



Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-P



Functional Specifications V1.06



Table of Contents

| | | |
|--------------|---|-----------|
| 1.0. | Overview | 4 |
| 1.1. | Target Audience | 4 |
| 1.2. | History of Modification for ACOSJ-P | 4 |
| 1.3. | Symbols and Abbreviations | 4 |
| 1.4. | Reference Documents | 6 |
| 2.0. | Card Specifications | 7 |
| 2.1. | Electrical | 7 |
| 2.2. | Environmental | 7 |
| 2.3. | Communication Protocols | 7 |
| 2.4. | Memory | 7 |
| 2.5. | Cryptographic Capabilities | 7 |
| 2.6. | Compliance to Standards | 7 |
| 2.7. | Application Installation Parameters | 8 |
| 2.8. | ATR (Contact Cards) | 8 |
| 3.0. | Card Life Cycle States | 10 |
| 4.0. | Personalization Data Management | 11 |
| 5.0. | Safety Management Mechanism | 12 |
| 5.1. | Session Key Calculation Method | 12 |
| 6.0. | Personalization Command | 13 |
| 6.1. | PBOC3.0 Debit/Credit Application Personalization Commands | 13 |
| 6.2. | INITIALIZE UPDATE | 13 |
| 6.3. | EXTERNAL AUTHENTICATE | 13 |
| 6.4. | STORE DATA | 13 |
| 7.0. | PBOC 3.0 Debit/Credit Application Dedicated Commands | 14 |
| 7.1. | SELECT | 14 |
| 7.2. | READ RECORD | 14 |
| 7.3. | GET DATA | 14 |
| 7.4. | GET RESPONSE | 14 |
| 7.5. | GET PROCESSING OPTIONS | 14 |
| 7.6. | INTERNAL AUTHENTICATE | 14 |
| 7.7. | VERIFY | 15 |
| 7.8. | GENERATE AC | 15 |
| 7.9. | EXTERNAL AUTHENTICATE | 15 |
| 7.10. | APPLICATION BLOCK | 15 |
| 7.11. | APPLICATION UNBLOCK | 15 |
| 7.12. | CARD BLOCK | 15 |
| 7.13. | PUT DATA | 16 |
| 7.14. | PIN CHANGE/UNBLOCK | 16 |
| 7.15. | UPDATE RECORD | 16 |
| 8.0. | Transaction Process | 17 |
| 8.1. | QPBOC Transaction Process | 17 |
| 8.2. | Debit/Credit (EC) Transaction Process | 18 |
| 9.0. | Life Support Application | 20 |
| 10.0. | Contact Information | 21 |

List of Figures

| | | |
|-------------------|------------------------------|-----------|
| Figure 1 : | Card Life Cycle | 10 |
|-------------------|------------------------------|-----------|



Figure 2 : ACOSJ-P Support QPBOC Transaction Process 17
Figure 3 : ACOSJ-P Support Standard PBOC3.0 Debit/Credit Transaction Process 19

List of Tables

Table 1 : History of Modification for ACOSJ-P..... 4
Table 2 : Symbols and Abbreviations..... 6
Table 3 : Application Installation Parameters 8
Table 4 : ATR Protocol Bytes 8
Table 5 : ATR Historical Bytes..... 9



1.0. Overview

The ACOSJ-P is a highly secure smart card that has a built-in PBOC 3.0-certified Java applet, making it the perfect solution for PBOC 3.0 debit/credit applications and QPBOC applications. It complies with Java Card Specification v3.0.4, GlobalPlatform Specification v2.2.1, and Mapping Guidelines 1.0.1. It supports DES, 3DES, 3KDES, AES, RSA, SHA1, SM2, SM3 and SM4. This document describes the features and functions of the ACOSJ-P.

1.1. Target Audience

This document is intended for software developers and technical specialists. The user is expected to be knowledgeable in the creation of banking applications.

1.2. History of Modification for ACOSJ-P

| Version | Date Released | Modifications |
|---------------|---------------|---|
| ACOSJ-P v1.01 | November 2016 | <ul style="list-style-type: none"> 12KB EEPROM Operating Voltage: Contact Only 1.62V to 5.5V, Dual Interface 2.7V to 5.5V |

Table 1: History of Modification for ACOSJ-P

1.3. Symbols and Abbreviations

| Abbreviation | Description |
|--------------|---------------------------------------|
| 3DES | Triple DES |
| AAC | Application Authentication Cryptogram |
| AAR | Application Authorization Referral |
| AC | Application Cryptogram |
| AFL | Application File Locator |
| ARPC | Authorization Response Cryptogram |
| ARQC | Authorization Request Cryptogram |
| AID | Application/Account Identifier |
| AIP | Application Interchange Profile |
| APDU | Application Protocol Data Unit |
| ATC | Application Transaction Counter |
| ATR | Answer To Reset |
| CA | Certificate Authority |
| CDA | Combined DDA/AC Generation |
| CDOL | Card Risk Management Data Object List |
| CID | Cryptogram Information Data |
| CKV | Check Key Value |
| CLA | Class byte of APDU commands |
| CM | Card Manager |
| CVM | Cardholder Verification Method |
| CVR | Card Verification Result |



| Abbreviation | Description |
|--------------|--|
| COS | Card Operating System |
| DDA | Dynamic Data Authentication |
| DOL | Data Object List |
| DDOL | Dynamic Data Authentication Data Object List |
| DES | Data Encryption Standard |
| DF | Dedicated File |
| DGI | Data Group Index |
| DEC(C, K) | Decryption of data C with key K using DES or 3DES |
| ENC(P, K) | Encryption of data P with key K using DES or 3DES |
| EF | Elementary File |
| FCI | File Control Information |
| GPO | Get Processing Option |
| IC | Integrated Circuit |
| INS | Instruction byte of APDU commands |
| M | Mandatory |
| O | Optional |
| MAC | Message Authentication Code |
| MSB | Most Significant Byte |
| PBOC | People's Bank of China specifications |
| PSE | Payment System Environment |
| P1 | Parameter1 |
| P2 | Parameter2 |
| P3 | Parameter3 |
| PDOL | Process Option Data Object List |
| PIN | Personal Identification Number |
| RFU | Reserved For Future Use |
| SAD | Signed Static Application Data |
| SDA | Static Data Authentication |
| SW1 | Status Word 1 |
| SW2 | Status Word 2 |
| SK | Session Key |
| TC | Transaction Certification |
| TDOL | Transaction Certification Data Object List |
| TLV | Tag-Length-Value |
| UDK | Unique DEA Key |
| EC | Low-value Payment Specifications Based on Debit/Credit Application (Electronic Cash Application) |



| Abbreviation | Description |
|--------------|---|
| QPBOC | Contactless Integrated Circuit Card Payment Specification |

Table 2: Symbols and Abbreviations

1.4. Reference Documents

- China Financial Integrated Circuit Card Specifications--Part 4: Debit/credit Application Specifications JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 5: Debit/Credit Application Card Specification JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 6: Debit/Credit Application Terminal Specifications JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 7: Debit/Credit Application Card Security Specifications JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 10: Debit/Credit card Personalization Guide JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 12: Contactless Integrated Circuit Card Payment Specification JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 13: Low-value Payment Specifications Based on Debit/Credit Application JR/T 0025.4—2013
- China Financial Integrated Circuit Card Specifications--Part 17: Enhanced Debit/Credit Application Security Specifications JR/T 0025.4—2013
- Java Card 3 API, Classic Edition Version 3.0.4
- Global Platform Card Specification Version 2.2.1



2.0. Card Specifications

This section summarizes the features and functionalities of the ACOSJ-P.

2.1. Electrical

- Operating voltage: 1.62 V – 5.5 V DC+/-10% (Contact only card)
2.7 V – 5.5 V DC +/-10% (Contact interface of dual interface card)
- Maximum supply current: < 10mA
- ESD protection: ≤ 5 KV

2.2. Environmental

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

2.3. Communication Protocols

- T=0, T=1 with baud up to 625 kbps (external clock frequency 5MHz)
- T=CL protocol with baud up to 848 kbps

2.4. Memory

- Capacity: 12 KB
- EEPROM endurance: 500,000 erase/write cycles
- Data retention: 30 years

2.5. Cryptographic Capabilities

- DES,2K3DES (ECB and CBC)
- RSA: 768 to 2048 bits
- Hash: SHA1, SHA224, SHA256, SHA384, SHA512
- SM2/SM3/SM4

2.6. Compliance to Standards

- Compliant with ISO 7816 Parts 1, 2, 3, 4
- Compliant with ISO 14443 Type A
- Compliant with PBOC 3.0 Debit/Credit
- Compliant with PBOC 3.0 QPBOC
- Compliant with Java Card Specification Version 3.0.4
- Compliant with Global Platform Specification Version 2.2.1



2.7. Application Installation Parameters

ACOSJ-P adopts the following parameter definitions:

| Program Package AID | Application AID | Privilege | Description |
|---------------------|------------------------------|-----------------------------------|----------------------|
| A000000333A1 | A000000333A101 (application) | Below are installation parameters | PBOC 3.0 application |
| | A000000333A102 (PSE,PPSE) | Null | |

Table 3: Application Installation Parameters

When installing the A000000333A101 (application), you can use a 1-byte parameter to indicate the application supported by the card.

| | b8 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | Description |
|----|--------------|----|----|----|----|----|----|----|-----------------------------------|
| C9 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Supports state secret algorithms. |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | |
| | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | Contact debit/credit application |
| | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | E-cash (EC) application |
| | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | QPBOC |
| | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | Support contactless debit/credit |
| | Other values | | | | | | | | Reserved |

2.8. ATR (Contact Cards)

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

The default ATR is as follows:

| Parameter | ATR | Description |
|-------------------------------------|-----|--|
| TS | 3Bh | Direct convention, the least significant bit is sent first |
| T0 | 69h | TB1, TC1 and TD1 followed by 9 historical characters |
| TB1 | 00h | No programming voltage required |
| TC1 | 02h | Extra guard time |
| 9 historical characters (ACOSJvXXX) | | |

Table 4: ATR Protocol Bytes

The 9 historical characters are composed of the following:

| Historical Bytes | ATR | Description |
|------------------|-----|---------------|
| T1 | 41h | Indicates 'A' |



| Historical Bytes | ATR | Description |
|------------------|-------------|-----------------|
| T2 | 43h | Indicates 'C' |
| T3 | 4Fh | Indicates 'O' |
| T4 | 53h | Indicates 'S' |
| T5 | 4Ah | Indicates 'J' |
| T6 | 76h | Indicates 'v' |
| T7-T9 | 31h 30h 30h | Indicates '100' |

Table 5: ATR Historical Bytes

3.0. Card Life Cycle States

The ACOSJ-P has three card states: initial state, user state, and card block state, as shown in the following figure.

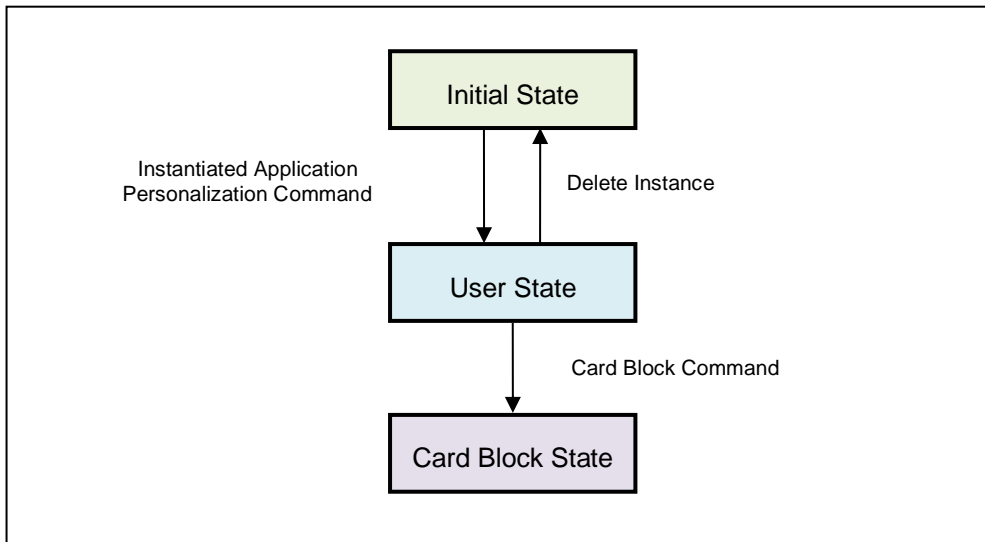


Figure 1: Card Life Cycle

1. **Initial State** – When the ACOSJ-P leaves the factory, the card is in the initial state.
2. **User State** – When the card is in the initial state, the user instantiates the PSE, PPSE, and PBOC 3.0 application Applet, and sends the personalization command to load user data so that the card will go to the user state. When the card is in the user state, the Delete Instance command can be sent to delete PSE, PPSE, and PBOC instances, so that the card will return to the initial state. Before deleting instances, you need to use the master key to initiate the secure channel session to successfully initiate the authentication secure channel.
3. **Card Block State** – When the card is in the user state, the user can send the Card Block command to make the card go to the card block state. After the card is blocked, all data in the card cannot be accessed, and Applet of all applications will become invalid.



4.0. Personalization Data Management

PBOC 3.0 application personalization means to organize data in the form of data grouping and add data to the ICC. The data grouping identifier (DGI) is a 2-byte hex value. The first byte of the DGI is 01h – 1Eh, indicating the data stored SFI. The second byte indicates the record number of the SFI. All the other DGIs whose first byte is out of the range are used to index data not stored in the SFI.

- Magnetic Track Data
- Cardholder Information Data
- Authentication Data and Issuer Public Key Certificate
- Authentication Data: Issuer Public Key Index, Reminder, and CA Public Key Index
- Authentication Data, SAD
- Authentication Data: ICC Public Key Certificate
- ICC Public Key Index and Reminder
- Static Application Data
- Card Risk Management Data
- Card Risk Management Data
- Static Application Data
- Terminal Velocity Checking Data
- Card Risk Management Data
- Card Authentication Related Data (QPBOC)
- Card Internal Risk Management Data
- Card Private Risk Management Data
- DES Key
- SM4 Key
- DES Check Key Value
- SM4 Check Key Value
- ICC Private Key (CRT)
- SM2 Public Key and Private Key
- Offline PIN Value
- PIN Attempt Count and Maximum Attempt Limit
- GPO Response Data of the Standard Debit/Credit Transaction
- GPO Response Data of the Standard Debit/Credit Transaction (State Secret)
- EC Transaction GPO Response Data
- EC Transaction GPO Response Data (State Secret)
- QPBOC Transaction GPO Response Data
- QPBOC Transaction GPO Response Data (State Secret)
- Issuer Application Data
- Select Application Response Data for Debit/Credit Transaction (Contact)
- Select Application Response Data (Contactless)
- Select PSE Response Data
- Select PPSE Response Data



5.0. Safety Management Mechanism

The ACOSJ-P card is a Java card of an open platform. Its security channel features conforms to GP2.2.1.

Note: For details about the security management methods, please refer to **Global Platform Card Specification Version 2.2.1**.

The ACOSJ-P card is also a PBOC 3.0 debit/credit application that meets all security requirements listed in PBOC 3.0 – Part 7: Debit/Credit Application Card Security Specifications. This chapter only describes security features of ACOSJ-P card personalization and application transactions.

Security Management Parts:

- Card personalization security management.
- Security management of PBOC 3.0 debit/credit application.

5.1. Session Key Calculation Method

The ACOSJ-P card adheres to security management of Secure Channel Protocol 02 (SCP02). This section mainly describes how to calculate SCP02 session keys.

Note: For details about security management, please refer to **Global Platform Card Specification Version 2.2.1**.

Personalization keys KENC, KMAC, and KDEK diversify their dispersing factors to generate personalization session keys SKUENC, SKUMAC, and SKUDEK. The diversification encryption algorithm is 3DES (CBC) and the initial vector.



6.0. Personalization Command

Card personalization indicates card operations required by a specific application. The main tasks of card personalization involve creating the application required file structure and writing data required by the application.

ACOSJ-P personalization includes Payment System Environment (PSE) personalization and debit/credit application personalization. PSE personalization does not need to initiate a session. After selecting a PSE application, directly send the personalization command. Debit/credit application personalization needs to send a successful session to the secure channel. All subsequent personalization commands are performed in this session.

The PSE and PBOC 3.0 debit/credit application instances must be installed before personalization of the ACOSJ-P card.

6.1. PBOC3.0 Debit/Credit Application Personalization Commands

6.2. INITIALIZE UPDATE

The INITIALIZE UPDATE command is used to initiate an ICC secure channel session while the personalized device authenticates card effectiveness. If the secure channel is corrupted or was not created, subsequent personalization commands will not precede.

The command is prohibited after packet data are completely stored (personalization is complete).

6.3. EXTERNAL AUTHENTICATE

During the secure channel session, the EXTERNAL AUTHENTICATE command is used by the card to authenticate the host and determine the security level required by all subsequent commands. The EXTERNAL AUTHENTICATE command can only be executed after the INITIALIZE UPDATE command is successfully executed.

The command is prohibited after packet data are completely stored (personalization is complete).

Note: The EXTERNAL AUTHENTICATE command is used in personalization. Its CLA is 84h, which is different from the EXTERNAL AUTHENTICATE command (CLA=00h) in **Section 7.9**.

6.4. STORE DATA

The STORE DATA command is used to download personalization packet data from the personalization device to an ICC. This command can be executed after the EXTERNAL AUTHENTICATE command is successfully executed. The data protection level of the STORE DATA command is determined by the EXTERNAL AUTHENTICATE command.

The command is prohibited after packet data are completely stored (personalization is complete).



7.0.PBOC 3.0 Debit/Credit Application Dedicated Commands

7.1. SELECT

The SELECT command is used to select ICC supported applications and obtain card supported application information including the directory name of the payment system environment (PSE) and PBOC 3.0 debit/credit applications supported by the card. After the commands are successfully executed, the PSE and debit/credit application are set. Subsequent commands are applicable to this application.

7.2. READ RECORD

The READ RECORD command is used to read a file record from a linear record file, or reads records included in the response returned by the ICC. JR/T 0025 describes SFIs in the range of 1-10, and the record structure is a BER-TLV structure data object. JR/T 0025 does not describe SFIs out of the range 1-10.

The READ RECORD command is not restricted by application temporary blocking, but restricted by the application permanent blocking and card blocking.

7.3. GET DATA

The GET DATA command is used to obtain an elementary data object, which is not encapsulated in a record, from the current application. The response data field contains the elementary data object specified by the command packet P1P2.

The GET DATA command is not restricted by the application temporary blocking, but restricted by the application permanent blocking and card blocking.

7.4. GET RESPONSE

The GET RESPONSE command is used to transmit part of APDU data from a card to an interface device.

Some commands return the status 61xx, with the xx value indicates the actual length of the returned response bytes.

7.5. GET PROCESSING OPTIONS

The GET PROCESSING OPTIONS (GPO) command is used to start transactions inside the ICC. GPO informs the ICC of starting the transaction. Every time the GPO command runs successfully, the ATC increases by 1. When the ATC increases to FF FFh, the application will be permanently blocked and 6283 is returned for all subsequent commands.

The GPO command can be executed only one time during each transaction.

The GPO command is not restricted by the application temporary blocking, but is restricted by the application permanent blocking and card blocking.

7.6. INTERNAL AUTHENTICATE

The INTERNAL AUTHENTICATE command triggers the card to use the random number and data received from the terminal and the private key stored in the card to compute the signed dynamic application data. This command is used in dynamic data authentication (DDA) of PBOC 3.0 debit/credit transactions. The INTERNAL AUTHENTICATE command can be executed only when a card application supports DDA.

The INTERNAL AUTHENTICATE command is not restricted by the application temporary blocking, but restricted by the application permanent blocking and card blocking.



7.7. VERIFY

The VERIFY command is used by the ICC to compare the PIN stored in the card with the PIN provided by the terminal. This command is used when offline PIN verification is selected from the cardholder verification method (CVM) list.

The VERIFY command can only be ran when the card supports the CVM. The PIN will be blocked if the number of consecutive failures reaches the maximum value set in the error counter.

7.8. GENERATE AC

The GENERATE AC command is used to transmit the transaction related data from a terminal to a card. After behavior analysis, the card calculates and returns an application cryptogram (AC) defined by JR/T 0025 to the terminal. Contents of the AC may be Application Authentication Cryptogram (AAC), Authorization Request Cryptogram (ARQC), or Transaction Certificate (TC).

Before the GENERATE AC command, the card should have received the GPO command notifying that the transaction is started. 6985 is returned for the GENERATE AC command over two times.

If an application is temporarily blocked, the GENERATE AC command always returns the AAC response.

7.9. EXTERNAL AUTHENTICATE

The EXTERNAL AUTHENTICATE command requests the card application to authenticate a cryptogram for issuer authentication.

Before the EXTERNAL AUTHENTICATE command, the card should have received the GPO command. The EXTERNAL AUTHENTICATE command can be executed only once during one debit/credit transaction. If external authentication fails, the card will record the issuer authentication failure.

Note: This EXTERNAL AUTHENTICATE command is used in debit/credit transactions. In this command, CLA=00h is used, which is different from the **INITIALIZE UPDATE** command in **Section 6.2** (CLA=84h, used in personalization).

7.10. APPLICATION BLOCK

The APPLICATION BLOCK command is an issuer script command. It is used to block the current application making the application invalid.

After the application is blocked, the response code 62 83h is returned for the SELECT command, and the application always returns AAC instead of AC as a response for the GENERATE AC command.

7.11. APPLICATION UNBLOCK

The APPLICATION UNBLOCK command is an issuer script command. It is used to restore an application currently blocked. After the APPLICATION UNBLOCK command is successfully executed, application restrictions caused by blocking will be removed.

7.12. CARD BLOCK

The CARD BLOCK command is an issuer script command. It is used to permanently terminate all applications in the ICC.

When the CARD BLOCK command is executed successfully, the status code 6A 81h is returned for all subsequent SELECT commands, and all other commands are prohibited.



7.13. PUT DATA

The PUT DATA command is an issuer script command. It is used to modify values of some basic data objects in a card. It is effective only for tagged data. After successful personalization, this command can be used to modify a data object only if the data object is allowed to be updated according to PBOC 3.0 or self-defined rules.

7.14. PIN CHANGE/UNBLOCK

The PIN CHANGE/UNBLOCK command is an issuer script command. It is used by the issuer to unblock the PIN, or unblock and change the PIN at the same time. After the command is successfully executed, the value of the PIN attempt counter will be reset to the maximum value.

If the command contains PIN data, the data should be encrypted for confidentiality.

7.15. UPDATE RECORD

The UPDATE RECORD command is an issuer script command. It is used to modify the content of a record in the record file. The modified content is in the command data field.

8.0. Transaction Process

8.1. QPBOC Transaction Process

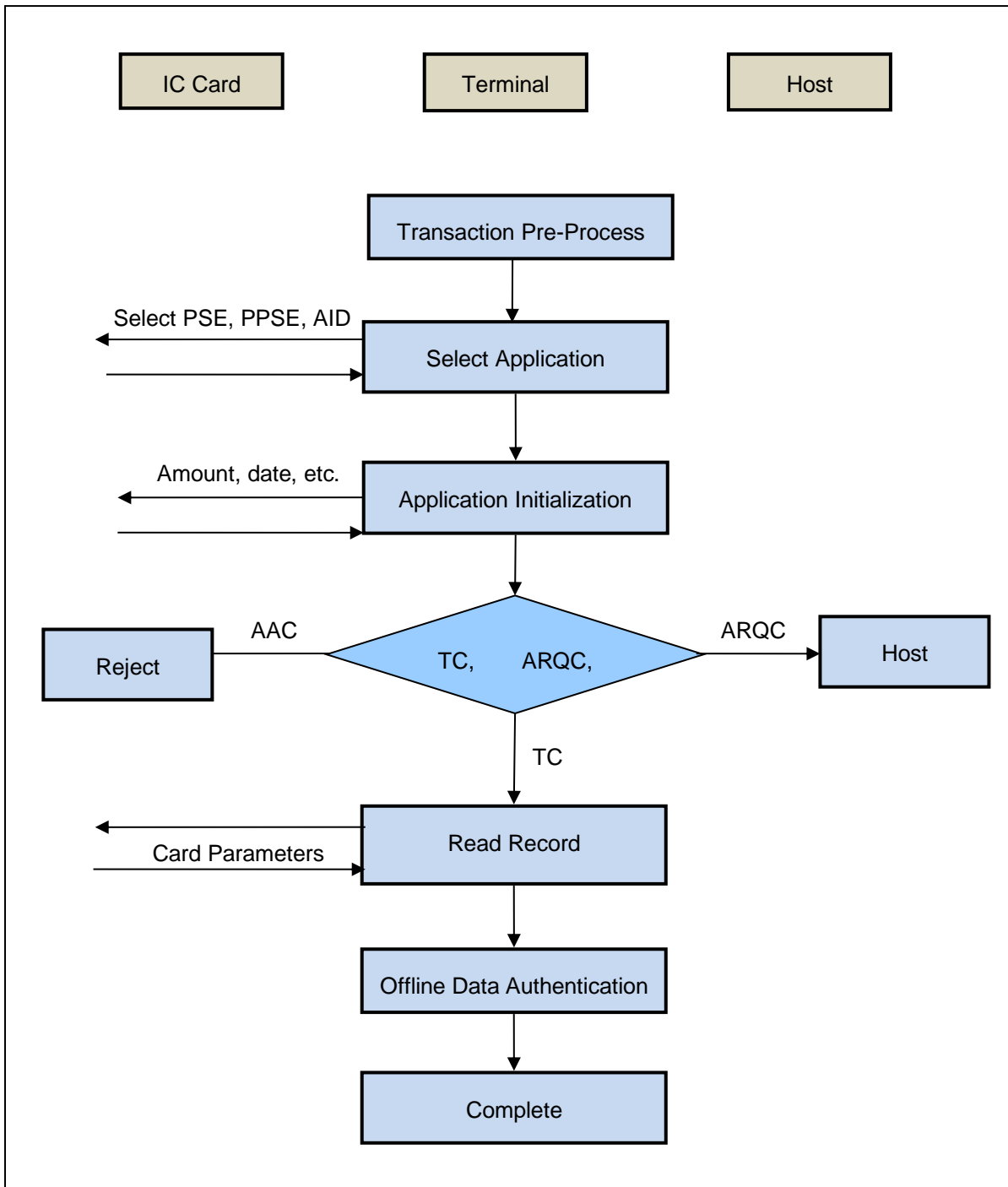
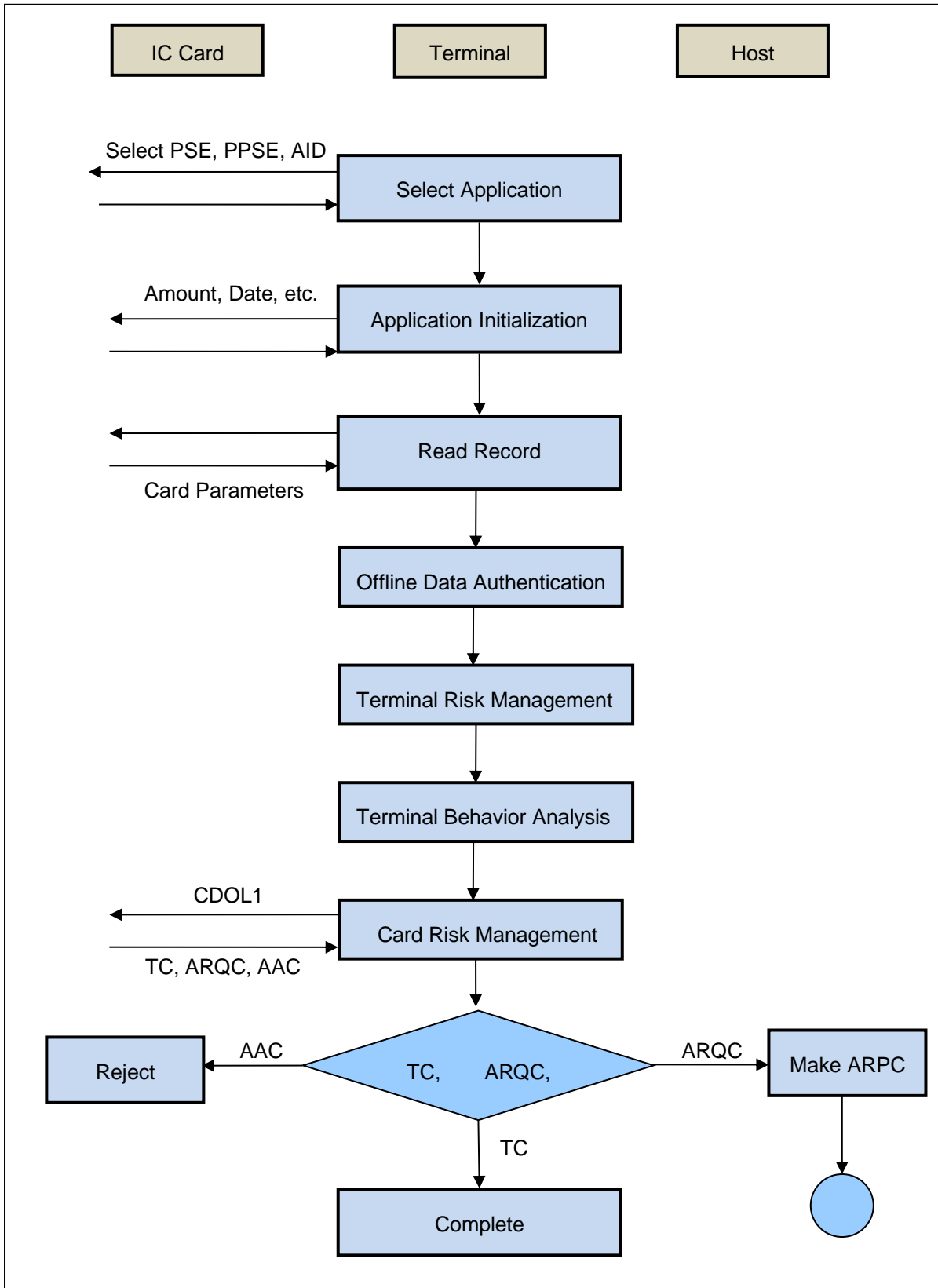


Figure 2: ACOSJ-P Support QPBOC Transaction Process

8.2. Debit/Credit (EC) Transaction Process



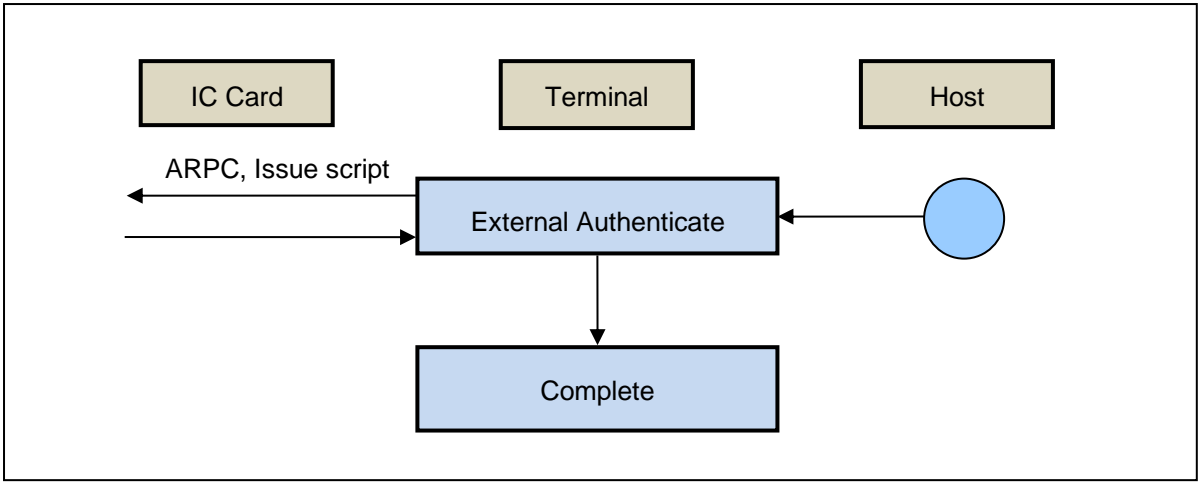


Figure 3: ACOSJ-P Support Standard PBOC3.0 Debit/Credit Transaction Process



9.0. 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.



10.0. Contact Information

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

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