Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5-64

Functional Specifications V2.09

Subject to change without prior notice

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

Table of Contents

List of Figures

1.0. Introduction

This document aims to describe the features and functions of the ACOS5-64, a cryptographic smart card developed by Advanced Card Systems Ltd.

The ACOS5-64 is an advanced cryptographic smart card with a FIPS 140-2 (US Federal Information Processing Standards) Level 3–certified mode of operation. It is specially designed for public key–based applications.

Here are the key features of the ACOS5-64 Cryptographic Smart Card:

- FIPS 140-2 Level 3–certified operation mode (see **Operation Mode Byte**)
- Common Criteria EAL5+ Certified (Chip Level)
- Backward compatibility mode available so the card may be used as in various modes: ACOS5-64 v2.00 mode, and NSH-1 mode (see **Operation Mode Byte**)
- File system that can reuse deleted files' memory space without compromising security
- File system that manages the EEPROM to prolong the card's life span
- Compliance with ISO 7816 Parts 1, 2, 3, 4, 8, 9
- High-speed transmission rate from 9.6 Kbps to 223.2 Kbps with modifiable ATR
- Mutual Authentication with Session Key Generation
- Secure Messaging ensures data transfers are confidential and authenticated
- Multi-level Secured Access Hierarchy
- Anti-tearing Function Support

For more information about capabilities, protection and access rights of the ACOS5-64 v3.00 (FIPS 140-2 Level 3–Certified) Cryptographic Module, check the ACOS5-64 FIPS 140-2 Level 3 Security Policy from the CMVP (Cryptographic Module Validation Program) webpage:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

1.1. History of Modifications

Date	Changes
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	ACOS5-64 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

Table 1: History of Modifications

1.2. 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
CBC	Cipher-Block Chaining Mode of Encryption
CCT	Cryptographic Checksum Template
CT	Confidentiality Template
CLA	Class byte of ISO 7816 APDU
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
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

Abbreviations	Description
MSb	Most Significant Bit
MSB	Most Significant Byte
P1	Parameter 1 of ISO 7816 APDU
P2	Parameter 2 of ISO 7816 APDU
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 V DC +/-10% (Class A) and 3 V DC +/-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 Protocol

- T=0 with baud up to 223,200 bps

2.4. Memory

- Capacity: 64 KB
- EEPROM Endurance: 500,000 erase/write cycles
- Data Retention: 30 years

2.5. Cryptographic Capabilities

ACOS5-64 supports a number of cryptographic algorithms, including:

- RSA: 512 – 4096 bits in 256 bits increments
- AES: 128/192/256-bits (ECB, CBC)
- DES/3DES: 56/112/168-bits (ECB, CBC)
- Hash: SHA1, SHA256
- MAC: CBC-MAC (DES/3DES)

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 submission).
- 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) using Triple DES with session key generation for encryption and MAC.
- Anti-tearing Function Support

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 Part 3. ACOS5-64 supports the protocol type T=0 in direct convention. For full description of ATR options, see ISO 7816 Part 3. The ATR may be completely changed using the ATR file.

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

The ACOS5-64 has a dynamic file system wherein memory wear and tear are properly managed to prolong its life span. The card operating system organizes, manages and administers the function of the card.

The fundamentals of the ACOS5-64 File System consist of the following:

- Card Life Cycle
- Card Header Block
- Hierarchy of Files on ACOS5-64 Cards
- 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 ACOS5-64 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

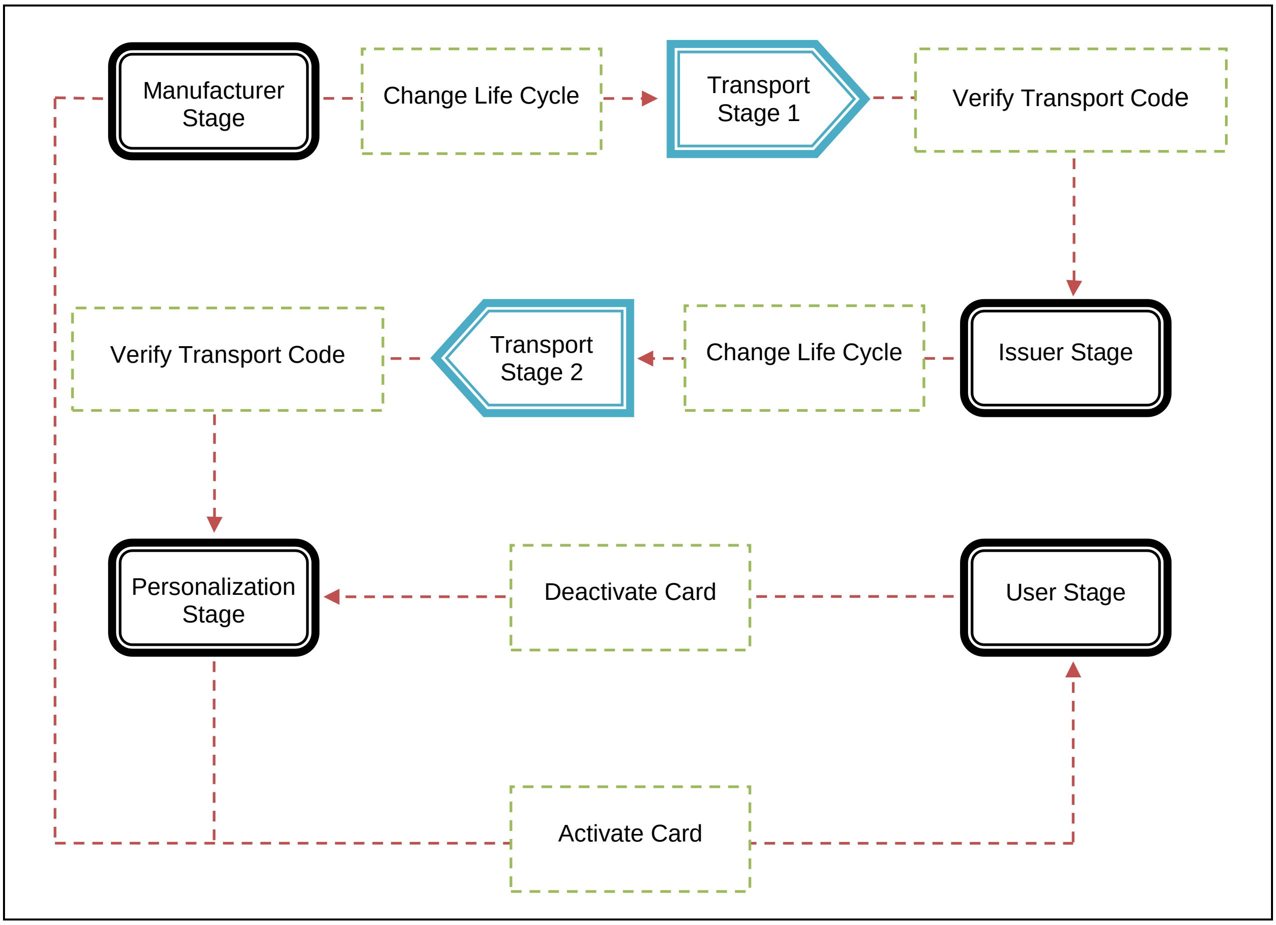

Figure 1: Card Life Cycle Stages

3.1.1. Manufacturer Stage

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

Note: *The ACOS5-64 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.*

All commands are allowed in this stage. The ACOS5-64 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. ACOS5-64 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)

Note: *Customized commands cannot be loaded at the User or Personalization Stage. The card cannot go back to Manufacturer Stage or Issuer Stage. 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. **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 ACOS5-64 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.

3.2.2. Card Life Cycle Byte

This byte is controlled by the COS. It is changed when Card Management Commands are used. Users do not need to set this byte. This byte should not be written but can be read to determine the card's life cycle state.

3.2.3. Operation Mode Byte

This byte selects the operation mode of the COS for the ACOS5 v3.00. Several things are changed whenever a different mode is selected which are explained in the succeeding sections.

3.2.3.1. FIPS 140-2–Compliant Mode

This mode of operation is in accordance to the ACOS5-64 FIPS 140-2 Level 3 Security Policy document.

Please refer to: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

- Default mode of operation
- Sets the COS to an "Approved Mode of operation" as of FIPS 140-2 Level 3
- Use and creation of keys that does not meet 112 bits of security strength is prohibited
- Use of hash functions that does not meet 112 bits of security strength is prohibited

Function	Size (bits)
Triple DES	168
AES	128/192/256
RSA Key Generation	2048/3072
RSA Signature Generation	2048/3072
RSA Signature Verification	2048/3072/4096
SHA-256	256

Table 3: Allowed Functions

- A SHA-256–based Deterministic Random Bit Generator compliant with NIST special publication 800-90 shall be used instead of the on-board True Random Number Generator.

3.2.3.2. 64K Mode

ACS also provides customers the option to set the operation of the COS to be fully backward-compatible with the previous version of the ACOS5-64.

- Full backward-compatibility with ACOS5-64 v2.00
- Full 64K access to user memory

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

3.2.3.3. NSH-1–Compliant Mode

The ACOS5-64 has also been tested with NSH-1 (ICP Brasil) and ACS provides an option for customers to use this mode of operation.

- Sets the COS to an NSH-1–approved mode of operation
- A SHA-256–based Deterministic Random Bit Generator compliant with NIST Special Publication 800-90A shall be used instead of the on-board True Random Number Generator.

3.2.4. 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.

3.2.5. Transport Code

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

3.2.6. Life Cycle Complement Byte

This is the complement value of the Life Cycle Byte. It is set internally. If this value is not complemented correctly, it will mute the card. Care should be taken to not to write to this byte or the Life Cycle Byte.

3.2.7. EEPROM Key Error Counter

If Error Counter is FFh, the retry limit is unlimited.

Incorrect verification will deduct the remaining count. If the transport code verification is correct, the Error counter will become FFh and the life cycle byte will increment by 1.

3.3. File System

3.3.1. Hierarchy

The ACOS5-64 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.

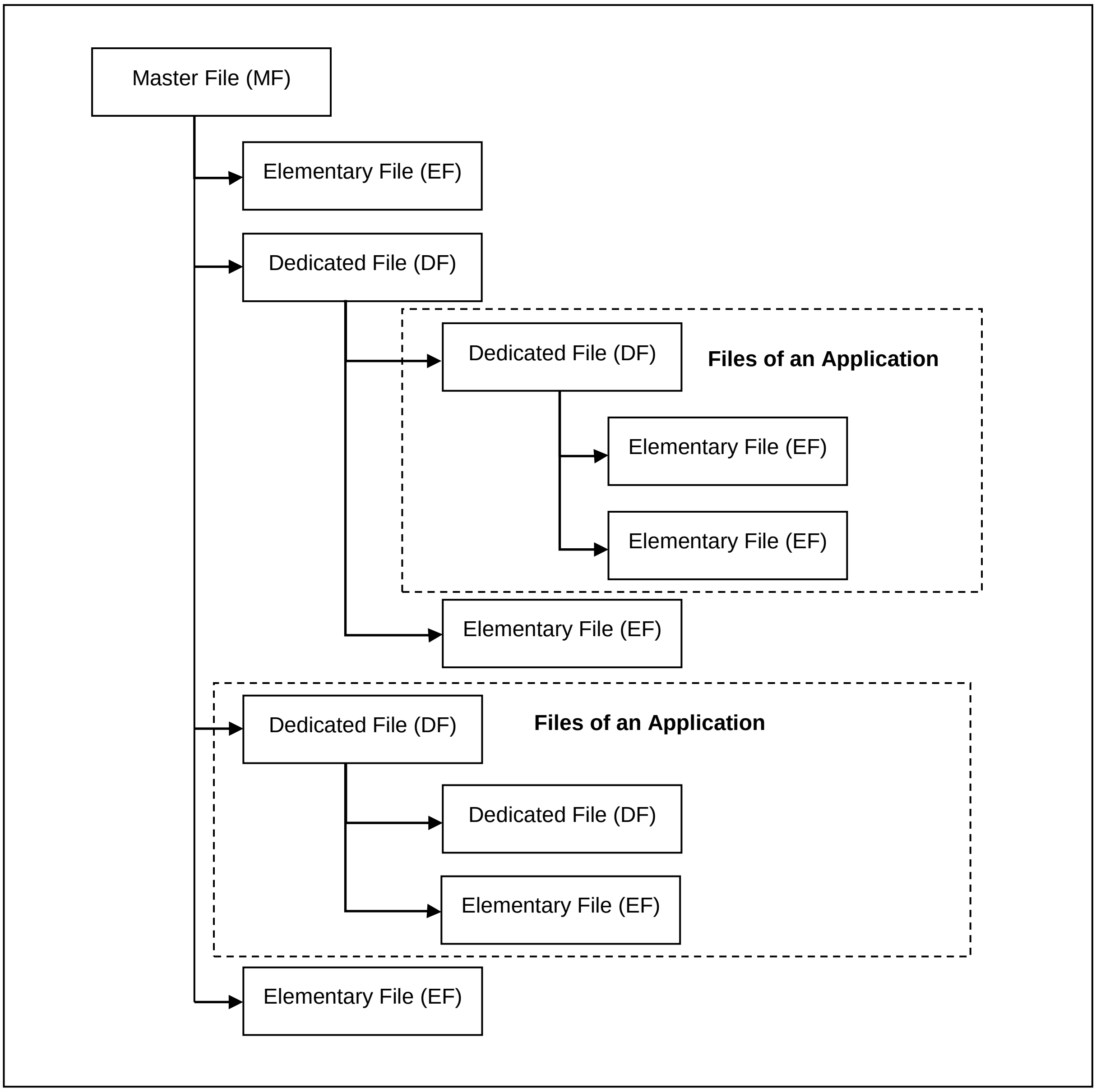

Figure 2: File System Hierarchy

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. The ACOS5-64 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.
- Working EF – Data files not interpreted by the card, i.e., data used by the user like names, dates and other personalized information.

ACOS5-64 supports four types of elementary files: transparent, linear-fixed, linear-variable, and cyclic.

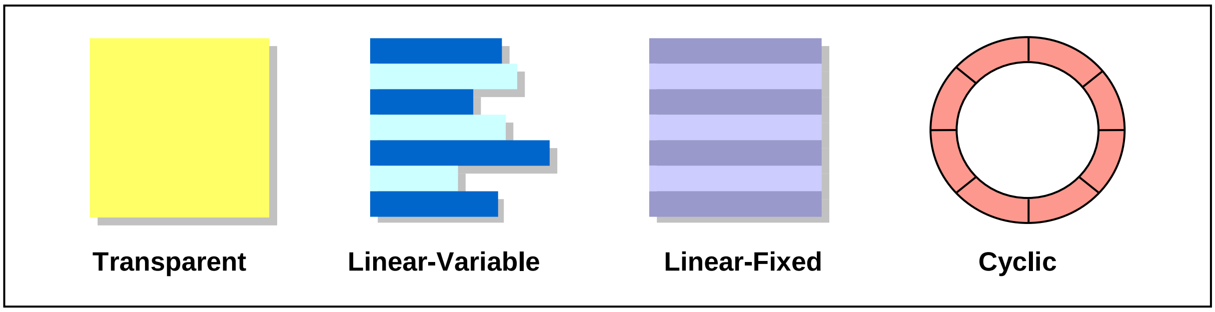

Figure 3: Structures of Elementary Files According to ISO 7816-4

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. Transparent EFs are useful for storing data units longer than 255 bytes, i.e., digital certificates and public/private RSA keys.

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 255 and it can be set to any value in between 1 to 255. The maximum number of records in this EF is also 255. However, setting the right record lengths and number of records require some estimation of the available memory of the card.

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 255. The maximum number of records in this EF is also 255. However, as with Linear-Fixed Elementary Files, setting the right record lengths and number of records require some estimation of the available memory of the card.

3.3.2.3.4. Cyclic Elementary Files

Cyclic files are like linear-fixed EF but 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 255 and it can be set to any value in between 1 to 255. The maximum number of records in this EF is also 255. Estimation is also needed when setting the right lengths and number of records just like linear EFs.

3.3.3. File Header Block

The ACOS5-64 organizes the user EEPROM 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 with the file creation and accurately plan for the usage of the EEPROM space.

3.3.4. File Life Cycle

ACOS5-64 files have four states during its life cycle. The figure below illustrates how it works:

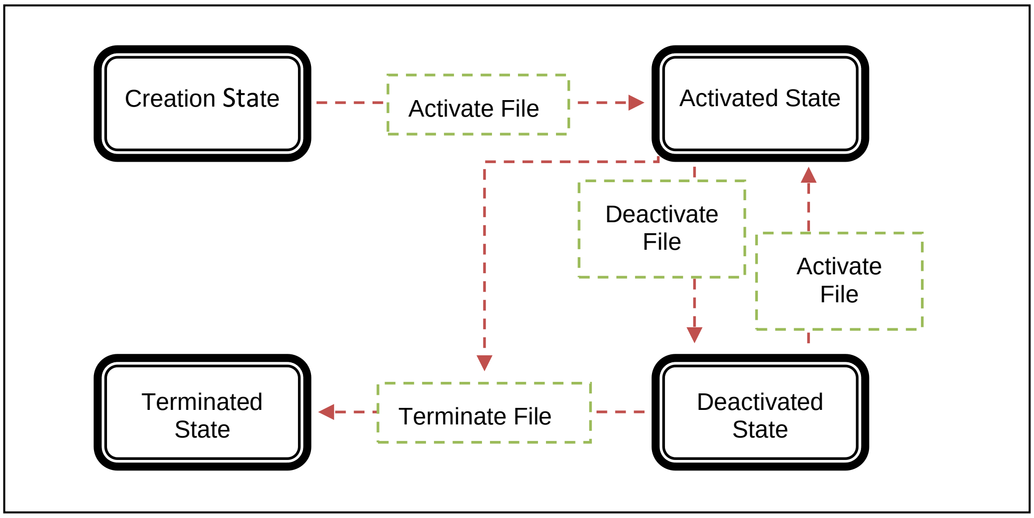

Figure 4: File Life Cycle States

1. In the 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.
2. In the Activated state, commands to the file are allowed only if the file's security conditions are met.
3. In the Deactivated state, most commands to the file are not allowed except SELECT FILE, ACTIVATE FILE, DELETE FILE, and TERMINATE DF/EF.
4. In the Terminated State, all commands to the file will not be 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 ACOS5-64 stems from the limited available RAM and EEPROM space. Hence, security capabilities are bound to this limitation:

- DF sub-levels can be as many as the EEPROM 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.

***Note:** File sizes are statically set during file creation and cannot be modified. However, ACOS5-64 allows file deletion anytime during its lifetime.*

3.3.7. Anti-tearing Mechanism

The ACOS5-64 uses a mechanism called *anti-tearing* in order to protect the card from data corruption due to card tearing (i.e. when the card is suddenly pulled out of reader during data update, or the reader suffered mechanical failure during card data update). Immediately on the next card reset or power up, the ACOS5-64 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 ACOS5-64 uses a mechanism where unfinished tasks are continued after a power interruption or card tearing. On reset, the ACOS5-64 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 ACOS5-64 card along with its structure and usage:

- Card Holder Verification (CHV) File
- Symmetric Key File
- RSA Private Key and Public 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 ACOS5-64'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. A DF or MF shall contain only one CHV file.
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. A DF or MF shall contain only one Symmetric Key File.
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. For non-CRT private key: Private Key Exponent (d) For CRT private key: P || Q || dP || dQ || qInv 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.
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 4: 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. Essentially, a DF or MF shall have only one CHV file. This file, when under a DF, is considered to store local PINs or PINs that are relevant within the DF only. When under an 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. Essentially, a DF or MF shall have only one symmetric key file. This file is considered to store local keys or keys that are relevant within the DF only, when under a DF. When under an MF, this file stores global keys or keys that are relevant throughout the whole card file hierarchy.

4.4. Internal RSA Key File

An 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”. An MF/DF is allowed to have multiple RSA Key Files within the capacity of the EEPROM.

4.5. Internal Purse File

Purse files are internal cyclic files. An ACOS5-64 Purse File should always have a record length of 16, and the number of records must at least be 3. The first 2 physical records store information on the purse, while the rest are used to store transactions records (LOG).

4.6. Internal Security Environment File

A Security Environment (SE) File is an internal linear-variable EF that stores security environments in the form of SE templates. Every DF shall have a designated SE File whose file ID is indicated in the parent DF’s header block. An SE file can have up to 15 identifiable records.

5.0. Card Access Rights and Security – Environment and Usage

This chapter illustrates the access rights and security capabilities of the ACOS5-64 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 ACOS5-64 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.

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 that the ACOS5-64 uses: Security Attribute-Compact (SAC) and Security Attribute-Expanded (SAE).

5.3. Security Environment

Security conditions are coded in a Security Environment File. Every DF has a designated Security Environment File or SE File, whose file ID is indicated in the DF's header block. Each SE record has the following format:

<Security Environment ID Template> <Security Environment DO Template>

5.4. Control Reference Templates

5.4.1. Authentication Template

The Authentication Template defines the security condition that must be met for this SE to be satisfied. The security conditions are either PIN or Key authentications.

5.4.2. Cryptographic Checksum Template (CCT)

The Cryptographic Checksum Template (CCT) defines which parameters to use in computing for the MAC, which is used in Secure Messaging and/or PSO.

5.4.3. Confidentiality Template (CT)

The Confidentiality Template (CT) defines which parameters to use in encrypting or decrypting data in Secure Messaging and/or PSO. This template is also applied to asymmetric encryption/decryption.

5.4.4. Digital Signature Template (DST)

The Digital Signature Template (DST) defines which parameters to use in asymmetric key-related operations.

5.4.5. Hash Templates (HT)

The Hash Template (HT) defines which parameters to use in PSO-HASH.

5.5. Mutual Authentication

Mutual Authentication is a process in which both the card and the card-accepting device verify that the respective entity is genuine. A Session Key is the result of a successful execution of mutual authentication. The session key is only valid during a session. A session is defined as the time after a successful execution of the mutual authentication procedure and a reset of the card of the execution of another mutual authentication procedure. The execution of a SELECT FILE command also ends a session.

5.6. Session Key Generation Procedure

ACS only supports 3DES session keys as DES is not considered secured anymore. Session key generation is automatically executed by ACOS5-64 after a Mutual Authentication procedure.

Length of Session Key is based on the length of Kc/Kt. Both keys should have the same length for compatibility purposes.

K_S-ENC is responsible for encryption for:

- Secure Messaging
- PSO commands with CT-symmetric set with DO tag 84h
- K_S-MAC is responsible for MAC:
- Secure Messaging
- PSO commands with CCT set with DO tag 84h

5.7. Secure Messaging

Secure Messaging (SM) allows secure communication between the terminal/server backend and the ACOS5-64, which supports secure messaging for authentication and confidentiality.

There are two Secure Messaging (SM) modes available for the ACOS5-64, namely:

1. Secure Messaging for Authenticity (SM-MAC) – This ensures the authenticity of the command.
2. Secure Messaging for Confidentiality (SM-ENC) – This ensures the confidentiality of the command.

5.8. Key Injection

Key Injection can be used to securely load a key or a diversified key from an application or terminal into an ACOS5-64 card.

For the process of key injection, the card will select a file where the key(s) will be injected. Then call the Put Key command, with the data containing the key(s) to be injected.

For more information about capabilities, protection and access rights of the ACOS5-64 v3.00 (FIPS 140-2 Level 3–Certified) Cryptographic Module, check the ACOS5-64 FIPS 140-2 Level 3 Security Policy from the CMVP (Cryptographic Module Validation Program) webpage:
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2664.pdf

6.0. 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.

7.0. Contact Information

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

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