Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS10 (Contactless)

Functional Specifications V1.08

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. History of Modification

Date	Changes
2012/03/05	**ACOS10 revision 6.01** • Support for PBOC 2.0 e-Deposit and e-Purse payment applications
2014/05/06	**ACOS10 revision 6.04** • Updated to new IC platform. All functionality remains the same. • Changed the default values of the ATR and the ATS
2015/08/11	**ACOS10 revision 6.08** • Added MIFARE 1K emulation

Table 1: History of Modification for ACOS10 Combi

1.2. Symbols and Abbreviations

Abbreviation	Description
3DES	Triple DES
AID	Application/Account Identifier
AMB	Access Mode Byte
AMDO	Access Mode Data Object
APDU	Application Protocol Data Unit
ATC	Account Transaction Counter
ATR	Answer to Reset
CHV	Card Holder Verify
COMPL	Bit-wise Complement
COS	Card Operating System
DEC (C, K)	Decryption of data C with key K using DES or 3DES
DES	Data Encryption Standard
DF	Dedicated File
ED	Electronic Deposit
ENC (P, K)	Encryption of data P with key K using DES or 3DES
EF	Elementary File
EF1	PIN File
EF2	KEY File
FCI	File Control Information
FCP	File Control Parameters
FDB	File Descriptor Byte

Abbreviation	Description
GSESPK	Session key of Grey Lock
ID	Identifier
INS	Instruction Byte of Command Message
LCSI	Life Cycle Status Integer
LEN	Length
LSb	Least Significant Bit
LSB	Least Significant Byte
MAC	Message Authentication Code
MF	Master File
MOC	Ministry of Construction
MRL	Maximum Record Length
MSb	Most Significant Bit
MSB	Most Significant Byte
NA	No Application
NOR	Number of Record
PBOC	Peoples Bank of China
PIN	Personal Identification Number
PSE	Payment System Environment
RFU	Reserved for Future Use
RMAC	Retail MAC
SAC	Security Attribute – Compact
SAE	Security Attribute – Expanded
SAM	Security Authentication Module
SC	Security Condition
SCB	Security Condition Byte
SFI	Short File Identifier
SM-MAC	Secure Messaging with MAC
SM-ENC	Secure Messaging with Encryption
SW1	Status Word One
SW2	Status Word Two
TAC	Transaction Authorization Cryptogram
TC	Transaction Counter
TLV	Tag-Length-Value
TTI	Transaction Type Indicator
UQB	Usage Qualifier Byte
||	Concatenation

Table 2: Symbols and Abbreviations

2.0. Technical Specifications

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

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

2.2. Environmental

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

2.3. Communication Protocol

- T=0 with baud up to 223.2 Kbps
- T=CL with baud up to 848 Kbps

2.4. Memory

- Capacity: 8KB
- EEPROM Endurance: 500,000 erase/write cycles
- Data retention: 10 years

2.5. Cryptographic Capabilities

- DES, 3DES (56/112-bits)
- MAC

2.6. File Security

- FIPS 140-2 compliant hardware based random number generator
- 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

2.7. Answer to Select (ATS)

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.

The following table shows the default ATS. For full descriptions of the ATS, kindly refer to ISO 14443 Part 4.

Parameter	ATS	Description
TL	08h	Length byte
T0	78h	Format byte … codes Y(1) and FSCI

Parameter	ATS	Description
TA1	33h	Interface bytes … codes DS and DR
TB1	B5h	Codes FWI and SFGI
TC1	02h	Codes protocol options
T1	41h	Indicates ACOS Card
T2	10h	Major Version
T3	08h	Minor version

Table 3: Answer-to-Select

Refer to **Section 3.3** for more information.

2.8. Compliance to Standards

- Compliance with ISO 14443 Parts 1, 2, 3, and 4

3.0. Card Management

This section outlines the card level features and management functions.

3.1. Card Life Cycle States

ACOS10 Contactless has the following card states:

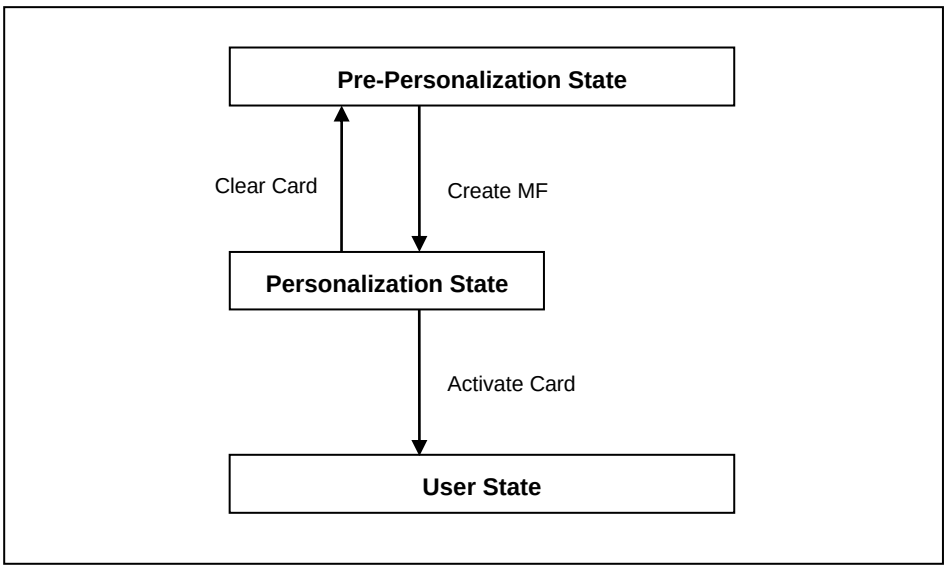

Figure 1: Card Life Cycle States

3.1.1. Pre-Personalization State

This is the initial state of the card.

3.1.2. 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.

3.1.3. 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.

3.1.4. 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.

3.2. 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.

3.3. Customizing the ATS

The ATR/ATS can be customized with custom TA1 values and historical bytes. The TA1 byte can be customized to increase the baud rate of the card. The Historical bytes can also be customized to have unique application identifiers.

Due to the difference in the firmware architecture between the ACOS10 Combi/Contactless IC and the ACOS10 contact IC, the TA1 value and historical byte must be modified at the ACS production facilities. Please contact your ACS representatives during ordering for custom TA1 and Historical bytes values.

3.3.1. Customized ATS TA1 value

The contactless protocol currently has TA1 = 33h as its bit rate capability. This means the card supports 106, 212, 424 kbps for both directions from PICC to PCD and vice versa. This is stated in ISO 14443 Part 4 Section 5.2.4. The ACOS10 Combi card can support up to 848 kbps by setting the TA1 value to 77h.

Similar to contact TA1 customization, the solution provider should ensure that the baud rate works with all their existing contactless smart card readers (PCDs) before a volume order of ACOS10 Combi cards. Please contact your ACS representatives for more information.

3.3.2. Customized ATR/ATS for Microsoft Windows Usage

For Windows® 7 and above operating systems: Windows automatically attempts to download the smart card's minidriver whenever a smart card is presented to the smart card reader. Since ACOS10 Combi is not intended to conform to Windows default usage, such smart card minidriver is not necessary. However, if the ACOS10 Combi is inserted into a Windows system, Windows may search online for the driver and may give a warning that the "device driver was not successfully installed" for the smart card. There are two ways to solve this issue:

1. Disable smart card plug and play and certificate propagation in Windows.
2. Change the ATS so Windows will recognize the ACOS10 Combi smart card to use ACS's Unified Null Driver.

For the first solution, please follow instructions in this Microsoft® support link to disable smart card plug and play. This may have to be done for every computer that will be used in this system. http://support.microsoft.com/kb/976832.

For the second solution, ACS has developed a Unified Null driver for the ACOS line of smart cards. The Unified Null driver will satisfy the Windows requirement to have a minidriver for the card, hence the warning from Windows every time the card is inserted will now be removed. In order for Windows to recognize the ACOS10 Combi smart card to use the Unified Null Driver, the ATR must be customized. The ATS customization will be done by ACS. Please contact your ACS representative for more information.

In the case of ACOS10 Contactless, the ATS should be:

ATS: 08 78 XX B5 02 41 4e 44h

The XX is the value of TA1. The TA1 value can be set to the baud rate that the smart card reader used can support. After the customization, these will be the customized value of the ATS:

ATS: 08 78 33 B5 02 41 4e 44h

4.0. File System

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

4.1. 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:

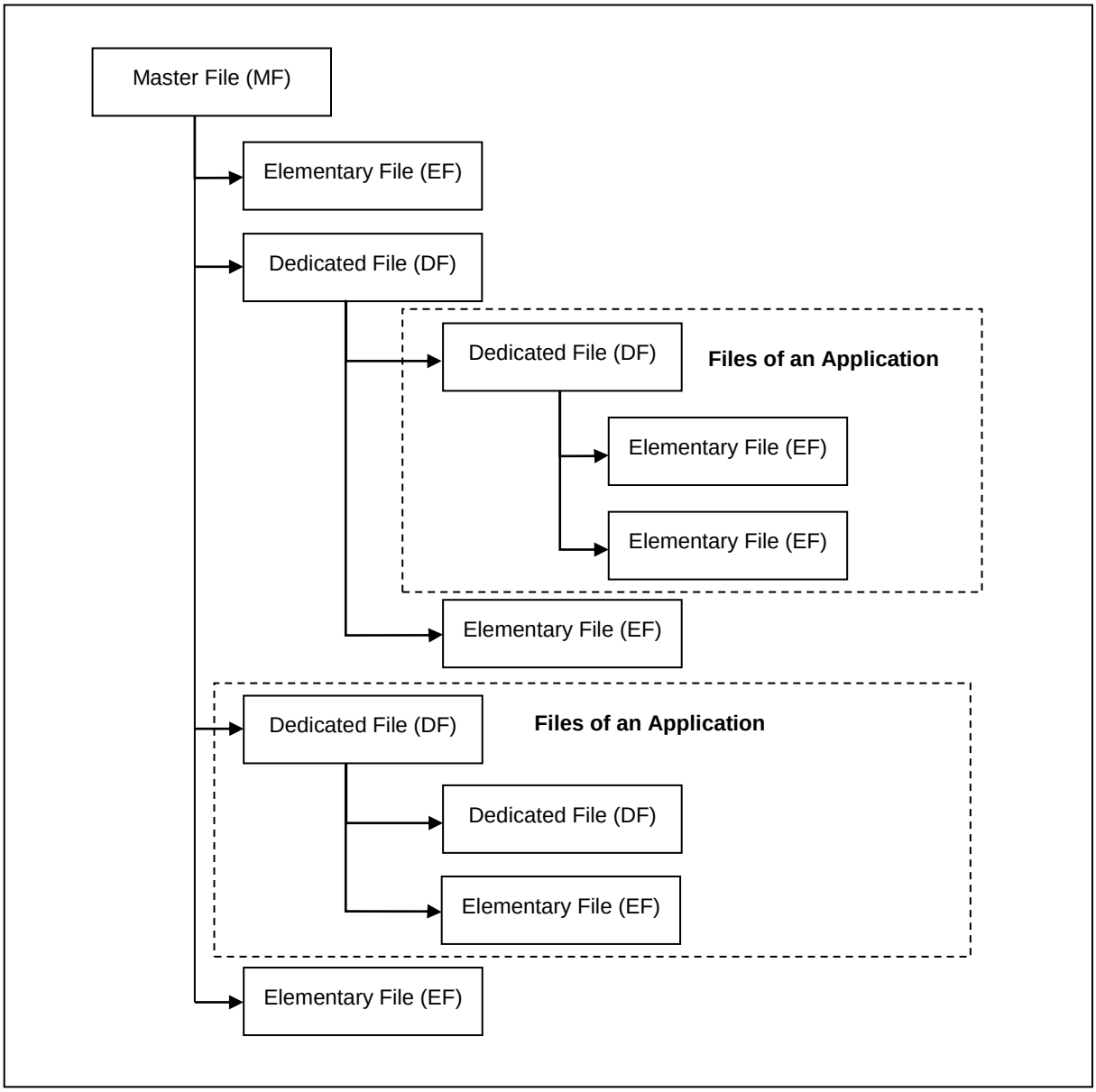

Figure 2: File System Hierarchy

4.2. 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.

4.2.1. 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 4: Master File – File Header Data Structure

4.2.2. 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 5: Dedicated File – File Header Data Structure

4.2.3. 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.

4.2.4. 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.

4.2.5. 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.

4.2.6. 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.

4.2.7. Elementary File: PIN File

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

4.2.8. Elementary File: Key File

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

4.2.9. Elementary File: Electronic Deposit File

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

4.2.10. Elementary File: Electronic Purse File

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

4.2.11. Elementary File: Transaction Log File

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

5.0. 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.

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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.*

5.5. 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.

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 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.

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.