Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS5

Reference Manual

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

Table of Contents

1.0. Introduction 3

1.1. Features 3
1.2. Technical Specifications 3
1.2.1. Electrical 3
1.2.2. EEPROM 3
1.2.3. Environmental 3
1.3. Symbols and Abbreviations 3

2.0. Card Management 5

2.1. Anti Tearing 5
2.2. Card Life States 5
2.3. Answer To Reset 6
2.3.1. Customizing the ATR 6

3.0. File System 7

3.1. Hierarchical File System 7
3.2. File Header Data 7
3.3. Internal Security Files 7

4.0. Security 8

4.1. File Security Attributes 8
4.2. Security Environment 8
4.3. Authentication 8
4.4. Secure Messaging 8

5.0. Life Support Application 9

6.0. Contact Information 10

Figures

Figure 1. Card life cycle states 5

Figure 2. Example of hierarchy of DFs 7

Tables

Table 1. Default Configuration of the Answer-to-Reset 6

1.0. Introduction

The purpose of this document is to describe in detail the features and functions of the ACS Smart Card Operating System Version 5.0 (ACOS5) developed by Advanced Card Systems Ltd.

1.1. Features

ACOS5 provides the following features:

- Full 32Kbytes of EEPROM memory for application data
- Compliance with ISO 7816 Parts 1,2,3,4,8,9
- ISO7816-2 compliant 8-contact module
- High baud rate switchable from 9.6 Kbps to 115.2 Kbps
- Supports ISO7816 Part 4 file structures: Transparent, Linear fixed, Linear Variable, Cyclic
- Hardware DES / Triple DES / SHA1 / RSA capability
- On-board RSA key generation of up to 2048 bit.
- AES-128 support.
- FIPS 140-2 compliant random number generator
- Mutual Authentication with Session Key generation
- Secure Messaging ensures data transfers are confidential and authenticated.
- Multilevel secured access hierarchy
- Anti-tearing ensures file headers and system information are protected.
- Common Criteria EAL5+ (Chip Level)
- FIPS140-2 compatible

1.2. Technical Specifications

1.2.1. Electrical

- Operates at 5V DC+/-10 %(Class A)
  3V DC +/-10% (Class B)
  1.8V DC +/-10% (Class C)
- Maximum supply current: <20 mA
- ESD protection: ≤ 5 KV

1.2.2. EEPROM

- Capacity: 32Kbytes
- EEPROM endurance: 500K Erase/Write cycles
- Data retention: 10 years

1.2.3. Environmental

- Operating temperature: -25 °C to 85 °C
- Storage temperature: -40°C to 100°C

1.3. Symbols and Abbreviations

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
CCT	Cryptographic Checksum Template
CRT	Chinese Remainder Theorem (RSA)
CRT	Control Reference Template
CT	Confidentiality Template
DES	Data Encryption Standard
DF	Dedicated File
DO	Data Object
DE	Data Element
DES	Data Encryption Standard
DST	Digital Signature Template
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
EF1	PIN File
EF2	KEY File
ESD	Electro-Static Discharge
HT	Hash Template
ISO	International Organization for Standardization
FCI	File Control Information
FCP	File Control Parameters
FDB	File Descriptor Byte
LCSI	Life Cycle Status Integer
LSb	Least Significant Bit
LSB	Least Significant Byte
MAC	Message Authentication Code
MF	Master File
MRL	Maximum Record Length
MSb	Most Significant Bit
MSB	Most Significant Byte
MSE	Management Security Environment
NOR	Number of Records
PSO	Perform Security Operation
RFU	Reserved for Future Use
RSA	Algorithm for 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	Secure Messaging
SM-enc	Secure Messaging for Confidentiality
SM-MAC	MAC for Secure Messaging
SM-Sign	Secure Messaging for Authenticity
TLV	Tag-Length-Value
UQB	Usage Qualifier Byte
XX_H	Hexadecimal representation of a byte.
||	Concatenate
⊕	Bitwise Exclusive OR

2.0. Card Management

This section outlines the card level features and management functions.

2.1. Anti Tearing

ACOS5 uses an anti-tearing mechanism in order to protect 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). On card reset, ACOS5 looks at the Anti-Tearing fields and does the necessary data recovery. In such case, the COS will return the saved data to its original address in the EEPROM.

2.2. Card Life States

ACOS5 has the following card states:

1. Pre-Personalization State
2. Personalization State
3. User State

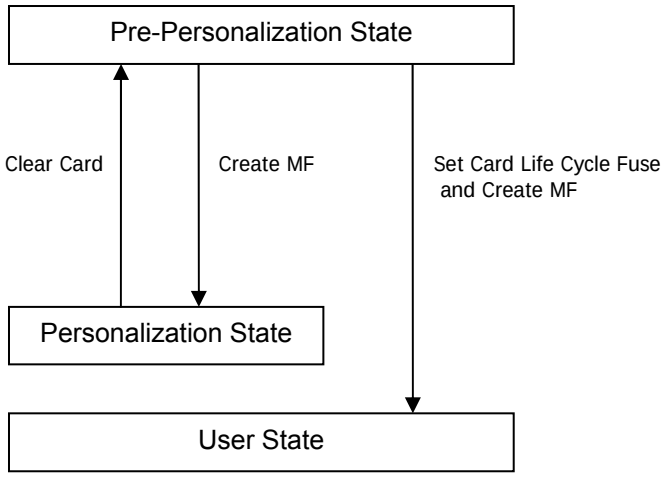

Figure 1. Card life cycle states

Pre-Personalization State – is the initial delivery state of the card from ACS. The card does not have a file system. In this state, the ATR TA1 (communication speed) and historical bytes can be personalized by writing directly to the card's physical memory. Users can create a MF with attributes according to their specifications.

Personalization State – card goes into this stage once the MF is successfully created from the previous stage. User can no longer directly access the card's header block. User can create and test files under the MF as if in Operational Mode.

A call to CLEAR CARD will return the card to Pre-personalization state. It is highly recommended to use the ACOS5 SDK's CLEAR CARD tool to clear the card. The tool will not only clear the card but also loads all the critical factory updates onto the card.

If application developers want to allow clear card but only after an authentication, a SAE condition can be set in MF and DF levels to limit the CLEAR CARD command after a PIN verification or KEY authentication.

User Stage – is equivalent to the card's Operational Mode, this is where all of the card's settings (security, file organizations, etc.) take effect.

2.3. Answer To Reset

After a hardware reset (e.g. power up), the card transmits an Answer-to-Reset (ATR) in compliance with ISO7816 part 3, and it follows the same format as that of ACOS2/3. ACOS5 supports the protocol type T=0 in direct convention. The following is the default ATR. For full descriptions of ATR options see ISO 7816 part 3.

Parameter	ATR	Description
TS	$3B_H$	Direct Convention.
T0	BE_H	TA1, TB1, TD1 follows with 14 historical characters.
TA1	18_H	Capable of high-speed data transfer.
TB1	00_H	No programming voltage required.
TD1	00_H	No further interface bytes follow.
T1	41_H	**Historical Data: Indicates ACOS Card**
T2	05_H	**Historical Data: Major version**
T3	01_H	**Historical Data: Minor version**
T4	00_H	These Historical bytes are not used.
T5	00_H	
T6	00_H	
T7	00_H	
T8	00_H	
T9	00_H	
T10	00_H	
T11	00_H	
T12	00_H	
T13	90_H	
T14	00_H	

Table 1. Default Configuration of the Answer-to-Reset

2.3.1. Customizing the ATR

ACOS5's ATR can be customized to change card speed or have specific identification information in the historical string. The new ATR must be compliant to ISO-7816 Part 3, otherwise the card may become unresponsive and non-recoverable at the next power-up or card reset.

The ATR can be customized in Pre-Perso Stage of the card.

3.0. File System

3.1. Hierarchical File System

ACOS5 is fully compliant to ISO 7816 Part 4 file system and structure. The file system is very similar to that of the modern computer operating system. The root of the file is the Master File (of MF). Each Application or group of data files in the card can be contained in a directory called a Dedicated File (DF). Each DF or MF can store data in Elementary Files (EF).

The ACOS5 allows arbitrary depth DF tree structure. That is, the DFs can be nested. Please see the figure below.

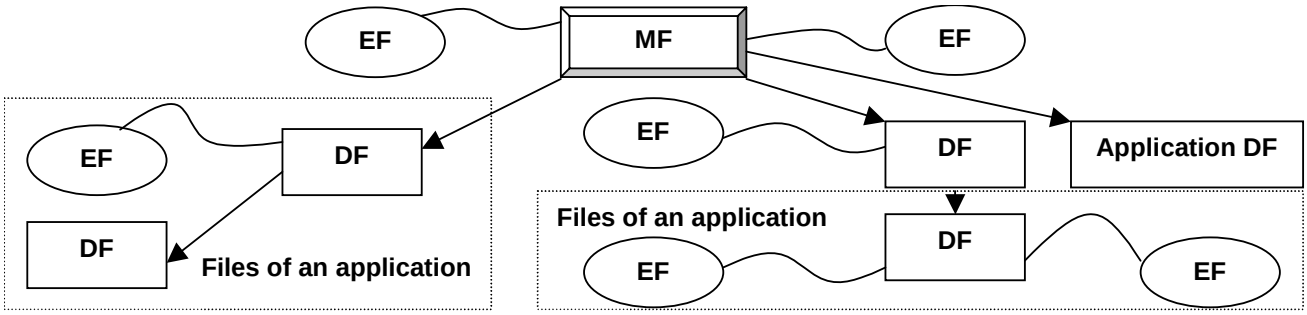

Figure 2. Example of hierarchy of DFs

3.2. File Header Data

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

The subsequent sections will describe each item in the header.

3.3. Internal Security Files

The behavior of the COS will depend on the contents of the security-related internal files. Typically, a DF should have: (1) a Key File to hold PIN codes (referred to as EF1) for verification, (2) a Key File to hold KEY codes (referred to as EF2) for authentication, (3) an SE file to hold security conditions and templates, and (4) an Asymmetric KEY EF to store RSA Keys.

A Key file is an Internal Linear Variable file. It may contain (1) PIN data structure or (2) KEY data structure.

4.0. Security

File commands are restricted by the COS 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. There can be a maximum of: 31 Global PINs, 31 Local PINs, 31 Global Keys, and 31 Local Keys at a given time.

4.1. File Security Attributes

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

4.2. Security Environment

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

<SE ID Template> <SE DO Template>

4.3. 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 or the execution of another mutual authentication procedure. The execution of a SELECT FILE command also ends a session.

4.4. Secure Messaging

Secure Messaging (SM) allows secured communication between the terminal/server backend and ACOS5. ACOS5 supports secure messaging for Authentication and Confidentiality.

There are 2 modes of SM that can be applied to two different situations. The first mode is SM for authenticity (*SM-sign*) the other is SM for confidentiality (*SM-enc*). The SM modes will be applied to both the command and response data.

5.0. Life Support Application

These products are not designed for use in life support appliances, devices, or systems where malfunction 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.

6.0. Contact Information

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

For sales inquiry please send e-mail to info@acs.com.hk