Advanced Card Systems Ltd.
Card & Reader Technologies

# ACOS5-EVO


Functional Specifications v1.01



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

# Table of Contents

# List of Figures



# List of Tables

# 1.0. About ACOS5-EVO

The ACOS5-EVO is the latest addition to the ACOS5 Series, a series of cryptographic smart card module from ACS specially designed for Public Key-based applications.

The ACOS5-EVO is fully compliant with ISO 7816 parts 1, 2, 3, 4, 8, 9 and ISO 14443 parts 1-4. It offers advanced cryptographic algorithms such as RSA and ECC and is also compliant with international standards for PKI smart cards such as FIPS 140-2 (US Federal Information Processing Standards) Level 3 and CC EAL 5+ (chip level).

## 1.1. Target Audience

This document is intended for software developers and technical specialists for cryptographic smart card applications. The user is expected to have knowledge in public key infrastructure and other cryptography concepts and standards.

## 1.2. History of Modification for ACOS5 Series

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

| Date | Changes |
|---|---|
| November 2018 | ACOS5-EVO revision 4.00<br>• 192KB memory<br>• Supports T=0 and T=1 (Default)<br>• Extended APDU support<br>• FIPS140-2 Level 3 compliant<br>• Cryptographic Algorithms<br>  ○ ECC up to 521 bits<br>  ○ RSA up to 4096 bits<br>  ○ 3DES, AES<br>  ○ SHA-1, SHA-256, SHA-512<br>• Operation Modes:<br>  ○ Default Configuration<br>  ○ FIPS Mode |
| April 2019 | ACOS5-EVO revision 4.10<br>• 192KB memory<br>• Contact Smart Card Interface<br>  ○ Supports T=0 and T=1 (Default)<br>• Contactless Smart Card Interface<br>  ○ ISO 14443 Type A<br>• Extended APDU support<br>• FIPS140-2 Level 3 compliant<br>• Cryptographic Algorithms<br>  ○ ECC up to 521 bits<br>  ○ RSA up to 4096 bits<br>  ○ 3DES, AES<br>  ○ SHA-1, SHA-256, SHA-512<br>• Operations Modes:<br>  ○ Default Configuration<br>  ○ FIPS Mode |

**Table 1**: History of Modification for ACOS5 Series

## 1.3. Symbols and Abbreviations

| Abbreviations | Description |
|---|---|
| 3KDES | 3-Key Triple DES |
| 3DES | Triple DES |
| AES | Advanced Encryption Standard |
| AMB | Access Mode Byte |
| AMDO | Access Mode Data Object |
| APDU | Application Protocol Data Unit |
| AT | Authentication Template |
| ATR | Answer to Reset |

| Abbreviations | Description |
|---|---|
| ATS | Answer to Select |
| CBC | Cipher-Block Chaining Mode of Encryption |
| CCT | Cryptographic Checksum Template |
| CT | Confidentiality Template |
| CLA | Class byte of ISO 7816 APDU |
| CMAC | Cipher-based Message Authentication Code |
| CRT | Control Reference Template |
| CSP | Cryptographic Service Provider |
| DES | Data Encryption Standard |
| DF | Dedicated File |
| DST | Digital Signature Template |
| ECB | Electronic Code Book Mode of Encryption |
| ECC | Elliptical Curve Cryptography |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECIES | Elliptic Curve Integrated Encryption Scheme |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EF | Elementary File |
| EF1 | PIN File |
| EF2 | KEY File |
| FCP | File Control Parameters |
| FDB | File Descriptor Byte |
| XXh | Hexadecimal representation of a byte. |
| HT | Hashing Template |
| IIS | Internet Information Services |
| INS | Instruction byte of ISO 7816 APDU |
| ISO | International Organization for Standardization |
| Lc | Length of command data of ISO 7816 APDU |
| LCSI | Life Cycle Status Integer |
| Le | Length of expected response data of ISO 7816 APDU |
| LSb | Least Significant Bit |
| LSB | Least Significant Byte |
| MAC | Message Authentication Code |
| MF | Master File |
| MSb | Most Significant Bit |
| MSB | Most Significant Byte |
| P1 | Parameter 1 of ISO 7816 APDU |
| P2 | Parameter 2 of ISO 7816 APDU |

| Abbreviations | Description |
|---|---|
| P3 | Parameter 3 (Lc or Le) of ISO 7816 APDU |
| RFU | Reserved for Future Use |
| ROM | Read-Only Memory |
| RSA | Public key cryptographic algorithm by Rivest, Shamir and Adleman |
| SAC | Security Attribute – Compact |
| SAE | Security Attribute – Expanded |
| SCB | Security Condition Byte |
| SCDO | Security Condition Data Object |
| SE | Security Environment |
| SFI | Short File Identifier |
| SHA | Secure Hash Algorithm |
| SM | Secure Messaging |
| SW1 SW2 | ISO 7816 Return Status Word from the card |
| TLV | Tag-Length-Value |
| UQB | Usage Qualifier Byte |
| Var. | Variable Length |
| \|\| | Concatenation of bytes |

**Table 2**: Symbols and Abbreviations

# 2.0. Technical Specifications

## 2.1. Electrical

- Operating Voltage: 5 VDC +/-10% (Class A) and 3 VDC +/-10% (Class B)
- Maximum Supply Current: < 20 mA
- ESD Protection: ≤ 5 KV

## 2.2. Environmental

- Operating Temperature: -25 °C to 85 °C
- Storage Temperature: -65 °C to 150 °C

## 2.3. Communication Protocols

- T=0, T=1 with baud up to 446,400 bps
- T=CL protocol with baud up to 424 kbps

## 2.4. Memory

- Capacity: 192Kb
- 500,000 Erase/Write cycle endurance
- 30-year Data retention

## 2.5. Cryptographic Capabilities

ACOS5-EVO supports a number of cryptographic algorithms, including:

- DES/3DES: 56/112/168-bits (ECB, CBC)
- AES: 128/192/256-bits (ECB, CBC)
- RSA: 512 – 4096 bits in 256 bits increments
- ECC: Curves P-224/P-256/P-384/P-521
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- MAC: CBC-MAC (DES/3DES, AES), CMAC (3DES, AES)

## 2.6. Random Number Generation

- Deterministic RNG according to FIPS 140-2
- Non-deterministic RNG compliant to AIS-31

## 2.7. File Security

- Private and secret key file read access can be set to “Never”.
- File access condition capability with ISO 7816–compliant Secure Attribute-Compact. File access is only allowed if the proper security conditions are met (e.g. PIN submissions).
- Command execution condition capability per Dedicated File (DF) with ISO 7816–compliant Secure Attribute-Extended. Commands are allowed only if the proper security conditions are met (e.g. PIN submission).
- Secure Messaging function for confidential and authenticated data transfers
- Mutual authentication (terminal-to-card and card-to-terminal) with session key generation for encryption and MAC

## 2.8. Answer to Reset (ATR)

After hardware reset (e.g. power up), the card transmits an Answer to Reset (ATR) in compliance with ISO 7816-3. For full descriptions of ATR options, see ISO 7816 Part 3. ACOS5-EVO supports the contact protocol type T=0 and T=1 with direct convention.

The following is the default ATR:

| Parameter | ATR | Description |
|---|---|---|
| TS | 3Bh | Direct convention, the least significant bit is sent first |
| T0 | 9Eh | Presence of TA1 and TD1 and 14 historical characters |
| TA1 | 96h | Clock frequency 223 200 bps |
| TD1 | 80h | Transmission protocol T=0, presence of TD2 |
| TD2 | 01h | Transmission protocol T=1 |
| 14 historical characters | | |

**Table 3**: Configuration of the Answer-to-Reset

The ATR value may be completely changed using the ATR file.

## 2.9. Answer to Select (ATS)

After receiving a Request for Answer to Select (RATS) from the card reader, the card transmits an Answer to Select (ATS) in compliance with ISO 14443 Part 4.

The following table shows the default ATS:

| Parameter | ATS | Description |
|---|---|---|
| TL | 13h | Length |
| T0 | 78h | Format byte …codes Y(1) and FSCI |
| TA1 | 33h | Interface byte…codes DS and DR |
| TB1 | 81h | Codes FWI and SFGI |
| TC1 | 02h | Codes protocol options |
| 14 historical characters | | |

**Table 4**: Configuration of Answer-to-Select

The historical bytes of the ATS may be changed using the ATR file.

## 2.10. Compliance to Standards

- Compliance with ISO 7816 Parts 1, 2, 3, 4, 8, and 9
- Compliance with ISO 14443 and fully compatible with ISO 14443 Type A
- Compliance with FIPS 140-2 Level 3
- Certified with Common Criteria EAL 5+ (Chip Level)

# 3.0. Card File System – User Files, Structures and Usage

The ACOS5-EVO has a dynamic file system wherein memory wear and tear is properly managed to prolong its life span. The card operating system organizes, manages and administers the function of the card.

The fundamentals of the ACOS5-EVO File System consist of the following:

- Card Life Cycle
- Card Header Block
- Hierarchy of Files
- File Types
- File Header Data
- File Life Cycle
- Predefined File Identifiers
- Limitations of the File System
- Anti-tearing and Roll-forward Mechanisms

## 3.1. Card Life Cycle

The ACOS5-EVO has the following card stages during its life cycle:

0. Manufacturer stage
1. Transport stage
2. Issuer stage
3. Transport stage
4. Personalization stage
5. User stage

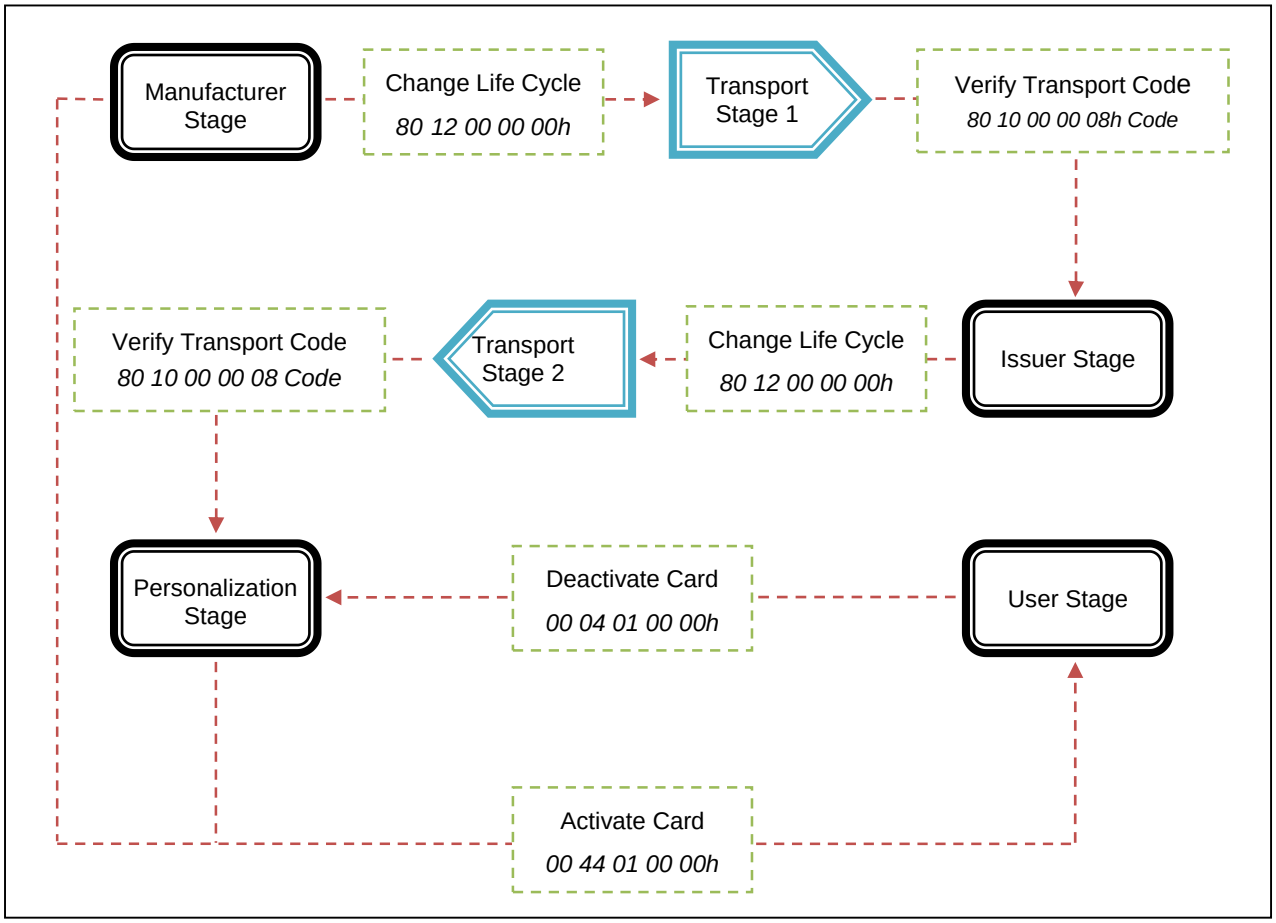


**Figure 1**: Card Life Cycle Stages

### 3.1.1. Manufacturer Stage

This stage is the initial state of the card. ACS factory or the application developer is allowed to freely access the card header block (described in **Card Header Block**). The card header block can be referenced by its address using the READ BINARY or UPDATE BINARY command.

***Note:*** *All commands are allowed in this stage. ACS may add customized commands for the customer at this stage. The ACOS5-EVO remains at this stage as long as: (1) It is not activated from this stage; and (2) the Card Life Cycle has not been changed to the Issuer Stage. The ACOS5-EVO does not allow going back to this stage once the life cycle is changed.*

### 3.1.2. Transport Stage 1

The Transport Stage should be activated when the card is being transported. The only command that may be used is the VERIFY TRANSPORT CODE command. After successfully submitting the transport key, the state of the card will be changed to the next applicable state.

### 3.1.3. Issuer Stage

In Issuer stage, the card is in set up stage. Only a limited number of commands are possible including Read and Update Binary and Change Life Cycle. UPDATE BINARY Command can be used to change the Transport Code to secure the transfer of card stock to the customer of the card issuer.

### 3.1.4. Transport Stage 2

The second Transport Stage should be activated when the card is being transported. Similar to the previous transport stage, the only command that may be used is the VERIFY TRANSPORT CODE command.

### 3.1.5. Personalization Stage

The successful submission of the *transport key* from the Issuer Stage grants access to a user at this stage. ACOS5-EVO users can no longer directly access the card header block as in the previous stage. Users can create and test files created in the card as if in Operational Mode. This stage is used for personalizing the card to a specific user like loading of names, etc. The ZEROIZE CARD USER DATA command is allowed in this stage (unless the Zeroize Card User Data Disable Flag is set - see **Zeroize Card User Data/Deactivate Card Disable Flag**).

***Note:***

1. *Customized commands cannot be loaded at the User or Personalization Stage. The card cannot go back to Manufacturer Stage or Issuer Stage.*
2. *Deleting Custom Commands is not allowed in the Personalization Stage and User Stage.*

### 3.1.6. User Stage

The card goes into this stage once the card is activated. The **Zeroize Card User Data** command is no longer allowed. Sending the *Deactivate Card* command deactivates the card and life cycle stage goes back to the Personalization Stage.

## 3.2. Card Header Block

The card header block is a special memory area accessed by the card operating system for its operation.

### 3.2.1. TA1 of ATR

The TA1 byte in the card header block allows the TA1 value of the ATR to be set so that the smart card reader and the ACOS5-EVO can negotiate and work at a faster communication baud rate. Although this command can accept any TA1 values from 11h to C8h, some well-established TA1 values should be used.

These TA1 values correspond to their respective baud rate when the smart card reader clock frequency is 3.5712 MHz.

### 3.2.2. Configuration Mode Byte

This byte selects the configuration mode of the ACOS5-EVO.

Several things are changed whenever a different mode is selected. The changes are explained in the succeeding sections.

| Operation Mode | Value |
|---|---|
| Default | 01h |
| FIPS 140-2 Level 3 | 00h |

**Table 5**: Configuration Mode Byte

***Note**: A hard reset needs to be performed before the settings of the chosen configuration mode can be used.*

#### 3.2.2.1. Default Mode

This is the default mode of operation for the ACOS5-EVO.

- All algorithms and functions in the card can be used.
- Non-compliant to FIPS 140-2 standard

***Note:** For those who have developed applications using the ACOS5 v3.00, please refer to a separate document, the ACOS5-EVO Backward Compatibility Guide, to help you with the migration.*

#### 3.2.2.2. FIPS 140-2 Level 3–Compliant Mode

This mode of operation is in accordance to the ACOS5-EVO FIPS 140-2 Level 3 Security Policy document.

- Sets the card to an “Approved Mode of operation” as of FIPS 140-2 Level 3.
- Use and creation of keys that do not meet 112 bits of security strength is prohibited
- Use of hash functions that do not meet 112 bits of security strength is prohibited for digital signature operations

| Algorithm | Characteristics |
|---|---|
| | |
| AES | 128/192/256-bit Keys |
| RSA | 2048/3072/4096-bit Keys |
| ECC | P-224/P-256/P-384/P-521 Curves |
| Hash | SHA1/SHA224/SHA256/SHA384/SHA512 |

**Table 6**: FIPS Configuration - Allowed Algorithms

### 3.2.3. Zeroize Card User Data/Deactivate Card Disable Flag

This byte specifies if the card can return from User Stage to Personalization Stage by using the DEACTIVATE CARD command and also if the card can issue the Zeroize card user data command.

This command is important for application developers to be able to clear the card during development.

### 3.2.4. Transport Code

This 8-byte value stores the transport code used in the two transport stages of the card life cycle.

### 3.2.5. Transport Code Error Counter

This byte is split into two parts. The high nibble indicates the allowed number of retries and the low nibble indicates the number of retries left.

## 3.3. File System

### 3.3.1. Hierarchy

The ACOS5-EVO is compliant with ISO 7816-4 file system and structure. The file system is very similar to that of the modern computer operating system. The root directory of the file system is the **Master File (MF)**. Each application or group of data files in the card may be contained in a directory called a **Dedicated File (DF)**. Each DF and MF may store data in their respective **Elementary Files (EF)**, as shown in the figure below.

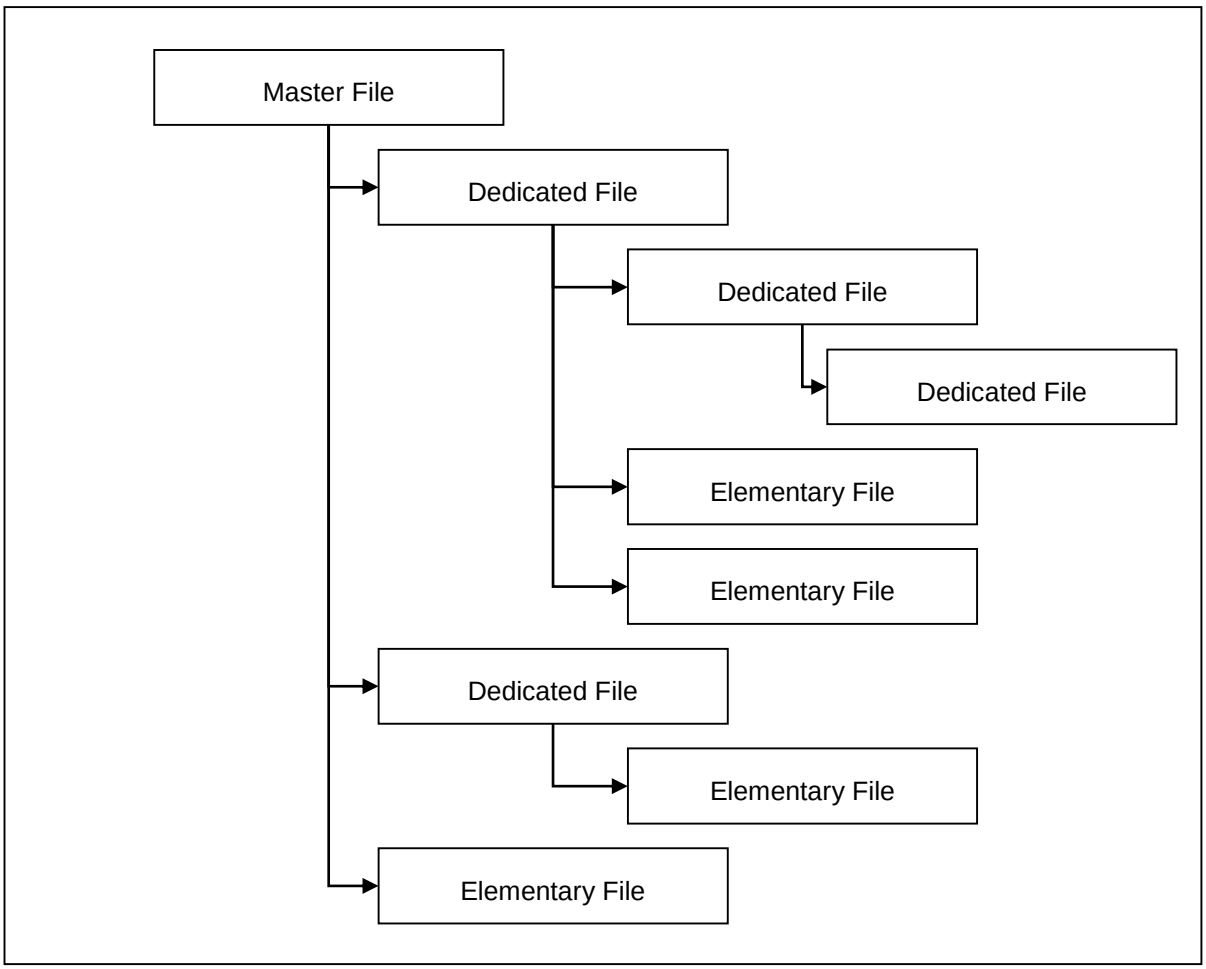


**Figure 2**: File System Hierarchy According to ISO 7816-4

## 3.3.2. File Types

### 3.3.2.1. Master File

The Master File (MF) is a special file that acts as the root or top-level directory file for the card. It contains Dedicated Files (DF) and Elementary Files (EF). An MF is also a DF, which has the reserved file identifier 3F 00h. After the card powers up or resets, the MF is selected by default. ACOS5-EVO could be shipped with or without the Master File.

***Note:*** *In the case where an MF is not present, it is the user's responsibility to create and secure the MF.*

### 3.3.2.2. Dedicated Files

A Dedicated File (DF) is a directory generally used for subdividing the card to host specific applications and/or group of files and/or store data objects. It may be a parent of other DFs and/or EFs. These files are said to be immediately under the DF.

### 3.3.2.3. Elementary Files

Elementary Files (EFs) are files that store data and can never be a parent of any other file. Two categories of EFs are defined:

- Internal EF – data files interpreted by the card, i.e., data used by the card for management and control purposes. There are certain internal files used by ACOS5-EVO for security-related functions such as:
  - Cardholder Verification (CHV) file
  - Symmetric Key File
  - Asymmetric Key File
  - Security Environment File
- Working EF – data files not interpreted by the card, i.e., data used by the user like names, dates and other personalized information

The ACOS5-EVO supports four types of elementary files: transparent, linear-fixed, linear variable, and cyclic.

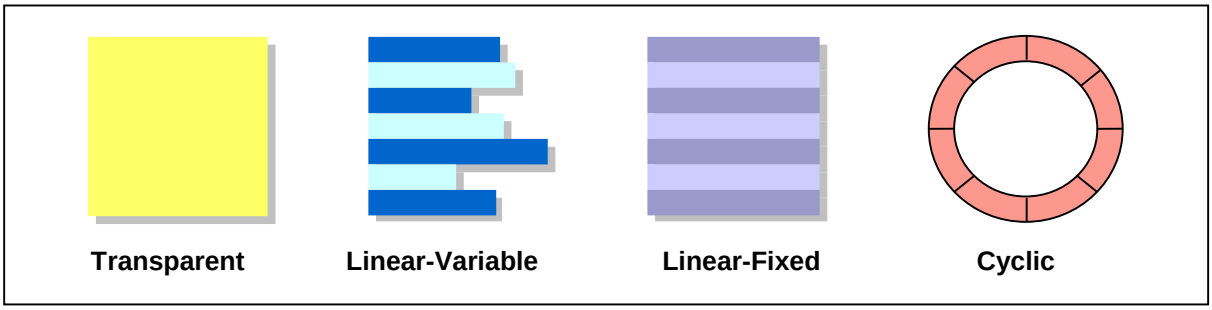


**Figure 3**: Structure of Elementary Files According to ISO 7816-4

#### 3.3.2.3.1. Transparent Elementary Files

Transparent elementary files work as a single continuous sequence of data units. Commands like READ BINARY and UPDATE BINARY are used together with the proper file offset to access the data in this file. There is no internal structure inside the file that is why offsets are used to determine where the card operating system will start accessing the file. The maximum length of this elementary file is 38911 bytes.

#### 3.3.2.3.2. Linear Fixed Elementary Files

This EF is viewed as a single contiguous chain of individual records with fixed and equal length. Commands like READ RECORD and UPDATE RECORD are used together with the proper record number to access the desired record within the file. The maximum record length for this EF is 4096 bytes and the maximum number of records in this EF is 65535 bytes. However, setting the right record

lengths and number of records require some estimation of the available memory that the card has. This EF requires the record size of the command to be equal to the record's actual size.

#### 3.3.2.3.3. Linear Variable Elementary Files

This EF is viewed as a single contiguous chain of individual records with variable length. Commands like READ RECORD and UPDATE RECORD are used together with the proper record number to access the desired record within the file. The maximum record length for this EF is 4096 bytes and the maximum number of records in this EF is 65535 bytes. However, as Linear Fixed Elementary Files, setting the right record lengths and number of records require some estimation of the available memory that the card has. This EF does not require record size to be equal to the record's actual size.

#### 3.3.2.3.4. Cyclic Elementary Files

Cyclic files are files that are like linear-fixed EF but are organized in a ring manner. This means that if the last record of the file is reached, the card operating system will go back to the first record and use it as the destination record. This EF is useful for logging transaction records. The maximum record length for this EF is 4096 bytes and the maximum number of records in this EF is 65535 bytes. Estimation is also needed when setting the right lengths and number of records just like linear EFs. This EF does not require record size to be equal to the record's actual size.

### 3.3.3. File Header Block

The ACOS5-EVO organizes the user memory area by files. Every file has a File Header Block, which is a block of data that describes the file's properties. Knowledge of the file header block will help the application developer for the file creation and accurately plan for the usage of the user memory.

### 3.3.4. File Life Cycle

ACOS5-EVO files have four states during its life cycle. The figure below illustrates how it works:

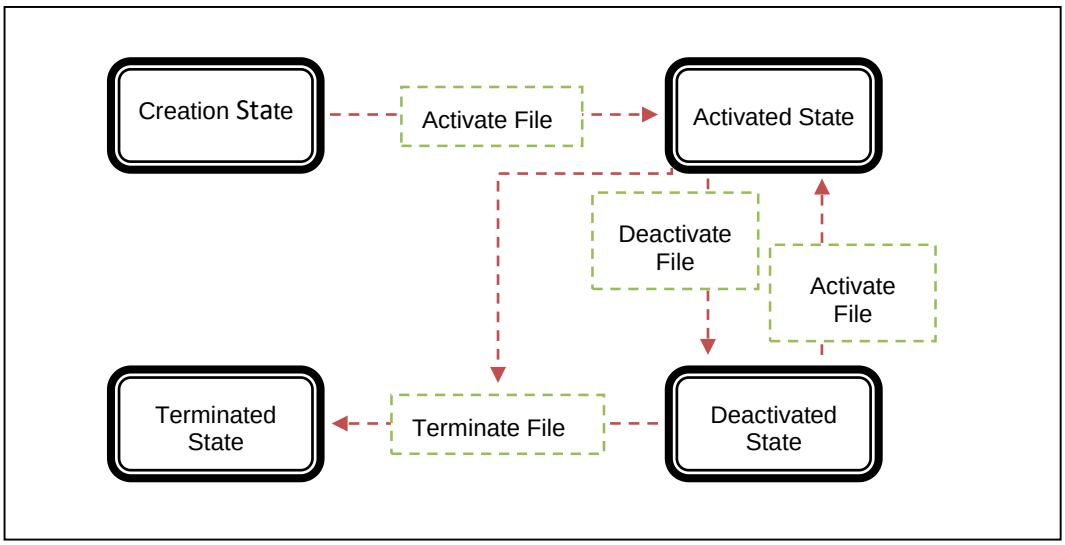


**Figure 4**: File Life Cycle States

- In Creation/Initialization states, all commands to the file will be allowed. After personalization, it is important to ACTIVATE the files to bring the card to operational state. This will enforce each file's security conditions.
- In Activated state, commands to the file are allowed only if the file's security conditions are met.
- In Deactivated state, commands to the file are not allowed except SELECT FILE, ACTIVATE FILE, DELETE FILE, and TERMINATE DF/EF.

- In Terminated State, only the DELETE FILE command is allowed.

### 3.3.5. Predefined File Identifiers

There are a few predefined File IDs. Since these are file identifiers that are implicitly known by the card operating system, they cannot be used for other files. The predefined file IDs are:

- 3F 00h – This file identifier is reserved for the Master File.
- 2F 01h – ATR file. Reserved under MF.
- 3F FFh – This file identifier is reserved for the current DF. When selecting a file, this file id is implicitly known by the card operating system to be the current DF regardless of the real file identifier of the file.
- FF FFh – Reserved for future use or RFU.

***Note:*** *A file cannot have an ID of 3F FFh, FF FFh and 00 00h. The card operating system will return an error during file creation if a file ID is equal to the pre-defined ones.*

### 3.3.6. Limitations

The limitations of the ACOS5-EVO stems from the limited available RAM and User Memory space. Hence, security capabilities are bound to this limitation:

- DF sub-levels can be as many as the memory can accommodate but the card operating system security conditions can only be up to the third sub-level in the file hierarchy.
- Local PINs and Keys and other security conditions of a DF are not saved when it goes below the fourth sub-level.
- DF Names are only up to 16-bytes of data.
- Only five CHV Files and five Symmetric Key Files are allowed under a DF. In FIPS Mode, only one CHV and one Symmetric Key is allowed under a DF/MF.

***Note:*** *File sizes are statically set during file creation and cannot be modified. However, the ACOS5-EVO allows file deletion anytime during its lifetime.*

### 3.3.7. Anti-tearing Mechanism

The ACOS5-EVO uses a mechanism called *anti-tearing* in order to protect the card from data corruption due to card tearing (i.e. card suddenly pulled out of reader during data update, or reader suffer mechanical failure during card data update). Immediately on the next card reset or power up, the ACOS5-EVO applies the necessary data recovery if tearing is detected. In such case, the operating system will return the corrupted data to its original state before the card tearing occurred.

### 3.3.8. Roll-Forward Mechanism

The ACOS5-EVO uses a mechanism where unfinished tasks are continued after a power interruption or card tearing. On reset, the ACOS5-EVO checks the roll-forwarding fields and does the necessary continuation of interrupted commands.

# 4.0. Card Internal Files – Structure and Usage

This is to illustrate the internal files of the ACOS5-EVO card along with its structure and usage:

- Card Holder Verification File
- Symmetric Key File
- Asymmetric Key File
- Security Environment File

## 4.1. Summary of Internal Files

The behavior of the COS will depend on the contents of the security-related internal files. The following are the internal files used by the ACOS5-EVO's security system:

| Internal File | Description |
|---|---|
| **CHV File** | Contains PIN records with the PIN valid bit, Resetting code valid bit, PIN identifier, Retries left, Allowed retries, PIN length, PIN, Resetting code counter, Resetting code length, Resetting code. The PIN is typically used for cardholder verification. |
| **Symmetric File** | Contains symmetric key records with the Key valid bit, Key identifier, Key type, Key Information, Algorithm reference, and the Key. The symmetric keys are typically used by symmetric-key algorithms such as DES, 3DES and AES for External Authentication, Internal Authentication and Mutual Authentication. |
| **RSA Private Key File** | Contains a single RSA Private Key with the Key type, Key length, File ID of the public key partner and Key valid byte.<br>For non-CRT private key: Private Key Exponent (d)<br>For CRT private key: P \|\| Q \|\| dP \|\| dQ \|\| qInv<br>Only one private key per file is allowed. |
| **RSA Public Key File** | Contains a single RSA Public Key with the Key type, Key length, File ID of the private key partner, Key valid byte, Public key exponent and the Modulus. Only one public key per file is allowed. |
| **ECC Private Key File** | Contains a single ECC Private Key Key with the Key type, Key length, File ID of the public key partner and Key valid byte, Private Key (d). Only one private key per file is allowed. |
| **ECC Public Key File** | Contains a single ECC Public Key with the Key type, Key length, File ID of the private key partner, Key valid byte, Public Key Point coordinates. Only one public key per file is allowed. |
| **Security Environment File** | Contains Security Environment templates. A DF or MF shall use only one SE File. The SE File ID corresponding to the DF or MF shall be embedded in the DF/MF's file header. |

**Table 7**: Internal Files

## 4.2. Internal Card Holder Verification File

A CHV file is an Internal Linear-fixed elementary file. This file is used by the card operating system to store PIN records for cardholder verification. This file, when under a DF, is considered to store local PINs or PINs that are relevant within the DF only. When under a MF, this file stores global PINs or PINs that are relevant throughout the whole card file hierarchy.

## 4.3. Internal Symmetric Key File

A *Symmetric Key* file is an Internal Linear-Variable Elementary File. This file is used by the card operating system to store symmetric key records for cryptographic use. Symmetric keys are used by symmetric-key algorithms such as DES, 3DES, and AES for cryptographic operations. This file is considered to store local keys or keys that are relevant within the DF only, when under a DF. When under a MF, this file stores global keys or keys that are relevant throughout the whole card file hierarchy.

## 4.4. Internal RSA Key File

A RSA Key File is an internal transparent file with an FDB of 09h. This file holds a single RSA key that could be either a “Private Key” or a “Public Key”. A MF/DF is allowed to have multiple RSA Key Files within the capacity of the card memory

## 4.5. Internal ECC Key File

An ECC Key File is an internal transparent file with an FDB of 19h. This file holds a single ECC key that could be either a “Private Key” or a “Public Key”. A MF/DF is allowed to have multiple ECC Key Files within the capacity of the card memory.

## 4.6. Internal Purse File

Purse files are Internal Cyclic Files. An ACOS5-EVO Purse File should always have record length of 16, and number of records must at least be 3. The 1$^{st}$ 2 physical records store information on the purse, while the rest are used to store transactions records (LOG).

## 4.7. Internal Security Environment File

A Security Environment (SE) File is an Internal Linear Variable EF which stores Security Environments in the form of SE templates which are security operations required by a certain file or application in the card.

# 5.0. Card Access Rights and Security – Environment and Usage

This chapter illustrates the access rights and security capabilities of the ACOS5-EVO card along with its environment and usage. They are:

- File Security Attributes
- Security Environment
- Control Reference Templates
- Mutual Authentication Procedure
- Session Key Generation

## 5.1. Introduction

Commands are restricted by the ACOS5-EVO depending on the target file's (or current DF's) Security Access Conditions. These conditions are based on PINs and KEYs being maintained by the system. Card Commands are allowed if certain PINs or KEYs are submitted or authenticated.

Global PINs are PINs that reside in a PIN EF (EF1) directly under the MF. Likewise, local keys are KEYs that reside in a KEY EF (EF2) under the currently selected DF.

## 5.2. File Security Attributes

Each file (MF, DF, or EF) has a set of security attributes in its headers. There are two types of security attributes the ACOS5-EVO uses, namely, Security Attribute Compact (SAC) and Security Attribute Expanded (SAE).

## 5.3. Security Environment

Security conditions are coded in a Security Environment File and each SE can have several Security Environment Data Objects (SE DO).

## 5.4. Control Reference Templates

### 5.4.1. Authentication Template

The Authentication Template defines either the PIN or Key authentications security condition that must be met.

### 5.4.2. Cryptographic Checksum Template

The CCT defines which parameters to use in computing for the MAC, which is used in Secure Messaging and/or Compute/Verify Cryptographic Checksum command.

### 5.4.3. Confidentiality Template

The CT defines which parameters to use in encrypting/decrypting data in Secure Messaging, Symmetric Key Encrypt / Decrypt and/or Public Key Encrypt / Private Key Decrypt.

### 5.4.4. Digital Signature Template

The DST defines which parameters to use in asymmetric key-related operations.

### 5.4.5. Hash Template

The HT defines which parameters to use in PSO-HASH.

### 5.4.6. Key Agreement Template

The KAT defines which parameters to use in key derivation operations.

## 5.5. Mutual Authentication Procedure

To provide maximum flexibility, the ACOS5-EVO uses two different pairs of 3DES/AES keys: A *terminal key* $K_T$ and a *card key* $K_C$. These pair of keys should both be on-board, and they both should have the same key algorithm and key length.

A random number generator is on-board the ACOS5-EVO to generate a *card random number,* $RND_C$, in response to the *GET CHALLENGE* command.

## 5.6. Session Key Generation Procedure

The ACOS5-EVO supports AES session and 3DES session keys only as DES is not considered secured anymore. Session key ($K_S$) generation is automatically executed after a Mutual Authentication procedure.

# 6.0. Secure Messaging

The ACOS5-EVO supports *Secure Messaging* (SM) for *Authentication* and *Confidentiality*. SM with Authentication means the APDU is transmitted together with a MAC while SM with Confidentiality means the APDU is transmitted in encrypted format. Secure messaging ensures data transmitted between card and terminal/server is secured and not susceptible to eavesdropping, replay attack and unauthorized modifications.

## 6.1. SM Modes

There are two modes of SM that can be applied in two different security levels. The first mode is *SM for authenticity* (SM-sign) and the other mode is *SM for confidentiality* (SM-enc).

## 6.2. SM for Authenticity

SM-sign ensures that command and response were issued by the authenticated terminal and card respectively. The data can be trusted to have come from the trusted source and it has not been altered or replayed.

## 6.3. SM for Authenticity and Confidentiality

In addition to the security enhancement of SM-sign, SM-enc has added encryption to the transmitted data to ensure data confidentiality.

# 7.0. Life Support Application

These products are not designed for use in life support appliances, devices or systems, where malfunctions of these products can reasonably be expected to result in personal injury. ACS customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify ACS for any damages resulting from such improper use or sale.

# 8.0. Contact Information

For additional information, please visit http://www.acs.com.hk.

For sales inquiry, please send an email to info@acs.com.hk.