Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-P
【双界面】

功能规格书 V1.06

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

目录

图目录

表目录

1.0. 概览

ACOSJ-P 是龙杰智能卡有限公司（ACS）自主研发的智能卡操作系统，由于符合 PBOC 3.0 规范，适用于各类 PBOC 3.0 借贷记应用和 QPBOC 应用。

本手册介绍了 ACOSJ-P 操作系统的特性与功能，旨在帮助用户了解 ACOSJ-P 的性能并熟练使用。

1.1. ACOSJ-P 修改历史

版本	发布日期	修改内容
ACOSJ-P v1.01	2016 年 11 月	• 12KB EEPROM • 工作电压： 仅接触式：1.62V - 5.5V；双界面：为 2.7V - 5.5V

表1：ACOSJ-P 修改历史

1.2. 参考文件

- 中国金融集成电路（IC）卡规范－第 4 部份：借记贷记应用规范 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 5 部份：借记贷记应用卡片规范 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 6 部份：借记贷记应用终端规范 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 7 部份：借记贷记应用安全规范 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 10 部份：借记贷记应用个人化指南 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 12 部份：非接触式 IC 卡支付规范 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 13 部份：基于借记贷记应用的小额支付规范 JR/T 0025.4—2013
- 中国金融集成电路（IC）卡规范－第 17 部份：借记贷记应用安全增强规范 JR/T 0025.4—2013
- Java Card 3 API, Classic Edition Version 3.0.4
- Global Platform Card Specification Version 2.2.1

1.3. 符号和缩写

缩写	说明
3DES	3 重数据加密算法 (Triple DES)
AAC	应用认证密文 (Application Authentication Cryptogram)
AAR	应用授权参考 (Application Authorization Referral)
AC	应用密文 (Application Cryptogram)
AFL	文件定位器 (Application File Locator)
ARPC	授权响应密文 (Authorization Response Cryptogram)
ARQC	授权请求密文 (Authorization Request Cryptogram)
AID	应用标识符 (Application/Account Identifier)
AIP	应用交互特征 (Application Interchange Profile)
APDU	应用协议数据单元 (Application Protocol Data Unit)

缩写	说明
ATC	应用交易计数器 (Application Transaction Counter)
ATR	复位应答 (Answer To Reset)
CA	认证中心 (Certificate Authority)
CDA	复合动态数据认证/应用密文生成 (Combined DDA/AC Generation)
CDOL	卡片风险管理数据对象列表 (Card Risk Management Data Object List)
CID	密文信息数据 (Cryptogram Information Data)
CKV	密钥校验值 (Check Key Value)
CLA	APDU 命令的类别字节 (Class byte of APDU commands)
CM	卡片管理 (Card Manager)
CVM	持卡人验证方法 (Cardholder Verification Method)
CVR	卡片验证结果 (Card Verification Result)
COS	卡片操作系统 (Card Operating System)
DDA	认证动态数据 (Dynamic Data Authentication)
DOL	数据对象列表 (Data Object List)
DDOL	动态数据认证对象列表 (Dynamic Data Authentication Data Object List)
DES	数据加密标准 (Data Encryption Standard)
DF	专用/目录文件 (Dedicated/Directory File)
DGI	数据分组索引 (Data Group Index)
DEC(C, K)	用密钥 K 对数据 C 进行 DES 或 3DES 解密 (Decryption of data C with key K using DES or 3DES)
ENC(P, K)	用密钥 K 对数据 P 进行 DES 或 3DES 加密 (Encryption of data P with key K using DES or 3DES)
EF	基本文件 (Elementary File)
FCI	文件控制信息 (File Control Information)
GPO	获取处理选项 (Get Processing Option)
IC	集成电路 (Integrated Circuit)
INS	APDU 命令的指令字节 (Instruction byte of APDU commands)
M	必选 (Mandatory)
O	可选 (Optional)
MAC	报文认证码 (Message Authentication Code)
MSB	最高有效字节 (Most Significant Byte)
PBOC	中国人民银行标准 (People's Bank of China specifications)
PSE	支付系统环境 (Payment System Environment)
P1	参数 1 (Parameter1)
P2	参数 2 (Parameter2)

缩写	说明
P3	参数 3 (Parameter3)
PDOL	处理选项数据对象列表 (Process Option Data Object List)
PIN	个人识别码 (Personal Identification Number)
RFU	保留为将来使用 (Reserved For Future Use)
SAD	签名的静态应用数据 (Signed Static Application Data)
SDA	认证静态数据 (Static Data Authentication)
SW1	状态码 1 (Status Word 1)
SW2	状态码 2 (Status Word 2)
SK	过程密钥 (Session Key)
TC	交易证书 (Transaction Certification)
TDOL	交易证书数据对象列表 (Transaction Certification Data Object List)
TLV	标签-长度-值 (Tag-Length-Value)
UDK	独有的数据加密子密钥 (Unique DEA Key)
EC	电子现金 (Electronic Cash)
QPBOC	非接触式 IC 卡支付规范 (Contactless Integrated Circuit Card Payment Specification)

表2:符号和缩写

2.0. 卡片规格

2.1. 电气参数

- 工作电压： 1.62 V – 5.5 V DC+/-10% （接触式卡）
  2.7 V – 5.5 V DC +/-10% （双界面卡的接触式界面）
- 最大源电流：< 10mA
- ESD 保护：≤ 5 KV

2.2. 环境参数

- 工作温度：-25°C - 85°C
- 存储温度：-40°C - 100°C

2.3. 通信协议

- T=0 和 T=1，最高 625 kbps 波特率（外部时钟频率 5MHz）
- T=CL 协议，最高 848 kbps 波特率

2.4. 内存

- 容量：12 KB
- EEPROM 重复檫写次数：50 万次
- 数据存储时间：30 年

2.5. 加密功能

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

2.6. 符合标准

- 通过 PBOC 3.0 认证
- 符合 ISO 7816 第 1、2、3 和 4 部分规定
- 符合 ISO 14443 A 类标准
- 符合 JAVA Card Specification（3.0.4 版）
- 符合 Global Platform Specification（2.2.1 版）

2.7. 应用安装参数

ACOSJ-P 应用遵循以下的参数定义：

程序包 AID	应用 AID	应用权限	说明
A000000333B1	A000000333B101 (应用)	安装参数如下	PBOC 3.0 应用
	A000000333B102 (PSE,PPSE)	无	

表3 ：应用安装参数

安装 A000000333B101（应用）时，可以带一个字节的参数来表示卡片支持的应用。

	b8	b7	b6	b5	b4	b3	b2	b1	说明
C9	1	0	0	0	0	0	0	0	支持国密算法
	0	0	0	0	0	0	0	0	
	0	0	0	0	0	0	0	1	接触借记贷记应用
	0	0	0	0	0	0	1	0	电子现金应用
	0	0	0	0	0	1	0	0	QPBOC
	0	0	0	0	1	0	0	0	支持非接借记贷记
	其他值								保留

2.8. 复位应答（ATR，接触卡）

硬件复位（如上电）后，卡片按照 ISO 7816 第 3 部分的规定传送复位应答（ATR）。ACOSJ-P 支持正向约定的 T＝0 协议。

以下是默认的 ATR：

参数	ATR	说明
TS	3Bh	正向约定，首先发送最低有效位
T0	69h	TB1、TC1 和 TD1 存在，跟随 9 个历史字符
TB1	00h	无需额外编程电压
TC1	02h	额外保护时间
9 个历史字符（ACOSJvXXX）		

表4 ：ATR 协议字节

9 个历史字符结构如下：

历史字节	ATR	说明
T1	41h	表示“A”
T2	43h	表示“C”
T3	4Fh	表示“O”
T4	53h	表示“S”
T5	4Ah	表示“J”
T6	76h	表示“v”
T7~T9	31h 30h 30h	表示“100”

表5 ：ATR 历史字节

3.0. 卡片生命周期状态

ACOSJ-P 卡片有三种状态：初始化状态、用户状态、卡片锁定状态，如下图所示：

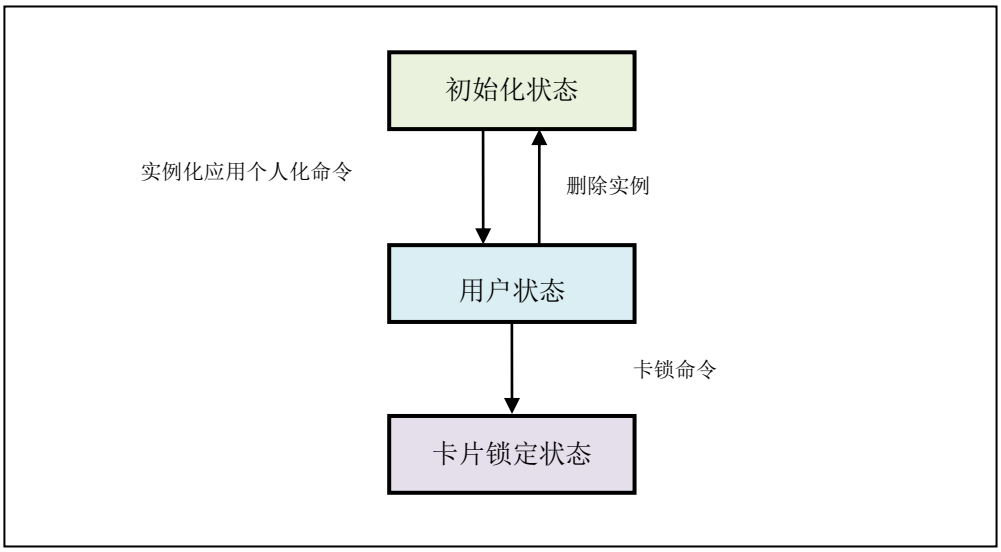


图1:卡片生命周期

1. **初始化状态** - ACOSJ-P 出厂时，卡片处于初始化状态。
2. **用户状态** - 卡片在初始化状态下实例化 PSE, PPSE 及 PBOC 3.0 应用 Applet，并通过个人化命令加载用户数据，个人化完成后卡片进入用户状态。卡片在用户状态下通过删除实例命令将 PSE, PPSE 及 PBOC 应用实例删除，卡片将回到初始化状态，删险实例前须用主密钥发起安全通道会话，成功发起认证安全通道。
3. **卡片锁定状态** - 卡片在用户状态下通过卡片锁定命令使卡片变为锁定状态，锁定后卡片内部所有数据均不可访问，所有应用 Applet 失效。

4.0. 个人化数据管理

PBOC 3.0 应用的个人化是以数据分组的形式将数据组织起来，并添加到 IC 卡中。数据分组标识符（DGI）是两字节的十六进制数，数据分组标识的第一个字节等于 01h 到 1Eh，表明数据存储的 SFI，第二个字节表明 SFI 记录的记录编号。其他那些第一个字节在此范围之外的数据分组标识都用于索引并不存储于 SFI 的数据。

- 磁道数据
- 持卡人信息数据
- 认证数据和发卡行公钥证书
- 认证数据：发卡行公钥指数、余项、CA 公钥索引
- 认证数据，签名静态应用数据
- 认证数据：IC 卡公钥证书
- IC 卡公钥指数、余项
- 静态应用数据
- 卡片风险管理数据
- 卡片风险管理数据
- 静态应用数据
- 终端频度检查数据
- 卡片风险管理数据
- 卡片认证相关数据（QPBOC）
- 卡片内部风险管理数据
- 卡片私有风险管理数据
- DES 密钥
- SM4 密钥
- DES 密钥校验值
- SM4 密钥校验值
- IC 卡私钥（CRT）
- SM2 公私钥
- 脱机 PIN 值
- PIN 尝试次数、最大尝试限制数
- 标准借记贷记交易 GPO 响应数据
- 标准借记贷记交易 GPO 响应数据（国密）
- 电子现金交易 GPO 响应数据
- 电子现金交易 GPO 响应数据（国密）
- QPBOC 交易 GPO 响应数据
- QPBOC 交易 GPO 响应数据（国密）
- 发卡行应用数据
- 借记贷记交易选择应用响应数据（接触）
- 选择应用响应数据（非接触）
- 选择 PSE 响应数据
- 选择 PPSE 响应数据

5.0. 安全管理机制

ACOSJ-P 卡为开放式平台的 Java 卡，卡片的安全通道特性符合 GP2.2.1 标准。

注：*具体安全管理方法请参考《****Global Platform Card Specification Version 2.2.1****》。*

ACOSJ-P 卡片也是 PBOC 3.0 借记贷记应用，符合 PBOC 3.0 - 第 7 部分：借记贷记应用卡片规范。本章节只简单介绍 ACOSJ-P 卡片个人化及应用交易中的安全特性。

安全管理：

- 一部分是卡片个人化的安全管理；
- 另一部分是 PBOC 3.0 借记贷记应用的安全管理。

5.1. 过程密钥的计算方法

ACOSJ-P 卡片符合安全通道协议 02（SCP02）的安全管理。本节主要描述 SCP02 过程密钥计算方法。

注：*如需了解具安全管理的详情，请参考《****Global Platform Card Specification Version 2.2.1****》。*

个人化过程密钥 SKUENC，SKUMAC，SKUDEK 由个人化密钥 KENC、KMAC、KDEK 对各自分散因子分散产生，分散加密算法采用 CBC 模式 3DES 加密运算，初始向量为 8 字节 00h。

6.0. 个人化命令

卡片个人化是根据特定应用的需要对卡片所进行的操作，卡片个人化所要完成的主要任务包括创建应用所需要的文件结构和写入应用所要求的数据。

ACOSJ-P 的个人化分为支付环境（PSE）个人化和借记贷记应用个人化。PSE 的个人化不需要向安全通道发起会话，选择 PSE 应用后可直接发送个人化命令。借记贷记应用的个人化须先向安全通道发起一个成功的会话，所有后续的个人化命令在此会话过程中完成。

在对 ACOSJ-P 卡片进行个人化之前必须为卡片先安装 PSE 及 PBOC 3.0 借记贷记的应用实例。

6.1. PBOC 3.0 借记贷记应用个人化命令

6.2. 初始化安全通道

此命令用于发起 IC 卡安全通道会话，同时，个人化设备用于鉴别卡片的有效性。如果没有建立安全通道，或会话被破坏，后续的个人化命令将无法继续执行。

分组数据完全保存（即个人化完毕）后该命令将被禁止执行。

6.3. 外部认证

在安全通道发起会话过程中，外部认证命令用于卡片认证主机，并确定所有后续命令所需要的安全级别。外部认证命令须在初始化安全通道命令执行成功后方可执行。

分组数据完全保存（即个人化完毕）后该命令将被禁止执行。

注：*外部认证命令用于个人化。CLA=84h，与* ***7.9 节****的外部认证命令（CLA=00h）不同。*

6.4. 存储数据

此命令用于个人化设备向 IC 卡下载个人化分组数据，该命令须在外部认证命令执行成功后执行。添加数据命令的数据保护级别由外部认证命令决定。

分组数据完全保存（即个人化完毕）后该命令将被禁止执行。

7.0. PBOC 3.0 借记贷记应用专用命令

7.1. 选择

此命令用于选择 IC 卡中支持的应用，用于获取卡片支持的应用信息，包括支付系统环境目录名称 PSE 和卡片支持的 PBOC 3.0 借记贷记应用。成功执行命令后设定 PSE、借记贷记应用，后续命令将适用于该应用。

7.2. 读记录

此命令用于从一个线性记录文件中读取一条文件记录，或者从 IC 卡返回的响应中将包含读出的记录。JR/T 0025 描述对于在 1-10 范围内的 SFI，记录结构是一个 BER－TLV 结构数据对象，对于不在 1-10 范围内的 SFI 则不在描述范围内。

读记录命令不受应用临时锁定的限制，但受应用永久锁定及卡锁定的限制。

7.3. 取数据

此命令用来从当前应用中取得一个没有封装在记录中的基本数据对象，响应报文的数据域中包含有命令报文 P1P2 所指示的基本数据对象。

取数据命令不受应用临时锁定的限制，但受应用永久锁定及卡片锁定的限制。

7.4. 取应答

此命令用于从卡片向接口设备传送 APDU 的部份数据。

部分指令返回 61xx 状态，xx 值为返回响应数据字节数的实际长度。

7.5. 获取处理选项

获取处理选项命令（GPO 命令）用来启动 IC 卡内的交易，告知 IC 卡交易开始。GPO 命令执行成功一次，应用交易计数器 ATC 递增 1，在应用计数器 ATC 递增至 FF FFh 时，应用将被永久锁定，后续所有命令均返回 6283。

在一次交易中 GPO 命令只能执行一次。

GPO 命令不受应用临时锁定的限制，但受应用永久锁定及卡片锁定的限制。

7.6. 内部认证

此命令引发卡片使用从终端收到的随机数、数据和卡片中储存的私钥来计算出签名动态应用数据的过程，用于 PBOC 3.0 借记贷记交易的 DDA 动态数据认证。卡片应用只有支持 DDA 认证方可执行内部认证命令。

内部认证命令不受应用临时锁定的限制，但受应用永久锁定及卡片锁定的限制。

7.7. 验证

验证命令用于 IC 卡对终端提供的 PIN 与卡中存储的 PIN 进行校验，当从 CVM 列表中选择的持卡人验证方法（CVM）是脱机 PIN 时，使用验证命令进行校验。

卡片应用支持 CVM 时方可执行验证命令。当连续失败的次数达到错误计数器设定的最大值时，PIN 将被锁定。

7.8. 生成应用密文

此命令用于终端传送交易相关的数据到卡片，卡片经过行为分析后，计算并且返回一个由 JR/T 0025 定义的应用密文（AC）给终端，应用密文包括认证密文（AAC，拒绝交易）、授权请求（ARQC，请求联机授权）、交易证书（TC，批准交易）。

在生成应用密文命令之前，卡片应收到 GPO 命令告知交易开始，且一次交易中最多只能执行两次生成应用密文生成应用密文命令，超过两次的生成应用密文命令都将返回 6985。

如果应用处于临时锁定，生成应用密文命令总是返回 AAC 响应。

7.9. 外部认证

此命令要求卡片应用认证一个密文，用于发卡行认证。

在此命令之前，卡片应收到 GPO 命令。一次借记贷记交易中只能执行最多一次外部认证命令，如果外部认证失败，则卡片记录发卡行认证执行失败。

***注：**此命令用于借记贷记交易，CLA=00h，与 **6.2** 节的外部认证命令（CLA=84h，用于个人化）不同。*

7.10. 应用锁定

此命令属于发卡行脚本命令，用于锁定当前应用，使应用无效。

在应用被锁定后，对于选择命令，应用返回状态码 62 83h；对于生成应用密文命令，应用总是返回 AAC 代替 AC 作为响应。

7.11. 应用解锁

此命令属于发卡行脚本命令，用于恢复当前选择被锁定的应用，执行成功后，此前通过应用锁定附加在该应用上的限制将解除。

7.12. 卡片锁定

此命令属于发卡行脚本命令，用于永久地停止 IC 卡中所有应用。

执行成功后，所有后续的选择命令都将返回状态码 6A 81h，所有其他命令将禁止执行。

7.13. 设置数据

此命令属于发卡行脚本命令，用于修改卡片中的一些基本数据对象的值，只有有标签的数据才能使用该命令修改。在个人化成功后，只有 PBOC 3.0 规范规定允话更新或者自定义允许更新的数据对象才能用此命令修改。

7.14. PIN 修改/ 解锁

此命令属于发卡行脚本命令，用于发卡行解锁 PIN 或同时既改变 PIN 也解锁 PIN。命令执行成功后，PIN 尝试记数器的值将复位到 PIN 尝试限制数的最大值。

为了保密，如果本命令包含有 PIN 数据，则该数据应该加密。

7.15. 修改记录

此命令属于发卡行脚本命令，用于修改记录文件中一条记录的内容，修改的内容在命令数据域中。

8.0. 交易流程

8.1. QPBOC 交易流程

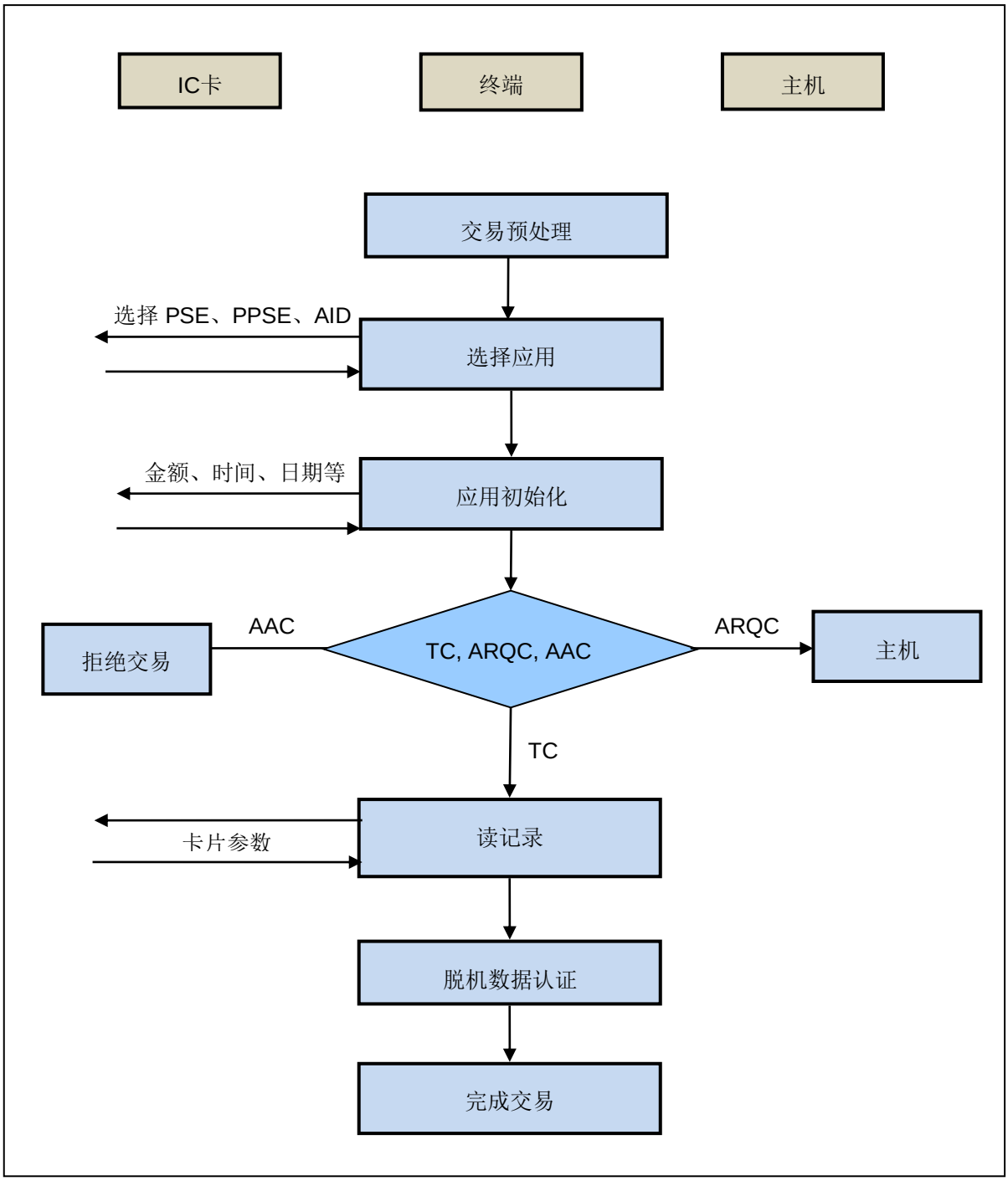
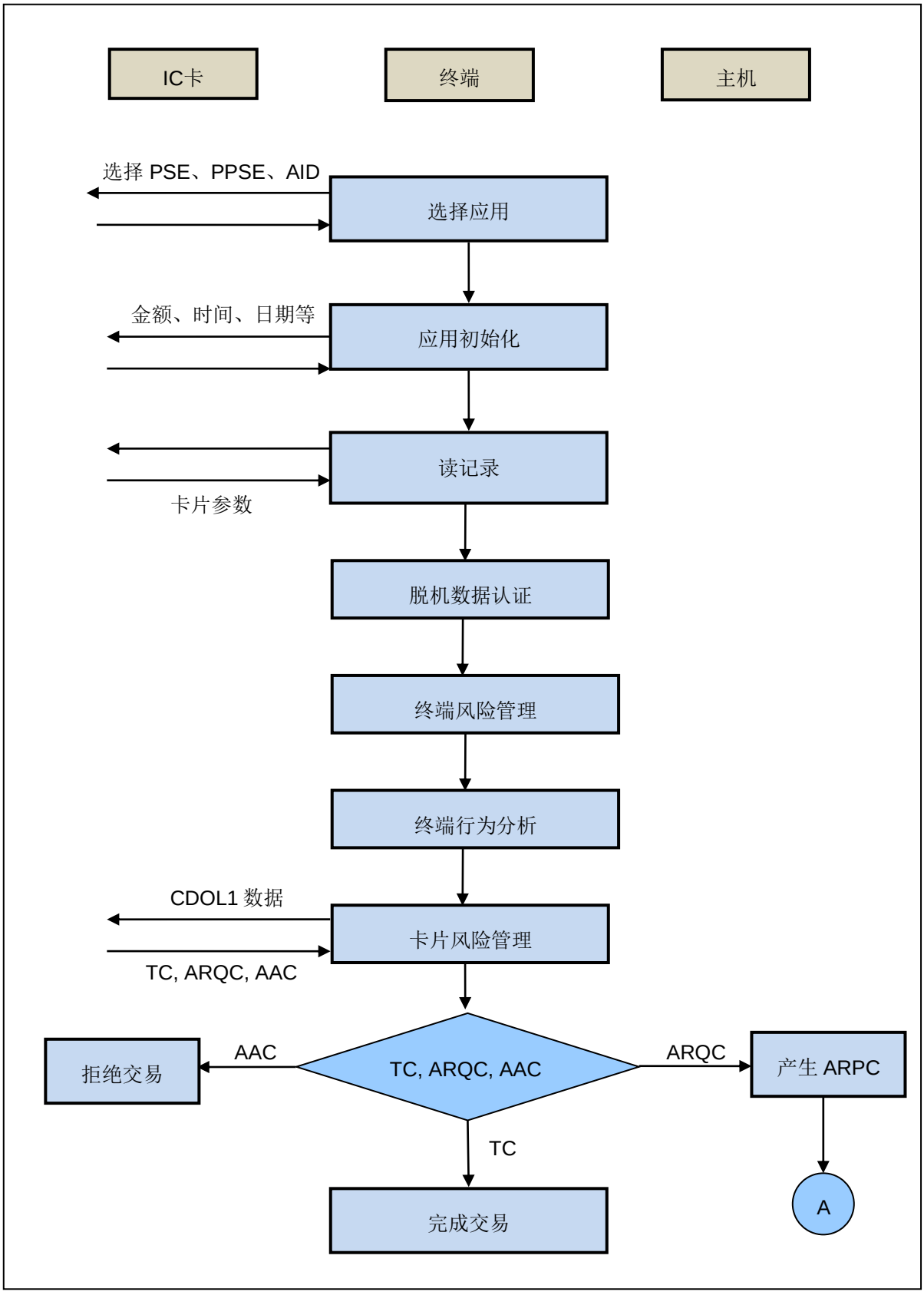


图2 :ACOSJ-P 支持的 QPBOC 交易流程

8.2. 借记贷记 (电子现金) 交易流程



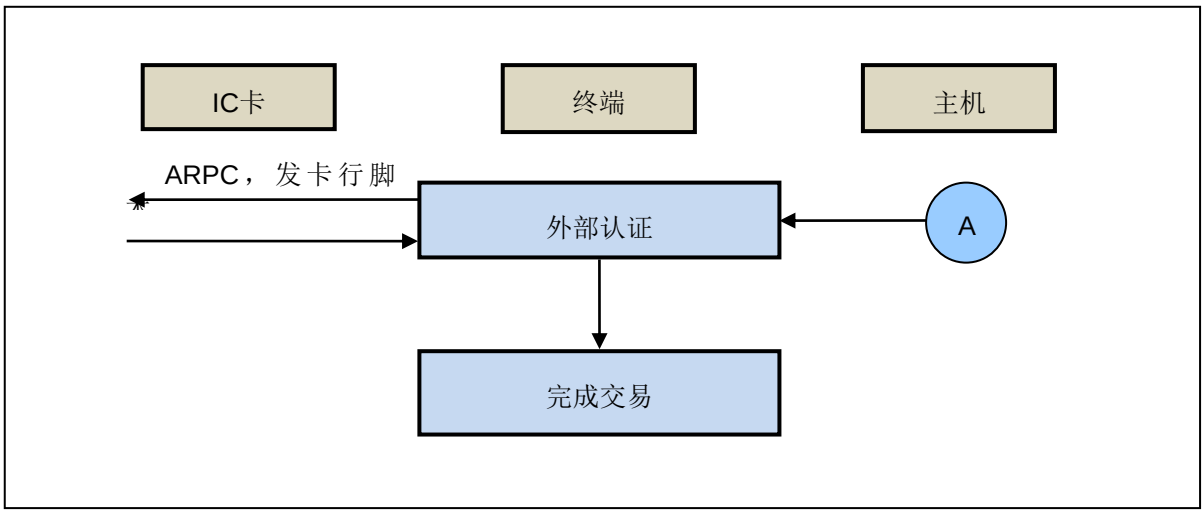


图3:ACOSJ-P 支持的标准 PBOC3.0 借记贷记 (电子现金) 交易流程

9.0. 生命支持应用

这些产品的设计并非用于生命支持设备或系统，在这些设备或系统中对这些产品的误操作可能导致人身伤害。如果 ACS 客户将这些产品使用于或者销售用于此类应用，则他们应该自行承担相应的风险，而且同意赔偿由于不当使用或销售从而给 ACS 造成的损失。

10.0.联系方式

如需了解其他信息请访问 ACS 网站 http://www.acs.com.hk.

如需销售咨询请发送邮件至 info@acs.com.hk.