Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-V

Functional Specification V1.00

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

Table of Contents

List of Figures

List of Tables

1.0. Overview

ACOSJ-V is a smart card operating system developed by Advanced Card Systems Ltd. It works based on the JAVA Card Virtual Machine and complies with GlobalPlatform Card Specification Version 2.2.1, JAVA Card Specification Version 3.0.4 and Mapping Guidelines 1.0.1 on its functions and configurations. It is a bank card product for Visa® payment application available as dual-interface.

The purpose of this document is to describe the features and functions of the ACOSJ-V smart card operating system.

1.1. Symbols and Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ATR	Answer-to-Reset
ATQ	Answer-to-Request (for contactless cards)
BCD	Binary Coded Decimal
BER	Basic Encoding Rules
CAT	Card Application Toolkit; or Cryptographic Authorization Template
CBC	Cipher Block Chaining
CCT	Control Reference Template for Cryptographic Checksum
CIN	Card Image Number/Card Identification Number
CLA	Class byte of the command message
CRT	Control Reference Template
CT	Control Reference Template for Confidentiality
CVM	Cardholder Verification Method
DAP	Data Authentication Pattern
DEK	Data Encryption Key
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DST	Control Reference Template for Digital Signature
ECB	Electronic Code Book
EMV	Europay, MasterCard, and VISA; used to refer to the ICC Specifications for Payment Systems
ENC	Encryption
FCI	File Control Information
HEX	Hexadecimal
HMAC	Keyed-Hash Message Authentication Code
ICC	Integrated Circuit Card

Abbreviation	Description
ICV	Initial Chaining Vector
IIN	Issuer Identification Number
INS	Instruction byte of the command message
ISO	International Organization for Standardization
Lc	Exact length of data in a case 3 or case 4 command
Le	Maximum length of data expected in response to a case 2 or case 4 command
LV	Length Value
MAC	Message Authentication Code
MEL	MULTOS Executable Language. The instruction set of the MULTOS™ runtime environment
OID	Object Identifier
P1	Reference control parameter 1
P2	Reference control parameter 2
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RAM	Random Access Memory
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
ROM	Read-only Memory
RSA	Rivest/Shamir/Adleman asymmetric algorithm
SCP	Secure Channel Protocol; or (ETSI) Smart Card Platform
SW	Status Word
SW1	Status Word One
SW2	Status Word Two
TLV	Tag Length Value
TP	Trust Point
'xx'	Hexadecimal values are expressed as hexadecimal digits between single quotation marks
'X'	A value in a cell of a table whose purpose is described in the 'Meaning' column of the table
'-'	A value (0 or 1) in a cell of a table that does not affect the 'Meaning' given for that row of the table

Table 1: Symbols and Abbreviations

2.0. Specifications

2.1. Features

- Supports T=0 protocol
- Supports T=CL protocol
- Supports AES
- Supports DES/3DES
- Supports RSA (768 to 2048 bits)
- Supports SHA1/SHA224/SHA256/SHA384/SHA512
- Compliance with ISO 7816 Parts 1, 2, 3, 4
- Compliance with ISO 14443
- Compliance with JAVA Card Specification Version 3.0.4
- Compliance with Global Platform Specification Version 2.2.1
- Compliance with Mapping Guidelines 1.0.1
- Compliance with VIS 1.5.4b
- Compliance with VCPS 2.1.3b
- Compliance with Visa Prepaid 1.1.3a

2.2. Technical Specifications

2.2.1. Electrical

- Operating Voltage: 2.1 V – 5.5 V
- Maximum External Clock Frequency: 10 MHz
- Maximum CPU Clock Frequency: 28 MHz
- ESD Protection: ≤ 5 KV

2.2.2. EEPROM

- Capacity: 60 KB
- EEPROM Endurance: 500,000 erase/write cycles (25°C)
- Data Retention: 30 years (25°C)

2.2.3. Environmental

- Operating Temperature: -25°C – 85°C

2.3. Answer-to-Reset (ATR, Contact Card)

After a card reset (e.g., power up) is performed, the card transmits an Answer-to-Reset (ATR) in compliance with ISO 7816 Part 3. ACOSJ supports the contact protocol type T=0 with direct or inverse convention.

2.4. Answer to Select (ATS, Contactless Card)

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

3.0. Card Life Cycle States

The ACOSJ-V has five card states: OP_READY, INITIALIZED, SECURED, CARD_LOCKED and TERMINATED. The figure below shows the card life cycle state transition:

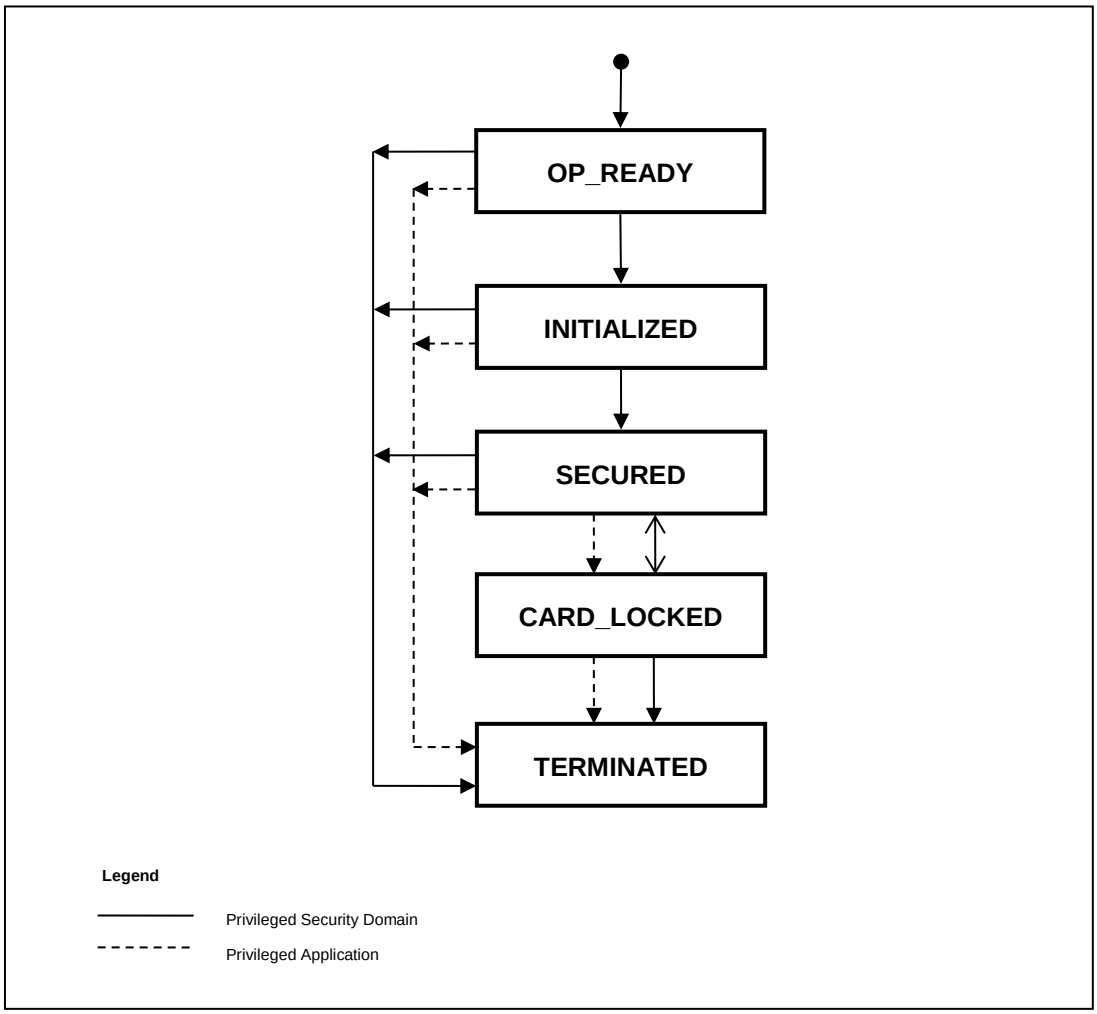

Figure 1: Card Life Cycle

3.1. OP_READY

This state indicates that the runtime environment shall be available and the Issuer Security Domain, acting as the selected Application, shall be ready to receive, execute and respond to APDU commands.

The card shall be capable of Card Content changes, the loading of the Load Files containing applications not already present in the card may occur.

The installation, from Executable Load Files, of any Application may occur.

Additionally, if any personalization information is available at this stage, Applications may be personalized.

3.2. INITIALIZED

This state is an administrative card production state. The state transition from OP_READY to INITIALIZED is irreversible. Its functionality is beyond the scope of this Specification. This state may be used to indicate that some initial data has been populated (e.g., Issuer Security Domain keys and/or data) but the card is not yet ready to be issued to the Cardholder.

3.3. SECURED

This state is the intended operating card Life Cycle State in Post-Issuance. This state may be used by Security Domains and Applications to enforce their respective security policies. The state transition from INITIALIZED to SECURED is irreversible.

The SECURED state should be used to indicate to off-card entities that the Issuer Security Domain contains all necessary keys and security elements for full functionality.

3.4. CARD_LOCKED

The card Life Cycle state CARD_LOCKED is present to provide the capability to disable the selection of Security Domain and Applications. The card Life Cycle state transition from SECURED to CARD_LOCKED is reversible.

Setting the card to the CARD_LOCKED state means that the card shall only allow selection of the application with the Final Application privilege.

Card Content changes, including any type of data management (specifically Security Domain keys and data), are not allowed in this state.

3.5. TERMINATED

This state signals the end of the card Life Cycle and the card. The state transition from any other state to TERMINATED is irreversible.

The state TERMINATED shall be used to permanently disable all card functionality with respect to any card content management and any life cycle changes. This card state is intended as a mechanism for an Application to logically 'destroy' the card for such reasons as the detection of a severe security threat or expiration of the card. If a Security Domain has the Final Application privilege only the GET DATA command shall be processed, all other commands defined in this specification shall be disabled and shall return an error. If an application has the Final Application privilege its command processing is subject to issuer policy.

The OPEN itself, or a Security Domain with Card Terminate privilege, or an Application with Card Terminate privilege (see GlobalPlatform Card Specification Version 2.2.1), may initiate the transition from any of the previous states to the state TERMINATED.

4.0. Card Architecture

To meet the GlobalPlatform specification for Java card, the ACOSJ-V card has the architecture for applications as shown in the figure below:

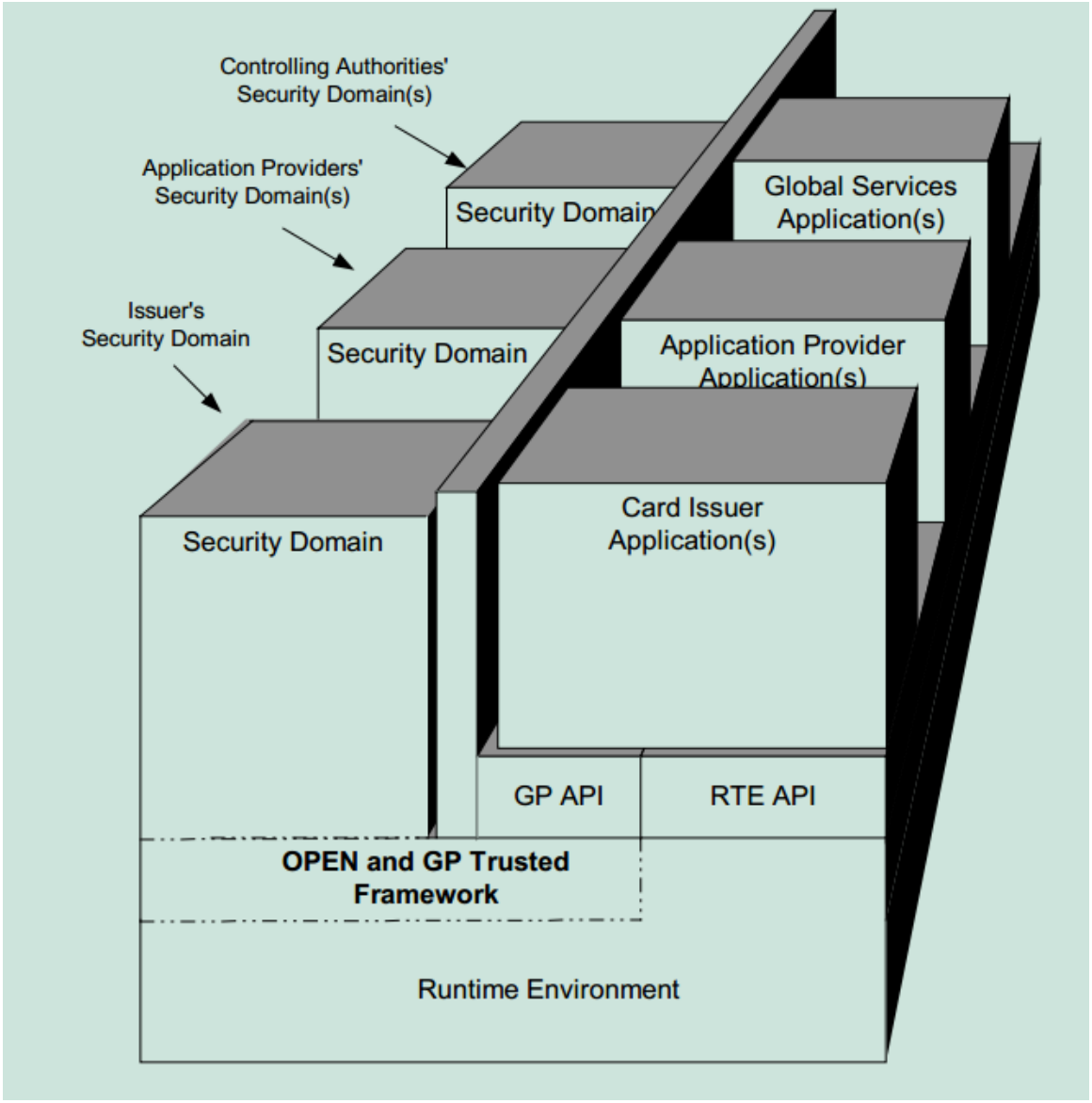

Figure 2: ACOSJ-V System Architecture

5.0. VSDC Applet

5.1. VSDC Applet Introduction

The VSDC 2.8.1G have loaded in the ACOSJ-V before delivery. The general information is shown in the table below:

Item	Description
Manufacturer	Visa International Service Association
Applet Name	VSDC 2.8.1G
Applet Type And Version	Visa Smart Debit Credit(VSDC) 2.8.1G
Platform Product Was Tested On	GlobalPlatform
VTF# Of Product Tested On	LBADVA03075A
Protocol	T=0 , T=TypeA

Table 2: VSDC General Information

The following are the applets that are supported by VSDC2.8.1G：

- Visa Smart Debit/Credit
- Quick Visa Smart Debit/Credit
- Visa prepaid

5.2. Personalization

This applet supports the EMV Card Personalization Specification (EMV CPS) version 1.1. This specification is available from EMVCo.

For additional personalization support, refer to VSDC Personalization Specification version 2.0.

6.0. ACOSJ-V ROOT Application

The commands in the ROOT application can be used only after the ROOT application is correctly selected (using the select command and transmission key). After entering into the ROOT Application, the user can read or configure card parameters through commands supported by the ROOT Application. To exit ROOT Application and select another application, the card must be reset.

Under the ROOT Application, parameters of the card can be read or configured.

The ROOT Application will become invalid once the card is activated.

6.1. ACOSJ-V ROOT Application Command Reference

6.1.1. SELECT Command

6.1.1.1. Definition and Scope

The SELECT command is used to select the ROOT application.

6.1.1.2. Processing State Returned in the Response Message

A successful execution of the command shall be indicated by status bytes 90 00h.

6.1.2. READ Command

6.1.2.1. Definition and Scope

This command is used to read from the configuration area. Configuration parameters of the card can be read through this command.

6.1.2.2. Data Field returned in the Response Message

The read configuration data.

6.1.2.3. Processing State returned in the Response Message

A successful execution of the command shall be indicated by status bytes 90 00h.

6.1.3. WRITE Command

6.1.3.1. Definition and Scope

This command is used to write data to the configuration area. Configuration parameters of the card can be set through this command.

6.1.3.2. Data Field returned in the Response Message

The data field of the response message shall not be present.

6.1.3.3. Processing State returned in the Response Message

A successful execution of the command shall be indicated by status bytes 90 00h.

6.1.4. ACTIVE Command

6.1.4.1. Definition and Scope

This command is used to activate the card. Once this command is implemented successfully, the ROOT Application will become invalid, and the configuration data of the card cannot be read or set directly any more.

6.1.4.2. Data Field returned in the Response Message

The data field of the response message shall not be present.

6.1.4.3. Processing State returned in the Response Message

A successful execution of the command shall be indicated by status bytes 90 00h.

7.0. ACOSJ-V IDENTIFY Application

7.1. ACOSJ-V IDENTIFY Application Description

After the IDENTIFY Application is selected with a SELECT Command, ACOSJ-V will return the version number of ACOSJ-V and indicates whether the card has been activated.

7.2. ACOSJ-V IDENTIFY Application Command Reference

7.2.1. SELECT Command

7.2.1.1. Definition and Scope

The SELECT command is used for selecting the IDENTIFY Application.

7.2.1.2. Response Message

7.2.1.2.1. Data Field returned in the Response Message

The SELECT response data field consists of information specific to the selected Application.

7.2.1.2.2. Processing State returned in the Response Message

A successful execution of the command shall be indicated by status bytes 90 00h.

Appendix A. References

The documents below served as references for the ACOSJ Reference Manual.:

- GlobalPlatform Card Specification Version 2.2.1
- GlobalPlatform Card API Version 1.6
- Java Card 3 API, Classic Edition Version 3.0.4
- Java Card 3 Platform Runtime Environment Specification, Classic Edition Version 3.0.4 September 2011
- Java Card 3 Platform Virtual Machine Specification, Classic Edition Version 3.0.4 September 2011
- GlobalPlatform Card Mapping Guidelines of Existing GP v2.1.1 Implementation on v2.2.1 Version 1.0.1
- Visa Integrated Circuit Card Specification (VIS) Version 1.5.4b
- Visa Contactless Payment Specification (VCPS) version 2.1.3b
- Pilot Visa Prepaid Chip Specification 1.1.3a

EMV is a registered trademark of EMVCo LLC in the United States and other countries.
MULTOS is a registered trademark of MAOSCO Limited.
Visa is a registered trademark of Visa International Service Association.