Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS10

接触式智能卡

功能规格书 V1.03

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

本手册阐述了龙杰智能卡有限公司（Advanced Card Systems Ltd., ACS）研发的 ACS 智能卡操作系统——版本 10（ACOS10）的特性和功能。

1.1. 特性

ACOS10 具有以下特性：

- 完整的 32K 字节 EEPROM 应用数据存储容量
- 符合 ISO 7816 第 1、2、3、4 部分
- 可转换的高速通讯波特率（ 9600 - 223,200 bps）
- 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
- 支持 DES 和 3DES 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
- 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 ACOS10 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）
- 最大电源电流：<10 mA
- ESD 保护：≤ 4 KV

1.2.2. EEPROM

- 容量：32 K 字节（32,768 字节）
- EEPROM 使用寿命：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 至 85 °C
- 存储温度：-40 °C 至 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 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
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

缩略语	描述
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

本节概述了卡片功能和管理。

2.1. 防拔插机制

ACOS10 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，ACOS10 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. 卡片头模块

ACOS10 是一个具有 32K EEPROM 的卡片操作系统。在其初始状态下（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 。

2.3. 卡片应用周期状态

ACOS10 卡具有以下状态：

1. **预个人化状态** – 是卡的初始状态。允许用户自由访问卡片头模块（在上一节中定义）。该卡片头模块可以通过使用地址模式被 READ BINARY 或 UPDATE BINARY 命令访问。

   用户可以随意个人化卡片头模块。

2. **个人化状态** – 一旦 MF 成功建立而卡片应用周期标识位未改变，卡片就会进入该状态。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，但是客户可以模拟实际操作模式在卡片中建立和测试文件。

   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。

3. **用户状态** –一旦 MF 成功建立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，但没有设置特殊功能标识的 b5 位（取消激活卡片使能标志），卡片将不能回复到之前的状态。此时 CLEAR CARD 命令和 DEACTIVATE CARD 命令将不再有效。

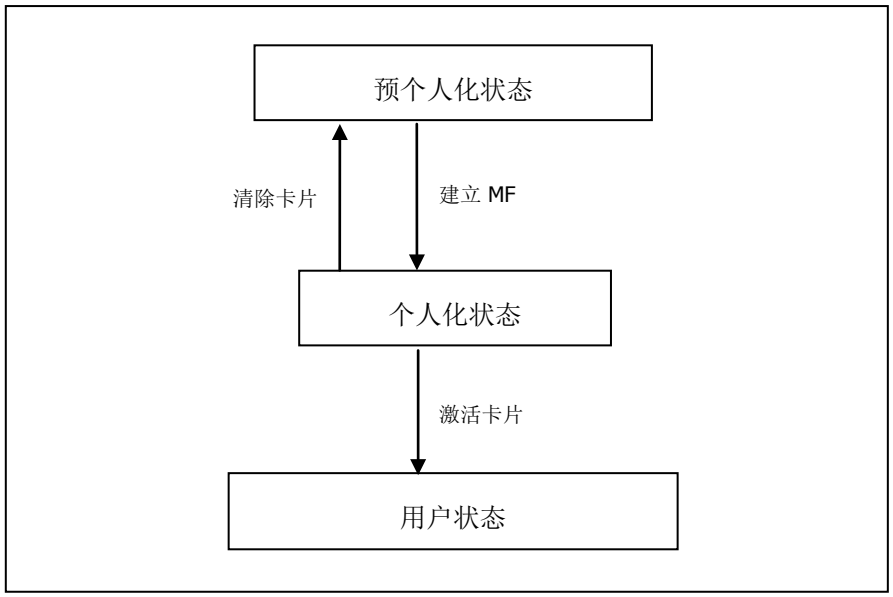

图1： 卡片应用周期状态

2.3.1. 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. 然后用户建立自己的卡片文件结构。先建立 MF，接着建立 DF、EF 等，卡片的安全与文件设计等将在该阶段被测试。如果发现任何设计的缺陷，用户可以毫不费力地通过 CLEAR CARD 命令返回到预个人化状态。
3. 一旦卡片的文件与安全设计完成测试并最终确认，执行 CLEAR CARD 命令，并使用 UPDATE BINARY 命令更改卡片应用周期标识位。
4. 重新创建 MF 后，卡片进入到实际操作模式。用户可以在此阶段重构文件系统。卡片将不能再恢复到之前的状态。

2.4. 复位应答（ATR）

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）。ACOS10 支持正向约定的 T=0 协议，但协议提及的其它功能卡片并不支持。

以下是默认的 ATR。详尽的叙述请参看 ISO 7816 第 3 部分。

2.4.1. 自定义 ATR

ACOS10 的 ATR 可以自定义，包括修改卡片传输速度或向卡片写入具体的身份信息。新的 ATR 必须符合 ISO 7816 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。

3.0. 文件系统

本节探讨 ACOS10 智能卡的文件系统。

3.1. 多层次的文件系统

ACOS10 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。

ACOS10 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。

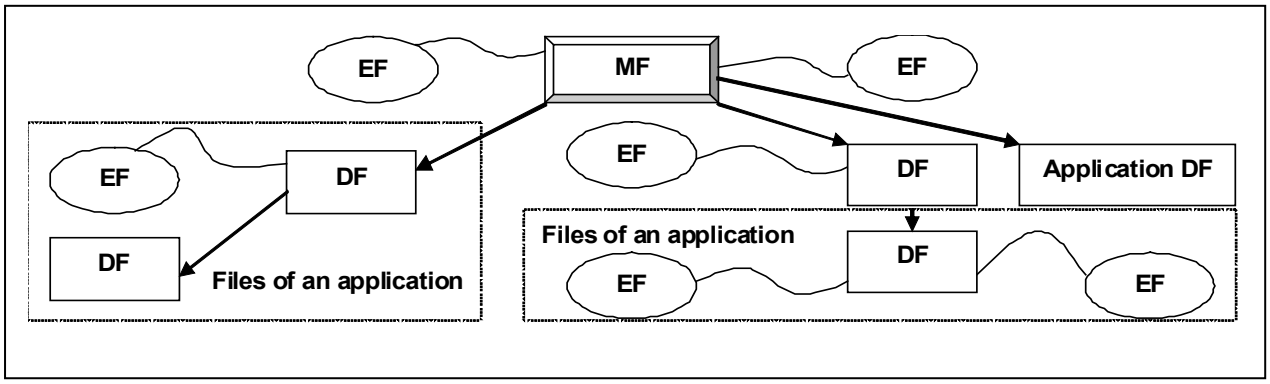

图2： 多层次的 DF 文件系统

3.2. 文件头数据结构

ACOS10 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。文件头模块的知识将有助于应用程序开发人员准确地规划 EEPROM 空间的使用。

3.2.1. 文件类型字节（FDB）

该字节标识文件的类型，文件头模块的长度取决于文件类型。

3.2.2. 数据编码字节（DCB）

ACOS10 不使用该数据域，它只是设置为文件头模块的一部分以符合 ISO 7816 第 4 部分。

3.2.3. 文件标识（File ID）

这是一个 16 位的数据域，它是卡片文件（含目录文件）的唯一标识。在同一个 DF（或 MF）下的文件必须是唯一的。

3.2.4. 文件大小

这是一个 16 位的数据域，用于指定文件的大小，但是不包含文件头模块的大小。对于记录类型的 EF，第一个字节表示记录的最大长度（MRL），而第二个字节表示记录的数量（NOR）。对于非记录类型的 EF，第一个字节代表文件长度的高字节，而第二个字节代表文件长度的低字节。对于 DF，该数据域无用途。

3.2.5. 文件短标识符（SFI）

这是一个 5 位的数值，表示文件的短标识符。ACOS10 允许通过 SFI 指定文件。文件标识（FID）的最后 5 位不一定要匹配这个 SFI。同一个 DF 下可能有 2 个文件使用同一个 SFI。在这种情况下，

ACOS10 将选择第一个创建的文件。

3.2.6. 应用周期状态字（LCSI）

正如 ISO 7816 标准第四部分定义，这个字节表明文件的应用状态。它可以有以下值：

b8	b7	b6	b5	b4	b3	b2	b1	Hex	含义
0	0	0	0	0	0	0	1	01	创建状态
0	0	0	0	0	1	0	1	05	操作状态（激活的）
0	0	0	0	0	1	0	0	04	操作状态（取消激活的）
0	0	0	0	1	-	-	-	08 – 0F	终止状态

表2：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，对该文件的命令只有在该文件的安全条件得到满足的情况下有效。
- 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，对该文件的全部命令都无效。

3.2.7. 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。

3.2.8. 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。

3.2.9. 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记录号。

其它情况，该数据域无用途。

3.2.10. 父目录地址

这 2 个字节表示文件父目录的物理 EEPROM 地址。

3.2.11. 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模块先前的全部字节。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。

3.2.12. 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的安全条件。如 ISO 7816 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** 部分。

3.2.13. 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的安全条件。该数据编码与 SAC 不同，但是同样符合 ISO 7816 定义。该数据域的最大长度是 32 字节，详情参看 **5.1.2** 部分。

对于 DF 文件，文件头模块中还包含附加数据域。

3.2.14. 安全环境文件标识（仅适用于 DF）

对于 DF，该数据域为 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（SE）文件，属于 COS 的内部操作文件。

3.2.15. FCI 文件标识（仅适用于 DF）

对于 DF，该数据域包含 2 个字节，分别是 FCI 文件与 Issuer FCI 文件的短文件标识符（SFI）。这 2 个文件都是该目录的子文件。

3.2.16. DF 名称（仅适用于 DF）

对于 DF，该数据域是文件的长名 。我们可以通过长名选择文件。DF 最长 16 个字节。

3.3. 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，它的读（Read）条件应设置为 Never。一般来说，一个 DF 应该具有：（1）一个内部线性变长文件（FDB=0C），存储用于校验的 PIN；（2）一个内部线性变长文件，存储用于认证的 KEY；及（3）一个安全环境（SE）文件，用于存储安全条件。

内部文件可能包括（1）PIN 数据结构或者（2）KEY 数据结构。

4.0. PBOC 应用

4.1. PBOC 文件

PBOC 文件可以为电子钱包（EP）文件/电子存折（ED）文件。在交易明细记录文件中，记录的固定长度是 23 个字节，最大记录个数是 20。一个 DF 只能包含一个 PBOC 文件。

ED 的读余额（Get Balance）命令的访问条件与 PBOC 文件的读访问条件相同。EP 的读余额（Get Balance）命令可以自由执行。

PBOC 的交易遵循以下标准：

1. <<中国金融集成电路（IC）卡规范>> – 第 1 部分 电子钱包/ 电子存折卡规范
2. <<中国金融集成电路（IC）卡规范>> – 第 2 部分 电子钱包/电子存折应用规范

4.2. PBOC 交易

关于 PBOC 交易更多的资料，请参看<<中国金融集成电路（IC）卡规范>>– 第 2 部分 电子钱包/电子存折应用规范。

5.0. 安全机制

文件命令受制于目标文件（或当前的 DF）的安全访问条件。这些条件是基于由系统当前维护的个人密码和密钥。如果对应的 PIN 或 KEY 的校验或认证通过，卡的命令将被允许。

全局 PIN 直接存储在 MF 的 PIN 文件（EF1），局部 PIN 存储在当前选择的 DF 的 PIN 文件。同样，全局 KEY 直接存储在 MF 的 KEY 文件（EF2），局部 KEY 存储在当前选择的 DF 的 KEY 文件。最多允许同时存在 31 个全局 PIN，31 个局部 PIN，31 个全局 KEY，31 个局部 KEY。

5.1. 文件安全属性

每个文件（MF、DF 或 EF）的文件头模块中都设置有一套安全属性。安全属性设置模式分为两种：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中的数据结构。它标识对于该文件什么样的文件操作是允许的，以及要符合哪些条件对应的文件操作才被允许。

- SE 记录存储在 SE 文件中，该 SE 文件的 ID 在当前 DF 的文件头中指定。

5.1.2. 扩展安全属性（SAE）

SAE 是一个存储在每个文件中的数据结构，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）加一个或多个安全条件数据对象（SCDO）。

5.2. 安全环境（SE）

安全条件被编码于一个 SE 文件中。每个 DF 都有一个专用的 SE 文件，该文件的 FID 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。

SE 认证模板（SE Authentication Template）：认证模板（AT）定义该 SE 需要满足的安全条件，所定义的安全条件是 PIN 校验或者 KEY 认证。

5.3. 外部认证

外部认证使用卡片随机数与终端响应的方法获取卡片的授权。

5.4. 安全报文

ACOS10 的安全报文模式分为两种，分别是：

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 Application Block Application Unblock Update Record Update Binary Read Record Read Binary	DAMK
PIN Unblock	DPUK
Reload PIN	DRPK

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

表3：安全报文需要的密钥

5.5. 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会话密钥（Session Key），该会话密钥只在会话中才有效。这个会话我们这样定义：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相互认证的执行。

5.6. 密钥导入

密钥导入可以确保密钥安全地从 ACOS6-SAM 导入或者分散到客户的 ACOS10 卡。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 ACOS10 卡为“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。

“Target Sam”使用 Set Key 命令，而“source SAM”使用 Get Key 命令来执行密钥注入。

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。