Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS10 (Contactless)

Functional Specifications V1.00

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

Table of Contents

List of Figures

List of Tables

1.0. Introduction

The purpose of this document is to describe in detail the features and functions of the ACOS10 Contactless Card, a versatile smart card operating system developed by Advanced Card Systems Ltd.

1.1. Features

- Full 8 KB of EEPROM for application data
- Compliance with ISO 14443 Parts 1, 2, 3, 4
  - Supports T=CL protocol and fully compatible with ISO 14443 A
- High-speed transmission rate from 106 Kbps to 848 kbps
- DES/Triple DES capability
- Hardware based random number generator compliant to FIPS 140-2
- Secure Messaging function for confidential and authenticated data transfers
- PBOC 2.0 e-Deposit and e-Purse payment application support
- Multi-level secured access hierarchy
- Anti-tearing function support

1.2. Technical Specifications

The succeeding sections provide information on the technical properties of the ACOS10 Contactless Card:

1.2.1. Electrical

- Operating Voltage: 5 V DC +/-10% (Class A) and 3 V DC +/-10% (Class B)
- Maximum Supply Current: < 10 mA
- ESD Protection: ≤ 4 KV

1.2.2. EEPROM

- Capacity: 8 KB
- EEPROM Endurance: 500,000 erase/write cycles
- Data Retention: 20 years

1.2.3. Environmental

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

2.0. Card Management

This section outlines the card level features and management functions. ACOS10 Contactless has the following card states:

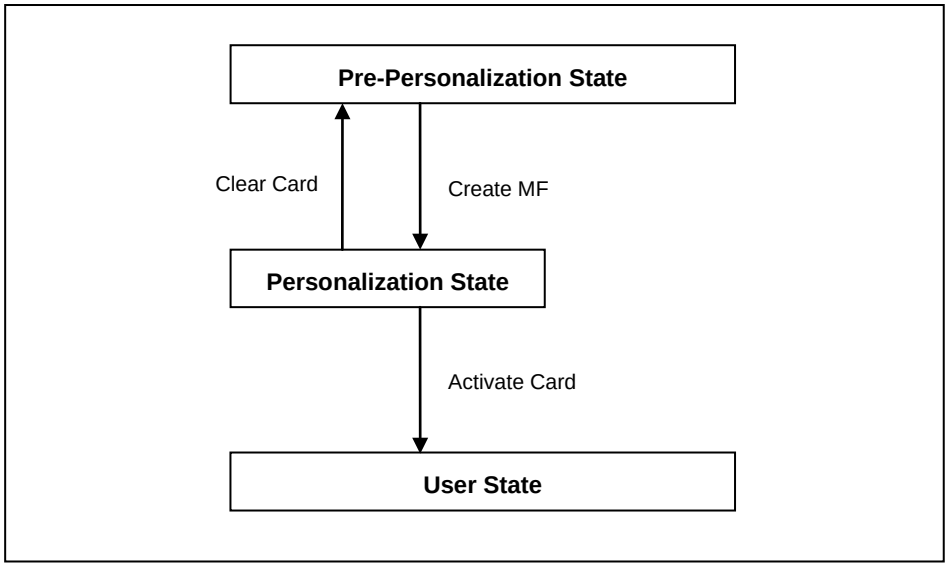

Figure 1: Card Life Cycle States

2.1.1. Pre-Personalization State

This is the initial state of the card.

2.1.2. Personalization State

The card goes into this state once the Master File (MF) is successfully created. During this state, the user can create and test the different files created in the card.

It is also important to note that the user can perform tests under this state and may revert to the Pre-Personalization State by using the CLEAR CARD command.

2.1.3. User State

After creating the desired file structure of the card, the user can now send the ACTIVATE CARD command so that the card will go to the User State.

After successfully running the ACTIVATE CARD command, the CLEAR CARD command will be disabled and the card can no longer go back to the previous state.

2.2. Typical Steps in Card Development

1. During the Personalization State, the user creates the card file structure, starting with the Master File (MF). Afterwards, the Dedicated File (DF) and different types of Elementary Files (EF) can be then created. Furthermore, the card's security design is tested in this state. If design flaws are found, the user can always return to the Pre-Personalization State using the CLEAR CARD command.
2. Once the card's file and security design are final and have been thoroughly tested, the user can then send the ACTIVATE CARD command to disable the CLEAR CARD command.
3. The card then goes into the User State and can no longer go back to previous states.

2.3. Answer To Select

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

3.0. File System

This section explores the file system of the ACOS10 Contactless Card.

3.1. Hierarchical File System

ACOS10 Contactless is fully compliant to ISO 7816 Part 4 file system and structure. The file system is similar to that of the modern computer operating system. The root of the file system is the **Master File (MF)**. Each application or group of data files in the card can be contained in a directory called a **Dedicated File (DF)**. The **Elementary Files (EF)** can be stored in the MF or the DF.

Furthermore, the ACOS10 Contactless allows arbitrary depth DF tree structure, which means that the DFs can be nested. Please see below an example of the ACOS10 Contactless File System Hierarchy:

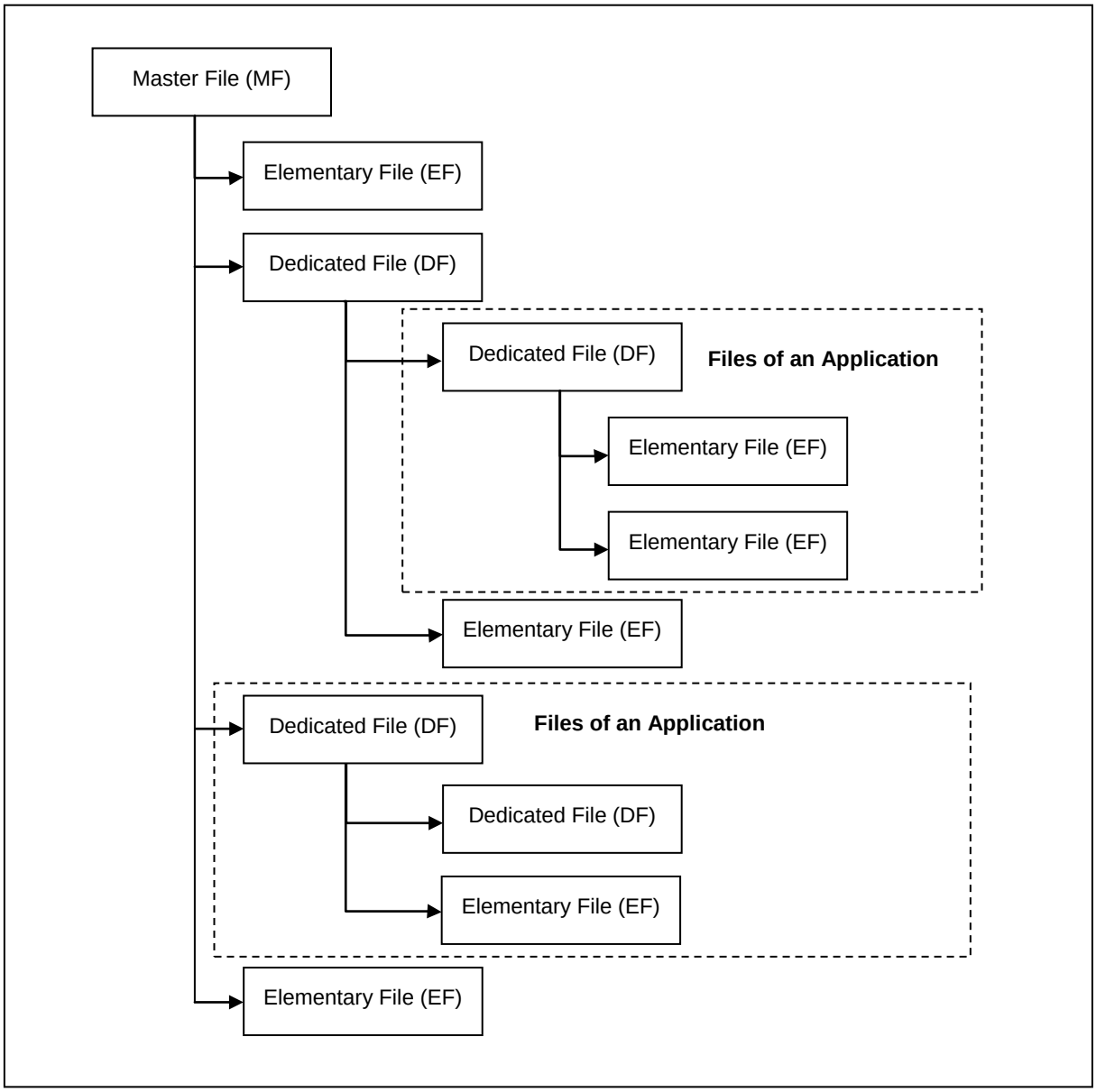

Figure 2: File System Hierarchy

3.2. File Header Data Structure

ACOS10 Contactless 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.

3.2.1. Master File

The Master File has the following file header data structure:

File Header	No. Bytes	Description
File Descriptor Byte (FDB)	1	This field indicates the file type: Master File: 3Fh
File ID	2	Note that the MF has a constant File ID which is 3F 00h.
FCI SFI	1	This field is the Short File ID of the FCI (File Control Information).
Issuer FCI SFI	1	This field is the Short File ID of the Issuer's FCI (File Control Information).
Access Condition	1	This byte contains the access condition under Current DF.
MF Name	5-16	For the MF, this field is the Long Name. The MF can be selected through its long name, which can be up to 16 bytes.

Table 1: Master File – File Header Data Structure

3.2.2. Dedicated File

The Dedicated File has the following file header data structure:

File Header	No. Bytes	Description
File Descriptor Byte (FDB)	1	This field indicates the file type: Dedicated File: 38h
File ID	2	This field uniquely identifies a file under the MF. The user can assign any file ID to the DF to uniquely identify it.
FCI SFI	1	This field is the Short File ID (SFI) of the FCI (File Control Information).
Issuer FCI SFI	1	This field is the Short File ID of the Issuer's FCI (File Control Information).
Access Condition	1	This byte contains the access condition under Current DF.
DF Name	5-16	For the DF, this field is the Long Name. The DF can be selected through its long name, which can be up to 16 bytes.

Table 2: Dedicated File – File Header Data Structure

3.2.3. Elementary File: Transparent /Binary File

Transparent or Binary File defines the data that is managed as a stream of bytes, which are addressed by an offset coming from the start of file.

3.2.4. Elementary File: Linear Fixed File

Linear Fixed File is the data grouped into records, which is a block of bytes with a pre-defined size. Likewise, data fields that are related are grouped into one record.

3.2.5. Elementary File: Linear Variable File

Linear Variable File is similar with Linear Fixed Variable, except that each record in *Linear Variable File* has variable sizes.

3.2.6. Elementary File: Cyclic File

Cyclic File is similar with Linear Fixed Variable, but it logically has no “last record.” An application views this file as having no limit, but in reality, the oldest record is overwritten with the newest record in the file.

3.2.7. Elementary File: PIN File

The PIN File is used for access control by using the VERIFY PIN command.

3.2.8. Elementary File: Key File

The Key File is used for access control and is needed for various authentication commands.

3.2.9. Elementary File: Electronic Deposit File

The Electronic Deposit (ED) File is specifically used for e-Deposit transactions.

3.2.10. Elementary File: Electronic Purse File

The Electronic Purse (EP) File is specifically used for e-Purse transactions.

3.2.11. Elementary File: Transaction Log File

The Transaction Log File is specifically used to store e-Deposit and e-Purse transactions.

4.0. Security Features

This chapter illustrates the access rights and security capabilities of the ACOS10 Contactless card along with its environment and usage. They are:

- File Security Attributes
- Secure Messaging
- Mutual Authentication
- Key Injection
- Anti-tearing Mechanism

Furthermore, the different file commands are restricted by the Card Operating System (COS) depending on the target file's security Access Conditions (AC). 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 residing in a PIN EF, directly under the MF. Likewise, Local Keys are KEYs residing in a KEY EF, under the currently selected DF. There can be a maximum of 14 Global PINs, 14 Local PINs, 14 Global Keys and 14 Local Keys at a given time.

4.1. File Security Attributes

Each MF and DF has a one-byte Access Condition (AC) byte for creating file access conditions. On the other hand, each EF file has a three-byte Access Condition for read and update access condition.

4.2. Secure Messaging

There are two Secure Messaging (SM) modes available for ACOS10 Contactless, namely:

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

4.3. Mutual Authentication

Mutual Authentication is a process in which both card and card-accepting device verify that the respective unit is genuine. A *Session Key* is the result of a successful execution of mutual authentication and 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.

4.4. Key Injection

Key Injection can be used to securely load a key or a diversified key from an ACOS6-SAM card into a client ACOS10 Contactless card. For the purpose of key injection, we shall refer to the ACOS6-SAM card with the key to inject as the "source SAM" and the ACOS10 Contactless card to receive the key the *"target SAM."*

This function allows a 'master and subordinate' SAM relationship and the subordinate SAM can perform different specific operations.

The target SAM uses the *Set Key* command while the source SAM will use the *Get Key* command to perform key injection.

Note: *The key injection feature is available for ACOS6-SAM. Kindly refer to the ACOS6-SAM Reference manual for more information about this feature.*

4.5. Anti-tearing Mechanism

ACOS10 Contactless uses an anti-tearing mechanism in order to protect the card from data corruption due to card tearing, which happens when the card is suddenly pulled out of the reader during data update or when the reader suffers from mechanical failure during the card data update. On card reset, ACOS10 Contactless 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.

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 customer 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.