Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS3X eXpress 智能卡

功能规格书 V1.02

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

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 3 eXpress（ACOS3X）的特性和功能。

1.1. 特性

- 完整的 256 KB EEPROM 应用数据存储容量
- 符合 ISO 7816 第 1、2、3 部分，支持 T=0 直接协议
- 可转换通讯波特率（9,600 – 223,200 kbps）
- 具有 DES/3DES 和 MAC 功能
- 内置硬件 3DES 协处理器，支持快速加密操作
- 5 组密码+发行商代码
- PIN 码可由持卡人更新
- 密钥对用于相互验证
- 基于随机数的会话密钥
- 符合 FIPS 140-2 的随机数产生器（基于硬件）
- 二进制文件和记录文件用于储存用户数据
- 安全报文发送功能确保用户数据传输的机密性和安全性
- 支持高度安全电子钱包支付应用

1.2. 技术参数

以下是 ACOS3X 卡的技术参数：

1.2.1. 电气参数

- 工作电压：5 V DC+/-10%（A 类），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：256K 字节（262,144 字节）
- EEPROM 使用寿命：10 万次擦写
- 数据保持时间：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

2.0. 芯片生命周期

在芯片卡的整个生命周期中，可以区分三个阶段和两种操作模式。

- 生产状态 (Manufacturing State)
- 个人化状态 (Personalization State)
- 用户状态 (User State)
- 用户状态—发行商模式 (Issue Mode)

卡在任何时候总是处于其中的一种状态，而且可能在这四种状态之间转换，如下图所示。

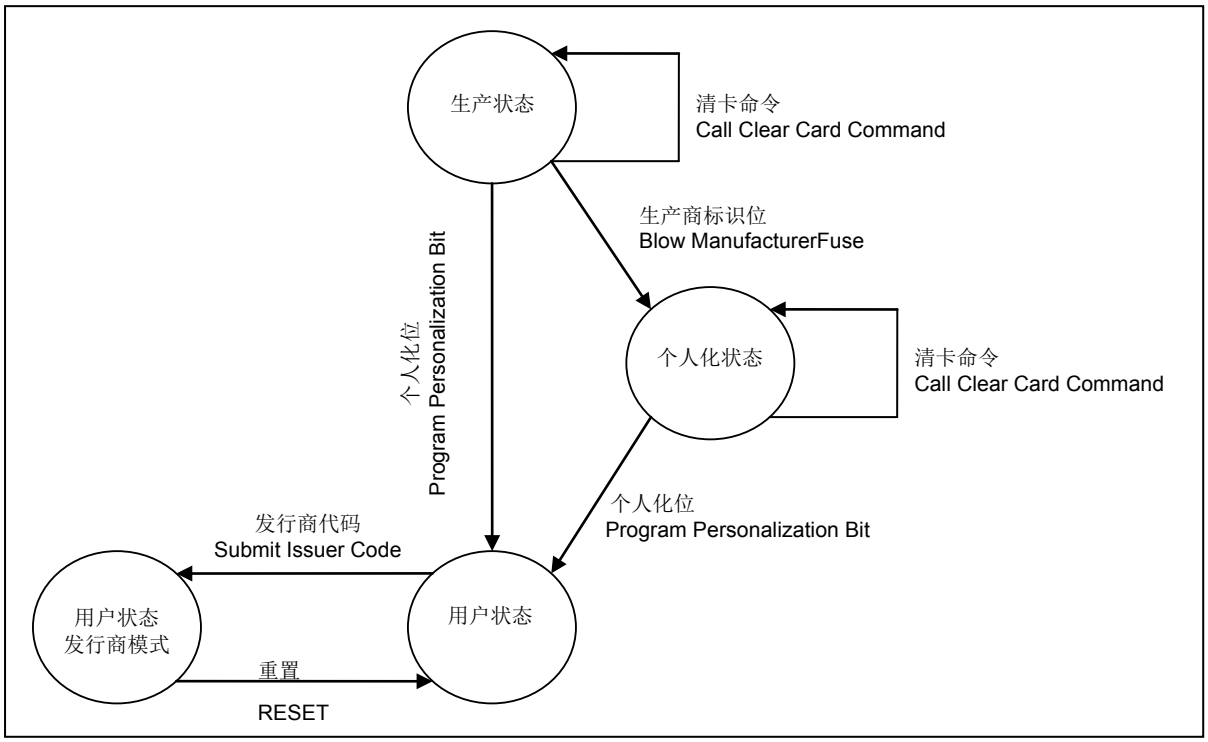

图1：芯片卡生命周期

实际的芯片生命周期状态是在复位后由卡片操作系统决定的。在操作过程中，芯片生命周期状态是不会改变的。在个人化状态和生产状态中可以发布清卡命令，用于清除卡片中除生产商和 IC 代码外的所有数据，但是这个命令在用户状态以后就无法使用了。

2.1. 生产状态

生产状态从芯片生产后即开始生效，直到一个相关的标识位（即 EEPROM 中的某一个位）——生产商标识位被编程为止。

IC 出示给卡时是没有加密的。

生产商状态中所有的命令均可用。另外，生产商文件 (Manufacturer File) (FF 01h)只能够在此状态中进行编写。

生产商文件包含与生产状态相关的 2 条记录，每条包括 8 个字节。此文件包含生产商标识位 (Manufacturer Fuse) 。对生产商标识位进行设置后，卡片即进入个人化状态，同时生产商文件变为只读。卡片的独特数据和共同数据均可被编程，例如卡生产商身份、卡序列号等等。卡片不会解读这些数据。

在此状态中，可以通过清卡命令 (CLEAR CARD) 物理擦除卡片的数据和密钥。此命令将会擦除 EEPROM 内存，但 IC 代码和生产商文件除外。

一旦生产商标识位被改变，从而终止生产状态后，则再也无法将卡片重设回生产状态。

2.2. 个人化状态

在生产状态终止后，卡片就会进入个人化状态，直到 EEPROM 中一个相关的位——即所谓的个人化位 (Personalization Bit) 被编程 。

在此状态中，可以通过清卡命令物理擦除卡片的数据和密钥。此命令将会擦除 EEPROM 内存，但是 IC 代码和生产商文件除外。另外，可以重新进行卡片个人化。

在个人化状态中，只有提交正确的 IC 代码后才能够对内部数据文件进行写访问以及对安全文件进行读访问。IC 代码是由卡片生产商在卡片位于生产状态时写入的。

IC 出示给卡时是没有加密的。在将正确密钥编入个人化状态之前不应该执行验证过程。

一旦个人化位被编程，从而终止个人化状态后，则再也无法将卡片重设回个人化状态。

2.3. 用户状态

用户状态是指卡片通常的操作模式。可以细分为两种，分别为用户状态及用户状态—发行商模式。在个人化状态终止后，卡片就会进入用户状态。持卡人对卡片的操作大部分都是在此状态中完成的。

一旦提交发行商代码，则卡片的操作模式就会被修改为发行商模式。某些内存区域只有在这种模式中才允许访问。

3.0. EEPROM 内存管理

由卡芯片提供的用户 EEPROM 内存空间完全用于储存用户数据。另有额外的 EEPROM 区域用于储存内部卡片配置数据。

- 用户数据内存储存由应用程序控制的卡片数据。
- 内部卡片配置数据被卡片操作系统用于管理卡片的功能。

3.1. 数据文件

在数据文件和数据记录的范围内，访问内部数据内存区域和用户数据内存区域都是可以的。内部数据内存的数据文件被称为内部数据文件 (Internal data Files)，而用户数据内存的数据文件被称为用户数据文件 (User Data Files)。

数据文件是可以具有独立安全属性的最小单位，这些安全属性用于控制对储存在 EEPROM 中的数据的读写访问。

数据文件可以是记录类型或透明类型。

3.2. 数据文件访问控制

每个数据文件都会被分配两种安全属性，即读安全属性 (Read Security Attribute) 和写安全属性 (Write Security Attribute)。安全属性定义了相关操作必须满足的安全条件：

- 读安全属性用于控制读记录（READ RECORD）/读二进制（READ BINARY）命令对文件中数据的读访问。如果没有满足读安全属性所指定的安全条件，则卡片就会拒绝对这个文件发送的读命令。
- 写安全属性用于控制写记录（WRITE RECORD）/写二进制（WRITE BINARY）命令对文件中数据的写访问。如果没有满足写安全属性所指定的安全条件，则卡片就会拒绝对这个文件发送的写命令。

每个数据文件的读安全属性和写安全属性说明了在允许相关的操作之前必须已经正确向卡片提交的应用代码，以及发行商代码和/或 PIN 码是否必须已经被提交。

逻辑 OR 函数应用在指定的应用代码(Application Codes，AC x)，也就是说，如果一个安全属性中指定了多个应用代码，则只要正确地提交其中任何一个应用代码即可满足安全条件。

PIN 和 IC 代码采用了逻辑 AND 函数。也就是说，如果一个安全属性中指定了 PIN 和/或 IC，则除了指定的应用代码之外还必须已经提交 PIN 和/或 IC 代码。

3.3. 内部数据文件

除了帐户数据结构（它们与一系列特别的命令相关联），内部数据内存的内存区域被作为数据文件处理。

内部数据文件的属性是在卡片操作系统中定义并且无法修改的。然而，安全属性取决于卡片生命周期的状态。

3.4. 用户数据文件

用户数据文件是在卡片生命周期的个人化状态中被分配的。用户数据文件可分为两种，记录文件和二进制文件。记录文件由记录数量和固定的记录长度指定。二进制文件由文件大小而定并通过偏移量进行访问。

如果可以满足数据文件的安全条件，则储存在用户数据文件中的数据可以通过 READ

RECORD/BINARY 命令读取，而且可以通过 WRITE RECORD/BINARY 命令更新。

用户数据文件是当卡片处于个人化状态时通过在用户文件管理文件的记录中写人相应的文件定义块完成定义的。一旦任何用户数据文件被使用，则无法再改变文件的记录数量。只要数据在卡内，用户就能使用这些数据。

3.5. 数据文件使用

内部数据文件和用户数据文件的访问过程是一样的。

3.6. 帐户数据结构

帐户数据结构（简称帐户）应用在某个“数量”的数值必须安全地被处理的应用中。帐户被储存在帐户文件中。

在卡生命周期中的用户状态，帐户中的数据无法像用户数据文件中的数据那样通过写命令进行更新。有一套专有的命令用于处理帐户，即为帐户充值或者从余额中扣减，以及阅读当前余额。

账户充值以及扣减和读取余额可以设置不同的访问条件。

关键帐户操作，如充值 (Credit)，受到严格的安全控制。

4.0. 安全结构

ACOS3X 卡片操作系统提供以下的安全机制：

- 防拔插机制
- DES/3DES 和 MAC 计算
- 基于随机数的相互验证和会话密钥
- 密码
- 数据文件安全报文发送
- 安全帐户交易处理

DES 是指用于数据加密和解密的 DEA 算法，如 ANSI X3.93 规格所指定。MAC 是指用于生成密码校验和的算法（密码块链接模式下的的数据加密算法 DEA），如 ANSI X3.93 所指定的。

相互认证是指这样的一个过程，其中卡和卡片接受设备互相认证对方身份的真实性。相互认证成功执行以后会产生一个会话密钥。它用于“会话”('SESSION')中的数据加密和解密。一个会话是指成功执行相互认证过程后至卡片复位或执行另外一个开始会话(START SESSION)命令之间的时间。

密码和 PIN 码是用于选择性地允许对卡片中储存的数据和卡片提供的功能与特征进行访问，例如 READ 和 WRITE 命令。

安全报文发送功能确保卡与终端/服务器之间数据传输的安全性，防止数据被监听、重放或被非授权地修改。这是通过使用 MAC 签署命令和响应以及加密命令和响应数据实现的。

帐户交易处理提供了一种对帐户数据结构中的数据（尤其是余额）进行安全的、可审查的控制的机制。

4.1. DES 和 MAC 计算

所有用于 DES/3DES 和 MAC 计算的密钥的长度都是 8 个或 16 个字节，具体取决于选项寄存器(Option Register) 中的 DES/3DES 选择。密钥中每个字节的最低有效位不用于计算，而且也不被卡片操作系统解释。

4.2. 相互认证和生成会话密钥

相互□□是基于卡和读卡设备之间的密钥交换和相互认证。密钥交换通过使用随机数和 DES/3DES 数据加密安全地进行。

会话密钥是相互认证过程的最后结果，它的生成是基于卡和终端的随机数。

相互认证的成功完成会被记录在卡中。生成的会话密钥 K_S 用于这一会话中所有的数据加密和解密。

卡片具有一个错误计数器 CNT K_T 用于计算和限制执行认证（AUTHENTICATE）命令连续失败的次数。

卡片随机数（RND_C）是由存储在安全文件中的随机数种子在复杂且不可预见的数学运算中生成的。每次执行完 START TRANSACTION 命令，卡片的操作系统都会对随机数种子进行内部更新。

4.3. 密码

卡中储存的密码用于限制对储存在用户数据文件中的数据以及对某些由卡片提供的命令的访问。若要读取用户数据文件中的数据或者向其写入数据，或者要执行某些特别的卡命令，则要先向卡提交密码。

4.4. 安全报文

ACOS3X 支持用于数据文件的安全报文(Secure Messaging, SM）。安全报文功能确保卡与终端/服务

器之间数据传输的安全性，防止数据被监听、重放或被非授权地修改。用户数据文件可被指定为 READ/WRITE RECORD/BINARY 命令时需要使用安全报文发送。几乎所有其他的命令也都能够使用由终端发起的安全报文发送。

ACOS3X 采用的安全报文发送既能够对传入也能够对传出卡片的数据进行加密或签名。

4.5. 帐户交易处理

与帐户相关的密钥有四种：

- 充值密钥(Credit Key) K_{CR}
- 消费密钥(Debit Key) K_D
- 证明密钥(Certify Key)K_{CF}
- 撤回消费密钥(Revoke Debit Key) K_{RD}

密钥储存在帐户安全文件中 (Account Security File)。

密钥被用于计算和验证在帐户处理中卡片和相应设备之间交换的命令和数据的 MAC 密码校验和。

4.6. 防拔插机制

防拔插机制用于保护卡片的数据和安全，避免由于卡片在操作过程中突然断电或者拔出而导致损坏。

向卡中写入用户数据时，ACOS3X 的防拔插机制能确保操作以原子方式执行。也就是说，要么数据被完全写入，要么在写操作前目标写区域处于之前的状态。执行 CREDIT/DEBIT/REVOKE DEBIT 命令时，账户数据文件也是以一种类似的方式受到保护。

5.0. 符合 ISO 标准与复位应答

硬件复位（如上电）后，卡片按照 ISO 7816 第 3 部分规定传送复位应答(ATR)。ACOS3X 支持 T=0 协议类型，但不支持协议类型选择功能。

5.1. 自定义 ATR

自定义 ACOS3X 的 ATR 的方式有两种。第一种是向个人化文件 FF 02h 的第一至第八字节添加个人化信息。这可以在上电时在上一节提到的默认的 ATR 的历史字节中获取。

ACOS3X 还允许修改卡片的传输速度或者按照应用程序开发员的喜好完全自定义历史字节。这些 ATR 修改是通过提交 IC 代码后写内部文件 FF 07h 来实现的。

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。