Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-64

加密智能卡

功能规格书 V1.01

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.）研发的 ACS 智能卡操作系统——版本 5.0-64K 字节（ACOS5-64）的特性和功能。

ACOS5-64 是一款先进的加密智能卡。它完全符合 ISO 7816 第 1、2、3、4、8 和 9 部分的规定，专为实现基于公钥的各种应用而设计。此外，它旨在提高 RSA 公钥加密操作的安全性与性能，对于需要智能卡公钥基础设施（PKI）和高级别安全要求的应用非常重要。

ACOS5-64 支持多种安全基础设施和应用，其中包括：

- Crypto-API 和 PKCS #11 中间件
- 智能卡微型驱动
- 智能卡域登录
- 安全的在线证书生成
- Outlook、Windows Mail、Outlook Express、Mozilla Thunderbird Mail 签名和加密(S/MIME)
- 加密文件系统（EFS）
- Mozilla Firefox
- Internet Explorer
- Microsoft VPN/Open VPN
- OpenID
- IIS SSL
- Adobe Acrobat
- Lotus Notes
- Netscape
- SSH

2.0. 符号和缩写

缩略语	描述
3DES	3 倍数据加密标准算法 Triple DES
AES	高级加密标准 Advanced Encryption Standard
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
AT	认证模板 Authentication Template
ATR	复位应答 Answer To Reset
CBC	密码块链接加密模式 Cipher-Block Chaining Mode of Encryption
CCT	密码校验和模板 Cryptographic Checksum Template
CT	保密模板 Confidentiality Template
CLA	ISO 7816 APDU 的类别字节 Class byte of ISO 7816 APDU
CRT	控制引用模板 Control Reference Template
CSP	加密服务提供程序 Cryptographic Service Provider
DES	数据加密标准 Data Encryption Standard
DF	专用/目录文件 Dedicated File
DST	数字签名模板 Digital Signature Template
ECB	电子密码本加密模式 Electronic Code Book Mode of Encryption
EEPROM	电可擦除可编程只读存储器 Electrically Erasable Programmable Read-Only Memory
EF	基本文件 Elementary File
EF1	个人识别码文件 PIN File
EF2	密钥文件 KEY File
FCP	文件控制参数 File Control Parameters
FDB	文件类型字节 File Descriptor Byte
XXh	1 个字节的十六进制表示 Hexadecimal representation of a byte.
HT	哈希模板 Hashing Template
IIS	互联网信息服务 Internet Information Services
INS	ISO 7816 APDU 的指令字节 Instruction byte of ISO 7816 APDU
ISO	国际标准化组织 International Organization for Standardization
Lc	ISO 7816 APDU 命令数据的长度 Length of command data of ISO 7816 APDU
LCSI	应用周期状态字 Life Cycle Status Integer
Le	ISO 7816 APDU 期待的响应数据的长度 Length of expected response data of ISO 7816 APDU

缩略语	描述
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 Master File
MSb	最高有效位 Most Significant Bit
MSB	最高有效字节 Most Significant Byte
P1	ISO 7816 APDU 的参数 1 Parameter 1 of ISO 7816 APDU
P2	ISO 7816 APDU 的参数 2 Parameter 2 of ISO 7816 APDU
P3	ISO 7816 APDU 的参数 3 Parameter 3 (Lc or Le) of ISO 7816 APDU
RFU	保留为将来使用 Reserved for Future Use
ROM	只读存储器 Read-Only Memory
RSA	Rivest、Sharmir 和 Adleman 提出的一种公钥加密算法 Public key cryptography by Rivest, Shamir and Adleman
SAC	标准安全属性 Security Attribute – Compact
SAE	扩展安全属性 Security Attribute – Expanded
SCB	安全条件字节 Security Condition Byte
SCDO	安全条件数据对象 Security Condition Data Object
SE	安全环境 Security Environment
SFI	短文件标识符 Short File Identifier
SHA	安全哈希算法 Secure Hash Algorithm
SM	安全报文 Secure Messaging
SW1SW2	由卡片返回的 ISO 7816 状态字 ISO 7816 return Status Word from the card
TLV	标签-长度-值 Tag-Length-Value
UQB	应用限定字节 Usage Qualifier Byte
Var.	变长 Variable Length
||	连接 Concatenation

表1：符号和缩写

2.1. 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、9 部分的规定
- 可转换的高速通讯波特率（9,600 - 223,200 bps）
- 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
- 具有相互认证功能，能够生成过程密钥
- 可生成 RSA 密钥，高达 4096 位
- 支持 AES-128/192/256
- 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）
- 符合 FIPS 140-2 标准
- 多层次的安全访问等级
- 支持防拔插功能
- 支持向后兼容模式，卡片可用作 ACOS5-32 卡

2.2. 技术规格

以下是 ACOS5-64 加密智能卡的技术参数：

2.2.1. 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：< 20 mA
- ESD 保护：≤ 5000 V

2.2.2. EEPROM

- 容量：64 KB（65,536 字节）
- EEPROM 耐久性：50 万次擦写
- 数据存储记忆：10 年

2.2.3. 环境温度

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

2.3. 复位应答（ATR）

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）。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。

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 和 3DES 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
- RSA 卡可验证的（CV）证书，采用使用 512 位、768 位或 1024 位长密钥签名的证书
- 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）。
- 符合 FIPS 140-2 的随机数产生器（基于硬件）

3.0. 卡片文件系统（用户文件、结构和应用）

ACOS5-64 具有一个动态的文件系统，通过对内存“磨损”进行妥善的管理来延长卡片的使用寿命。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. 卡片头模块

卡片头模块是一个特殊的内存区域，由卡片操作系统对其访问来进行操作。

3.2. 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. 多层次的文件系统

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，如图 1 所示：

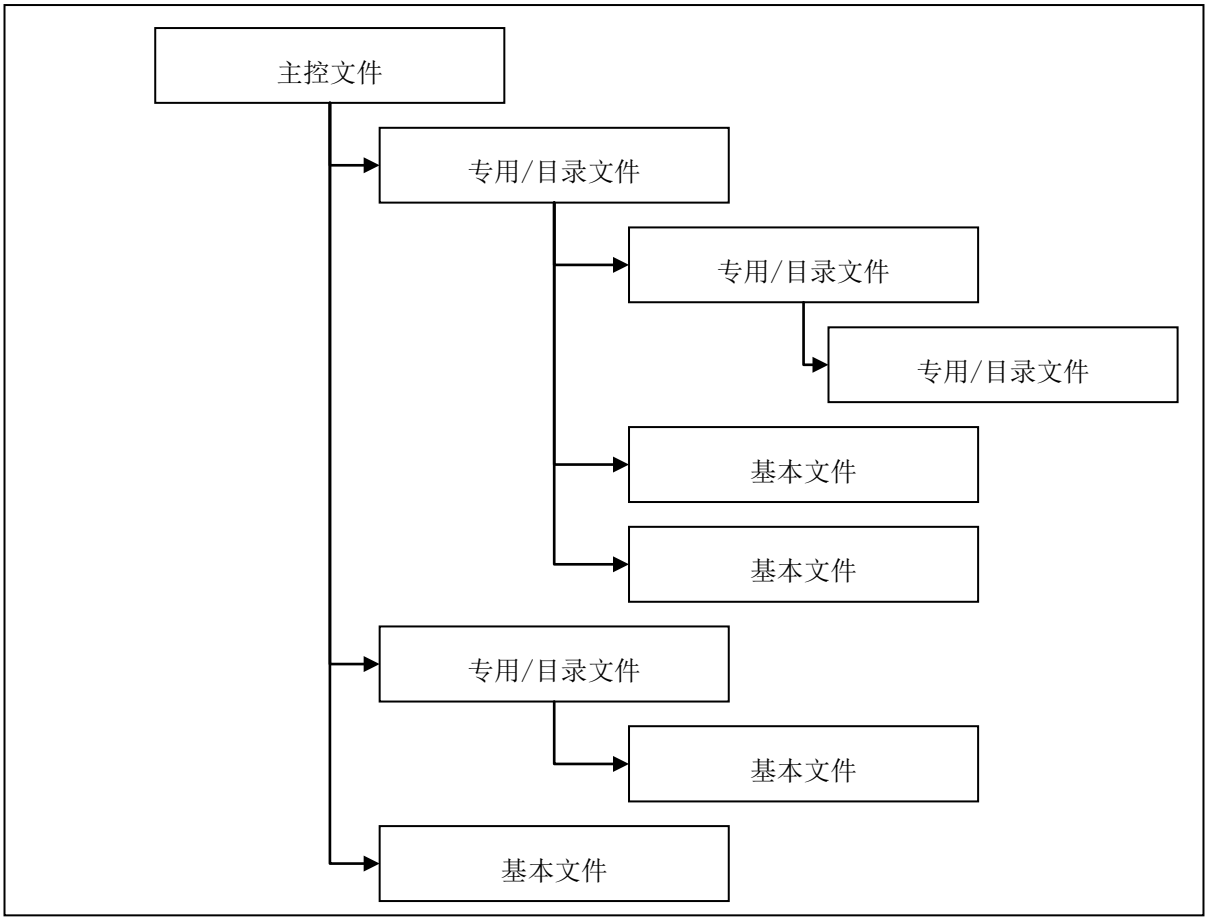

图1：按 ISO 7816-4 设计的文件系统层次结构

3.4. 文件生命周期

ACOS5-64 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：

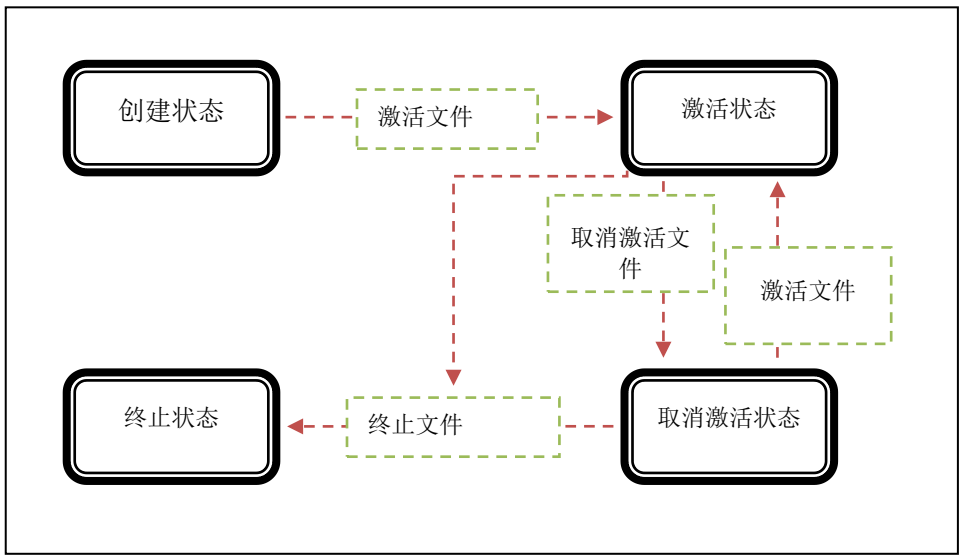

图2：文件生命周期状态

- 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。
- 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。
- 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。
- 在终止状态，不允许对该文件执行任何命令。

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。

3.6. 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。

3.7. 前滚机制

ACOS5-64 采用的一种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。

3.8. 卡片生命周期

ACOS5-64 卡在其生命周期中具有以下的状态：

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

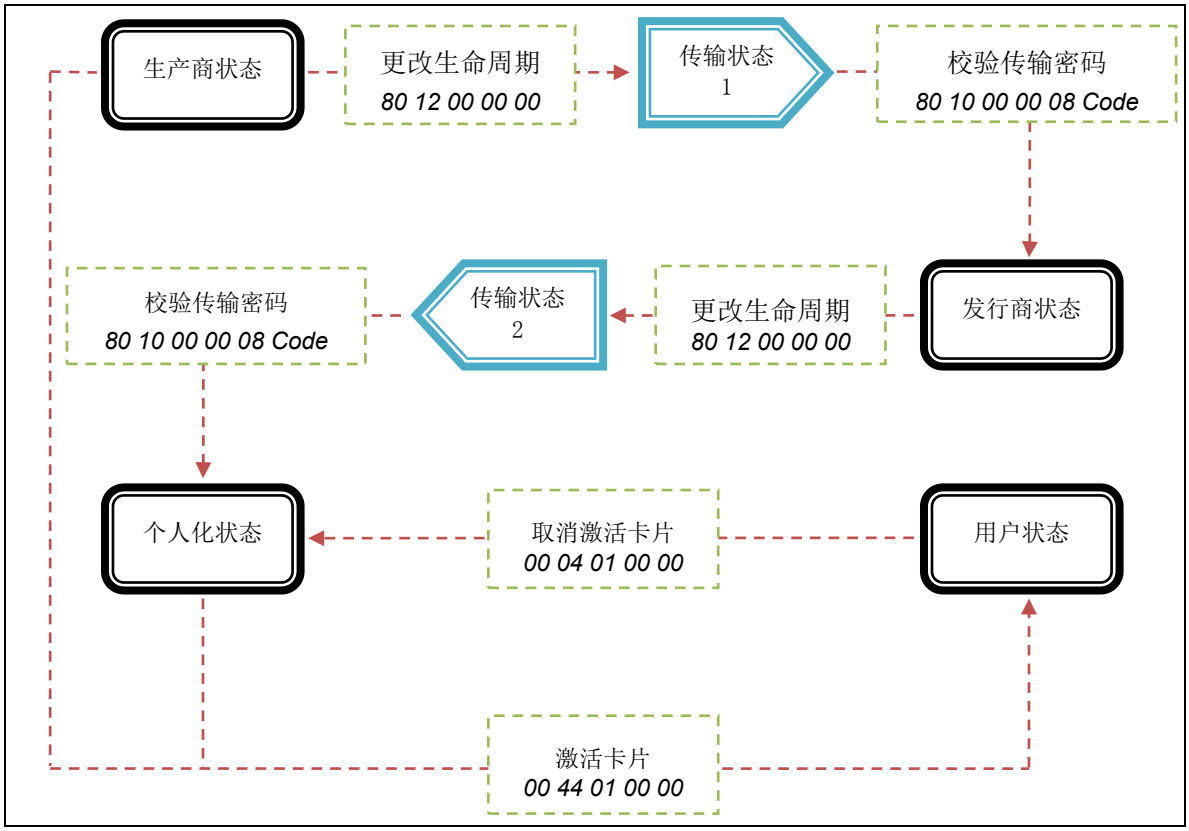

图3：卡片生命周期状态

3.8.1. 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：在此状态中，ACS 可以为客户添加定制命令。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。

3.8.2. 传输状态

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。

3.8.3. 个人化状态

在发行商状态成功提交传输密码后，用户即会进入此阶段。此时用户不能像在以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，在卡片中创建和测试文件。在此状态可以个人化卡片，使其成为特定的用户卡片，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，详见 3.2.4 节）。

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。

3.8.4. 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。

4.0. 卡片内部文件（结构和应用）

接下来将介绍 ACOS5-64 的内部文件及其结构和用途。

- 持卡人验证文件
- 对称密钥文件
- RSA 私钥和公钥文件
- 钱包文件
- 安全环境文件

4.1. 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。

4.2. 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。

4.3. 内部 RSA 密钥文件

RSA 密钥文件是一个内部透明文件，FDB 为 09h。该文件包含了一个单独的 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。

4.4. 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，而其它记录用于存储交易记录（日志）。

4.5. 内部安全环境文件

安全环境（SE）文件是一个内部线性变长的 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，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

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 EF（EF1）中。同样，局部 KEY 直接存储在当前选定的 DF 的 KEY 文件（EF2）中。最多可以有 31 个全局 PIN、31 个局部 PIN、31 个全局 KEY 和 31 个局部 KEY。

5.1. 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。ACOS5-64 安全属性分为两种：标准安全属性（SAC）和扩展安全属性（SAE）。

5.2. 安全环境

安全条件被编码于一个安全环境文件中。每个 DF 都有一个专用的安全环境（SE）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：

<SE ID 模板> <SE DO 模板>

5.3. 控制引用模板

5.3.1. 认证模板

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 KEY 认证。

5.3.2. 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。

5.3.3. 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。

5.3.4. 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操作时会用到的参数。

5.3.5. 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。

5.4. 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。

5.5. 安全报文

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。

安全报文（SM）有两种模式，可以分别用于两种不同的安全级别。第一种模式是确保真实性的安全报文（SM-sign），另一种是确保机密性的安全报文（SM-enc）。这两种模式均可应用于命令和响应数据。

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。