ACOSJ-P

Java卡 – PBOC 3.0

Advanced Card Systems Ltd.
Card & Reader Technologies

目录

产品概览

Advanced Card Systems Ltd.
Card & Reader Technologies

产品概览

ACOSJ-P产品

接触式\非接触\双界面
(12 KB EEPROM)

模块

接触式
(12 KB EEPROM)

全尺寸卡

非接触
(12 KB EEPROM)

全尺寸卡

双界面
(12 KB EEPROM)

全尺寸卡

关于PBOC 3.0标准

Advanced Card Systems Ltd.
Card & Reader Technologies

PBOC标准发展历程

1997

- 发布PBOC 1.0
- 电子钱包、电子存折系列

2005

- 发布PBOC 2.0
- 借/贷记系列
- 电子钱包、电子存折系列

2010

- 发布PBOC 2.0 (2010)
- 借/贷记（小额支付）
- 电子钱包、电子存折系列

2013

- 发布PBOC 3.0
- 更加关注行业合作、创新应用
- 借/贷记（小额支付）
- 电子钱包、电子存折系列

acs

中国人民银行 THE PEOPLE'S BANK OF CHINA

PBOC 3.0规范组成部分

PBOC 3.0标准功能分类

基本功能

- 标准借记贷记
- 基于标准借贷记的小额支付
- 非接触IC卡支付

注：PBOC 3.0新增电子现金圈存日志、非接交易日志、新版本的FDDA等。

扩展功能

- 非接小额支付应用
- 双币电子现金应用
- 增强安全算法
- IC卡互联网终端

PBOC 3.0规范新增主要功能

修订规范，在原版基础上修订和废止，完善金融IC卡交易流程，解决金融IC卡应用中出现的问题，适应国际发展趋势，并与国际规范保持同步

新增规范，实现卡片和终端密码算法的国产化，保证金融交易安全，实现自主可控

原版1-13部分

第14部分:非接小额扩展应用规范

第15部分:电子现金双币应用规范

第16部分:IC卡互联终端规范

第17部分:借贷记安全增强规范

新增规范，更好的满足金融IC卡在高铁、公交、地铁等公共服务领域的应用

新增规范，解决我国持卡人在港澳地区使用金融IC卡进行支付的问题

新增规范，满足金融IC卡在互联网、手机支付等创新支付方式中的应用

关于借贷记(DC)

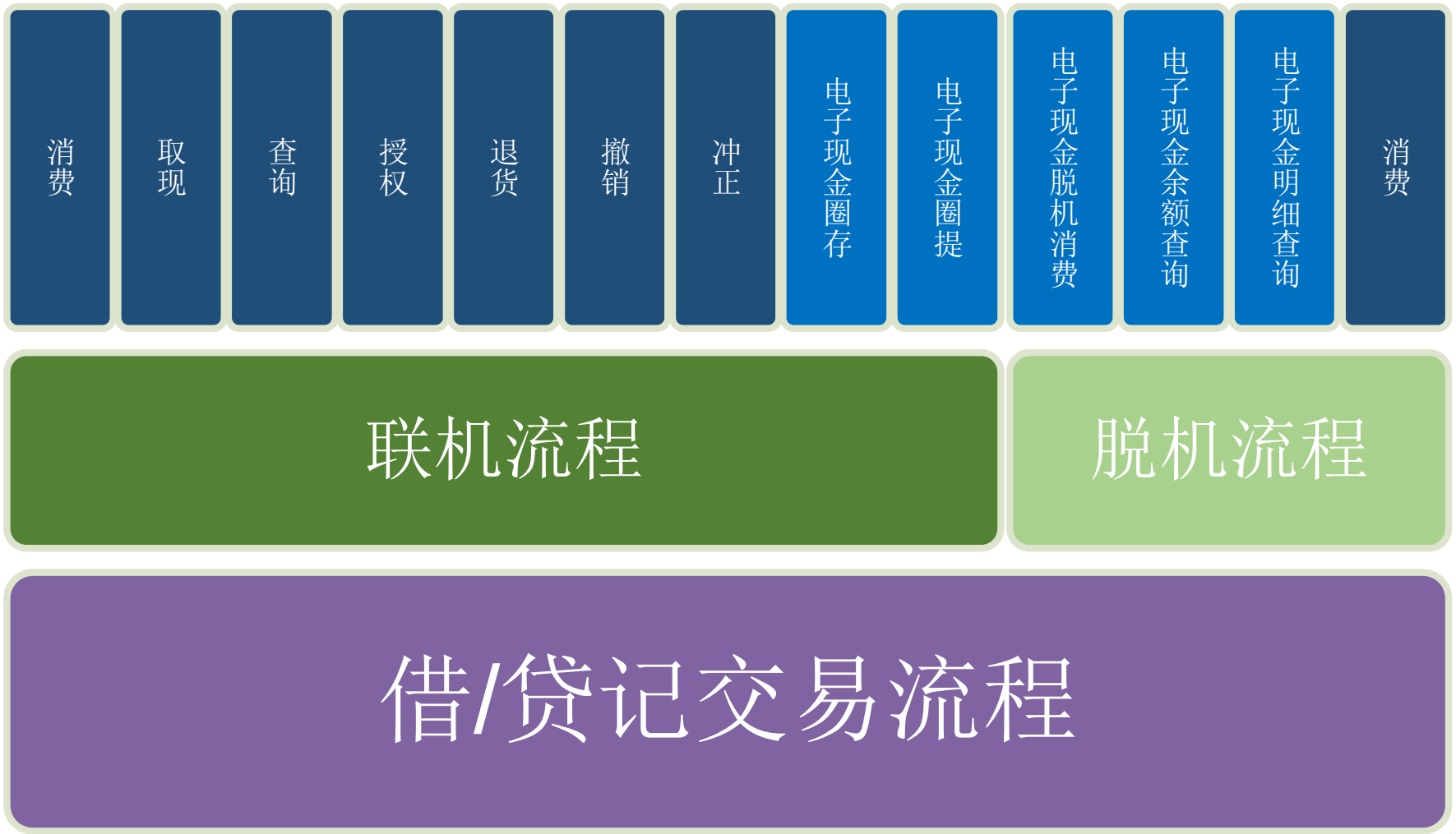
Advanced Card Systems Ltd.
Card & Reader Technologies

关于借贷记(DC)

PBOC借贷记应用脱胎于EMV 2000，通过以下实现卡片在POS终端上的脱机消费、联机消费和ATM终端上的取现交易：

- 采用PKI数字证书的形式
- 利用‘公私钥对’实现非对称算法
- 采取静态和动态数据认证
- 依据卡片和终端不同的参数设置

标准借贷记交易流程和交易类型



关于电子现金(EC)和QPBOC

Advanced Card Systems Ltd.
Card & Reader Technologies

小额支付的相关概念

基于标准借贷记的小额支付

基于快速借贷记的小额支付(QPBOC)

双界面（接触式/非接触式）

非接触式

标准借记贷记

关于电子现金(EC)

- PBOC规范中关于电子现金(EC)的概念在第十三部分《基于借贷记应用的小额支付规范》中进行了定义。电子现金是一种可以用于脱机应用的小额支付应用。

- 在原来借贷记应用的基础上增加了电子现金余额、电子现金余额上限、电子现金单笔交易限额、电子现金重置阈值等数据元来完成小额的电子现金脱机支付交易。

关于QPBOC

- QPBOC是在PBOC规范的第十二部分《非接触式IC卡支付规范》中进行描述的。可以概括的说，QPBOC是改进了交易速度的PBOC借贷记应用与电子现金小额支付应用的结合体。

- 在交易流程处理、加密算法实现和认证数据选择方面，QPBOC和标准借贷记应用以及基于标准借贷记的小额支付电子现金应用存在很大差异，主要是进行了流程的简化以便加快非接触界面的交易处理速度。

产品特性

Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-P产品特性

共同特性

- 一块芯片支持多种界面（接触式、双界面、非接触）。
- 标准/认证
  - Java Card 3.0.4
  - Global Platform 2.2.1
  - Mapping Guidelines 1.0.1
  - CC EAL5+ (芯片级)
  - EMVCo (芯片级)
  - 通过银行卡检测中心(BCTC)的PBOC 3.0认证
  - 全面支持PBOC 3.0中定义的DC/EC QPBOC
- 加密功能
  - DES/3DES
  - RSA (最高2048位)
  - HASH:SHA1, SHA224, SHA256, SHA384, SHA512
  - SM2/3/4

双界面

- 12 KB EEPROM
- 符合ISO 7816第1-4部分
- 符合ISO 14443 A类标准
- T=0协议
- T=1协议
- T=CL协议（非接触界面）

接触式

- 大容量EEPROM:12 KB
- 符合ISO 7816第1-4部分
- T=0协议
- T=1协议

非接触

- 12 KB EEPROM
- 符合ISO 14443 A类标准
- T=CL协议（非接触界面）

技术规格

智能卡特性	
界面	双界面/接触式/非接触
通信速率(kbps)	9.6 – 625 (接触式) 106 – 848 (非接触)
EEPROM (KB)	12
加密功能	
RSA	768 - 2048位
DES/3DES	56/112位
HASH	SHA1,SHA224,SHA256,SHA384, SHA512
SM2/SM3/SM4	✓
认证/标准	
PBOC	3.0
Java Card Classic	v3.0.4
Global Platform	v2.2.1
ISO 7816 – 1/2/3/4 T=0/T=1	T=0, T=1
ISO 14443 – A/B类	仅A类
CC EAL5+（芯片级）	✓

产品应用

Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-P应用领域


ATM交易
电子支付
银行卡相关
应用
小额支付
银行卡
积分卡
预付卡
第三方支付
相关应用
市民卡
水电缴费
acs
ACOS J
2086 0852 2791 7873
ADVANCED CARD SYSTEMS
Java

谢谢!

Advanced Card Systems Ltd.
Card & Reader Technologies

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