ACOSJ-P

Java Card – PBOC 3.0

Advanced Card Systems Ltd.
Card & Reader Technologies

Outline

1. Product Overview
2. What is PBOC 3.0?
3. What is DC?
4. What is EC and QPBOC?
5. Product Features
6. Product Application
    a. Bank Card Application
    b. Third-Party Payment Application

Product Overview

Advanced Card Systems Ltd.
Card & Reader Technologies

Product Overview

ACOSJ-P Products

Contact\Contactless\Combi
(12 KB EEPROM)

Module

Contact Interface
(12 KB EEPROM)

Full-sized Card

Contactless Interface
(12 KB EEPROM)

Full-sized Card

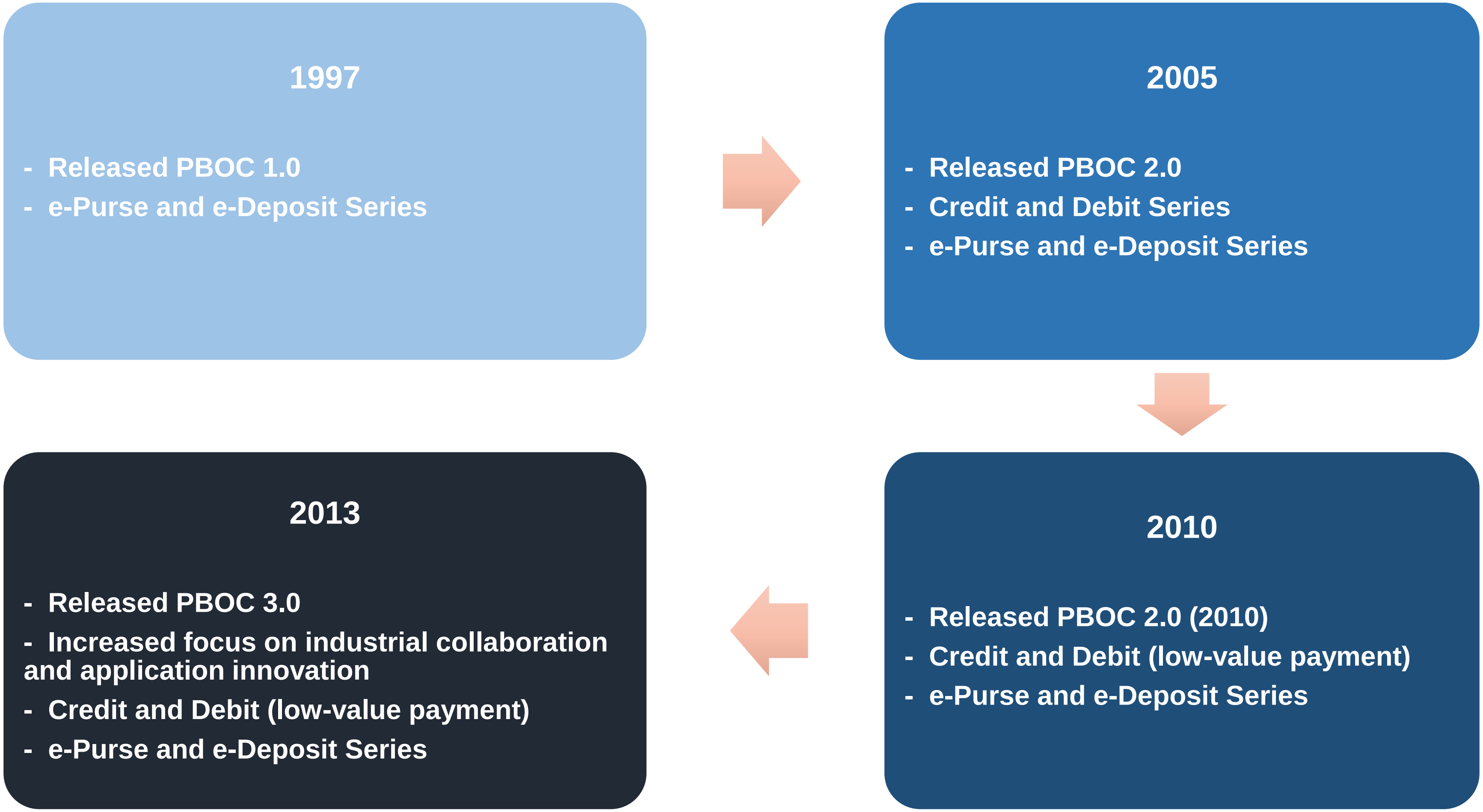
Combi Interface
(12 KB EEPROM)

Full-sized Card

What is PBOC 3.0?

Advanced Card Systems Ltd.
Card & Reader Technologies

Development Process of the PBOC Standard



1997

- Released PBOC 1.0
- e-Purse and e-Deposit Series

2005

- Released PBOC 2.0
- Credit and Debit Series
- e-Purse and e-Deposit Series

2010

- Released PBOC 2.0 (2010)
- Credit and Debit (low-value payment)
- e-Purse and e-Deposit Series

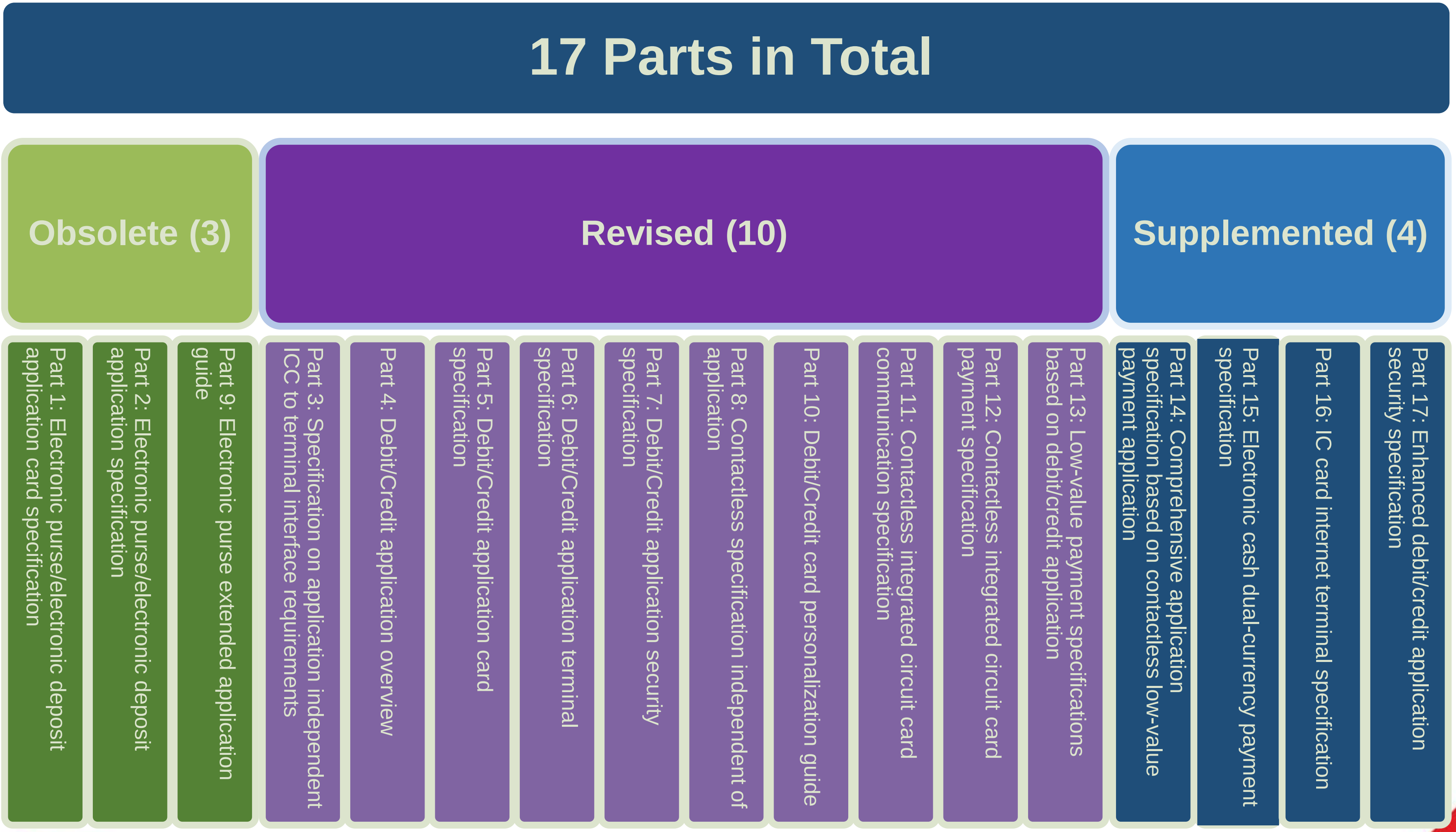
2013

- Released PBOC 3.0
- Increased focus on industrial collaboration and application innovation
- Credit and Debit (low-value payment)
- e-Purse and e-Deposit Series

acs

中国人民银行
THE PEOPLE'S BANK OF CHINA

Content of PBOC 3.0



17 Parts in Total

Obsolete (3)

- Part 1: Electronic purse/electronic deposit application card specification
- Part 2: Electronic purse/electronic deposit application specification
- Part 9: Electronic purse extended application guide

Revised (10)

- Part 3: Specification on application independent ICC to terminal interface requirements
- Part 4: Debit/Credit application overview
- Part 5: Debit/Credit application card specification
- Part 6: Debit/Credit application terminal specification
- Part 7: Debit/Credit application security specification
- Part 8: Contactless specification independent of application
- Part 10: Debit/Credit card personalization guide
- Part 11: Contactless integrated circuit card communication specification
- Part 12: Contactless integrated circuit card payment specification
- Part 13: Low-value payment specifications based on debit/credit application

Supplemented (4)

- Part 14: Comprehensive application specification based on contactless low-value payment application
- Part 15: Electronic cash dual-currency payment specification
- Part 16: IC card internet terminal specification
- Part 17: Enhanced debit/credit application security specification

PBOC 3.0 Function Classification

Basic Functions

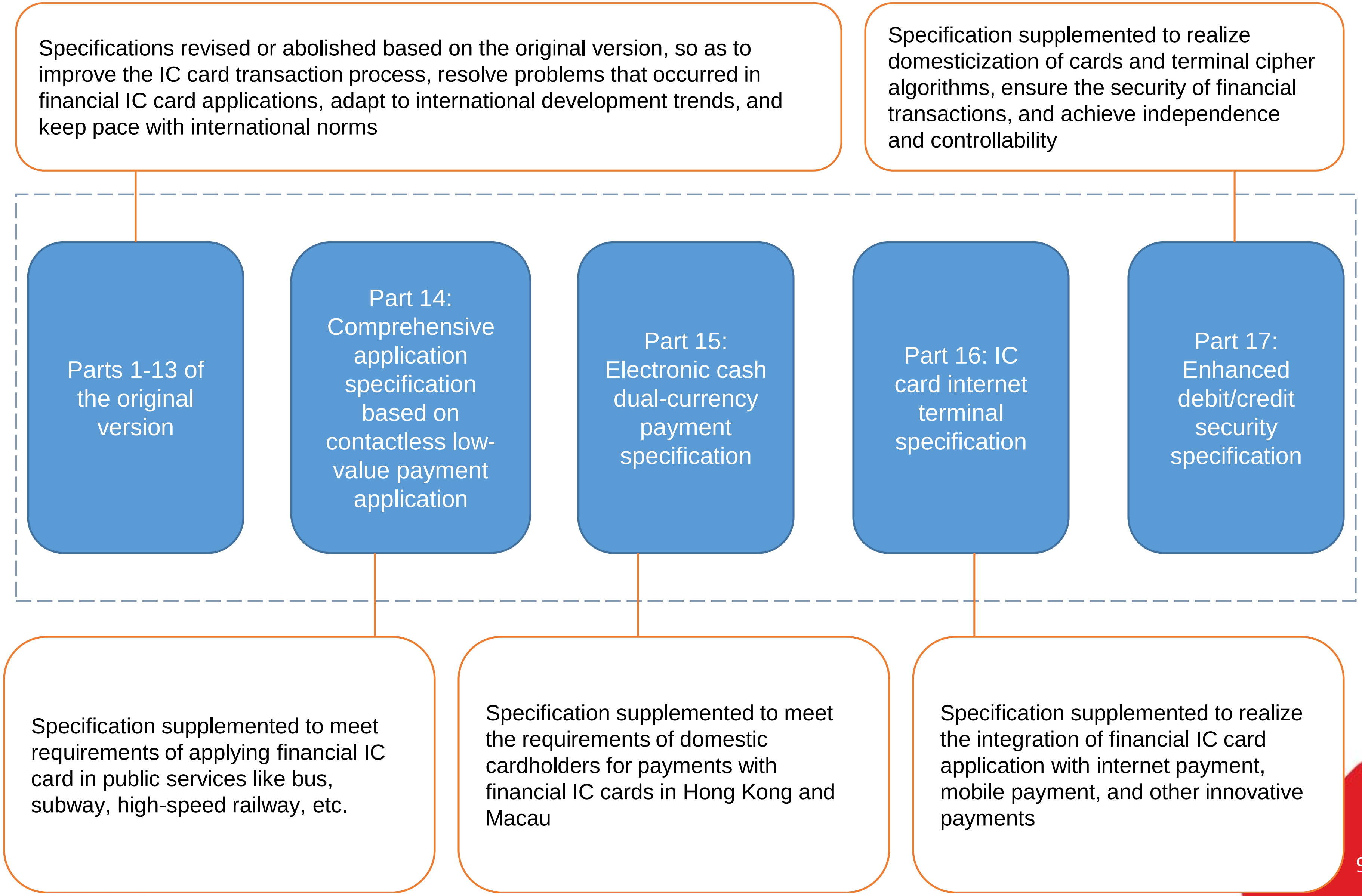
- Standard debit/credit
- Low-value payment based on standard debit/credit
- Contactless IC card payment

Note: *PBOC 3.0 added the cash load log function, contactless transaction log function, new version FDDA, etc.*

Extended Functions

- Contactless low-value payment application
- Dual-currency electronic cash (EC) application
- Enhanced security algorithm
- IC card Internet terminal

Main Functions Upgraded in PBOC 3.0



Specifications revised or abolished based on the original version, so as to improve the IC card transaction process, resolve problems that occurred in financial IC card applications, adapt to international development trends, and keep pace with international norms

Specification supplemented to realize domesticization of cards and terminal cipher algorithms, ensure the security of financial transactions, and achieve independence and controllability

Parts 1-13 of the original version

Part 14: Comprehensive application specification based on contactless low-value payment application

Part 15: Electronic cash dual-currency payment specification

Part 16: IC card internet terminal specification

Part 17: Enhanced debit/credit security specification

Specification supplemented to meet requirements of applying financial IC card in public services like bus, subway, high-speed railway, etc.

Specification supplemented to meet the requirements of domestic cardholders for payments with financial IC cards in Hong Kong and Macau

Specification supplemented to realize the integration of financial IC card application with internet payment, mobile payment, and other innovative payments

What is DC?

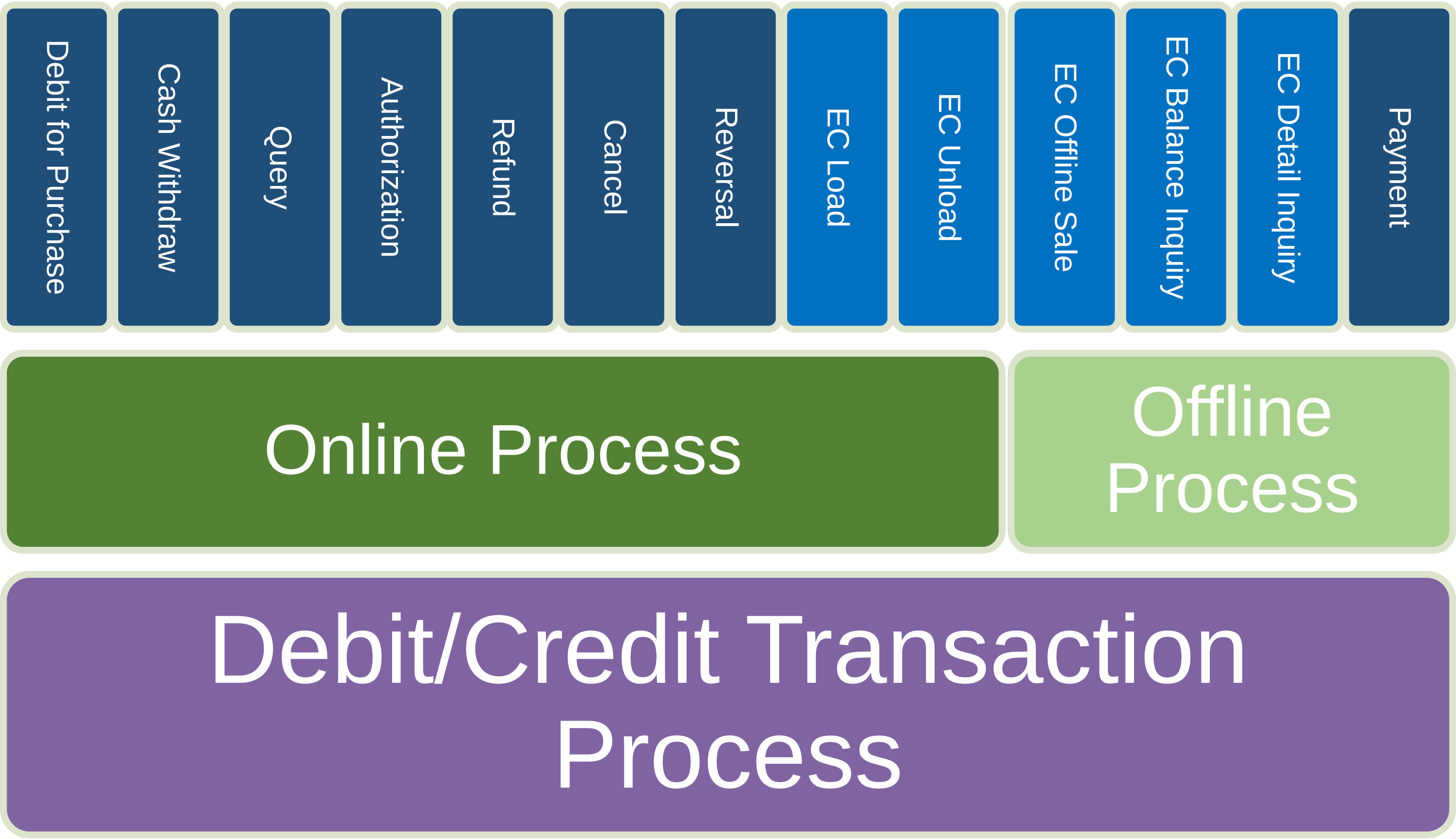
Advanced Card Systems Ltd.
Card & Reader Technologies

What is DC?

The PBOC debit/credit (DC) application is rooted in EMV 2000. The application realizes offline/online payment at POS terminals and cash withdrawal transactions at ATM terminals by:

- Using the format of PKI digital certificates
- Realizing the asymmetric algorithm through “public key pair”
- Adopting static and dynamic data authentication
- Referring to different parameter settings in the card and the terminal

Standard DC Transaction Process and Types



Debit for Purchase

Cash Withdraw

Query

Authorization

Refund

Cancel

Reversal

EC Load

EC Unload

EC Offline Sale

EC Balance Inquiry

EC Detail Inquiry

Payment

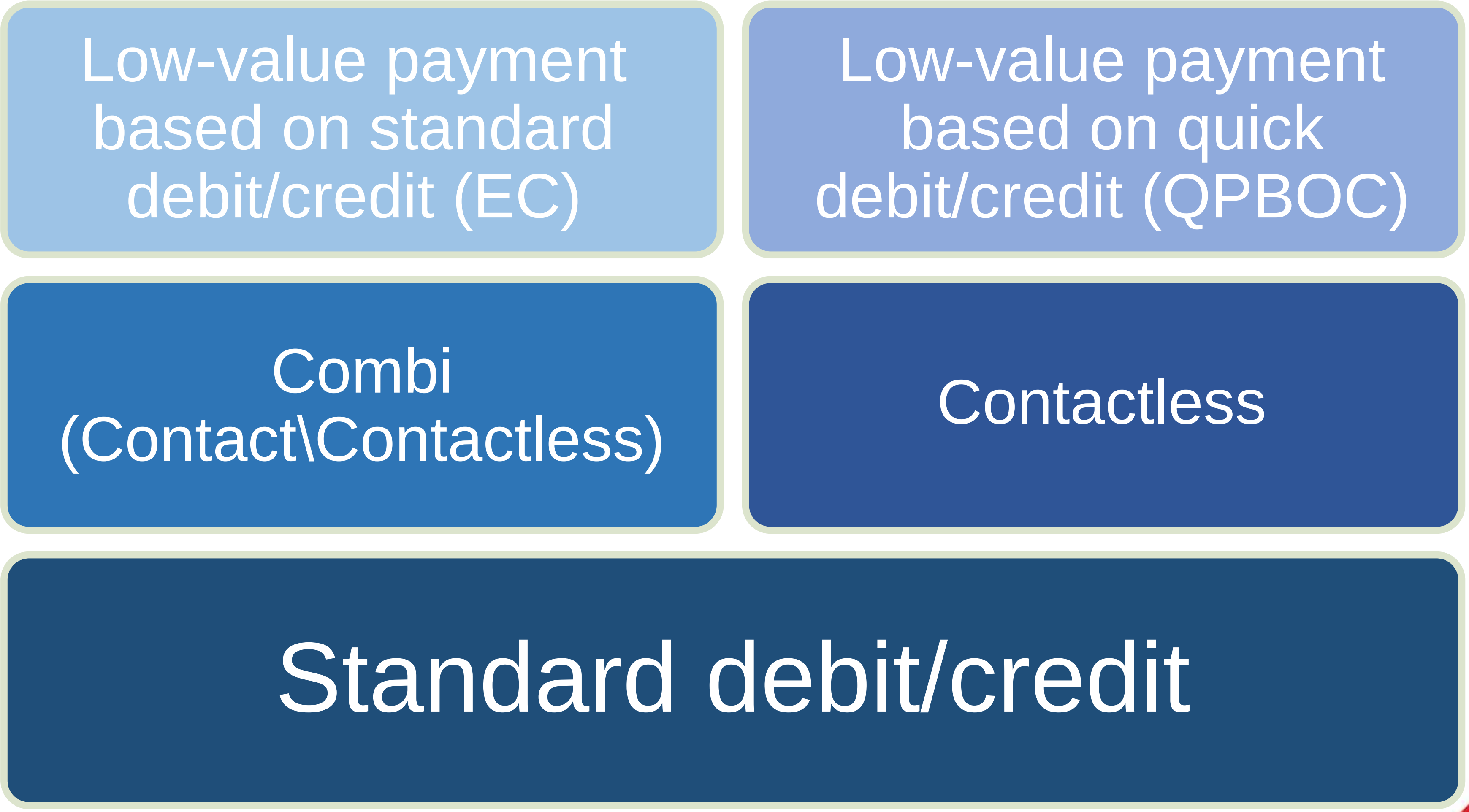
Online Process

Offline Process

Debit/Credit Transaction Process

What is EC & QPBOC?

Concepts Related to Low-value Payment



Low-value payment based on standard debit/credit (EC)

Low-value payment based on quick debit/credit (QPBOC)

Combi (Contact\Contactless)

Contactless

Standard debit/credit

What is EC?

- The concept of EC is defined in PBOC Part 13: Low-value payment specifications based on debit/credit application. EC is a low-value payment application that can be used in offline transactions.

- To complete low-value EC offline payment transactions, data elements such as EC Balance, EC Balance Upper Limit, EC Single Transaction Limit, and EC Reset Threshold are added on the basis of the original DC application.

What is QPBOC?

- QPBOC is described in PBOC Part 12: Contactless integrated circuit card payment specification. In a nutshell, QPBOC is a combination of the PBOC DC application with improved transaction speed and the EC small-value payment application.

- In aspects of transaction process handling, encryption algorithm implementation, and authentication data selection, QPBOC is greatly different from the standard DC application and the low-value payment EC application developed on the basis of the standard DC application. The main difference is the QPBOC process is simplified to speed up the transaction handling of the contactless interface.

Product Features

Advanced Card Systems Ltd.
Card & Reader Technologies

ACOSJ-P Product Features

Common Features

- Same chip supports all interfaces (contact, combi, contactless).
- Compliance/Certifications
  - Java Card 3.0.4
  - Global Platform 2.2.1
  - Mapping Guidelines 1.0.1
  - CC EAL5+ (chip level)
  - EMVCo (chip level)
  - Passed PBOC 3.0 authentication of Bank Card Test Center (BCTC)
  - Full support for DC/EC QPBOC defined in PBOC 3.0
- Cryptographic Features
  - DES/3DES
  - RSA (up to 2048 bits)
  - HASH: SHA1, SHA224, SHA256, SHA384, SHA512
  - SM2/3/4

Combi Interface

- 12 KB EEPROM
- Compliance with ISO 7816 Parts 1-4
- Compliance with ISO 14443 Type A standard
- T=0 protocol
- T=1 protocol
- Protocol T=CL (for contactless interface)

Contact Interface

- Large-sized EEPROM: 12 KB
- Compliance with ISO 7816 Parts 1-4
- T=0 protocol
- T=1 protocol

Contactless Interface

- 12 KB EEPROM
- Compliance with ISO 14443 Type A standard
- Protocol T=CL (for contactless interface)

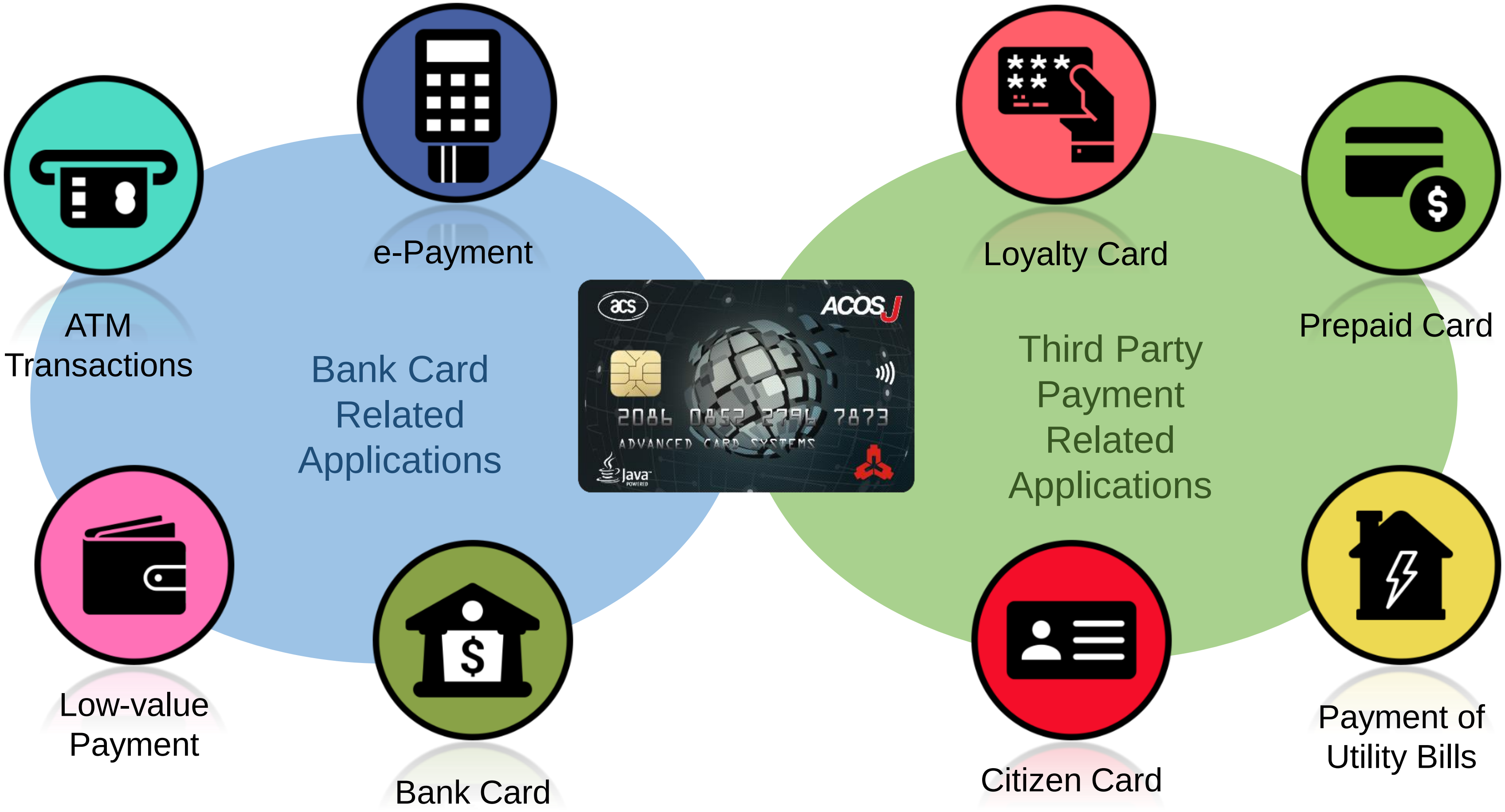
Technical Specifications

Smart Card Features	
Interface	Combi/ Contact/ Contactless
Communication Speed (kbps)	9.6 – 625 (Contact) 106 – 848 (Contactless)
EEPROM (KB)	12
Cryptographic Capabilities	
RSA	768 to 2048 bits
DES/3DES	56/112-bits
HASH	SHA1,SHA224,SHA256,SHA384, SHA512
SM2/SM3/SM4	✓
Certifications/Compliance	
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 – Type A/B	Type A Only
CC EAL5+ (chip level)	✓

Product Application

Advanced Card Systems Ltd.
Card & Reader Technologies

In what areas can we apply ACOSJ-P?



Bank Card Related Applications

ATM Transactions

e-Payment

Low-value Payment

Bank Card

Third Party Payment Related Applications

Loyalty Card

Prepaid Card

Citizen Card

Payment of Utility Bills

Thank You!

Advanced Card Systems Ltd.
Card & Reader Technologies

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