Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS10
【非接触式】

功能规格书 V1.08

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——ACOS10 非接触卡的特性和功能。

1.1. 更改记录

日期	说明
2012/03/05	ACOS10 6.01 版 • 支持 PBOC 2.0 电子存折和电子钱包支付应用
2014/05/06	ACOS10 6.04 版 • 更新新的 IC 平台，所有功能保持不变。 • 修改 ATR 和 ATS 的默认值
2015/08/11	ACOS10 6.08 版 • 增加 MIFARE 1K 模拟功能

表1 ：ACOS10 双界面卡更改记录

1.2. 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 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 Encryption of data P with key K using DES or 3DES
EF	基本文件 Elementary File

缩略语	描述
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
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

缩略语	描述
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2 ：符号和缩写

2.0. 技术规格

2.1. 电气参数

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

2.2. 环境温度

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

2.3. 通信协议

- T=CL, 最高 848 Kbps 波特率

2.4. 内存

- 容量：8KB
- EEPROM 耐久性：50 万次擦写
- 数据存储时间：10 年

2.5. 加密功能

- DES, 3DES (56/112 位)
- MAC

2.6. 文件安全

- 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 2.0 EP/ED 支付应用
- 多级安全访问层次
- 具有防拔插功能

2.7. 选择应答（ATS）

收到应用程序的请求选择应答（RATS）命令后，卡片按照 ISO 14443 第 4 部分规定传送选择应答（ATS）。

以下是默认的 ATS。关于 ATS 的详细描述请参看 ISO 14443 第 4 部分。

参数	ATS	说明
TL	08h	长度字节
T0	78h	格式字节… 编码 Y(1)及 FSCI
TA1	33h	接口字节… 编码 DS 及 DR
TB1	B5h	编码 FWI 及 SFGI
TC1	02h	编码协议选项
T1	41h	表示卡片类型为 ACOS 卡
T2	10h	主版本号
T3	08h	副版本号

表3 ：选择应答（ATS）

详情请参考 Error! Reference source not found.节。

2.8. 符合的标准

- 符合 ISO 14443 第 1、2、3 和 4 部分的规定

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. 卡片生命周期状态

ACOS10 非接触卡存在以下卡片状态:

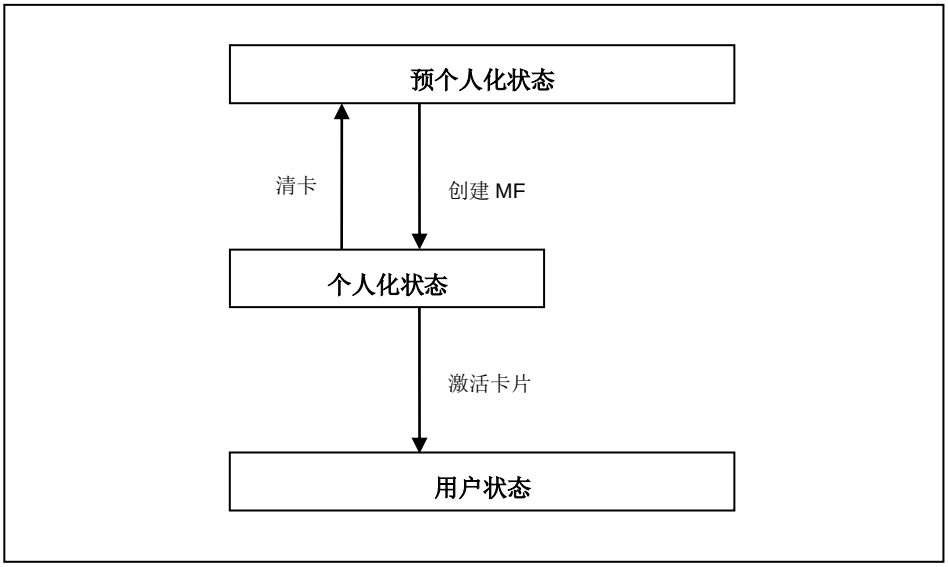

图1 ：卡片应用周期状态

3.1.1. 预个人化 状态

预个人化状态是卡的初始状态。

3.1.2. 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。

3.1.3. 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 命令将不再有效，卡片将不能再恢复到之前的状态。

3.1.4. 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，此时不能再回到之前的状态。

3.2. 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 部分规定传送选择应答（ATS）。

3.3. 自定义 ATS

ATR/ATS 可以自定义，包括定制 TA1 值和历史字节。TA1 字节能够自定义来提高卡片的波特率，历史字节能够自定义来具有唯一的应用标识符。

由于 ACOS10 双界面/非接触 IC 卡和 ACOS10 接触式 IC 卡的固件架构不同，TA1 的值和历史字节只能够在 ACS 工厂进行修改。如需定制 TA1 和历史字节的值，请与 ACS 的销售代表联系。

3.3.1. 自定义 ATS 的 TA1 值

目前非接触式通信协议以 TA1=33h 代表其支持的比特率，也就意味着卡片既支持从 PICC 至 PCD 也支持从 PCD 至 PICC 的 106、212 和 424 kbps 的传输速率。这在 ISO 14443 标准第 4 部分的 5.2.4 节中有相关规定。ACOS10 双界面卡可以将 TA1 值设为 77h 来支持最高 848 kbps 的传输速率。

类似于接触式卡 TA1 的定制，解决方案供应商在大批量订购 ACOS10 双界面卡之前，需要确保定制的波特率与其现有的非接触式智能卡读写器（PCD）兼容。要了解更多信息，请联系 ACS 的销售代表。

3.3.2. 针对 Microsoft Windows 自定义 ATR/ATS

在 Windows® 7 及更高版本的操作系统中，当智能卡插入读写器后，Windows 会尝试自动下载并安装智能卡微型驱动程序。由于 ACOS10 双界面卡并不按照 Windows 系统默认的方式来应用，因此没有必要下载智能卡微型驱动程式。但如果将 ACOS10 卡插入 Windows 系统，系统仍会在线搜索智能卡驱动并发出警告信息，提示“未能成功安装设备驱动程序”。为此我们提供了两种解决方案：

1. 在 Windows 中禁用智能卡即插即用，并关闭为智能卡提供证书（certificate propagation）的服务。
2. 修改 ATS，使 Windows 系统识别出 ACOS10 双界面智能卡，并使用 ACS 统一的 NULL 驱动程序

关于第一种解决方案，请按照下方 Microsoft®支持链接中的指令禁用智能卡的即插即用。您需要在系统中的所有电脑上执行此操作 http://support.microsoft.com/kb/976832。

关于第二种解决方案，ACS 开发出了适用于 ACOS 智能卡产品线的统一的 NULL 驱动程序。该 NULL 驱动程序可以满足 Windows 的要求并为卡片提供微型驱动程序，卡片插入后，Windows 系统不再每次都发出警告。要使 Windows 识别出 ACOS10 双界面智能卡并使用 ACS 统一的 NULL 驱动程序，需要对卡片的 ATR 进行自定义。ATS 自定义的过程由 ACS 来完成。如需了解更多信息，请联系 ACS 的销售代表。

ACOS10 非接触界面的 ATS 应为：

ATS：08 78 XX B5 02 41 4e 44h

XX 表示 TA1 的值。TA1 值可以被设置为所用到的智能卡读写器支持的波特率。自定义完成后，ATS 的自定义值如下：

ATS：08 78 33 B5 02 41 4e 44h

4.0. 文件系统

本节探讨 ACOS10 非接触卡的文件系统。

4.1. 多层次的文件系统

ACOS10 非接触式卡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。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，ACOS10 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 ACOS10 非接触卡文件系统示例：

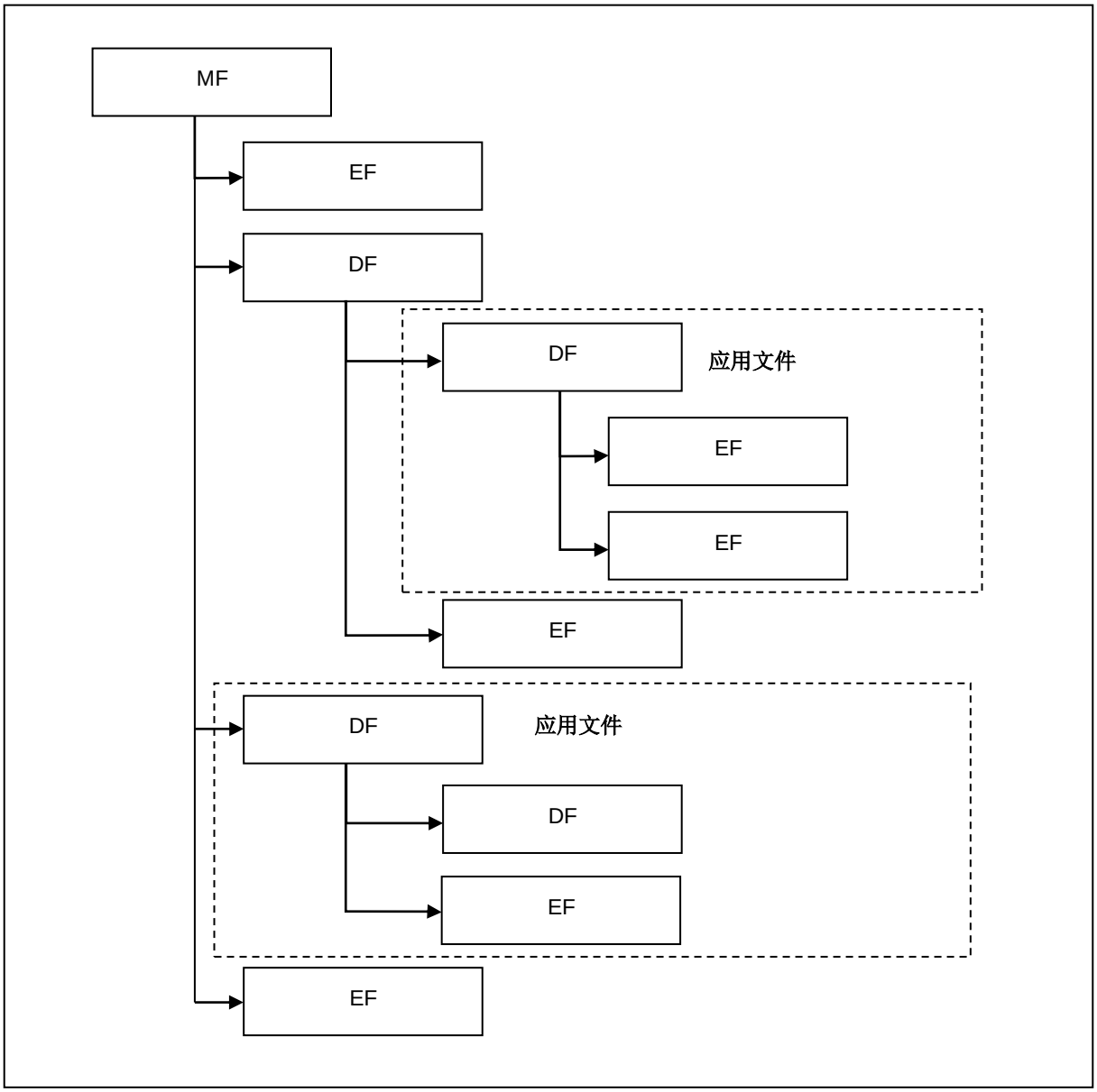

图2 ： 文件系统层次

4.2. 文件头数据结构

ACOS10 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。

4.2.1. 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4 ：主文件 - 文件头数据结构

4.2.2. 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	代表文件的类型， DF 的文件类型为：38h
文件标识符（FID）	2	标识同一 MF 下唯一的文件 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5 ：专用文件 - 文件头数据结构

4.2.3. 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。

4.2.4. 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。

4.2.5. 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。

4.2.6. 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。

4.2.7. 基本文件： PIN 文件

PIN 文件用于通过 VERIFY PIN 命令进行访问控制。

4.2.8. 基本文件：KEY 文件

KEY 文件用于权限控制以及各种验证指令。

4.2.9. 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。

4.2.10. 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。

4.2.11. 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。

5.0. 安全特性

本章对 ACOS10 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。

5.1. 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。

5.2. 安全报文发送

ACOS10 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。

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. 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ACOS10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ACOS10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可以执行各种特定操作。

"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。***

5.5. 防拔插机制

ACOS10 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，ACOS10 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。

6.0. 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。

7.0. 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。