Advanced Card Systems Ltd.
Card & Reader Technologies

# ACOS7 MOC 卡


功能规格书 V1.06

*如有任何更改，恕不另行通知*

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

# 目录



# 图目录

# 表目录

# 1.0. 简介

本手册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 7（ACOS7）的特性和功能。

## 1.1. 特性

ACOS7 支持以下特性:

- 符合 ISO 7816 1, 2, 3, 4 部分
- 接触卡可转换高速通讯波特率 (9,600 – 223,200 bps)
- 符合 ISO 14443 1, 2, 3, 4 部分
- 非接触接口完全符合 ISO 14443 A
- 非接触接口根据相应 ISO 14443-4，完全支持 T=CL 协议
- 非接触接口支持 106 kbps、212 kbps、424 kbps 与 848 kbps 的数据传输率
- 完整的 8K 字节 EEPROM 应用数据存储容量
- 支持 ISO 7816 第 4 部分的文件结构: 二进制文件, 线性定长, 线性变长, 循环记录文件
- DES/3 DES 加密算法
- 符合 FIPS 140-2 的随机数产生器（基于硬件）
- 安全报文机制保证数据传输的安全与机密
- 支持中国人民银行规定的电子钱包和电子存折等功能
- 符合建设部（MOC）标准
- 符合《建设事业 CPU 卡操作系统技术要求》
- 支持安全的多级目录管理与多应用
- 支持防拔插功能

## 1.2. 技术参数

以下是 ACOS7 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)
- 最大负载电流: <10 mA
- ESD 保护: ≤ 4 KV

### 1.2.2. EEPROM

- 容量: 8 K 字节 (8,192 字节)
- 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 | 账户交易计数器 Account Transaction Counter |
| ATR | 复位应答 Answer To Reset |
| CHV | 要求持卡人校验 PIN Card Holder Verify |
| 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<br>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 |
| ED | 电子存折 Electronic Deposit |
| ENC (P, K) | 用密钥 K 对数据 P 进行 DES 或 3DES 加<br>Encryption of data P with key K using DES or 3DES |
| EF | 基本文件 Elementary File |
| EF1 | 个人识别码文件 PIN File |
| EF2 | 密钥文件 KEY File |
| FCI | 文件控制信息 File Control Information |
| FCP | 文件控制参数 File Control Parameters |
| FDB | 文件类型字节 File Descriptor Byte |
| GSESPK | 灰锁过程的中间密钥 Session key of Grey Lock |
| ID | 标识符 Identifier |
| INS | 命令报文的指令字节 Instruction Byte of Command Message |
| LCSI | 应用周期状态字 Life Cycle Status Integer |
| LEN | 长度 Length |
| LSb | 最低有效位 Least Significant Bit |
| LSB | 最低有效字节 Least Significant Byte |

| 缩略语 | 描述 |
|---|---|
| MAC | 报文认证码 Message Authentication Code |
| MF | 主控文件/目录 Master File |
| MOC | 建设部 Ministry of Construction |
| MRL | 最大记录长度 Maximum Record Length |
| MSb | 最高有效位 Most Significant Bit |
| MSB | 最高有效字节 Most Significant Byte |
| NA | 无应用 No Application |
| NULL | 无 Null |
| NOR | 记录的数量 Number Of Record |
| PBOC | 中国人民银行 Peoples Bank of China |
| PIN | 个人识别码 Personal Identification Number |
| PSE | 支付系统环境 Payment System Environment |
| RFU | 保留为将来使用 Reserved for Future Use |
| RMAC | 零售 报文认证码 Retail MAC |
| SAC | 标准安全属性 Security Attribute – Compact |
| SAE | 扩展安全属性 Security Attribute – Expanded |
| SAM | 安全认证模块 Security Authentication Module |
| SC | 安全条件 Security Condition |
| SCB | 安全条件字节 Security Condition Byte |
| SFI | 短文件标识符 Short File Identifier |
| SM-MAC | 带 MAC 的安全报文 Secure Messaging with MAC |
| SM-ENC | 带加密的安全报文 (在本文档很多场合指的是加密+MAC) Secure Messaging with Encryption |
| SW1 | 状态码 1 Status Word One |
| SW2 | 状态码 2 Status Word Two |
| TAC | 交易验证码 Transaction Authorization Cryptogram |
| TC | 交易计数器 Transaction Counter |
| TLV | 标签-长度-值 Tag-Length-Value |
| TTI | 交易类型标识 Transaction Type Indicator |
| UQB | 应用限定字节 Usage Qualifier Byte |
| \|\| | 连接 Concatenation |

**表1**：符号和缩写

# 2.0. 卡片管理

本节概述了 ACOS7 智能卡的卡片级特性和管理功能。

## 2.1. 防拔插

ACOS7 采用**防拔插**机制以保护卡片数据，避免由于卡片拔插导致的损坏（如在数据更新时突然拔出卡片，或者读卡器在卡片数据更新过程中出现机械故障等）。在卡片复位后，ACOS7 应用防拔插机制会进行必要的数据恢复。COS 将返回事前保存的数据到 EEPROM 原来的地址。

## 2.2. 卡片应用周期状态

ACOS7 卡具有以下状态:

1. **预个人化状态** – 是卡的初始状态。
2. **个人化状态** – 一旦 MF 成功建立，卡片进入该状态。客户可以在卡片模拟实际操作模式在卡片建立与测试文件。

   用户可以在该状态进行测试，可以通过 CLEAR CARD 命令返回到预个人化状态。详情请参见 **ACOS7 MOC 卡参考手册**。
3. **用户状态** – 创建好预期的文件结构后，用户可以通过 ACTIVATE CARD 命令从个人化状态过渡到用户状态。详情请参见 **ACOS7 MOC 卡参考手册**。

   当通过 ACTIVATE CARD 激活卡片后，卡片将不能再恢复到之前的其它状态，且 CLEAR CARD 命令将不再有效。

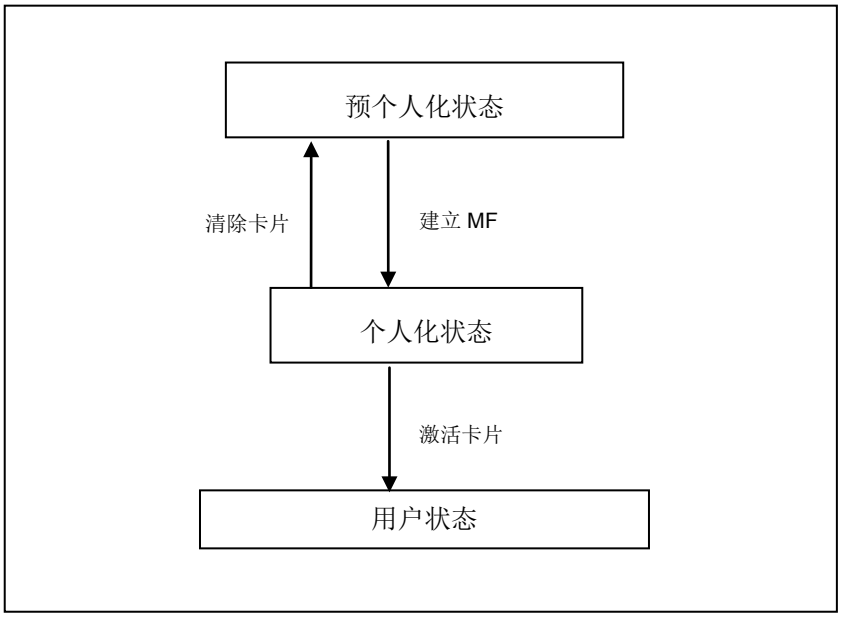


**图1**：卡片应用周期状态

### 2.2.1. 典型的卡片开发步骤

1. 在个人化状态，用户可以建立自己的卡片文件结构。先建立 MF，接着建立 DF 和不同类型的 EF。卡片的安全设计也在该阶段进行测试。如果发现任何设计的缺陷，用户可以通过 CLEAR CARD 命令返回到预个人化状态。
2. 一旦卡片的文件与安全设计测试并最终确认，用户可以执行 ACTIVATE CARD 命令激活卡片，

使 CLEAR CARD 命令失效。

3. 卡片进入到实际操作模式，此时卡片不能再回到之前的状态。

## 2.3. 复位应答(ATR, 接触卡)

硬件复位后（如上电），卡片按照 ISO 7816 第 3 部分规定传送复位应答(ATR)，ACOS7 支持正向约定的 T=0 协议。

***注:*** *详尽的叙述请参看 ISO 7816 第 3 部分.*

## 2.4. 选择应答(ATS, 非接触卡)

收到读卡器的请求选择应答后, 卡片按照 ISO 14443 第 4 部分规定传送选择应答(ATS).

***注:*** *ATS 详尽的叙述请参看 ISO 14443 第 4 部分.*

# 3.0. ACOS7 文件系统

本节探讨 ACOS7 智能卡的文件系统。

## 3.1. 多层次的文件系统

ACOS7 的文件系统和结构完全符合 ISO 7816 第 4 部分的规定。该文件系统非常类似于现代计算机操作系统。该文件系统的根是主文件（MF）。卡中的每个应用或数据文件组可以包含在称为专用文件（DF）的目录中。每个基本文件（EF）都可以在目录下的 DF 或 MF 中存储数据。

此外，ACOS7 允许任意深度的 DF 树结构，也就是说，DF 可以嵌套，参看下面的示例。

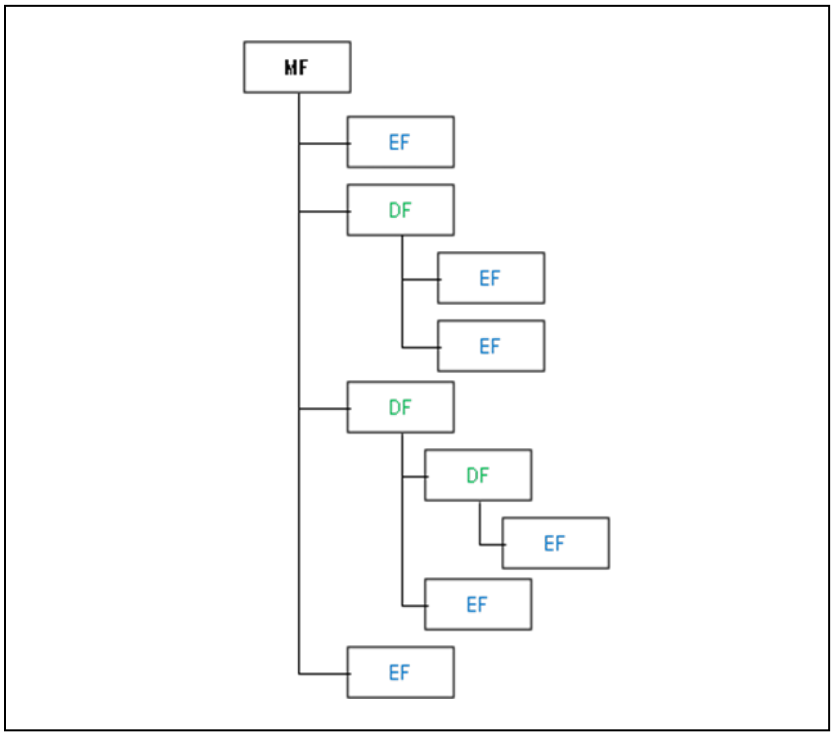


**图2** : ACOS7 多层次文件系统

## 3.2. 文件头数据结构

ACOS7 通过文件组织用户 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。

### 3.2.1. 主文件 MF

MF 文件头数据结构如下：

| 文件头 | 字节数 | 描述 |
|---|---|---|
| 文件类型字节 FDB | 1 | 该字节标识文件的类型，MF 的文件类型为：3Fh |
| 文件标识符 FID | 2 | 该字节标识文件 ID，MF 的 FID 为：3F 00h |
| FCI 文件的文件短标识符 SFI | 1 | 该数据项定义 FCI 文件的短文件标识符 SFI |
| 发卡行自定义 FCI 文件短标识符 SFI | 1 | 描述发卡行自定义 FCI 文件的短文件标识符 SFI |

| 文件头 | 字节数 | 描述 |
|---|---|---|
| 访问条件(AC) | 1 | 描述当前 DF 文件下的安全操作属性 |
| MF 名称 | 5-16 | 对于 MF，该数据域是文件的名称，最大长度 16 字节，可以通过名称选择 MF 文件 |

**表2**：主控文件 – 文件头数据结构

### 3.2.2. 专用文件 DF

DF 文件头数据结构如下：

| 文件头 | 字节数 | 描述 |
|---|---|---|
| 文件类型字节 FDB | 1 | 该字节标识文件的类型，DF 的文件类型为：38h |
| 文件标识符 FID | 2 | 是 MF 内文件的唯一标识。<br>用户可以为 DF 指定任意的 FID 作为唯一的标识。 |
| FCI 文件的文件短标识符 SFI | 1 | 该数据项定义 FCI 文件的短文件标识符 SFI |
| 发卡行自定义 FCI 文件短标识符 SFI | 1 | 描述发卡行自定义 FCI 文件的短文件标识符 SFI |
| 访问条件(AC) | 1 | 描述当前 DF 文件下的安全操作属性 |
| DF 名称 | 5-16 | 对于 DF，该数据域是文件的名称，最大长度 16 字节，可以通过名称选择 DF 文件 |

**表3**：专用文件 – 文件头数据结构

### 3.2.3. 基本文件：透明文件/二进制文件

透明文件/二进制文件是一串字符数据，采用起始地址偏移量。

### 3.2.4. 基本文件：线性定长记录文件

线性定长记录文件是一串预设大小的分组记录数据，各个相关字段的数据分组成一个记录。

### 3.2.5. 基本文件：线性变长记录文件

和线性定长记录文件相似，只是字符数据大小不同。

### 3.2.6. 基本文件：线性循环记录文件

和线性定长记录文件相似，逻辑上不存在“最后记录”。应用视此文件无限制，但文件中的旧记录会被最新记录覆盖。

### 3.2.7. 基本文件：CAPP 文件

CAPP 文件专用于 CAPP 消费。CAPP 文件创建之后，需要使用 Append Record 或 Update 命令向 CAPP 记录添加数据。

### 3.2.8. 基本文件：PIN 文件

PIN 文件用于通过 Verify PIN 命令进行访问控制。

一个 DF 下只能有一个 PIN 文件，一个 PIN 文件可以创建多条不同 ID 的 PIN 记录。

### 3.2.9. 基本文件：灰锁文件

灰锁文件用于 MOC 指令， 文件用于存储电子钱包交易记录，包括储存 MAC，交易日志文件以及其它不同的电子钱包交易记录。

### 3.2.10. 基本文件：密钥（Key）文件

密钥文件用于权限控制以及各种验证指令。

需要指出的是，一个 DF 文件内只能包含一个密钥文件。然而，密钥文件内可以创建不同的密钥记录。各个记录由密钥用途和密钥索引来识别。

### 3.2.11. 基本文件：电子存折文件（ED）

ED 文件用于电子存折的交易应用。

### 3.2.12. 基本文件：电子钱包文件（EP）

EP 文件用于电子钱包的交易应用。

### 3.2.13. 基本文件：交易明细文件

交易明细文件用于保存 ED/EP 交易产生的交易记录。

# 4.0. 安全机制

不同的文件命令根据目标文件的安全访问条件受制于卡片操作系统（COS）。这些条件是基于由系统当前维护的个人识别码和密钥。如果对应的 PIN 或 KEY 的校验或认证通过，卡的命令将被允许执行。

全局 PIN 直接存储在 MF 的 PIN 文件，局部 PIN 存储在当前选定的 DF 的 PIN 文件。同样，全局 KEY 直接存储在 MF 的 KEY 文件，局部 KEY 存储在当前选定的 DF 的 KEY 文件。最多允许同时存在 14 个全局 PIN，14 个局部 PIN，14 个全局 KEY，14 个局部 KEY。

## 4.1. 文件安全属性

每个 MF 或者 DF 都有一个 AC 字节控制在该目录下建立文件的权限，每个 EF 则有 3 个 AC 字节控制读、写等权限。

## 4.2. 安全报文

ACOS7 有 2 种安全报文模式:

1. 带 MAC 的安全报文 (SM - MAC)，它确保了命令的真实性。
2. 带数据加密与 MAC 的安全报文(SM-ENC)，它确保了命令的机密性。

下表总结概括了 SM-MAC 和 SM-ENC 的不同点:

| SM-MAC | |
|---|---|
| 命令 | 用于安全报文的密钥 |
| Card Block<br>Application Block<br>Application Unblock<br>Update Record<br>Update Binary<br>Read Record<br>Read Binary | DAMK |
| PIN Unblock | DPUK |
| Reload PIN | DRPK |

| SM-ENC | |
|---|---|
| 命令 | 用于安全报文的密钥 |
| Update Record<br>Update Binary | DAMK |
| PIN Unblock | DPUK |

**表4**: 安全报文需要的密钥

## 4.3. 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与合法性的过程。相互认证成功执行以后会产生一个过程密钥 *Session Key*，该过程密钥只在过程有效，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。

## 4.4. 密钥导入

密钥导入可以确保密钥安全地从 ACOS6-SAM 导入或者分散到 ACOS7 用户卡(当然密钥也可以由终端导入到卡片，但是出于安全理由，我们不提倡这样做)。为了描述方便，我们定义含有待导入密钥的 ACOS6-SAM 为“*source SAM*”，接收导入密钥的 ACOS7 卡片为“*target SAM*”。

该功能允许主从 SAM 关系，从属的 SAM 可以执行不同的特定操作。

目标卡(ACOS7)使用 Set Key 命令而 source SAM 使用 Get Key 命令来执行密钥导入。

***注：****ACOS6-SAM 具有密钥注入功能。如需更多信息，请参阅 ACOS6-SAM 参考手册。*

# 5.0. 生命支持应用

这些产品的设计并非用于生命支持设备或系统，在这些设备或系统中对这些产品的误操作可能导致人身伤害。如果 ACS 客户将这些产品使用于或者销售用于此类应用，则他们应该自行承担相应的风险，而且同意赔偿由于不当使用或销售从而给 ACS 造成的损失。

# 6.0. 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.