Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS7 (非接触式)

功能规格书 V1.00

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

目录

图目录

表目录

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）自主研发的多应用智能卡操作系统——ACOS7 非接触卡的特性和功能。

1.1. 特性

- 完整的 8K 字节 EEPROM 应用数据存储容量
- 符合 ISO 14443 第 1、2、3 和 4 部分
  - 支持 T=CL 协议，完全符合 ISO 14443 A 标准
- 可实现高速传输（106 Kbps - 848 Kbps）
- 具备 DES/3DES 加密能力
- 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机密性和安全性
- 支持 PBOC 规定的 EP/ED 支付功能
- 符合建设部（MoC）标准
- 多级安全访问层次
- 支持防拔插功能

1.2. 技术规格

以下是 ACOS7 非接触式卡的技术参数。

1.2.1. 电气参数

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

1.2.2. EEPROM

- 容量：8 KB
- EEPROM 耐久性：50 万次擦写
- 数据存储记忆：20 年

1.2.3. 环境温度

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

2.0. 卡片管理

本节概述了卡片级别的特性和管理功能。

2.1. 卡片应用周期状态

ACOS7 非接触式卡具有以下状态：

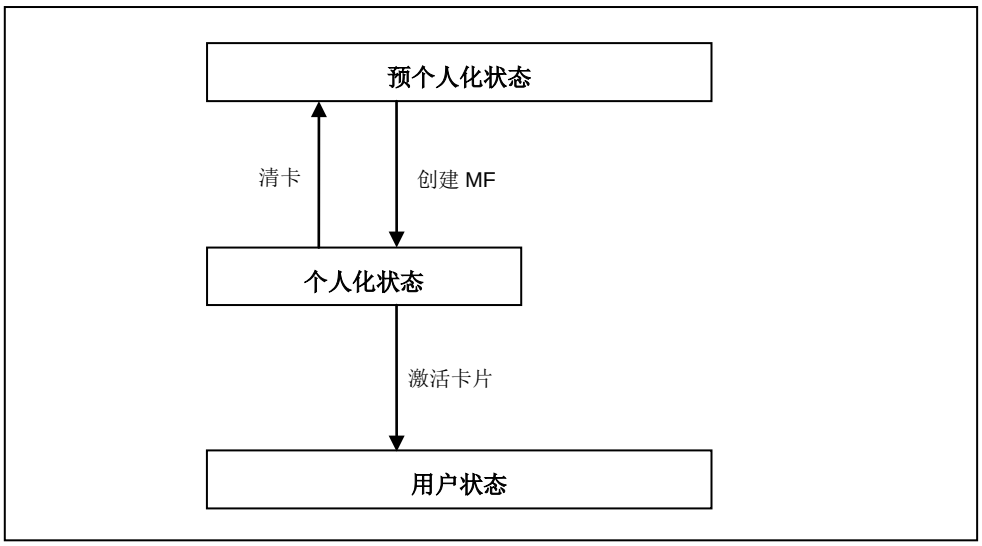

图1 ：卡片应用周期状态

2.1.1. 预个人化状态

预个人化状态是卡的初始状态。

2.1.2. 个人化状态

一旦成功建立主文件（MF），卡片即进入此状态，客户可以在卡片中建立和测试各种文件。

需要注意的是，用户可以在该状态进行测试，并可以通过清卡（CLEAR CARD）命令返回到预个人化状态。

2.1.3. 用户状态

在卡片中建立了需要的文件结构后，用户就可以通过激活卡片（ACTIVATE CARD）命令从个人化状态进入用户状态。

成功运行 ACTIVATE CARD 命令后，CLEAR CARD 命令将失效，卡片不能再恢复到之前的状态。

2.2. 典型的卡片开发步骤

1. 在个人化状态，用户可以建立卡片文件结构。先建立主文件（MF），接着可以建立专用文件（DF）和各种基本文件（EF）。卡片的安全设计也将在该阶段被测试。如果发现任何设计上的缺陷，用户可以随时通过 CLEAR CARD 命令返回到预个人化状态。
2. 卡片的文件与安全设计确定下来并通过全面测试后，用户可以执行 ACTIVATE CARD 命令激活卡片，同时使 CLEAR CARD 命令失效。
3. 卡片进入到用户状态，不能再回到之前的状态。

2.3. 选择应答（ATS）

收到读卡器的请求选择应答（RATS）命令后，卡片按照 ISO 14443 第 4 部分的规定传送选择应答（ATS）。

3.0. 文件系统

本节探讨 ACOS7 非接触式智能卡的文件系统。

3.1. 多层次的文件系统

ACOS7 非接触式卡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计算机操作系统。文件系统的根目录是**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。**基本文件（EF）**可以存储在 MF 或 DF 下。

此外，ACOS7 非接触式卡允许任意深度的 DF 树结构，也就是说，DF 可以嵌套。请参看下面关于多层次的 ACOS7 非接触卡文件系统示例：

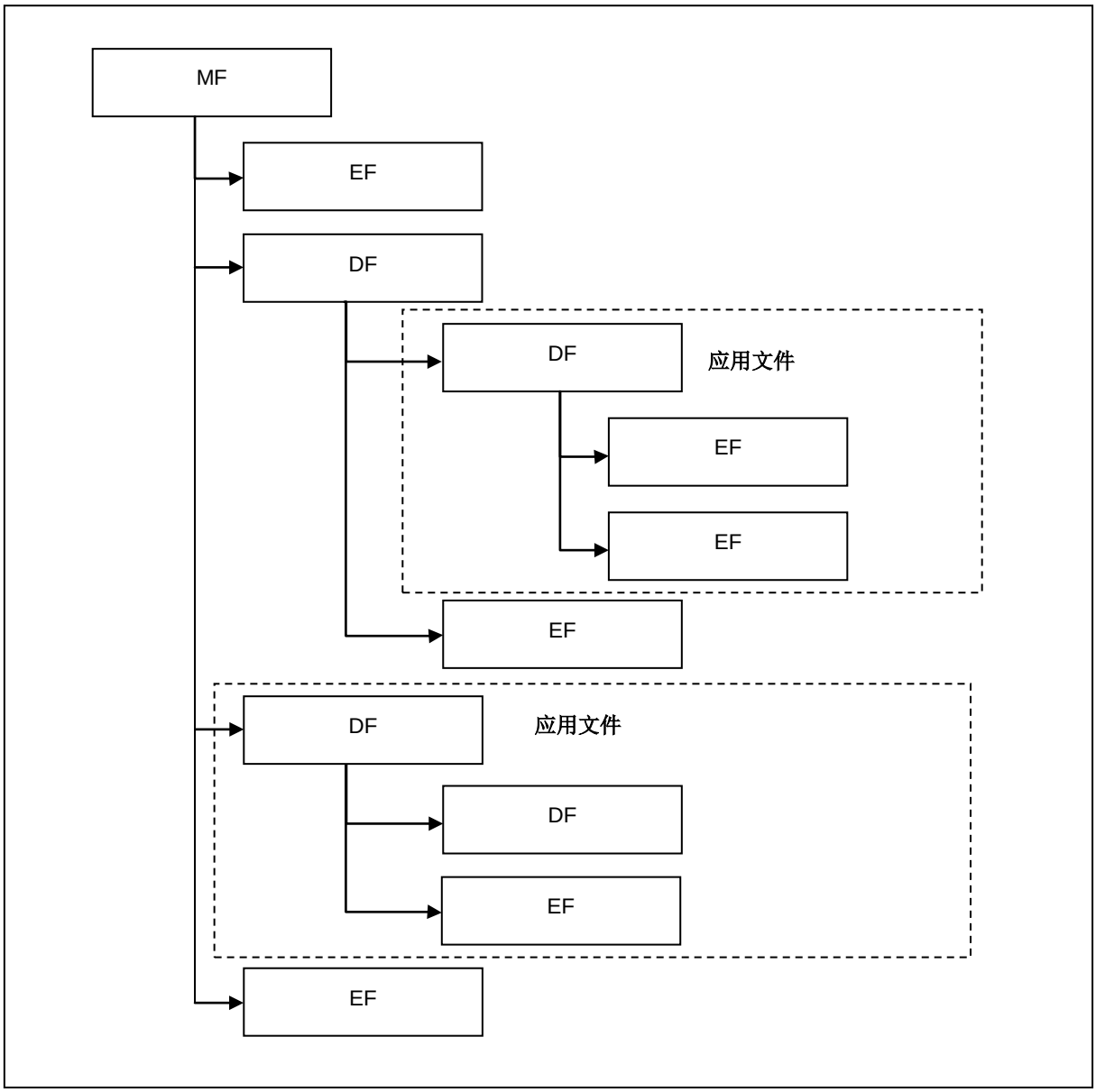

图2 ： 文件系统层次

3.2. 文件头数据结构

ACOS7 非接触卡通过文件组织用户的 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。

3.2.1. 主文件

主文件（MF）的文件头数据结构如下

文件头	字节数	说明
文件类型字节（FDB）	1	代表文件的类型， MF 的文件类型为：3Fh
文件标识符（FID）	2	MF 的 FID 统一为 3F 00h。
FCI 文件的短文件标识符 SFI	1	定义 FCI（文件控制信息）文件的短文件标识符 SFI。
发卡行自定义 FCI 文件的短文件标识符 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 文件下的访问条件
MF 名称	5-16	对于 MF，该数据域是文件的长名。最大长度 16 字节，可以通过名称选择 MF 文件

表1 ：主文件 - 文件头数据结构

3.2.2. 专用文件

专用文件（DF）的文件头数据结构如下

文件头	字节数	说明
文件类型字节（FDB）	1	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 用户可以为 DF 指定任意的 FID 作为唯一的标识。
FCI 文件的短文件标识符 SFI	1	定义 FCI（文件控制信息）文件的短文件标识符（SFI）。
发卡行自定义 FCI 文件的短文件标识符 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 文件下的访问条件
DF 名称	5-16	对于 DF，该数据域是文件的长名。最大长度 16 字节，可以通过名称选择 DF 文件

表2 ：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定位。

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

线性变长记录文件同线性定长记录文件相似，只是记录数据长短不同。

3.2.6. 基本文件：循环记录文件

循环记录文件和线性定长文件相似，只是逻辑上不存在“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。创建 CAPP 文件后，需要使用 APPEND RECORD 命令或 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。

3.2.9. 基本文件：灰锁文件

灰锁文件是用于 MOC 命令的特殊文件。文件用于存储电子钱包交易记录，包括存储 MAC、交易日志文件以及其它与不同的电子钱包交易记录。

3.2.10. 基本文件：KEY文件

KEY 文件用于权限控制以及各种验证指令。

3.2.11. 基本文件：电子存折文件（ED）

ED 文件专门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 文件专门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. 安全特性

本章对 ACOS7 非接触式卡的访问权限和安全功能，以及其环境和应用做了说明。分别是：

- 文件安全属性
- 安全报文发送
- 相互认证
- 密钥注入
- 防拔插机制

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 PIN 和 KEY。如果对应的 PIN 或 KEY 的校验或认证通过，则允许执行卡的命令。

全局 PIN 直接存储在 MF 下的 PIN 文件。同样，局部 KEY 直接存储在当前选定的 DF 的 KEY 文件。最多可以有 14 个全局 PIN、14 个局部 PIN、14 个全局 KEY 和 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 则有三个 AC 字节控制读、写等权限。

4.2. 安全报文发送

ACOS7 非接触卡有 2 种安全报文（SM）模式：

1. 确保真实性的安全报文（SM-MAC） - 它确保了命令的真实性。
2. 确保机密性的安全报文（SM-MAC） - 它确保了命令的机密性。

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。

4.4. 密钥注入

密钥注入可以用于将密钥安全地从ACOS6-SAM卡注入或分散到ACOS7非接触式用户卡中。为了描述方便，我们定义含有待注入密钥的ACOS6-SAM卡为"*source SAM*"，而接受导入密钥的ACOS7非接触卡为"*target SAM*"。

该功能允许SAM存在“主从”关系，并且从属的SAM可以执行不同的特定操作。

"Target SAM"使用SET KEY命令而"source SAM"使用GET KEY命令来执行密钥注入。

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。

4.5. 防拔插机制

ACOS7 非接触卡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，ACOS7 非接触卡会检查防拔插数据域，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。

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

如需了解其他信息请访问 ACS 网站 http://www.acs.com.hk。

如需销售咨询请发送邮件至 info@acs.com.hk。