Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5 – 64

Functional Specification

Subject to change without prior notice

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

Table of Contents

1.0. Introduction 3

2.0. Abbreviations and Notations 4

2.1. Features 5
2.2. Technical Specifications 5
2.3. Answer to Reset (ATR) 5
2.4. Cryptographic Capabilities 6

3.0. Card File System (User Files, Structures and Usage) 7

3.1. Card Header Block 7
3.2. File Header Block 7
3.3. Hierarchical File System 8
3.4. File Life Cycle 9
3.5. Predefined File Identifiers 9
3.6. Anti-tearing Mechanism 9
3.7. Roll Forward Mechanism 9
3.8. Card Life Cycle 10
3.8.1. Manufacturer Stage 10
3.8.2. Transport Stage 11
3.8.3. Personalization Stage 11
3.8.4. User Stage 11

4.0. Card Internal Files (Structure, Usage) 12

4.1. Internal Card Holder Verification (CHV) File 12
4.2. Internal Symmetric Key File 12
4.3. Internal RSA Key File 12
4.4. Internal Purse File 12
4.5. Internal Security Environment File 12

5.0. Card Access Rights and Security (Environment and Usage) 13

5.1. File Security Attributes 13
5.2. Security Environment 13
5.3. Control Reference Templates 13
5.3.1. Authentication Template 13
5.3.2. Cryptographic Checksum Template (CCT) 13
5.3.3. Confidentiality Template (CT) 13
5.3.4. Digital Signature Template (DST) 13
5.3.5. Hash Templates (HT) 13
5.4. Authentication 14
5.5. Secure Messaging 14

6.0. Life Support Application 15

7.0. Contact Information 16

Figures

Figure 1: File System Hierarchy According to ISO 7816-4 8

Figure 2: File Life Cycle States 9

Figure 3: Card Life Cycle Stages 10

1.0. Introduction

This document aims to describe the features and functions of the ACS Smart Card Operation System Version 5.0 64 kilobytes version (ACOS5-64) as developed by Advanced Card Systems Ltd.

ACOS5-64 is an advanced cryptographic smart card that fully complies with ISO 7816-1~4, 8 and 9 standards, and is specially designed for public key-based applications. In addition, the card is intended for enhancing security and performance of RSA public key cryptographic operations that are essential in smart card Public Key Infrastructure (PKI) and high-level security requirements.

Furthermore, ACOS5-64 supports a number of security infrastructures and applications, including:

- Adobe Acrobat
- Crypto-API and PKCS #11 Middlewares
- Domain Smart Card Logon
- Encrypting File System (EFS)
- IIS SSL
- Internet Explorer
- Lotus Notes
- Microsoft VPN/Open VPN
- Mozilla Firefox
- Netscape
- OpenID
- Outlook, Windows Mail, Outlook Express and Mozilla Thunderbird mail signing and encryption (S/MIME)
- Secure Online Certificate Generation
- Smart Card Minidriver
- SSH

2.0. Abbreviations and Notations

3DES – Triple Data Encryption Standard

AMB – Access Mode Byte

AMDO – Access Mode Data Object

APDU – Application Protocol Data Unit

ATR – Answer to Reset

CSP – Cryptographic Service Provider

DF – Dedicated File

EEPROM – Electrically Erasable Programmable Read-Only Memory

EF – Elementary File

EF1 – PIN File

EF2 – KEY File

IIS – Internet Information Services

ISO – International Organization for Standardization

FCP – File Control Parameters

FDB – File Descriptor Byte

LCSI – Life Cycle Status Integer

LSb/LSB – Least Significant Bit/Least Significant Byte

MAC – Message Authentication Code

MF – Master File

MSb/MSB – Most Significant Bit/Most Significant Byte

RFU – Reserved for Future Use

RSA – Public key cryptography 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-MAC – MAC for Secure Messaging

TLV – Tag-Length-Value

UQB – Usage Qualifier Byte

|| - Concatenation of bytes

2.1. Features

ACOS5-64 Cryptographic Smart Card has these feature highlights:

- 64 KB of user memory for application data
- ISO 7816 Parts 1, 2, 3, 4, 8, 9 compliance
- ISO 7816-2 compliant 8-contact module
- High baud rate switchable between 9.6 Kbps and 223 Kbps
- Fast EEPROM writing speed
- Supports ISO 7816 Part 4 file structures: Transparent, Linear Fixed, Linear Variable, Cyclic
- On-board RSA key generation of up to 4096 bit
- AES-128/192/256 support
- Mutual Authentication with Session Key generation
- Secure Messaging ensures data transfers are confidential and authenticated.
- Multi-level secured access hierarchy
- Anti-tearing done on file headers and system information
- Common Criteria EAL5+ (Chip Level)
- FIPS140-2 compatible
- File system has the capability of reusing deleted files' memory space without compromising speed
- File system manages the EEPROM to prolong its life span

2.2. Technical Specifications

ACOS5-64 Cryptographic Smart Card has these technical characteristics:

- Operating voltage is at 5 VDC ±10% for Class A and 3 V ±10% for Class B
- Maximum supply current: < 20 mA
- ESD protection ≤ 5000 V
- Capacity: 64 KB
- EEPROM endurance: 500K Erase/Write cycles
- Data retention: 30 years
- Operating temperature: -25 °C to 85 °C
- Storage temperature: -65 °C to 150 °C

2.3. 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 standard. ACOS5-64 supports the protocol type T=0 in direct mode. ATR may be completely changed using the ATR file. For full descriptions of ATR options, see ISO 7816-3 standard and specifications.

2.4. Cryptographic Capabilities

ACOS5-64 Cryptographic Smart Card supports a number of cryptographic capabilities, including:

- Triple DES and AES data encryption and decryption in cipher block chaining mode (CBC) and electronic codebook (ECB) with 64-bit, 128-bit and 192-bit keys; AES 256-bit is also supported
- Secure on-card RSA key pair generation with 512-bit, 768-bit, 1024-bit, 1280-bit, 1536-bit, 1792-bit, 2048-bit, 2304-bit, 2560-bit, 2816-bit, 3072-bit, 3328-bit, 3584-bit, 3840-bit and 4096-bit keys
- RSA signature computation and verification with 512-bit, 768-bit, 1024-bit, 1280-bit, 1536-bit, 1792-bit, 2048-bit, 2304-bit, 2560-bit, 2816-bit, 3072-bit, 3328-bit, 3584-bit, 3840-bit and 4096-bit keys
- RSA CV certificate verification with 512-bit, 768-bit and 1024-bit key signed certificate
- Private key file read access can be set to “Never”
- Mutual authentication (terminal-to-card and card-to-terminal) using Triple DES with session key generation for encryption and MAC
- SHA-1 and SHA-256 message hashing
- Secure messaging – authenticity and confidentiality of data transmission
- File access condition capability with ISO 7816 compliant Secure Attribute Compact (SAC). 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 (SAE). Commands are allowed only if the proper security conditions are met (e.g. PIN submission)
- Real-time random number generator

3.0. Card File System (User Files, Structures and Usage)

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

- 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
- Card Life Cycle

3.1. Card Header Block

Card Header Block is a special memory area accessed by the card operating system for its operation.

3.2. File Header Block

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 in the file creation and accurately plan for the usage of the EEPROM space.

3.3. Hierarchical File System

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, where the root directory of the file system is the Master File (MF). Each application of 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 Figure 1.

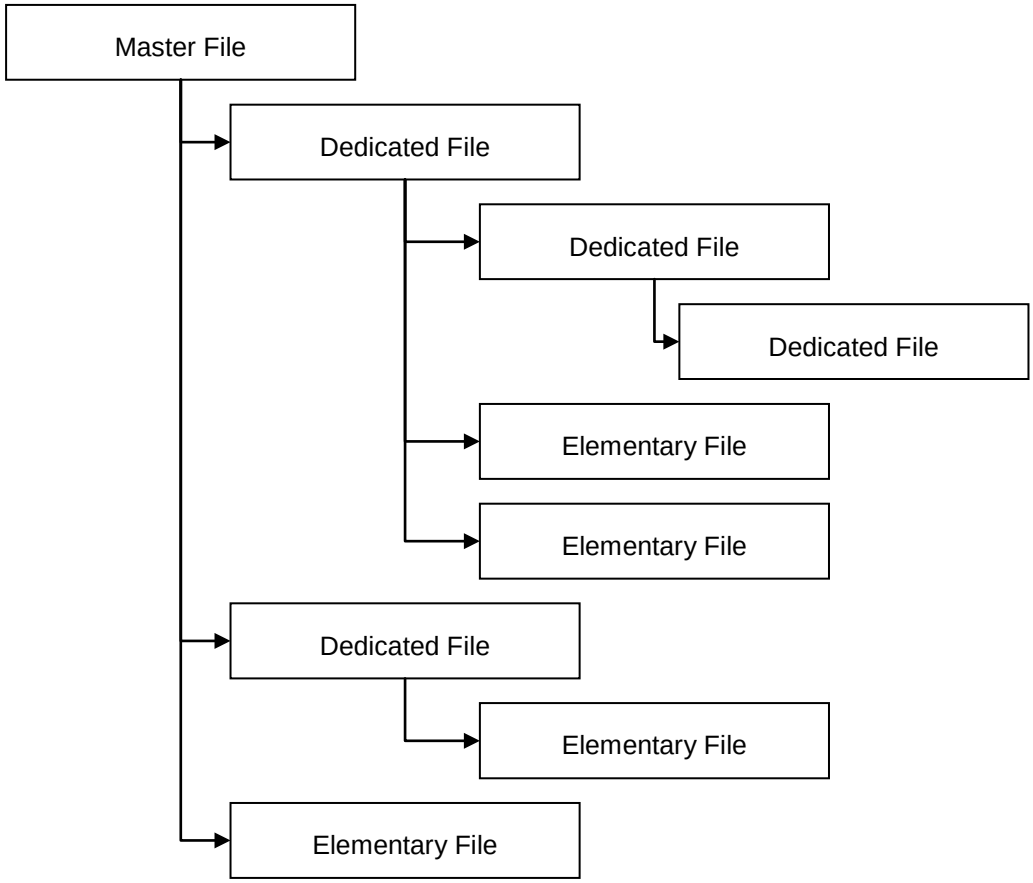

Figure 1: File System Hierarchy According to ISO 7816-4

3.4. File Life Cycle

ACOS5-64 files have four states during its life cycle; Figure 2 illustrates how it works:

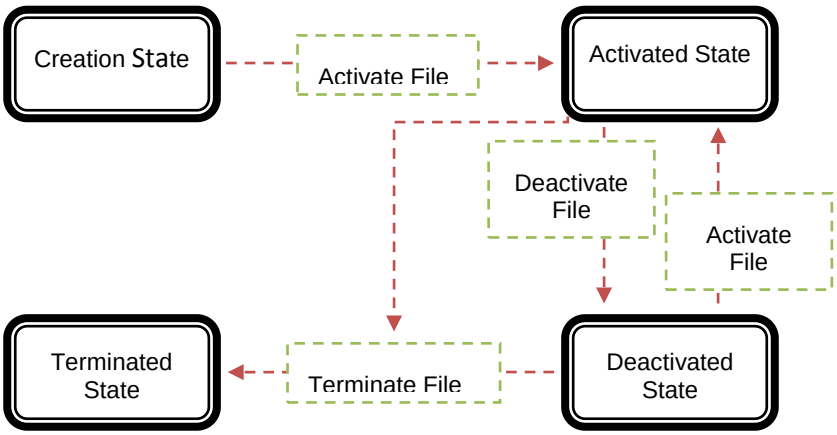

Figure 2: File Life Cycle States

- In Creation/Initialization State, all commands to the file will be allowed. After Personalization, it is important to ACTIVATE the files to make the card operational.
- In Activated State, commands to the file are allowed only if the file's security conditions are met.
- In Deactivated State, only most commands to the file are not allowed except SELECT FILE, ACTIVATE FILE, DELETE FILE, and TERMINATE DF/EF.
- In Terminated State, no commands to the file will be allowed.

3.5. Predefined File Identifiers

There are 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.

3.6. Anti-tearing Mechanism

ACOS5-64 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 the reader during data update, or reader suffers with mechanical failure during card data update). Immediately on the next card reset or power up, ACOS5-64 applies the necessary data recovery if tearing is detected. In such cases, the operating system will return the corrupted data to its original state before the card tearing occurred.

3.7. Roll Forward Mechanism

ACOS5-64 uses a mechanism where unfinished tasks are continued after a power interruption or card tearing. On reset, ACOS5-64 checks the roll forwarding fields and does the necessary continuation of interrupted commands.

3.8. Card Life Cycle

ACOS5-64 has the following card stages during its life cycle:

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

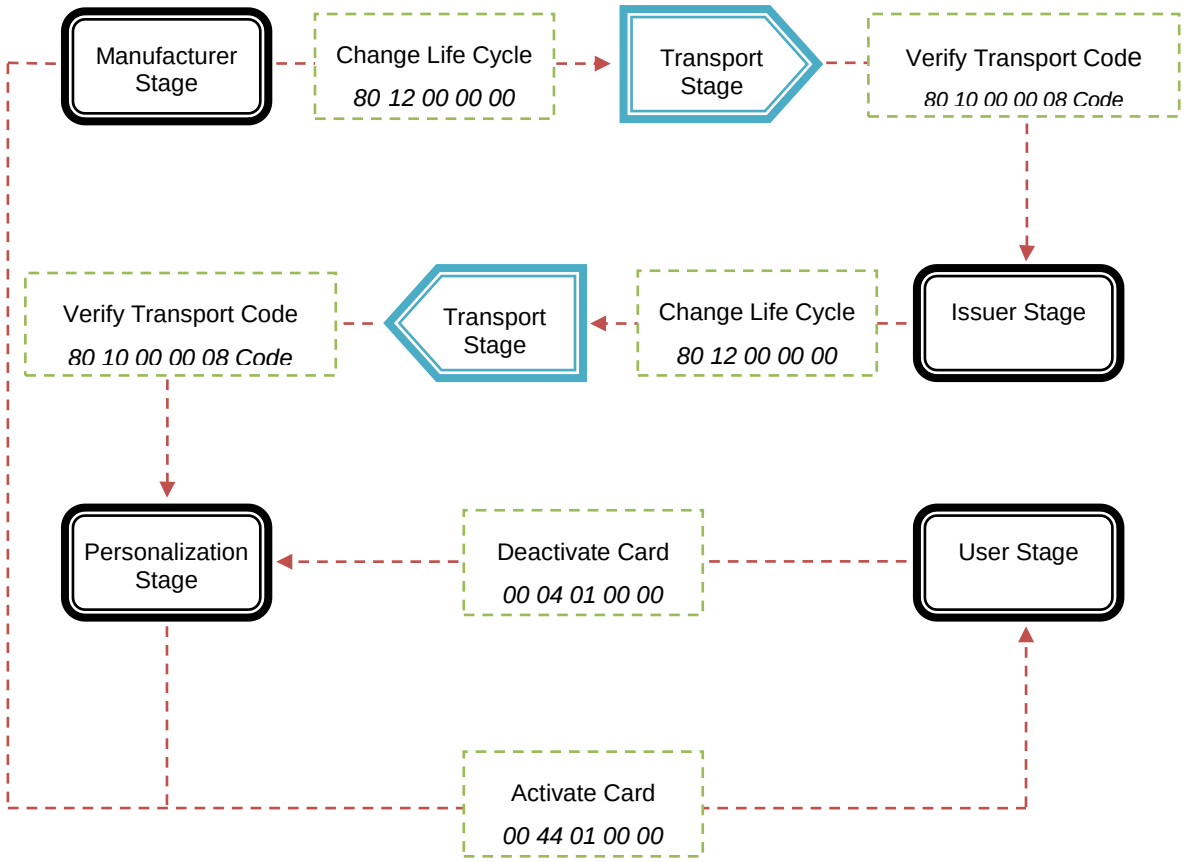

Figure 3: Card Life Cycle Stages

3.8.1. Manufacturer Stage

Manufacturer stage of the smart card refers to its initial state. The user is allowed to freely access the card header block (section xxx). The card header block can be referenced by its address using the READ BINARY or UPDATE BINARY command.

Note: ACS may add customized commands for the customer at this stage. 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.

3.8.2. Transport Stage

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.

3.8.3. 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 Operation Mode. This stage is used for personalizing the card to a specific user like loading of names, etc. **Zeroize Card User Data** and **Zeroize Soft Mask** commands are allowed in this stage.

> **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.

3.8.4. User Stage

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

4.0. Card Internal Files (Structure, Usage)

This is to illustrate the internal files of the ACOS5-64 card along with its structure and usage:

- Card Holder Verification File
- Symmetric Key File
- RSA Private Key and Public Key File
- Purse File
- Security Environment File

4.1. Internal Card Holder Verification (CHV) File

A CHV file is an Internal Linear – Fixed EF. 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 to the whole card file hierarchy.

4.2. Internal Symmetric Key File

A Symmetric Key file is an Internal Linear – Variable EF. This file is used by the card operating system to store symmetric key records for cryptographic use. Symmetric key algorithms such as 3DES, and AES for cryptographic operations use symmetric keys. Essentially, a DF or an MF shall have only one symmetric key file. This file is considered to store local keys or keys that are relevant with the DF only when under a DF. When under an MF, this file store global keys or keys that are relevant to the whole card file hierarchy.

4.3. Internal RSA Key File

A RSA Key File is an internal transparent file with an FDB of `0x09`. 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 EEPROM.

4.4. Internal Purse File

Purse files are Internal Cyclic Files. An ACOS5-64 Purse File should always have record length of 16, and number of records must at least be 3. The 1st 2 physical records store information on the purse, while the rest are used to store transactions records (LOG).

4.5. 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 DF’s header block. An SE file can have up to 15 identifiable records.

5.0. Card Access Rights and Security (Environment and Usage)

Commands are restricted by ACOS5-64 depending on the target file's (or current DF's) SAC. 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 an MF. Likewise, local keys are Keys that reside in a Key EF (EF2) under the currently selected DF. There can be a maximum of 31 Global PINs, 31 Local PINs, 31 Global Keys, and 31 Local Keys at a given time.

This is to illustrate the access rights and security capabilities of the ACOS5-64 card along with its environment and usage:

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

5.1. 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 ACOS5-64 use, namely Security Attribute Compact (SAC) and Security Attribute Expanded (SAE).

5.2. 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>

5.3. Control Reference Templates

5.3.1. Authentication Template

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.

5.3.2. Cryptographic Checksum Template (CCT)

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

5.3.3. Confidentiality Template (CT)

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.

5.3.4. Digital Signature Template (DST)

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

5.3.5. Hash Templates (HT)

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

5.4. 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.

5.5. Secure Messaging

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

There are two modes of SM that can be applied to two different situations: the first mode is SM for authenticity (*SM-Sign*); and the other is SM for confidentiality (*SM-enc*). The SM modes will be applied to both command and response data.

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.