Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-64

功能规格书 V1.05

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

目录

图目录

1.0. 简介

本文件介绍了龙杰智能卡有限公司（Advanced Card Systems Ltd.，ACS）自主研发的加密智能卡（PKI 卡）—ACOS5-64 的功能和特性。

ACOS5-64 是一款先进的加密智能卡，其操作模式通过了 FIPS 140-2 （美国联邦信息处理标准）的第 3 级认证。这款智能卡完全符合 ISO 7816 第 1、2、3、4、8 和 9 部分的规定，专为基于公钥的各类应用而设计。此外，它旨在提高 RSA 公钥加密操作的安全性与性能，对于智能卡公钥基础设施（PKI）和具有高级别安全要求的应用而言非常重要。

ACOS5-64 支持多种安全基础设施和应用，其中包括：

- Microsoft® Crypto-API、Microsoft® CNG 和 PKCS #11 中间件
- 安全的在线证书生成
- Microsoft® Outlook 、 Windows® Mail 、 Microsoft® Outlook Express 以及 Mozilla® Thunderbird®邮件签名和加密(S/MIME)
- Mozilla® Firefox®
- Internet Explorer®
- Windows®智能卡登录
- Microsoft® Office
- Open Office
- Adobe® Reader®

1.1. 卡片特性

ACOS5-64 加密智能卡的主要特性包括：

- 完整的 64 KB EEPROM 应用数据存储容量
- 快速 EEPROM 写入
- 文件系统能够在不影响安全性的前提下重新使用已删除文件的内存空间
- 通过文件系统对 EEPROM 进行管理，延长卡片的使用寿命
- 符合 ISO 7816 第 1、2、3、4、8 和 9 部分的规定
  - 支持 ISO 7816 第 4 部分的文件结构：透明、线性定长、线性变长、循环
- 可通过修改 ATR 实现高速传输（9.6 Kbps - 223.2 Kbps）
- 具有相互认证功能，能够生成过程密钥
- 支持 DES/3DES/3K3DES/AES-128/AES-192/AES-256/RSA (最高 4,096 位)
- 具有安全报文发送功能，确保数据传输的机密性和真实性
- 通用标准 EAL5+（芯片级）
- 通过 FIPS 140-2 第 3 级认证的操作模式（参考**操作模式字节**）
- 支持向后兼容模式，卡片可用于多种模式：ACOS5-64 v2.00 模式、NSH-1 模式（参考**操作模式字节**）
- 多级安全访问层次
- 支持防拔插功能

如需了解更多关于 ACOS5-64 v3.00（通过 FIPS 140-2 第 3 级认证）加密模块功能、防护措施和访问权限的信息，请参考 CMVP（加密模块验证体系）网页上提供的《ACOS5-64 FIPS 140-2 第 3 级安全策略》：
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

1.2. 修改历史

日期	说明
March 2006	ACOS5-32 revision 1.00 • Initial version with 32KB EEPROM • Compliant to ISO 7816 Part 1, 2, 3, 4, 8 and 9 • DES/3DES, RSA up to 2048-bit • Mutual Authentication with Session Key Generation • Multi-level Secured Access Hierarchy
September 2009	ACOS5-64 revision 2.00 • New product hardware with 64KB EEPROM • DES/3DES/3K3DES/AES-128/AES-192/AES-256/RSA (up to 4,096 bits) support • Electronic Purse commands • Anti-tearing Function Support • Operations Modes: o ACOS5-64 v2.00 mode (Default) o ACOS5-32 mode
October 2015	ACOS5-64F revision 3.00 • FIPS140-2 Level 3–certified o Secure Key/PIN entry o RSA Key Generation, Signature 2048 and 3072 o 3DES o Key data Zeroization o FIPS approved Deterministic Random Number Generation • Operations Modes: o ACOS5-64 FIPS 140-2 (Default) o ACOS5-64 v2.00 mode o ACOS5-64 NSH-1 mode

表1 ：修改历史

2.0. 技术规格

以下是 ACOS5-64 加密智能卡的技术参数：

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：< 20 mA
- ESD 保护：≤ 5 KV

2.2. EEPROM

- 容量：64 KB
- EEPROM 耐久性：50 万次擦写
- 数据存储记忆：10 年

2.3. 环境温度

- 工作温度：-25 °C – 85 °C
- 存储温度：-65 °C – 150 °C

2.4. 加密功能

ACOS5-64 加密智能卡具有多种加密功能，其中包括：

- 在 ECB 和 CBC 模式下采用 64/128/192 位密钥对数据进行 DES、3DES 和 3K3DES 加密。AES 还支持采用 128/192/256 位密钥。
- RSA 密钥对的智能卡内安全生成，采用 512 位至 4096 位长的密钥，步长为 256 位
- RSA 签名运算和验证，采用 512 位至 4096 位长的密钥，步长为 256 位
- 可设置为“永不”读取私钥和密钥文件
- 采用 3DES 进行相互认证（终端对卡和卡对终端），生成过程密钥用于加密和 MAC
- SHA-1 和 SHA-256 消息混编函数
- 安全报文机制保证数据传输的机密性和安全性
- 通过符合 ISO 7816 的安全属性（标准）来设置文件访问条件，访问文件前必须满足相应的安全条件（如：提交 PIN）。
- 通过符合 ISO 7816 的安全属性（扩展）来设置各个专用文件（DF）的命令执行条件。执行命令前必须满足相应的安全条件（如：提交 PIN）。
- 确定性随机数生成

2.5. 复位应答（ATR）

硬件复位（如上电）后，卡片会按照 ISO7816 第 3 部分的规定传送复位应答（ATR）。ACOS5-64 支持正向约定的 T=0 协议。关于 ATR 选项的详细描述请参看 ISO 7816 第 3 部分的规定。用户可以通过 ATR 文件完全改变 ATR。

3.0. 卡片文件系统（用户文件、结构和应用）

ACOS5-64 采用动态的文件系统，通过对内存“磨损”进行妥善的管理来延长卡片使用寿命。卡片操作系统可以组织、管理和执行卡片的各项功能。

ACOS5-64 文件系统的基本面构成如下：

- 卡片生命周期
- 卡片头模块
- ACOS5-64 卡片的文件层次结构
- 文件类型
- 文件头数据
- 文件生命周期
- 预定义的文件标识符
- 文件系统限定
- 防拔插和前滚机制

3.1. 卡片生命周期

ACOS5-64 卡在其生命周期中具有以下状态：

0. 生产商状态
1. 传输状态
2. 发行商状态
3. 传输状态
4. 个人化状态
5. 用户状态

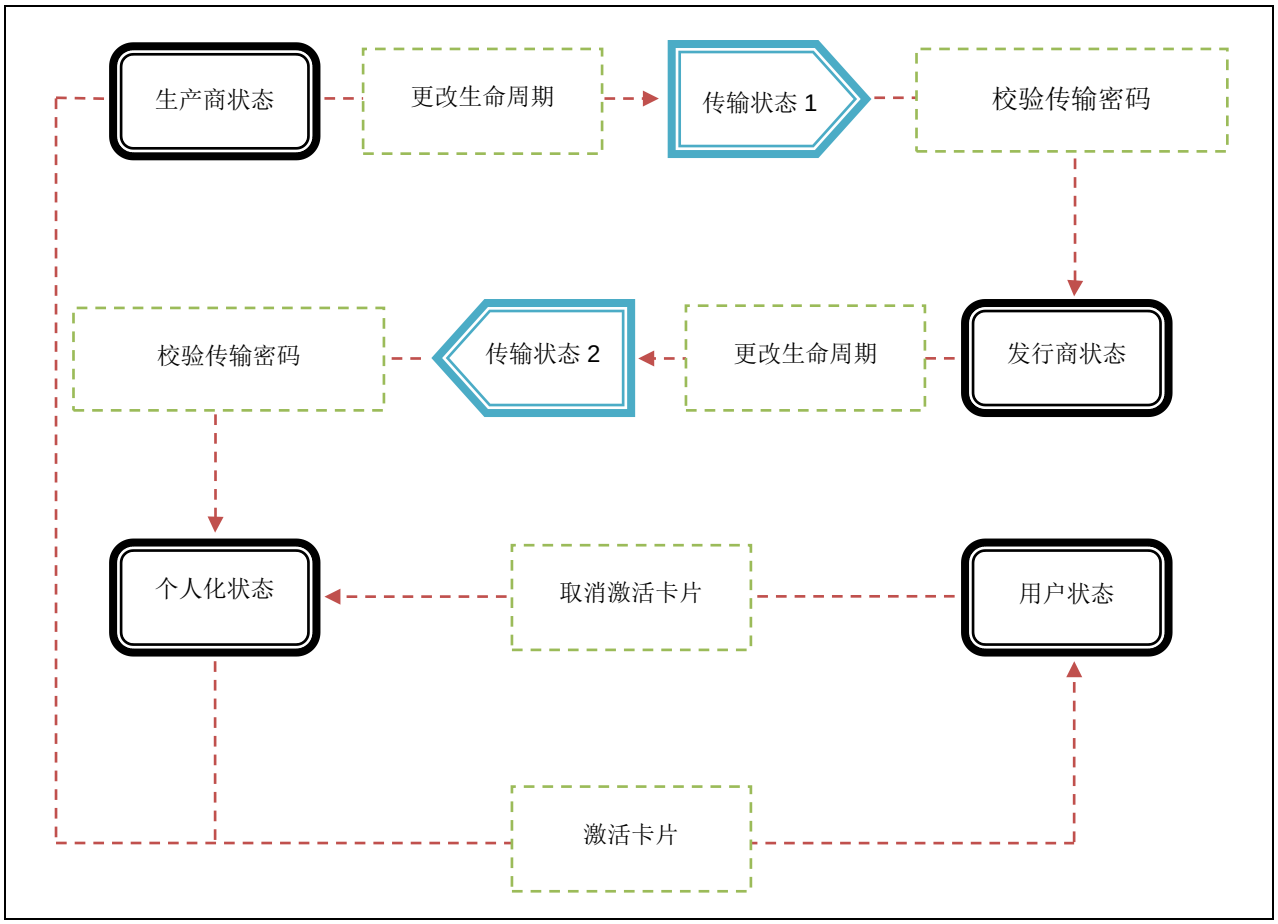

图1 ：卡片生命周期状态

3.1.1. 生产商状态

生产商状态是卡的初始状态。在此状态中，ACS 工厂或应用程序开发人员可以自由访问卡片头模块。使用 READ BINARY 命令或 UPDATE BINARY 命令可以通过地址对卡片头模块进行引用。

注：*在下列情况下 ACOS5-64 会一直保持在此状态：(1)尚未从此状态激活，且(2)卡片应用周期尚未更改为发行商状态。*

在此阶段可以执行所有的命令。一旦应用周期发生更改，ACOS5-64 即不可以返回此状态。

3.1.2. 传输状态 1

卡片在传输过程中应当启用传输状态。在此状态中唯一能够使用的命令是 VERIFY TRANSPORT CODE 命令。成功提交传输密钥后，卡片的状态就会被更改为接下来的应用状态。

3.1.3. 发行商状态

在发行商状态下的卡片处于设置阶段。此时可以调用的命令数量有限，其中包括了 READ BINARY、UPDATE BINARY 和 CHANGE LIFE CYCLE 命令。UPDATE BINARY 命令可以用于修改传输密码来确保卡片在从发卡商到发卡商的客户的传输过程中受到保护。

3.1.4. 传输状态 2

卡片在传输过程中应当启用第二种传输状态。与前面介绍的传输状态类似，在此状态中唯一能够使用的命令是 VERIFY TRANSPORT CODE 命令。

3.1.5. 个人化状态

在发行商状态成功提交传输密码后，卡片即会进入此阶段。此时用户不能像在之前的状态中那样可以直接访问卡片的头模块，但可以像在操作模式下一样在卡片中创建文件并进行测试。在此状态中可以个人化卡片使其成为特定的用户卡，例如加载姓名等。另外还允许使用 ZEROIZE CARD USER DATA 命令（除非设置了 ZEROIZE CARD USER DATA 禁用标志）。

注：*在用户状态或个人化状态下不允许加载定制的命令，卡片也不能返回到生产商状态或发行商状态。在个人化状态和用户状态不允许删除自定义命令。*

3.1.6. 用户状态

卡片被激活后会立即进入此状态，之后将不能再调用 **ZEROIZE CARD USER DATA** 命令。发送 DEACTIVATE CARD 命令会取消激活卡片，并使卡片返回个人化状态。

3.2. 卡片头模块

卡片头模块是一个特殊的内存区域，可以通过卡片操作系统对其访问来进行操作。

3.2.1. ATR 的 TA1

卡片头模块中的 TA1 字节允许对 ATR 的 TA1 值进行设置，这样智能卡读写器和 ACOS5-64 之间就可以进行协商并使用更快的波特率进行通信。虽然此命令可以接受从 11h 到 C8h 的任意 TA1 值，用户还是应当使用一些已经确定了的 TA1 值。

3.2.2. 卡片应用周期字节

卡片应用周期字节由卡片操作系统（COS）进行控制。使用卡片管理命令时此字节会发生改变，用户无需对其进行设置。虽然该字节不应被写入，但可以被读取来确定卡片的生命周期状态。

3.2.3. 操作模式字节

此字节用于选择 ACOS5 v3.00 的 COS 的操作模式。选择不同模式时有几个方面会发生变化，将在后续章节中进行解释。

3.2.3.1. 符合 FIPS 140-2 的模式

此操作模式符合《ACOS5-64 FIPS 140-2 第 3 级安全策略》的要求。

请参考：http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

- 默认操作模式
- 将 COS 设为“批准的操作模式”（自 FIPS 140-2 第 3 级开始）
- 禁止使用和创建不满足 112 位安全强度的秘钥
- 禁止使用不满足 112 位安全强度的散列函数

功能	长度（位）
3DES	168
AES	128/192/256
RSA 秘钥生成	2048/3072
RSA 签名生成	2048/3072
RSA 签名验证	2048/3072/4096
SHA-256	256

表2 ： 允许的功能

- 应当使用符合 NIST 特殊出版物 800-90 的基于 SHA-256 的确定性随机比特生成器，而不是内部自带的真随机数生成器。

3.2.3.2. 64K 模式

ACS 还为客户提供了将 COS 操作设为完全向后兼容 ACOS5-64 的以前版本的选项。

- 完全向后兼容 ACOS5-64 v2.00
- 可访问全部 64 KB 用户存储空间
- 不符合 FIPS 140-2 标准

- 可以使用卡片中的所有算法和函数

3.2.3.3. 符合 NSH-1 的模式

ACOS5-64 还经过 NSH-1（ICP 巴西）测试。ACS 为客户提供了使用这种操作模式的选项。

- 将 COS 设置为 NSH-1 批准的操作模式
- 应当使用符合 NIST 特殊出版物 800-90A 的基于 SHA-256 的确定性随机比特生成器，而不是内部自带的真随机数生成器。

3.2.4. Zeroize Card User Data/Deactivate Card 命令禁用标志

Zeroize Card User Data/Deactivate Card 命令禁用标志字节用于指定卡片可否通过 DEACTIVATE CARD 命令从用户状态返回到个人化状态，以及卡片可否调用 ZEROIZE CARD USER DATA 命令。

3.2.5. 传输密码

传输密码是一个 8 字节长的值，里面存储了在卡片生命周期的两个传输状态会用到的传输密码。

3.2.6. 生命周期补足字节

生命周期补足字节是生命周期字节的补值，在内部自行设置。如果补值不正确，会使卡片变得没有响应。用户应小心不要向此字节或生命周期字节进行写入操作。

3.2.7. EEPROM 密钥错误计数器

若错误计数器的值为 FFh，则可以无限次重试输入。

每次验证失败，剩余的计数值会减 1。如果传输密码验证正确，错误计数器的值将变为 FFh，同时生命周期字节的值会加 1。

3.3. 文件系统

3.3.1. 文件层次

ACOS5-64 的文件系统和结构符合 ISO 7816 第 4 部分的规定。该文件系统非常类似于现代的计算机操作系统。文件系统的根目录是**主控文件（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 都可以在各自的**基本文件（EF）**中存储数据，如下图所示

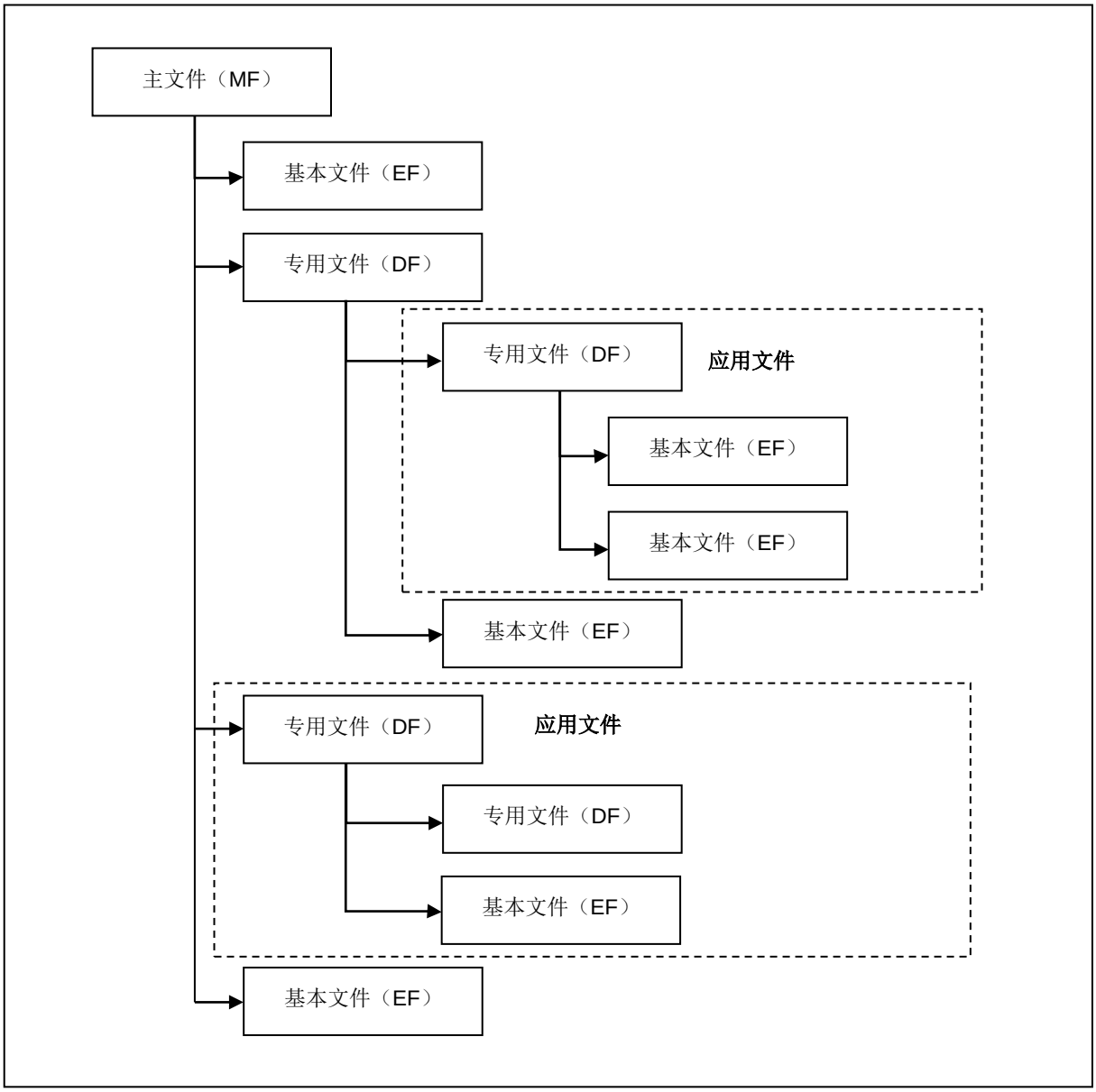

图2 ： 文件系统层次

3.3.2. 文件类型

3.3.2.1. 主控文件

主控文件（MF）是一个特殊的文件。它作为卡片的根文件或顶层目录文件，包含了多个目录文件（DF）和基本文件（EF）。MF 本身也是一个 DF，它的专用文件标识符是 3F 00h。卡片上电或重启后，默认选择了 MF。ACOS5-64 在出货时可以带，也可以不带主控文件。

注：*如果卡内不存在 MF，则用户要负责创建 MF 并设定相应的安全条件。*

3.3.2.2. 专用/目录文件

专用/目录文件（DF）是一个目录，通常用于对卡片进行细分来支持特定的应用程序和/或文件组，及/或存储数据对象。其下可以建立其他 DF 及/或 EF 文件。这些文件直接存储在 DF 下。

3.3.2.3. 基本文件

基本文件（EF）是用于存储数据的文件，其下不能再建立任何其它文件。EF 可以定义为下列两种类型：

- 内部 EF——由卡所解析的数据文件，即，为了管理和控制目的而由卡所使用的数据文件。
- 工作的 EF——不由卡所解析的数据文件，即，由用户所使用的数据，例如姓名、日期等个性化信息。

ACOS5-64 支持 4 种类型的 EF 结构：透明、线性定长、线性变长和循环。

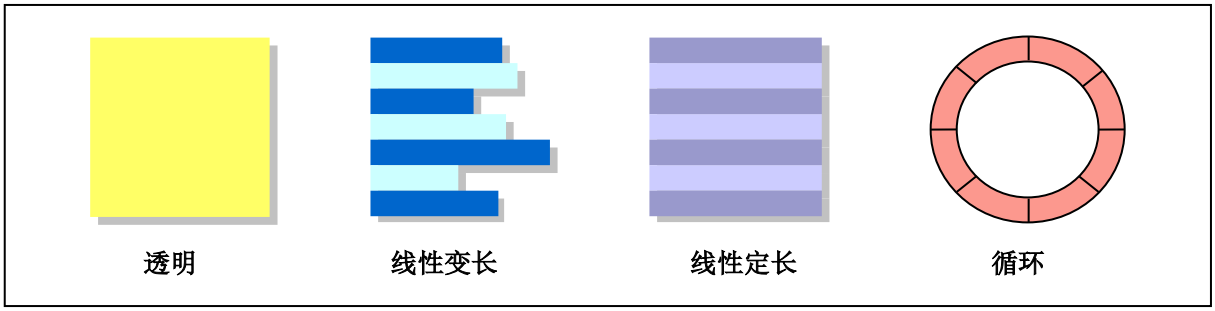

图3 ：ISO 7816-4 定义的 EF 的结构

3.3.2.3.1. 透明 EF

透明结构的 EF 可看作一序列数据单元。其内部的数据可以通过正确的文件偏移量（在 READ BINARY 和 UPDATE BINARY 命令中）来访问。由于透明结构的 EF 根本就没有内部结构，所以要通过偏移来确定卡片操作系统访问文件内容的位置。它们可以用于存储长度超过 255 个字节的数据单元，例如数字证书和公共/私密 RSA 密钥。

3.3.2.3.2. 线性定长 EF

线性定长结构的 EF 可看做一序列具有固定相同长度的记录。其中的记录可以通过记录编号（在 READ RECORD 和 UPDATE RECORD 命令中）来访问。在此类 EF 中记录的最大长度是 255 个字节。由于记录的长度可以设为 1-255 个字节中的任意值，因此在此类 EF 中最多可以存在 255 个记录。不过，要设定正确的记录长度和数量还需要估计到卡片中可用内存的大小。

3.3.2.3.3. 线性变长 EF

线性变长结构的 EF 可看做一序列具有有可变长度的记录。其中的记录可以通过记录编号（在 READ RECORD 和 UPDATE RECORD 命令中）来访问。在此类 EF 中记录的最大长度是 255 个字节。一个 EF 中最多可以存在 255 个记录。不过，与线性定长结构的 EF 类似，要设定正确的记录长度和数量还需要估计到卡片中可用内存的大小。

3.3.2.3.4. 循环 EF

循环结构的 EF 与线性定长结构的 EF 类似，但是记录的组织结构采用环形方式。也就是说如果达到了文件的最后一个记录，则卡片操作系统就会返回第一个记录并将其用作目标记录。此类 EF 可用于记录交易记录。在此类 EF 中，记录的最大长度是 255 个字节。由于记录的长度可以设为 1-255 个字节中的任意值，因此在此类 EF 中最多可以存在 255 个记录。设置记录长度和数量时也要考虑所需的空间，就像线性 EF 一样。

3.3.3. 文件头模块

ACOS5-64 通过文件组织用户的 EEPROM 区。每个文件都有一个文件头模块，即一个描述文件属性的数据块。了解文件头模块的知识将有助于应用程序开发人员创建文件并准确的规划 EEPROM 空间的使用。

3.3.4. 文件生命周期

ACOS5-64 中的文件在其生命周期中具有以下四种状态，下图对此进行了说明：

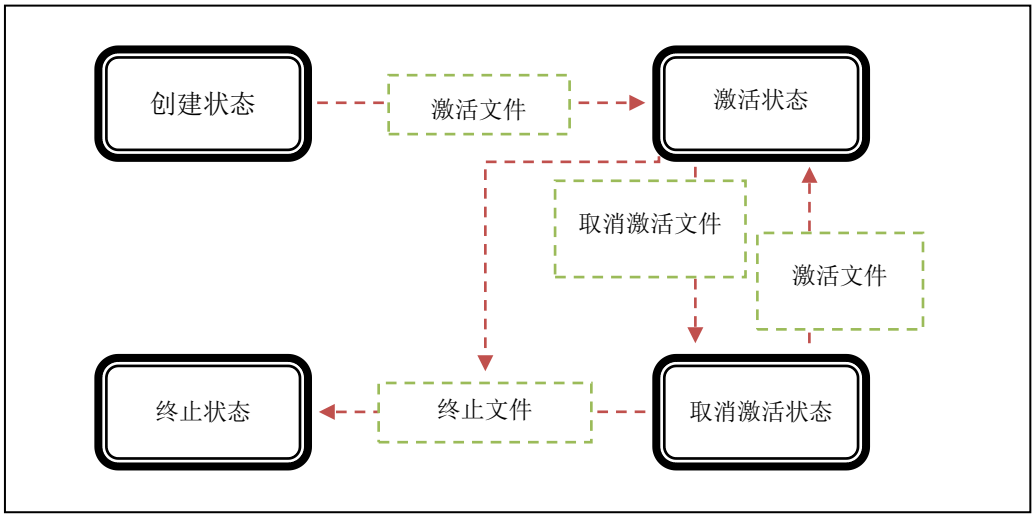

图4 ： 文件生命周期状态

1. 在创建/初始化状态，允许执行对该文件的所有命令。个人化结束后，要使卡片进入操作状态，一定要激活（ACTIVATE）文件。这将使各个文件的安全条件生效。
2. 在激活状态，只有满足该文件的安全条件，对该文件的命令才会有效。
3. 在取消激活状态，不允许对该文件执行大部分的命令，但 SELECT FILE、ACTIVATE FILE、DELETE FILE 和 TERMINATE DF/EF 命令除外。
4. 在终止状态，不允许对该文件执行任何命令。

3.3.5. 预定义的文件标识符

有几个预定义的文件标识符。由于它们对于卡片操作系统来说是隐含已知的，因此不能被其它文件所使用。预定义的 FID 包括：

- 3F 00h – 此 FID 被保留给主控文件。
- 2F 01h – ATR 文件。保留在 MF 下。
- 3F FFh – 此 FID 被保留给当前 DF。选择文件时，文件操作系统会隐式地将此 FID 认作当前 DF，而不管文件的真实 ID 是什么。
- FF FFh – 保留为将来使用，或者 RFU.

注：*文件不可以使用 3F FFh、FF FFh 或 00 00h 作为标识符。在创建文件的过程中，如果文件 ID 采用了这些预定义的标识符，卡片操作系统就会返回一个错误消息。*

3.3.6. 限制条件

ACOS5-64 的限制条件源自有限的可用 RAM 和 EEPROM 空间，因而其安全功能要受到以下限制：

- 只要 EEPROM 有足够的空间，就可以随意添加 DF 子层级，不过卡片操作系统安全条件只能到达文件层次结构的第三子级。若一个 DF 低于第四子级，则此 DF 的局部 PIN、局部 KEY 以及其它的安全条件不会被保存起来。
- DF 名称最长为 16 个字节。

注：*文件的大小在文件创建阶段静态地设置并且不能再被更改。但在其生命周期中，ACOS5-64 允许随时删除文件。*

3.3.7. 防拔插机制

ACOS5-64 采用防拔插机制保护卡片数据，避免由于卡片拔插导致的损坏（如在数据更新时突然从读写器中拔出卡片，或者读写器在卡片数据更新过程中发生机械故障）。下一次复位或上电后，如果检测到损坏发生，ACOS5-64 会立即执行必要的数据恢复。操作系统会在卡片损坏前将毁坏的数据返回至其最初的状态。

3.3.8. 前滚机制

ACOS5-64 采用前滚机制，可以在电源中断或卡片损坏后继续未完成的任务。复位后，ACOS5-64 会对前滚字段进行检查，然后对中断的命令进行必要的继续。

4.0. 卡片内部文件 - 结构和应用

在本节中将介绍 ACOS5-64 的内部文件及其结构和用途。

- 持卡人验证（CHV)文件
- 对称密钥文件
- RSA 私钥和公钥文件
- 安全环境（SE）文件

4.1. 内部文件概览

COS 的运作取决于与安全相关的内部文件的内容。下面是 ACOS5-64 安全系统使用到的内部文件：

内部文件	说明
CHV 文件	内含 PIN 记录，其中包括 PIN 有效位、重置密码有效位、PIN 标识符、剩余尝试次数、PIN 长度、PIN、重置密码计数器、重置密码长度和重置密码。PIN 通常用于持卡人验证。一个 DF 或一个 MF 只应有一个 CHV 文件。
对称密钥文件	内含对称密钥记录，其中包括密钥有效位、密钥标识符、密钥类型、密钥信息、算法标识和密钥。对称密钥通常由对称密钥加密算法（例如 DES、3DES 和 AES）用于外部认证、内部认证和相互认证。一个 DF 或一个 MF 只应有一个对称密钥文件。
RSA 私钥文件	内含一个单个的 RSA 私钥，其中包括密钥类型、密钥长度、对应的公钥的文件 ID 和密钥有效字节。 对于非 CRT 私钥：私钥指数（d） 对于 CRT 私钥：P || Q || dP || dQ || qInv 每个文件内只允许有一个私钥。
RSA 公钥文件	内含一个单个的 RSA 公钥，其中包括密钥类型、密钥长度、对应的私钥的文件 ID、密钥有效字节、公钥指数和公钥系数。每个文件内只允许有一个公钥。
安全环境（SE）文件	内含 SE 模板。一个 DF 或一个 MF 只应使用一个 SE 文件。在 MF/DF 的文件头中应当含有该 DF 或 MF 对应的 SE 文件的标识符。

表3 ：内部文件

4.2. 内部持卡人验证（CHV）文件

CHV 文件是一个内部线性定长 EF。卡片操作系统用它来存储持卡人验证所需的 PIN 记录。基本上，一个 DF 或一个 MF 只应有一个 CHV 文件。如果 CHV 文件位于 DF 下，则认为它存储的是局部 PIN 或者说是只在 DF 内有关的 PIN。但如果位于 MF 下，则文件存储的是全局 PIN 或者说是与整个卡片文件层次结构相关的 PIN。

4.3. 内部对称密钥文件

对称密钥文件是一个内部线性变长 EF。卡片操作系统用它来存储加密应用所需的对称密钥记录。对称密钥由对称密钥加密算法（例如 DES、3DES 和 AES）用于进行加密操作。基本上，一个 DF 或一个 MF 只应有一个对称密钥文件。如果对称密钥文件位于 DF 下，则认为它存储的是局部 KEY 或者说是只在 DF 内有关的 KEY。但如果位于 MF 下，则文件存储的是全局 KEY 或者说是与整个卡片文件层次结构相关的 KEY。

4.4. 内部 RSA 密钥文件

RSA 密钥文件是一个内部透明文件，FDB 为 09h。该文件包含一个单独的 RSA 密钥，可以是“私钥”或者是“公钥”。只要 EEPROM 空间允许，MF/DF 下可以有多个 RSA 密钥文件。

4.5. 内部钱包文件

钱包文件是一个内部循环文件。ACOS5-64 钱包文件的记录长度总是 16，记录数量至少为 3。前两条物理记录用于存储钱包的信息，而其它记录则用于存储交易记录（LOG）。

4.6. 内部安全环境文件

安全环境（SE）文件是一个内部线性变长 EF。它以 SE 模板的形式存储安全环境。每个 DF 都应有一个专用的 SE 文件，SE 文件的 ID 在父 DF 的头模块中指定。一个 SE 文件最多可以有 15 条可识别的记录。

5.0. 卡片访问权限和安全（环境及应用）

本章对 ACOS5-64 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
- 安全环境
- 控制引用模板
- 相互认证的步骤
- 过程密钥的生成

5.1. 说明

命令由 ACOS5-64 系统根据目标文件（或当前 DF）的安全访问条件进行限制。这些条件都基于当前由系统维护的 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。

5.2. 文件安全属性

每个文件（MF、DF 或 EF）都在文件头中设置了一套安全属性。ACOS5 的安全属性分为两种：标准安全属性（SAC）和扩展安全属性（SAE）

5.3. 安全环境

安全条件被编码于一个安全环境（SE）文件中。每个 DF 都有一个专用的安全环境文件，该文件的标识符在 DF 的头模块中指定。每个 SE 记录的结构如下：

<安全环境 ID 模板> <安全环境 DO 模板>

5.4. 控制引用模板（CRT）

5.4.1. 认证模板（AT）

认证模板（AT）定义了满足此 SE 必须符合的安全条件。该安全条件为 PIN 认证或者 KEY 认证。

5.4.2. 密码校验和模板（CCT）

密码校验和模板（CCT）定义了计算 MAC 要使用的参数，MAC 用在安全报文发送和/或 PSO 中。

5.4.3. 保密模板（CT）

保密模板（CT）定义了进行安全报文发送和/或 PSO 时用于数据加密和解密的参数，同时适用于非对称加密/解密，

5.4.4. 数字签名模板（DST）

数字签名模板（DST）定义了执行与非对称密钥有关的操作时会用到的参数。

5.4.5. 散列模板（HT）

散列模板（HT）定义了执行 PSO-HASH 命令时要用到的参数。

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相互认证的执行。执行 SELECT FILE（选择文件）命令也可以结束一个会话。

5.6. 过程密钥的生成步骤

由于 DES 被认为是不再安全的，我们只支持 3DES 过程密钥。ACOS5-64 在相互认证的步骤完成之后自动生成过程密钥。

过程密钥的长度取决于 Kc/Kt 的长度。为了实现兼容，两个密钥的长度必须相同。

K_S-ENC 负责加密：

- 安全报文
- 带 DO 标签为 84h 的 CT-sym 的 PSO 命令。
- K_S-MAC 负责 MAC：
- 安全报文
- 带 DO 标签为 84h 的 CCT 的 PSO 命令。

5.7. 安全报文发送

安全报文发送（SM）功能确保 ACOS5-64 和终端/服务器之前通信的安全性。ACOS5-64 支持安全报文发送，用于确保真实性和机密性。

ACOS5-64 有两种安全报文（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。

5.8. 密钥注入

密钥注入可以用于将密钥或分散密钥从应用程序或者终端中安全地载入到 ACOS5-64 卡中。

执行密钥注入的过程中，卡片会选择一个文件来接受要注入的密钥。之后调用数据中含有待导入密钥的 PUT KEY 命令。

如需了解更多关于 ACOS5-64 v3.00（通过 FIPS 140-2 第 3 级认证）加密模块功能、防护措施和访问权限的信息，请参考 CMVP（加密模块验证体系）网页上提供的《ACOS5-64 FIPS 140-2 第 3 级安全策略》：
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

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. 联系方式

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。

Adobe 和 Reader 是 Adobe Systems Incorporated 在美国和/或其他国家的注册商标或商标。
Microsoft、Windows、Internet Explorer 和 Outlook 是 Microsoft Corporation 在美国和/或其他国家的注册商标。
Mozilla Firefox 和 Mozilla Thunderbird 是 Mozilla Corporation 的商标或注册商标。