Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS3 Contact Smart Card

Functional Specifications V1.04

Subject to change without prior notice

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

Table of Contents

List of Figures

1.0. Introduction

The purpose of this document is to describe in detail the features and functions of the ACS Smart Card Operating Systems Version 3 (ACOS3) developed by Advanced Card Systems Ltd.

1.1. Features

- Full 32 KB or 72 KB of EEPROM for application data
- Compliance with ISO 7816 Parts 1, 2, 3; supporting the T=0 direct protocol
- For contact interface, the switchable baud rate from 9600 to 223200 bps is supported
- High-speed transmission rate (9.6 to 223.2 kbps) with modifiable ATR
- DES/Triple DES and MAC capability
- Five secret codes + issuer code
- PIN code that can be updated by card holder
- Key pair for mutual authentication
- Session key based on random numbers
- FIPS 140-2 compliant hardware based random number generator
- Binary files and record files that are available for user data storage
- Secure Messaging function for confidential and authenticated data transfers
- Support for highly secured e-Purse for payment applications

1.2. Technical Specifications

The following are the technical properties of the ACOS3 card:

1.2.1. Electrical

- Operating voltage: 5 VDC +/-10% (Class A) and 3 VDC +/-10% (Class B)
- Maximum supply current: < 10 mA
- ESD protection: ≤ 4 KV

1.2.2. EEPROM

- Capacity: 32 KB (32,768 bytes) or 72 KB (73,728 bytes)
- EEPROM endurance: 100K 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

2.0. Chip Life Cycle

During the whole life cycle of the chip-card, three phases and two different operating modes can be distinguished:

- Manufacturing State
- Personalization State
- User State
- User State - Issuer Mode

The card is at any moment in one of these four states. The following diagram shows the possible transitions between the four states:

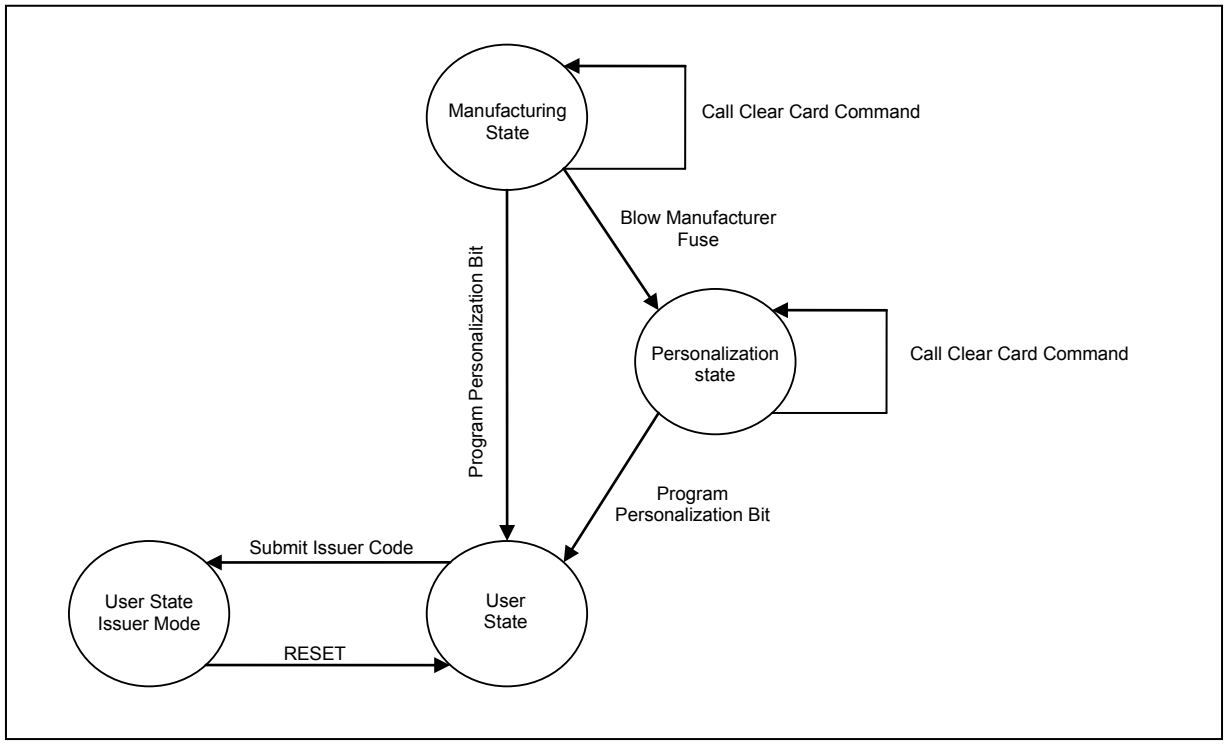

Figure 1: Chip Life Cycle Diagram

The actual chip life cycle state is determined by the card operating system immediately after a reset. The life cycle state does not change during the operation of the card. CLEAR CARD command can be issued in the personalization state and manufacture state to clear the card of all data except the manufacturer data and IC code. However, this command cannot be used to User State.

2.1. Manufacturing State

The ***Manufacturing State*** is effective from the moment of chip manufacturing until an associated fuse (i.e., a certain bit in the EEPROM), the *Manufacturer Fuse*, has been programmed.

The IC is presented to the card in plain, without encryption.

All commands are available in manufacturer state. In addition, the *Manufacturer File* (FF01h) can only be written in this state.

The manufacturer file contains two records, 8 bytes each, associated to the manufacturing state. In this file, it contains the *Manufacturer Fuse*. After programming the Manufacturer Fuse, the card enters the personalization state and the manufacturer file is on read-only. Data unique to each card and common card data can be programmed, such as, card manufacturer identification, card serial number,

etc. The card does not interpret the data.

In this state, the card's data and keys can be erased by calling the CLEAR CARD command. This command will physically erase the EEPROM memory except for the IC code and manufacturer file.

Once the manufacturer fuse has been blown the manufacturing state will be terminated, thus there is no possibility of resetting the card back into the manufacturing state.

2.2. Personalization State

Personalization State is effective from the moment of termination of the manufacturing state until an associated bit in the EEPROM, the so-called *Personalization Bit,* has been programmed.

In this state, the card's data and keys can be erased by calling the CLEAR CARD command. This command will physically erase the EEPROM memory except for the IC code and manufacturer file. Re-personalization of the card is possible.

In the Personalization State, any write access to Internal Data Files, as well as the read access to the Security File is only possible after the presentation of the correct IC code. The card manufacturer writes the IC code in the Manufacturing State.

The IC is presented to the card in plain, without encryption. The Authentication Process should not be executed prior to programming the correct keys in the Personalization State.

Once the Personalization Bit has been programmed and the Personalization State has thus been terminated, there is no possibility of resetting the card back into the personalization state.

2.3. User State

User State designates the normal operating mode of the card. There are two types of User States – the User State and the User State - Issuer Mode. The User State is effective from the moment of termination of the personalization state. Most card holder operation should occur in this state.

A submission of the Issuer Code changes the operation mode to Issuer Mode. This privileged mode allows access to certain memory areas, which are otherwise not accessible.

3.0. EEPROM Memory Management

The user EEPROM memory area provided by the card chip is fully usable for user data storage. There is an additional EEPROM area that stores internal card configuration data.

- The User Data Memory stores the data of the card under the control of the application.
- The internal card configuration data is used by the card operating system to manage card functionalities.

3.1. Data Files

Access to both the Internal Data Memory area and the User Data Memory area is possible within the scopes of data files and data records. Data files in the Internal Data Memory are referred to as *Internal Data Files*. Data files in the User Data Memory are called *User Data Files*.

Data files are the smallest entity to which individual security attributes can be assigned to control the read and write access to the data stored in the EEPROM.

Data files are of either record type or transparent type.

3.2. Data File Access Control

Two security attributes are assigned to each Data File: the Read Security Attribute and the Write Security Attribute. Security attributes define the security conditions that must be fulfilled to allow the respective operation:

- The Read Security Attribute controls the read access to the data in a file through the READ RECORD/BINARY command. If the security condition specified in the Read Security Attribute is not fulfilled, the card will reject a READ command to that file.
- The Write Security Attribute controls the write access to the data in a file through the WRITE RECORD/BINARY command. If the security condition specified in the Write Security Attribute is not fulfilled, the card will reject a WRITE command to that file.

The Read Security Attribute and the Write Security Attribute for each data file specify which Application Code, if any, were submitted correctly to the card to allow the respective operation, and whether the Issuer Code and/or the PIN code must have been submitted.

A logical OR function applies to the specified Application Codes, AC x, i.e., if more than one Application Code is specified in a security attribute, the security condition is fulfilled if any one of the specified Application Codes has been correctly submitted.

A logical AND function applies to the PIN and the IC code, i.e., if PIN and/or IC are specified in a security attribute, the PIN and/or IC code(s) must have been submitted in addition to the specified Application Codes(s).

3.3. Internal Data Files

With exception of the Account Data Structure, which has associated a special set of commands, the memory areas of the Internal Data Memory are processed as data files.

The attributes of the Internal Data Files are defined in the card operating system and cannot be changed. However, the security attributes depend on the card life cycle state.

3.4. User Data Files

User Data Files are allocated in the Personalization State of the card life cycle. There are two types of User Data Files, Record and Binary files. Record files are specified by number of records and a fixed record length. Binary files are specified by a file size and accessed via offsetting into the file.

The data stored in a User Data File can be read through the READ RECORD/BINARY command and updated through the WRITE RECORD/BINARY command when the security conditions associated to the data file are fulfilled.

User Data Files are defined by writing the corresponding File Definition Blocks in the records of the User File Management File during the Personalization State. It is not possible to change the number of records of a file once any of the User Data Files has been used. User will be able to access these data as long as it's within the capacity of the card.

3.5. Data File Access

The process of data file access is identical for Internal Data Files and for User Data Files.

3.6. Account Data Structure

The Account Data Structure - *Account*, for short - is dedicated for the use in applications in which a numeric value representing some 'amount' must be securely processed. The Account is stored in the Account File.

In the User State of the card life cycle, the data in the Account cannot be manipulated by WRITE instructions like the data in User Data Files. A set of dedicated instructions is available for the processing of the Account, i.e. for adding value to and subtracting value from the balance in the Account and for reading the current balance.

Different access conditions can be specified for adding to, subtracting from and reading the Account.

Critical Account operations, for example, CREDIT, are carried out under strict security control conditions.

4.0. Security Architecture

The following security mechanisms are provided by the ACOS3 card operating system:

- Anti-tearing mechanism
- DES/3DES and MAC calculation
- Mutual Authentication and Session Key based on Random Numbers
- Secret Codes
- Secure Messaging for data files
- Secure Account Transaction Processing

DES refers to the DEA algorithm for data encryption and decryption as specified in the standard ANSI X3.93. MAC refers to the algorithm for the generation of cryptographic checksums (DEA in Cipher Block Chaining mode) as specified in the standard ANSI X3.93.

Mutual Authentication is a process in which both the card and the Card Accepting Device verify that the respective counterpart is genuine. The Session Key is a result of the successful execution of the Mutual Authentication. It is used for data encryption and decryption during a 'session'. A session is defined as the time between the successful execution of a Mutual Authentication procedure and a reset of the card or the execution of another START SESSION command.

Secret Codes and the PIN code are used to selectively enable access to data stored in the card and to features and functions provided by the card, for example, the READ and WRITE commands.

Secure messaging ensures data transmitted between the card and terminal/server is secured and not susceptible to eavesdropping, replay attack and unauthorized modifications. This is achieved by signing the command and response with a MAC and encrypting command and response data.

The Account Transaction Processing provides mechanism for the secure and auditable manipulation of data in the Account Data Structure, in particular, the balance value.

4.1. DES and MAC Calculation

All keys used in DES/3DES and MAC calculation are 8/16 bytes long depending on Single/Triple DES selection in *Option Register*. The least significant bit of each byte of the key is not used in the calculation and is not interpreted by the card operating system.

4.2. Mutual Authentication and Session Key Generation

The Mutual Authentication is based on the exchange and mutual verification of secret keys between the Card and the Card Accepting Device. The key exchange is performed in a secure way by use of random numbers and DES/3DES data encryption.

The session key is the final result of the Mutual Authentication process and it is based on the random numbers of both card and terminal.

The successful completion of the Mutual Authentication is recorded in the card. The resulting Session Key K_S is used for all data encryption and decryption during the same session.

The card maintains an error counter CNT K_T to count and limit the number of consecutive unsuccessful executions of the AUTHENTICATE command.

The Card Random Number RND_C is derived in a complex non-predictable mathematical process from the Random Number Seed stored in the Security File. The Random Number Seed is internally updated by the Operating System after each START TRANSACTION command.

4.3. Secret Codes

Secret codes stored in the card are used to restrict the access to data stored in user data files and to certain commands provided by the card. Secret codes must be presented to the card in order to be able to read data from or write data to user data files and to execute certain privileged card

commands.

4.4. Secure Messaging

ACOS3 Version 1.07 and above support Secure Messaging (SM) for data files. Secure messaging ensures data transmitted between the card and terminal/server is secured and not susceptible to eavesdropping, replay attack and unauthorized modifications. User data file can be specified that secure messaging is required for READ/WRITE RECORD/BINARY commands. Almost all the other commands can also use secure messaging initiated by the terminal.

The SM employed in ACOS3 both encrypts and signs the data transmitting into and out of the card.

4.5. Account Transaction Processing

Associated to the Account are four keys:

- The Credit Key K_{CR}
- The Debit Key K_{D}
- The Certify Key K_{CF}
- The Revoke Debit Key K_{RD}

The keys are stored in the Account Security File.

The keys are used in the calculation and verification of MAC cryptographic checksums on commands and data exchanged between the card and the Card Accepting Device in the Account processing.

4.6. Anti-Tearing Mechanism

Anti-tearing mechanism help protects card data and security in the event that the card is suddenly powered down or pulled out during a card operation.

When writing user data into the card, ACOS3's anti-tearing mechanism ensures the operation is performed atomically. That is, data is either completely written or the target writing area is left at its previous state before the write operation. The account data file is protected similarly when performing CREDIT/DEBIT/REVOKE DEBIT commands.

5.0. ISO Compliance and Answer To Reset

After a hardware reset (e.g., power up), the card transmits an Answer To Reset (ATR) in compliance with the standard ISO 7816, Part 3. ACOS3 supports the protocol type T=0. The protocol type selection function is not implemented.

5.1. Customizing the ATR

There are two ways of customizing ACOS3's ATR. The first way is to add personalization information to the Personalization File FF 02h byte 1 to byte 8. This will be fetched upon power-up in the default ATR's historical bytes stated in the previous section.

In ACOS3, additional capabilities allow for the modification to the card's transmission speed or completely customizing the historical bytes based on the application developer's preference. These ATR modifications are achieved by writing to the internal file FF 07h after submission of the IC code.

6.0. 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.

7.0. Contact Information

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

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