

1.0. 简介

本手册详细介绍了龙杰智能卡有限公司（Advanced Card Systems Ltd., ACS) 自主研发的 ACS 智能卡操作系统版本 6-安全存取模块，也称作 ACOS6-SAM 的特性和功能。

1.1. 特性

ACOS6-SAM 支持以下特性:

- 符合 ISO 7816 1、2、3 和 4 部分
- 高速通讯波特率，可在 9600 bps 至 223,200 bps 间转换
- 完整的 32K 字节 EEPROM 应用数据存储容量
- 支持 ISO 7816 第 4 部分的文件结构：透明、线性定长、线性变长、循环记录文件
- 具备 DES/3DES 加密能力
- 支持 AES-128
- 符合 FIPS140-2 的随机数生成器（基于硬件）
- 生成过程密钥用于相互认证
- 安全报文机制保证数据传输的机密性和安全性
- 与 ACOS3、ACOS6、ACOS7、ACOS10 及 Mifare Ultralight C、DESFire、DESFire EV1 和 Mifare Plus 卡片配用的安全存取模块
- 存储、执行所有的密钥操作，用于相互认证、加密的 PIN 提交、安全报文发送和电子钱包命令
- 多级安全访问层次
- 文件头和 PIN 命令具有防破坏功能

1.2. 技术规范

以下是 ACOS6-SAM 卡片的技术参数

1.2.1. 电气参数

- 工作电压：5 V DC+/-10% (A 类)与 3 V DC +/-10% (B 类)
- 最大电源电流：<10 mA
- ESD 保护：≤ 4 KV

1.2.2. EEPROM

- 容量：32 KB (32,768 字节)，包含文件头
- EEPROM 耐久：10 万次擦写
- 数据存储记忆：10 年

1.2.3. 环境温度

- 工作温度：-25°C - 85°C
- 存储温度：-40°C - 100°C

1.3. 符号和缩写

缩略语	描述
3DES	3 倍数据加密标准算法 Triple DES
AID	应用标识符 Application/Account Identifier
AMB	访问模式字节 Access Mode Byte
AMDO	访问模式数据对象 Access Mode Data Object
APDU	应用协议数据单元 Application Protocol Data Unit
ATC	帐户交易计数器 Account Transaction Counter
ATR	复位应答 Answer to Reset
ATREF	帐户交易参考 Account Transaction reference
CLA	APDU 命令的类别字节 Class byte of APDU commands
COMPL	逐位补 Bit-wise Complement
COS	卡片操作系统 Card Operating System
DEC(C, K)	用密钥 K 对数据 C 进行 DES 或 3DES 解密 Decryption of data C with key K using DES or 3DES
DES	数据加密标准 Data Encryption Standard
DF	专用/目录文件 Dedicated File
ENC(C, K)	用密钥 K 对数据 P 进行 DES 或 3DES 加密 Encryption of data P with key K using DES or 3DES
EF	基本文件 Elementary File
EF1	个人密码文件 PIN File
EF2	密钥文件 Key File
FCP	文件控制参数 File Control Parameters
FDB	文件类型字节 File Descriptor Byte
INS	APDU 命令的指令字节 Instruction byte of APDU commands
IV_Seq	用于 SM-MAC 的带序号初始向量 Initialization vector with sequence number used in SM-MAC
LCSI	应用周期状态字 Life Cycle Status Integer
LSb	最低有效位 Least Significant Bit
LSB	最低有效字节 Least Significant Byte
MAC	报文认证码 Message Authentication Code
MF	主控文件/目录 Master File
MFP	Mifare Plus 卡 Mifare Plus
MOC	中国建设部标准 Ministry of Construction – China specifications
MSb	最高有效位 Most Significant Bit

缩略语	描述
MSB	最高有效字节 Most Significant Byte
Nibble	半字节；一个字节包含两个半字节 four- bit aggregation; a byte consists of two nibbles
PBOC	中国人民银行标准 People's Bank of China specifications
RFU	保留为将来使用 Reserved for Future Use
RMAC	零售报文认证码 Retail MAC
SL0	Mifare Plus 安全级别 0 Mifare Plus Security Level 0
SL1	Mifare Plus 安全级别 1 Mifare Plus Security Level 1
SL2	Mifare Plus 安全级别 2 Mifare Plus Security Level 2
SL3	Mifare Plus 安全级别 3 Mifare Plus Security Level 3
SAC	标准安全属性 Security Attribute – Compact
SAE	扩展安全属性 Security Attribute – Expanded
SAM	安全存取模块 Secure Access Module
SCB	安全条件字节 Security Condition Byte
SCDO	安全条件数据对象 Security Condition Data Object
SE	安全环境 Security Environment
Seq#	用于 SM-ENC 的序号 Sequence number used in SM-ENC
SFI	短文件标识符 Short File Identifier
SM-ENC	带加密的安全报文 Secure Messaging with Encryption
SM-MAC	带 MAC 的安全报文 Secure Messaging with MAC
TLV	标签-长度-值 Tag-Length-Value
$TTREF_C$	终端交易编号-存款 Terminal Transaction Reference for Credit
$TTREF_D$	终端交易编号-扣款 Terminal Transaction Reference for Debit
UQB	使用限定字节 Usage Qualifier Byte
II	连接 Concatenation

表 1: 符号和缩写

2.0. ACOS6-SAM

ACOS6-SAM 是一款专为 ACOS3、ACOS6、ACOS7、ACOS10、Mifare Ultralight C、DESFire、DESFire EV1 和 Mifare Plus 客户卡而设计的通用密码计算模块，也可作为安全验证模块来使用。SAM 卡可以安全地存储密钥，并利用这些密钥为其他应用程序或智能卡计算密码。通过使用 ACOS6-SAM，密钥离开 SAM 的时候总是会被加密，从而极大的提高了系统的安全性。此外，SAM 还可以为 ACOS3/6/7/10 卡片执行认证过程和钱包 MAC 运算。

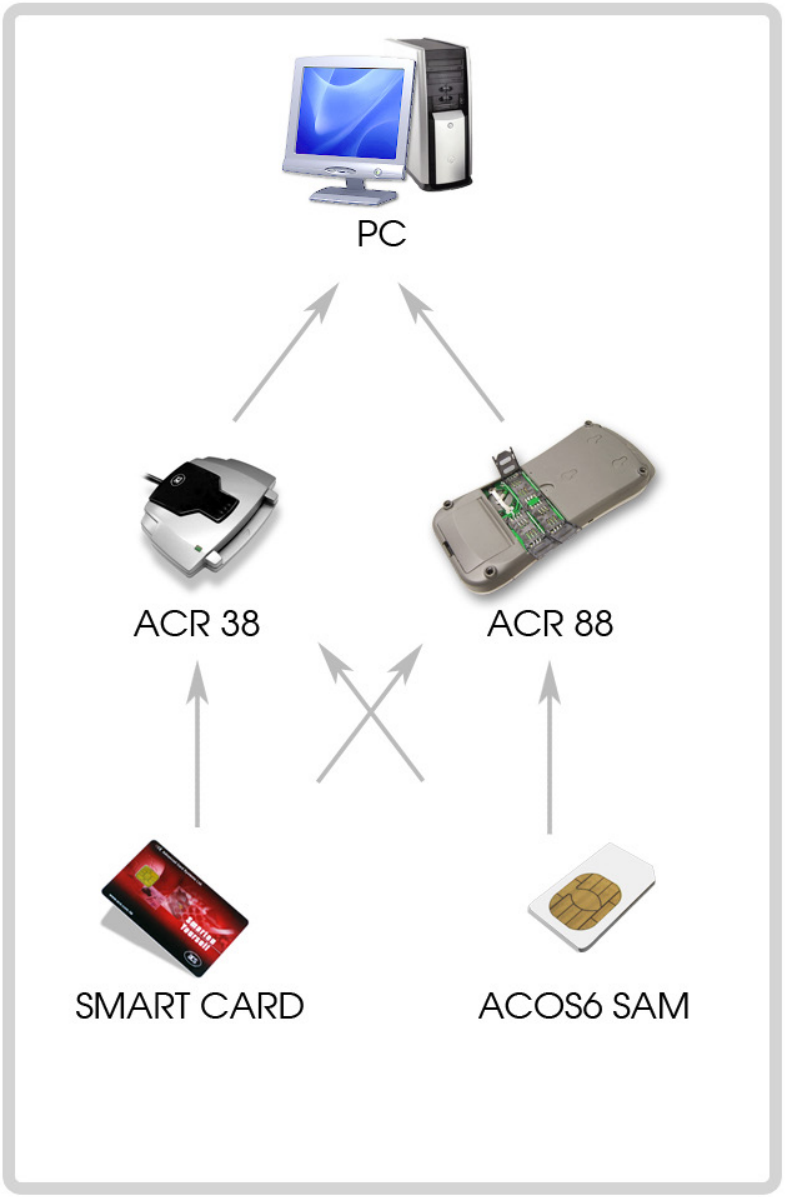

图 1: ACOS6-SAM 的设置

ACOS6-SAM 可部署于任何应用程序当中，用于实现下列目的：

- 存储和保护应用程序的 DES/3DES 主密钥
- 基于主密钥集生成并分散出应用密钥
- 与客户智能卡一起执行加密功能
- 用作安全的加密模块

与 ACOS3 或 ACOS6 客户智能卡一起使用时，ACOS6-SAM 具有以下功能：

- 利用基于卡片唯一序列号的分散密钥初始化 ACOS3/6 卡片
- 执行相互认证过程，并生成过程密钥
- 与 ACOS3/6 一起执行安全报文发送
- 计算安全的电子钱包命令
- 与 ACOS6 一起执行安全密钥注入

与 ACOS7、ACOS10 和 ACOS10-PSAM 智能卡一起使用时，ACOS6-SAM 具有以下功能：

- 利用基于卡片唯一序列号的分散密钥初始化 ACOS7/10/10-PSAM 卡片
- 执行相互认证过程，并生成过程密钥
- 与 ACOS7/10 一起执行安全密钥注入

注意：*ACOS6-SAM 不执行基于 PBOC/MOC 的钱包命令，关于这一点，请使用符合 PBOC 的支付 SAM - ACOS10-PSAM。*

与 Mifare Ultralight C 智能卡一起使用时，ACOS6-SAM 具有以下功能：

- 利用基于卡片唯一序列号的分散密钥初始化 UL-C 客户卡
- 执行相互认证过程

与 Mifare Plus、DESFire/DESFire EV1 智能卡一起使用时，ACOS6-SAM 具有以下功能：

- 利用基于卡片唯一序列号的分散密钥初始化 Mifare Plus 和 DESFire / DESFire EV1 客户卡
- 执行相互认证过程
- 执行安全报文发送
- 执行安全密钥注入

ACOS6-SAM 的编程方法与 ACOS3 不同。它的设计符合 ISO7816 第 4 部分有关文件系统和命令集的要求。为了提高应用开发人员的速度，此文件给出了快速入门指南以及个人化操作的一些示例。特有的 SAM 功能如以下小节所述。

3.0. 卡片管理

本节概述了卡片级别的特性和管理功能。

3.1. 防插拔

ACOS6-SAM 使用*防插拔*机制保护卡片数据免受卡片插拔导致的损坏（如在更新数据时突然拔出卡片，或者读卡器在卡片数据更新过程中出现机械故障等）。卡片复位后，ACOS6-SAM 会检查防插拔数据域，并进行必要的数据恢复。之后，COS 将事前保存的数据返回到 EEPROM 中原来的地址。

3.2. 卡片头模块

ACOS6-SAM 是一个具有 32K 的 EEPROM 的卡片操作系统。在初始状态下（没有文件存在），用户可以通过指定地址的读/写二进制文件方式访问该卡片头模块。

3.3. 卡片应用周期状态

ACOS6-SAM 卡具有以下状态：

1. **预个人化状态–**卡片的初始状态,允许用户自由地使用卡片头模块（在 **3.2 节–卡片头模块**中定义）。用户可以使用 READ BINARY 命令或 UPDATE BINARY 命令通过地址指定该卡片头模块。

   用户可随意个性化卡片头模块。在下列情况下卡片会一直保持在预个人化状态：(1)主控文件（MF）尚未生成；且(2)*卡片头模块*内的*卡片应用周期标识位*（地址：EEC7）为 0xFF。

2. **个人化状态–**一旦成功创建 MF 而且*卡片应用周期标识位*未改变（仍是 0xFF），卡片即会进入该状态。此时用户不能再像预个人化状态那样直接访问卡片的存储器，但可以像在个人化状态中或在*操作模式*下一样，在卡片中创建和测试文件。

   用户可以在此状态进行测试，也可以通过 CLEAR CARD 命令恢复到预个人化状态。

3. **用户状态–**一旦成功创建 MF 而且*卡片应用周期标识位*改变，卡片即会进入该状态。另外用户也可以通过 ACTIVATE CARD 命令从个人化状态过渡到用户状态。

   一旦设置了卡片应用周期标识位（0x00)而没有设置*特殊功能标志*的 bit 5（取消激活卡片使能标志），卡片将不能再恢复到之前的状态。CLEAR CARD 和 DEACTIVATE CARD 命令将不再有效。

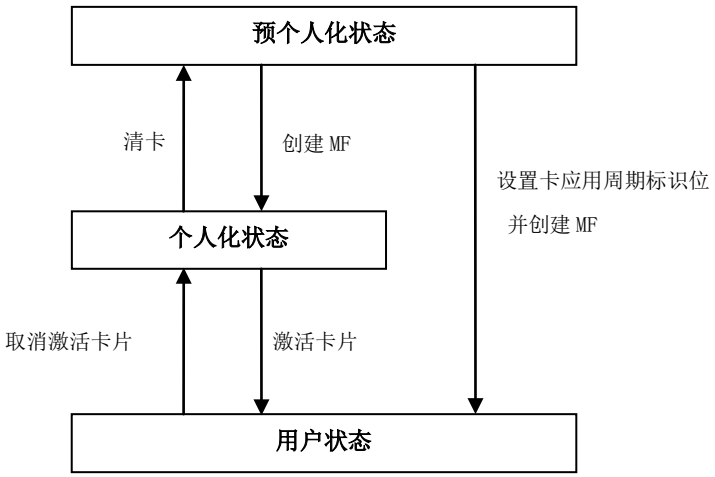

图 2: 卡片应用周期状态

3.3.1. 典型的卡片开发步骤：

1. 用户使用 UPDATE BINARY 命令个人化卡片的头模块。
2. 用户建立自己的卡片文件结构。先建立 MF，接着建立 DF 和 EF。卡片的安全设计也将在该阶段被测试。如果发现任何设计的缺陷，用户可以毫不费力的通过 CLEAR CARD 命令返回到状态 1。
3. 一旦卡片的文件与安全设计确定下来并完成测试，执行 Clear Card 命令，并使用 UPDATE BINARY 命令变更*卡片应用周期标识位*（在地址 `0xEEC7` 写入 `0x00`）
4. MF 重新创建后，卡片进入到实际操作模式。然后，用户可以在此阶段重构文件系统。此时卡片不能再回到之前的状态。

用户可以在卡片头模块进行设置，使 Deactivate Card 命令能够使用，这样就可以通过 Activate Card 命令来代替步骤 3 和步骤 4。如果应用程序开发人员希望清除卡片内容，可以使用 Deactivate Card 命令。若需要控制对 Deactivate Card 命令的使用，可以设置扩展安全属性。

3.4. 复位应答

硬件复位（如上电）后，卡片会按照 ISO7816 第 3 部分的规定传送**复位应答**（**ATR**）。ACOS6-SAM 支持正向约定的 T=0 协议。

3.4.1. 自定义 ATR

ACOS6-SAM 的 ATR 可定制传输速度或该卡的具体身份信息。新的 ATR 必须符合 ISO7816 第 3 部分的规定，否则卡可能变得没有反应或者在下次上电或复位后不可恢复之前状态。因此，只建议改变 T0（低半字节）、TA1 和历史字节。

4.0. 文件系统

本节探讨 ACOS6-SAM 智能卡的文件系统。

4.1. 多层次的文件系统

ACOS6-SAM 的文件系统和结构完全符合 ISO7816 第 4 部分的规定。该文件系统非常类似于现代的计算机操作系统。文件的根是主文件（MF)。卡中的每个应用或数据文件组均可包含在称为专用文件（DF)的目录中。每个 DF 或 MF 都可以在目录下的基本文件（EF)中存储数据。

ACOS6-SAM 允许任意深度的 DF 树结构。也就是说，DF 可以嵌套，如下图所示。

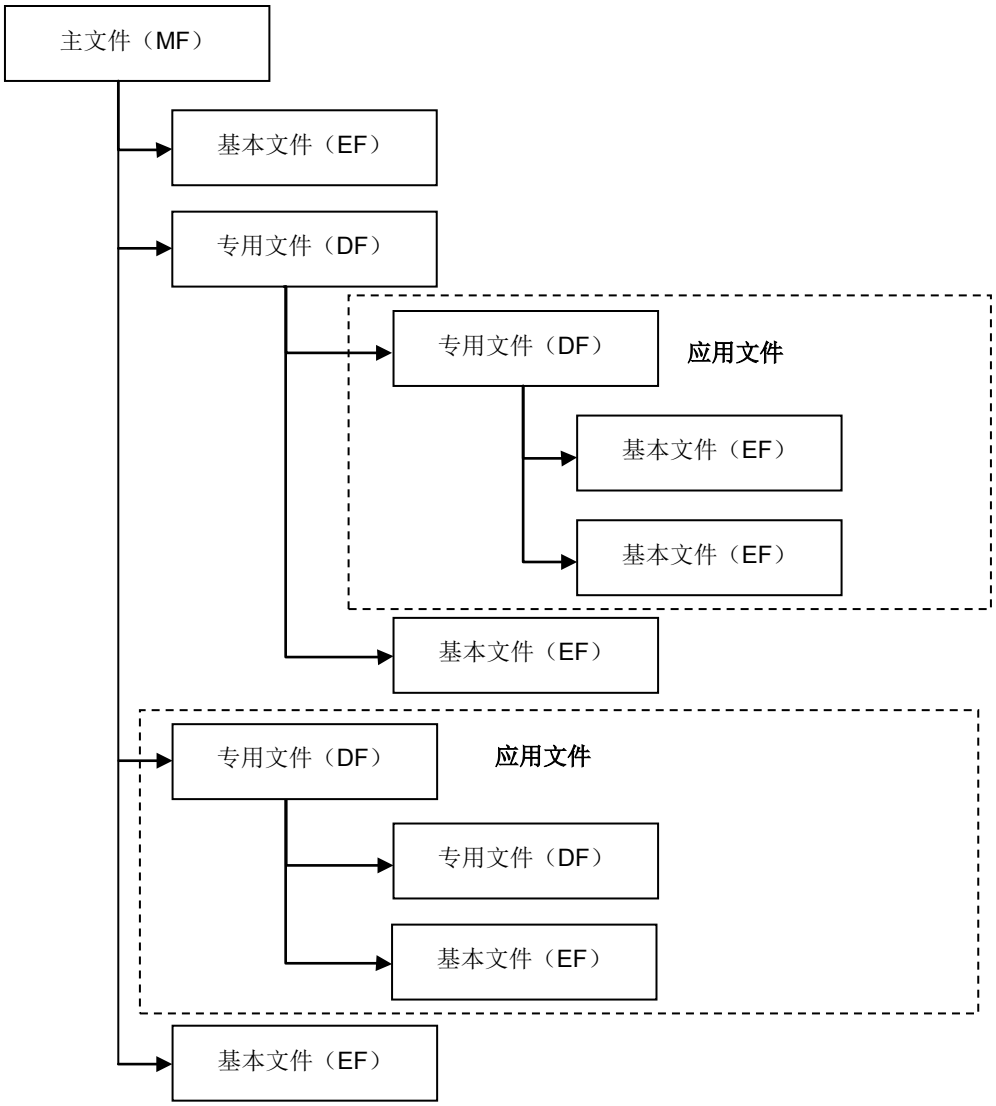

图 3: 文件系统结构示例

4.2. 文件头数据结构

ACOS6-SAM 通过文件来组织用户的 EEPROM 区。每个文件都有一个文件头，即一个描述文件属性的数据块。了解文件头模块的知识有助于应用程序开发人员准确的规划 EEPROM 空间的使用。

4.2.1. 文件类型字节（FDB)

该数据域标识文件的类型，文件头模块的大小取决于文件的种类。

4.2.2. 数据编码字节（DCB）

ACOS6-SAM 不使用该数据域，它只是设置为文件头的一部分以符合 ISO7816 第 4 部分的规定。

4.2.3. 文件标识（File ID）

这是一个 16 位的数据域，它是 MF 或 DF 内文件的唯一标识，DF（或 MF)下的文件必须是唯一的。

4.2.4. 文件大小（File Size)

这是一个 16 位的数字域，用于定义文件的大小，但是不包括文件头的大小。对于记录类型的 EF,第一个字节表示*记录的最大长度*（MRL），第二个字节表示*记录的数量*（NOR)对于非记录类型的 EF 来说,第一个字节表示文件大小的高字节，第二个字节表示文件大小的低字节。对于 DF 来说,该数据域无用途。

4.2.5. 短文件标识符（SFI）

*短文件标识符*是一个五位的数值，表示文件的短 ID。ACOS6-SAM 允许通过 SFI 指定文件。文件标识的最后 5 位不一定要匹配这个 SFI。同一个 DF 下可能有 2 个文件使用相同的 SFI。在这种情况下，ACOS6-SAM 会选择先创建的文件。

4.2.6. 应用周期状态字（LCSI)

正如 ISO7816 标准第 4 部分定义的一样，这个字节表明文件的应用状态。它可以有以下值

b7	b6	b5	b4	b3	b2	b1	b0	Hex	含义
0	0	0	0	0	0	0	1	01	创建状态
0	0	0	0	0	0	1	1	03	初始化状态
0	0	0	0	0	1	-	1	05 或 07	操作状态（激活的）
0	0	0	0	0	1	-	0	04 或 06	操作状态（取消激活的）
0	0	0	0	1	1	-	-	0C - 0F	终止状态

表 2: 周期状态字节

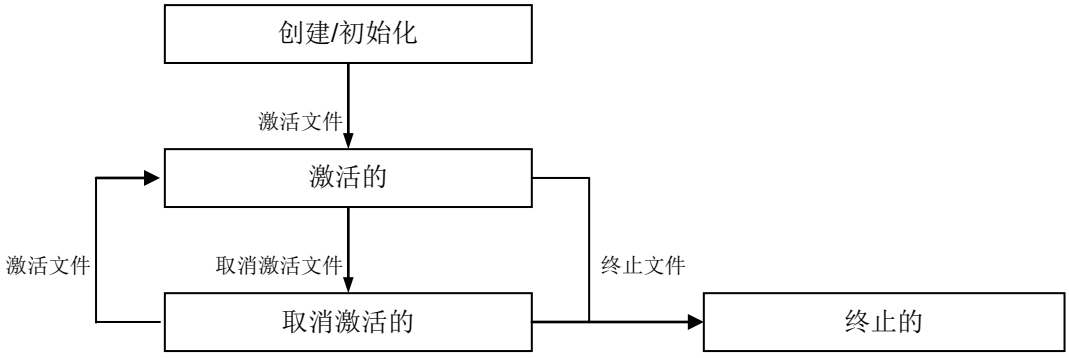

图 4: 应用周期状态字

- 在创建/初始化状态，COS 允许执行对该文件的全部命令。
- 在激活状态，只有满足该文件的安全条件，对该文件的命令才有效。
- 在取消激活状态，COS 不允许执行大部分对该文件的命令。
- 在终止状态，COS 不允许执行全部对该文件的命令。

4.2.7. 标准安全属性的长度（SAC Len）

该字节表示包含在文件头下的 SAC 结构的长度。

4.2.8. 扩展安全属性的长度（SAE Len）

该字节表示包含在文件头下的 SAE 结构的长度。

4.2.9. DF 名称长度/第一个循环记录

如果文件是 DF，该数据域表示 DF 名称的长度。

如果文件是循环 EF，该数据域表示最后修改的记录的索引。

其他情况，该数据域无用途。

4.2.10. 父目录地址

这两个字节表示文件父 DF 的物理 EEPROM 地址。

4.2.11. 校验和

为了保证文件头数据的完整性，COS 使用校验和。计算方式是异或文件头中前面的全部字节。如果发现文件头的校验和错误，对该文件的命令将会被禁止。

4.2.12. 标准安全属性（SAC)

这是一个数据结构，描述对文件进行某些操作所需要满足的安全条件。如 ISO7816 定义，该数据编码成"AM-SC"模板形式，该数据域的最大长度是 8 字节。详情参看 **5.1.1 节 – 标准安全属性**。

4.2.13. 扩展安全属性（SAE）

这是一个数据结构，描述对卡片进行某些操作所需要满足的安全条件。该数据编码与 SAC 不同，但是同样符合 ISO7816 定义。该数据域的最大长度是 32 字节。详情参看 **5.1.2 节 – 扩展安全属性**。

对于 DF 文件，文件头模块中还包含附加数据域。

4.2.14. SE 文件标识（仅适用于 DF)

对于 DF,该数据域包含 2 字节的文件标识（FID），对应的文件为该 DF 下的一个子文件。这个子文件

叫做*安全环境文件*，由 COS 在内部进行处理。

4.2.15. FCI 文件标识（仅适用于 DF)

对于 DF,该数据域包含 2 字节的文件标识（FID），对应的文件为该 DF 下的一个子文件。这个子文件叫做*文件控制信息文件*，由 COS 在内部进行处理。

4.2.16. DF 名称（仅适用于 DF）

对于 DF，该数据域是文件的*长名*。我们可以通过最长 16 字节的长名来选择文件。

4.3. 内部安全文件

COS 的运作取决于与安全内容相关的内部文件。内部文件被激活时，它的 READ 条件必须设置为 NEVER。一般来说，一个 DF 应该具有：(1)一个密钥文件，储存用于校验的 PIN（称为 EF1),(2)一个密钥文件，储存用于认证的密钥（称为 EF2）；及 (3)一个 SE 文件,储存安全条件。

密钥文件是一种内部线性变长文件。它可能包含(1)PIN 数据结构或者 (2)密钥数据结构。

5.0. 安全机制

文件命令由 COS 系统根据目标文件（或当前 DF）的安全访问条件进行限制。这些条件基于由系统维护的 PIN 和密钥。如果对应的个人密码或密钥通过校验或认证，卡的命令将被允许。

全局 PIN 直接存储在 MF 下的 PIN EF(EF1）。同样，局部密钥直接存储在当前选定的 DF 下的 Key EF(EF2)。最多允许同时存在：31 个全局 PIN、31 个局部 PIN、31 个全局密钥和 31 个局部密钥。

5.1. 文件安全属性

每个文件（MF、DF 或 EF）的文件头中都设置有一套安全属性。安全属性模式分为两种：*标准安全属性（SAC)*和*扩展安全属性(SAE*）。

5.1.1. 标准安全属性（SAC)

SAC 是一个存储在每个文件内的数据结构。它标识对于该文件什么样的文件操作是被允许的，以及要符合哪些条件对应的文件操作才被允许。

5.1.2. 扩展安全属性（SAE)

SAE 是一个存储在每个文件的数据结构。它指示 COS 系统是否允许文件命令被执行。SAE 比 SAC 更通用。它的格式是访问模式数据对象（AMDO）紧随一个或多个安全条件数据对象（SCDO）。

5.2. 安全环境

安全条件被编码于一个安全环境（SE）文件中。每个 DF 都有一个专用的 SE 文件，该文件的标识符在 DF 的头模块中指定。每个 SE 记录的结构如下：

<SE ID Template> <SE Authentication Template>

SE 标识模板（SE ID Template）：SE 标识模板是一个强制性数据对象，它的值代表了 SAC 和 SAE 的 SC 字节所指定的标识符。它的标记是 `0x80`，长度是 `0x01`。

SE 认证模板（SE Authentication Template）:认证模板（AT）定义了满足 SE 所须具备的安全条件。该安全条件为 PIN 或者密钥认证。

5.3. 相互认证

相互认证是卡片与读卡设备之间相互认证对方真实性的过程。相互认证成功执行以后会产生一个*过程密钥*，该过程密钥只在*过程*中有效。这个过程我们这样定义：在相互认证成功执行以后，直到卡片的重新复位或者另外一次成功的相互认证。

5.4. 短密钥外部认证

短密钥外部认证使用卡片随机数结合终端响应的方法获得对卡的授权。从而缩短了外部认证的时间或者允许采用更适用于人工输入的一次性密码。

5.5. 确保真实性的安全报文（SM-MAC）

ACOS6-SAM 支持两种安全报文 - *确保真实性的安全报文(SM-MAC)*和*确保机密性的安全报文(SM-ENC)*。本节将讨论用于确保真实性的安全报文。用于确保机密性的安全报文将在 **5.6 节中讨论**。

确保真实性的安全报文允许对传入或传出卡片的数据和命令进行验证，从而确保命令没有被修改或重放。由发送方传送到接收方的数据块附带有四字节的 MAC。接收方在继续操作之前会先查验 MAC。在执行安全报文前，发送发与接收方必须先通过 **5.3 节 – 相互认证**中所述的相互认证获得过程密钥。

5.6. 用于确保机密性的安全报文（SM-ENC)

ACOS6 4.02 及更高的版本均支持 ISO 安全报文（SM）。安全报文可以确保在卡片和终端/服务器之间传输的数据处于安全状态，不易受到窃听、重放攻击或者未经授权的更改。需要执行安全报文的条件可以在适当的安全条件字节中进行设置，详情参**见 5.1.1 – 标准安全属性**。几乎所有的命令也可以采用由终端发起的安全报文。不接受安全报文发送的命令是 GET CHALLENGE、MUTUAL AUTHENTICATION 和 GET RESONSE。

5.7. 密钥注入

密钥注入可以用于安全地将密钥或分散密钥从 ACOS6-SAM 卡片导入目标 ACOS6-SAM 或客户的 ACOS6、ACOS7 或 ACOS10 卡中。为了描述方便，我们定义含有待注入密钥的 ACOS6-SAM 为 "*source SAM*"，接受导入密钥的 ACOS6/ACOS6-SAM/ACOS7 及 ACOS10 客户卡为"*target SAM*"。

该功能允许了 SAM 存在主次关系，并且次 SAM 可以执行各种特定操作。

"Target SAM"卡使用 Set Key 命令而"source SAM"使用 Get Key 命令来执行密钥注入。

注意：*密钥注入的功能在 ACOS6-SAM 版本 4.02、ACOS6 版本 3.02 和之后的版本可行。*

6.0. 生命支持应用

所设计的产品并不旨在用于生命支持器具、设备或系统之中，产品在上述使用过程中不当使用可能会造成人身伤害。ACS 客户对产品在此类应用中的使用或销售，需承担不当使用可能造成人身伤害的风险。

7.0. 联系信息

关于更多的信息，敬请您访问我们的网站 http://www.acs.com.hk.

销售咨询，敬请您发邮件至 info@acs.com.hk.