Mobile Security Application Current Status Overview in Taiwan

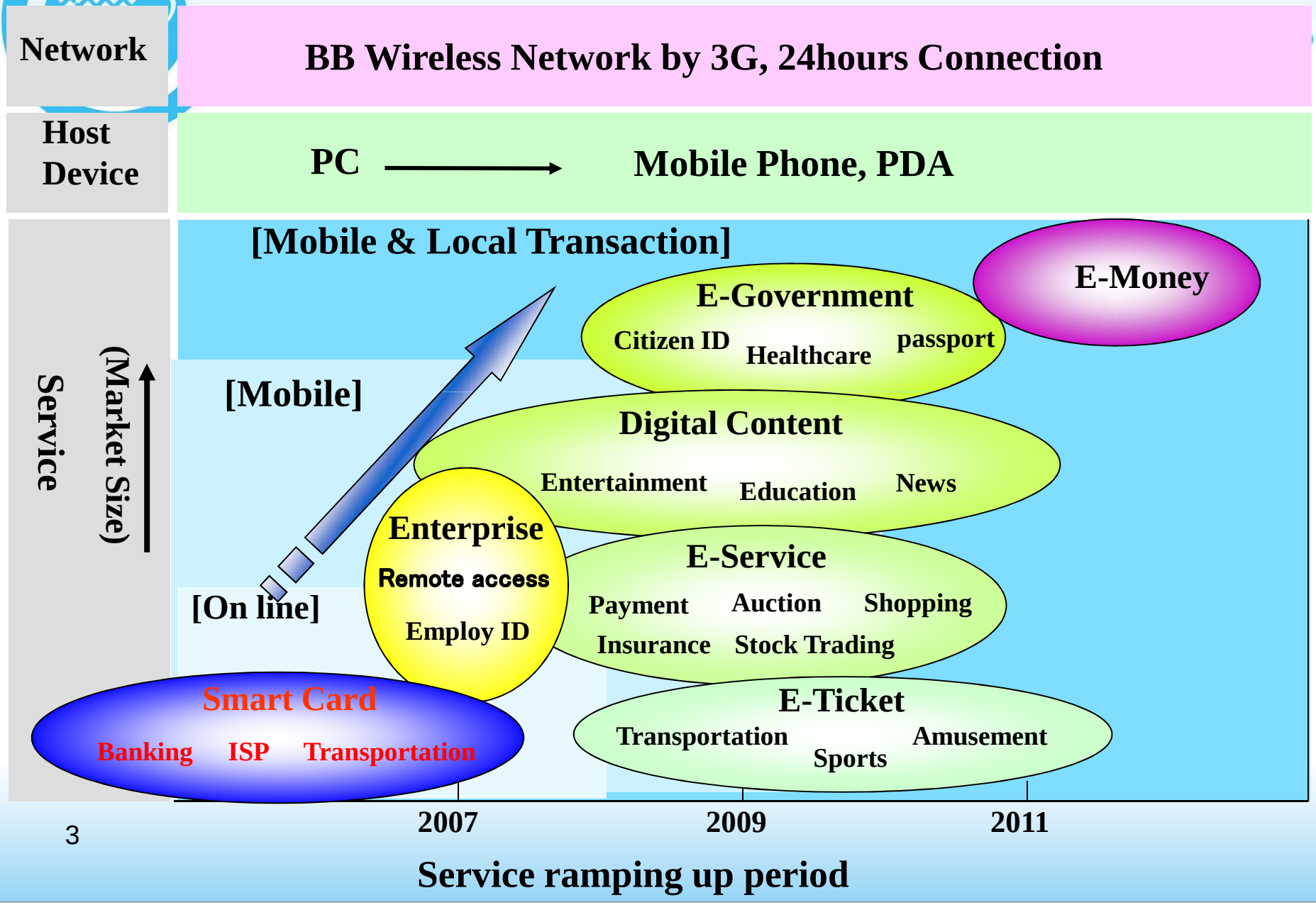
Dr. Char-Shin Miou
Chunghwa Telecom. Co.

April 7, 2011

Content

- Problems and Current Status
- Approach for the Mobile Security Application
- Mobile PKI and Mobile NFC
- Case Study
- Conclusions

Market Trend of E-Commerce to M-Commerce



Mobile Security Applications

Employ

-Enterprise
-Government
-Public org.
(Remote access)

Public

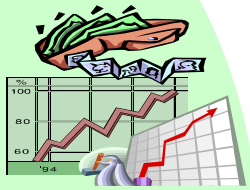
-Citizen card
(Driver license,Passport)
-Health care
-Education

Member

-Mileage Club
-Private Club (Hobby)
-Internet member site

Financial

-e-Money
-Payment
-m-Banking
-Stock Trade

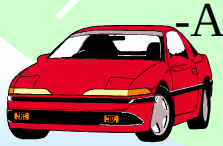


Linkage of Services in Mobile Device

-Advertisement
(Bargain sale,catalog)
-CRM
-Town Guide

Retail

-Content
(movie,
music, game,
publishing)
-Home electronics
-Automotive



Consumer

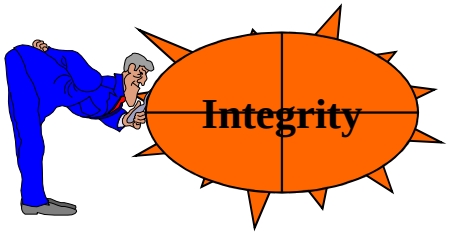
-Network (W-LAN, ISP)
-Transportation
-Telematics
-Insurance
-Travel

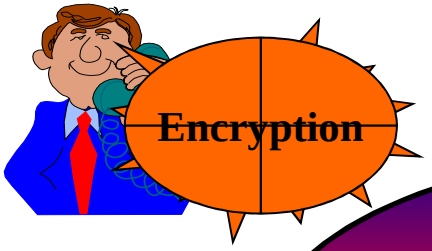
Service

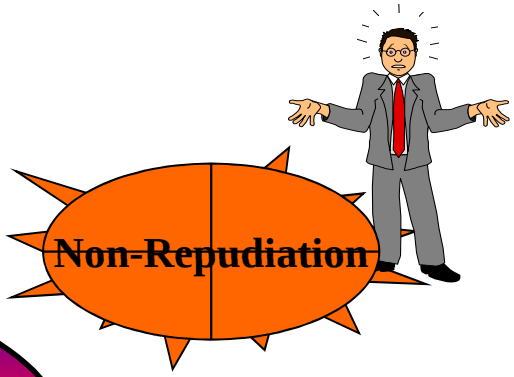
-Sports
-Amusement,
-Cinema
-Concert

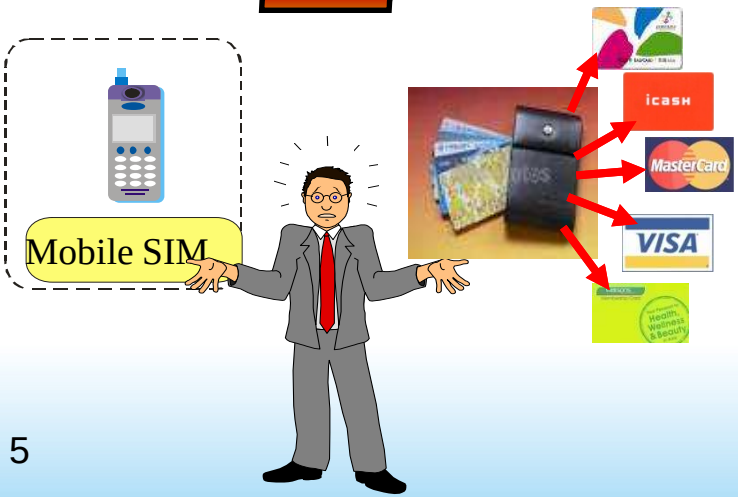
e-Ticket

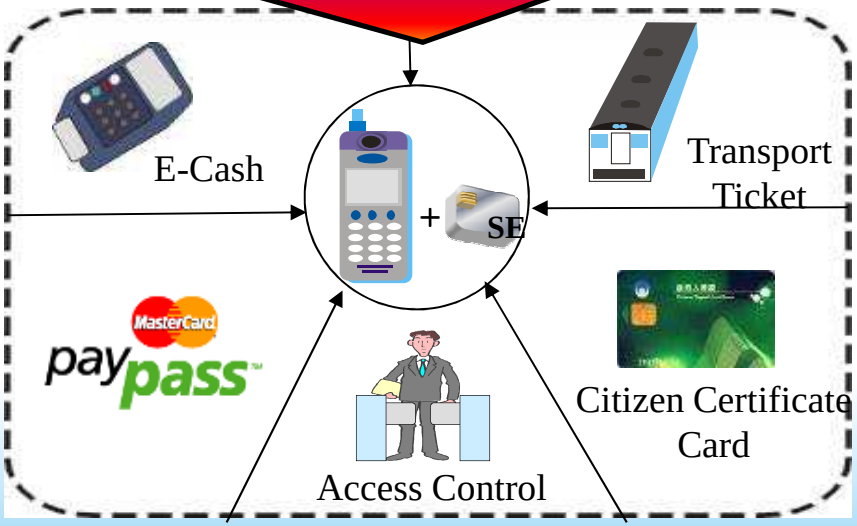
Secure Issues in Mobile Environment







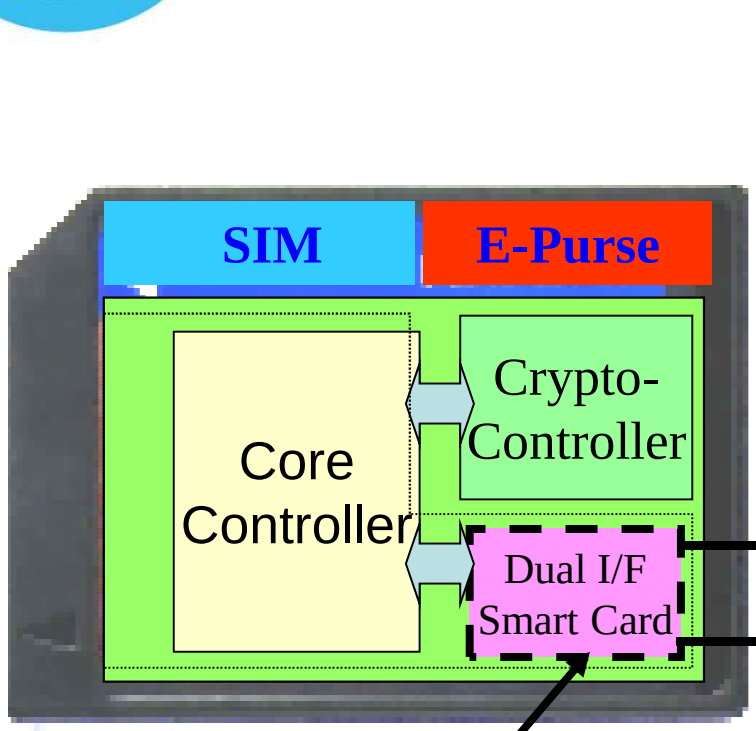


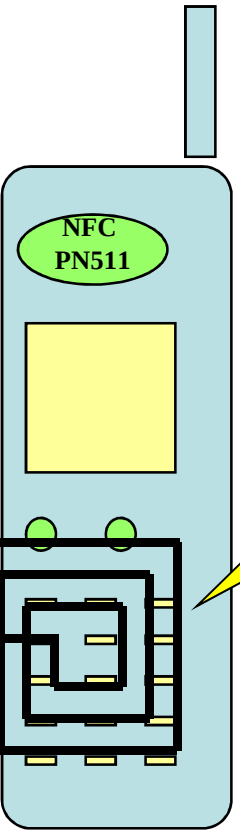


5

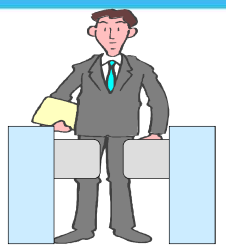
- Problems and current status
- **Approach for the Mobile Security Application**
- Mobile PKI and Mobile NFC
- Case Study
- Conclusions

Dual Interface and Multiple function





- Contact [ISO7816]
- Contact-less [ISO14443]

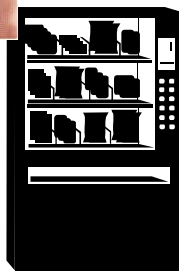


Transportation

Telematics

ISO14443

RFID



Vending Machine

POS

ISO7816

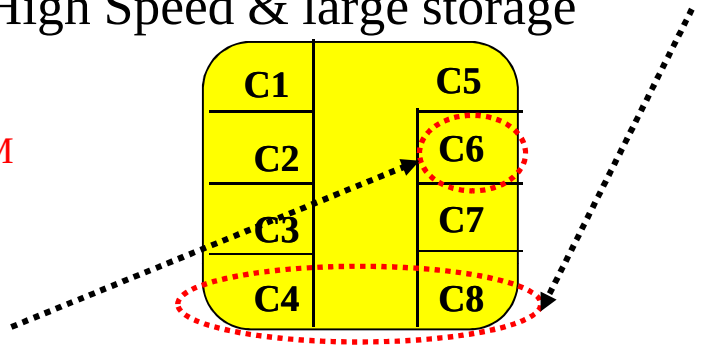
E-ID Service

SIM Card Evolution

☑ High Speed & large storage Interface

- In 2006 Nov., USB was selected as High Speed & large storage Interface by ETSI committee

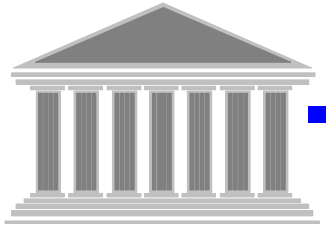
C1、C2、C3、C5、C7: Already used by SIM



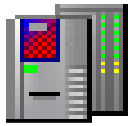
☑ Contact-less Interface

- In 2007 Nov. SWP(Single Wired Protocol) was adapted as contactless interface for NFC (Near Field Communication) service by ETSI and GSMA

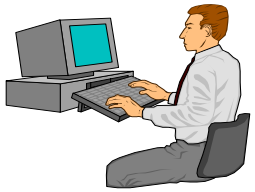
Mobile PKI Service Architecture



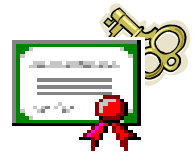
Certification Authority



Registration Authority



RAO



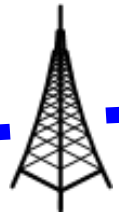
Secure Token for Key & Certificate storage

\+

PKI enable API and Device middleware

User

E-service

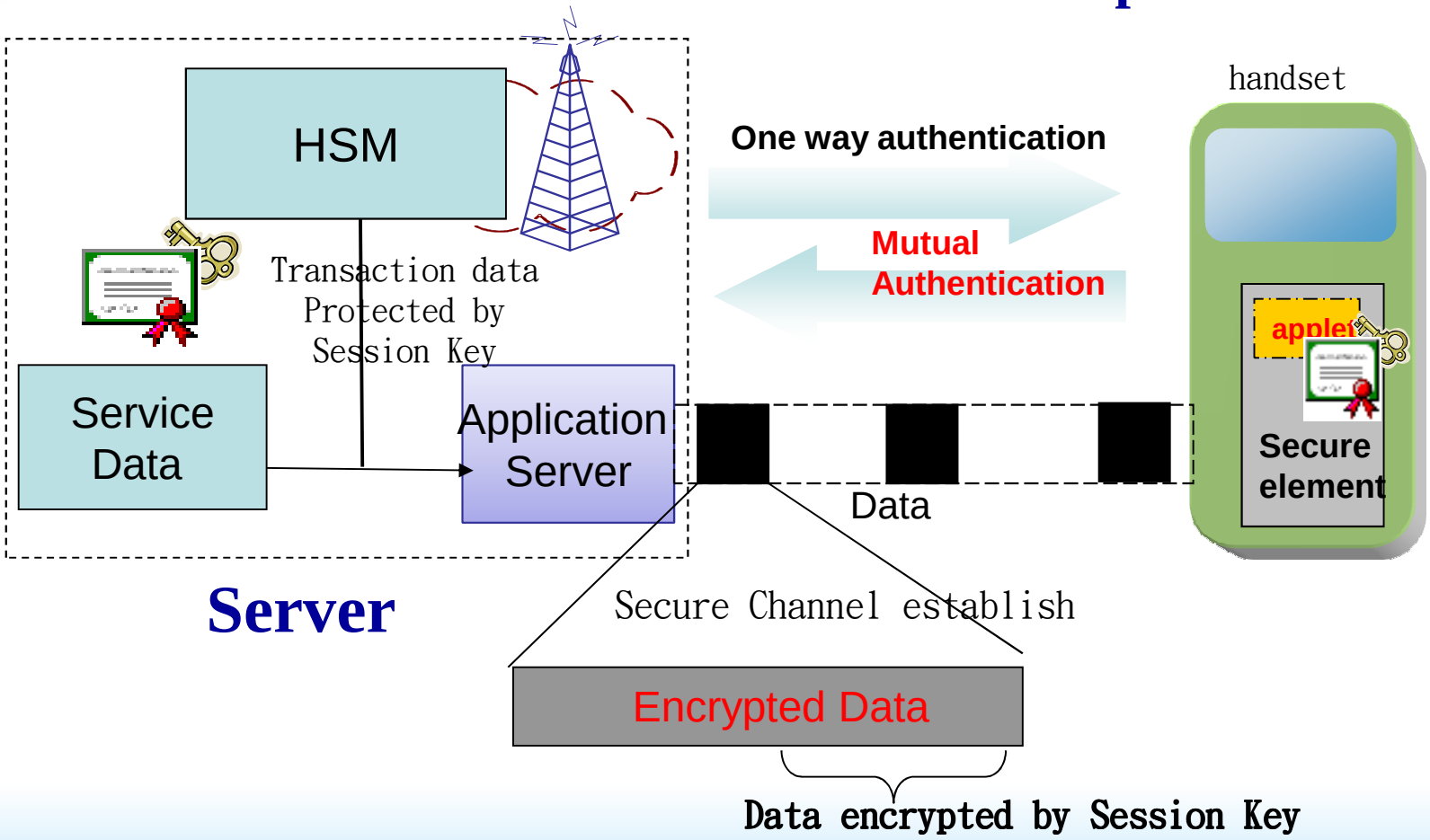


Mobile Network

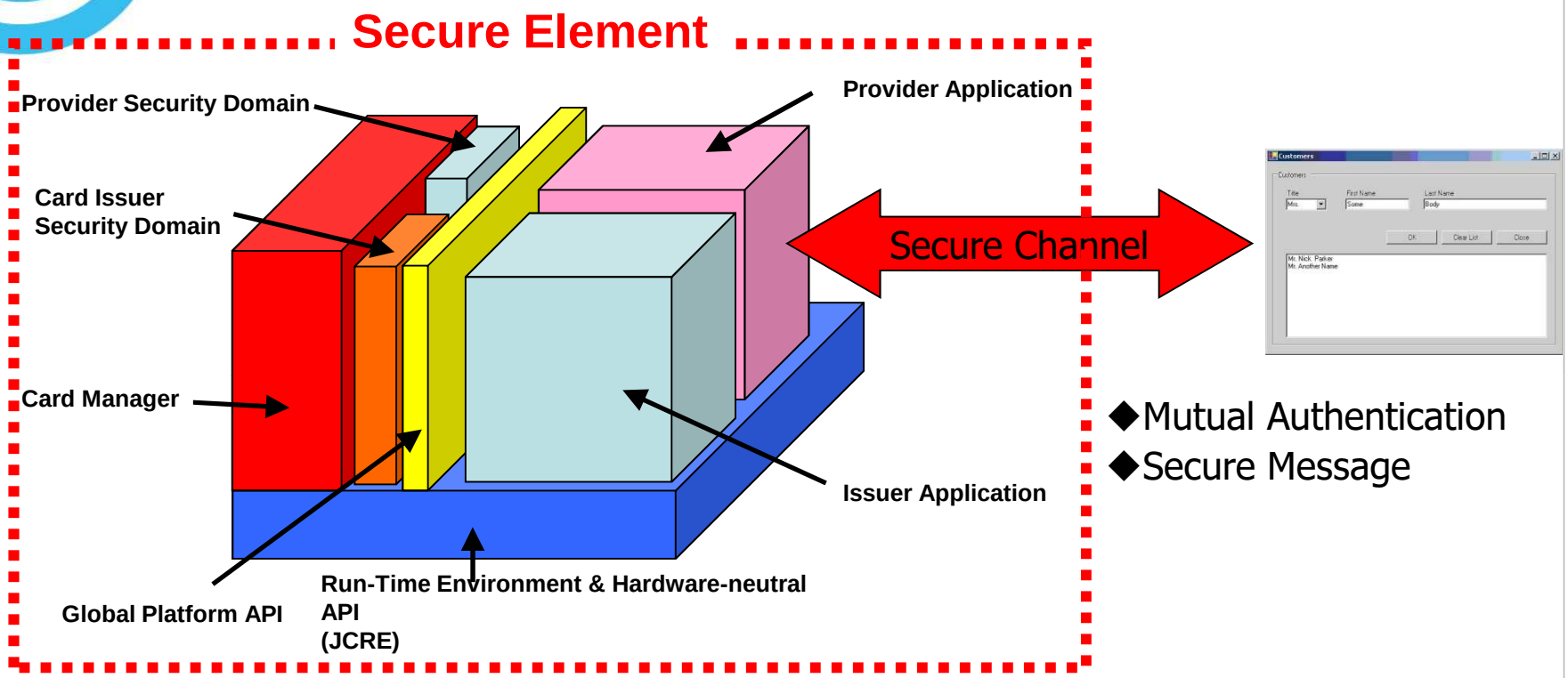
Platform and Mobile Handset

One way authentication → Mutual authentication

Ensure transaction date secure and non-repudiation



What is a SE (Secure Element) ?



- ◆Mutual Authentication
- ◆Secure Message

◆ Key Set:

- ➢ To establish **Secure Channel** between card application (Applet) and host application.
- ➢ A Key Set:
  - ✓ Secure Channel Encryption Key (**S-ENC**)
  - ✓ Secure Channel Message Authentication Code Key (**S-MAC**)
  - ✓ Key Encryption Key (**KEK**)

◆ Security Domain:

- ➢ It is a key container.
- ➢ To store Key Sets belong to an application provider

Mobile Device + Secure Element

Browser-based (MIDlet)

Text-based (STK Menu)

Mobile PKI Enable API

Middleware

Mobile PKCS # 11

JSR 177

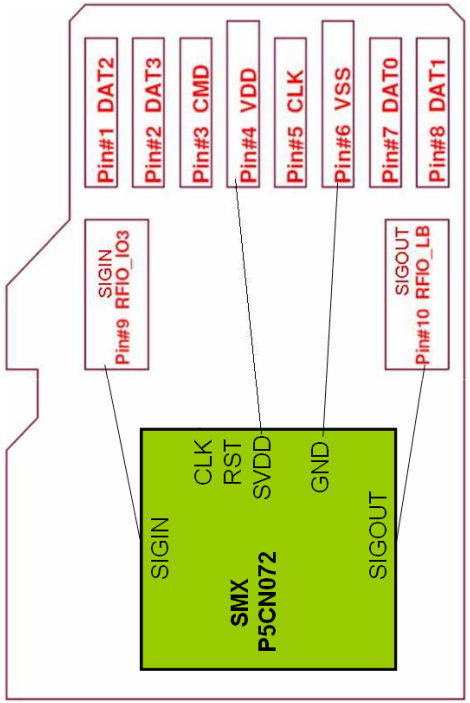
JSR 257

(U)SAT

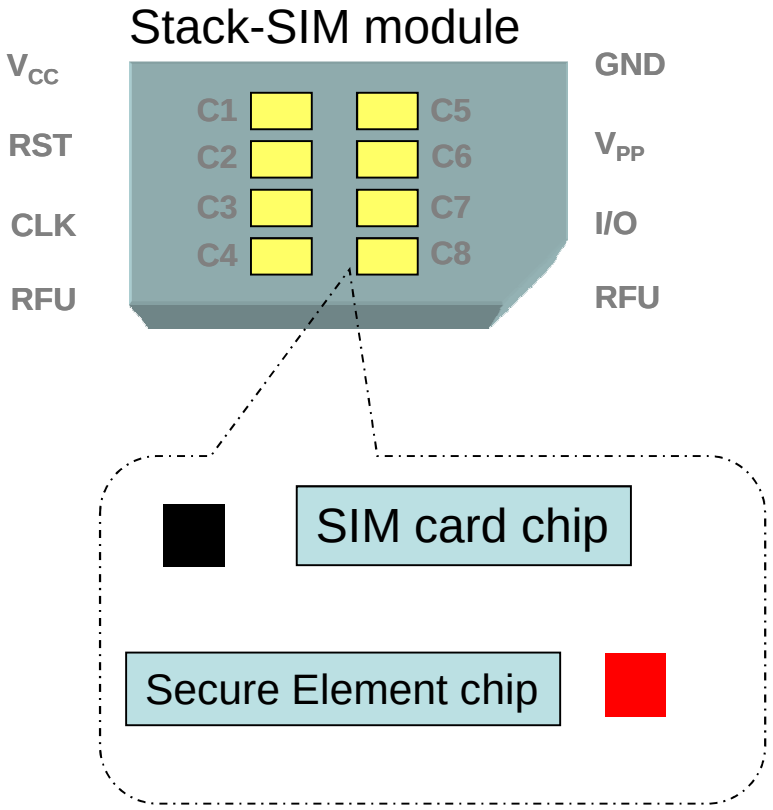
USIM/Secure Element Access interface (ISO 7816/USB/)

J2ME/Native OS (WIN Mobile、iPhone OS、 Android、Symbian…)

Hardware Secure Element Approach

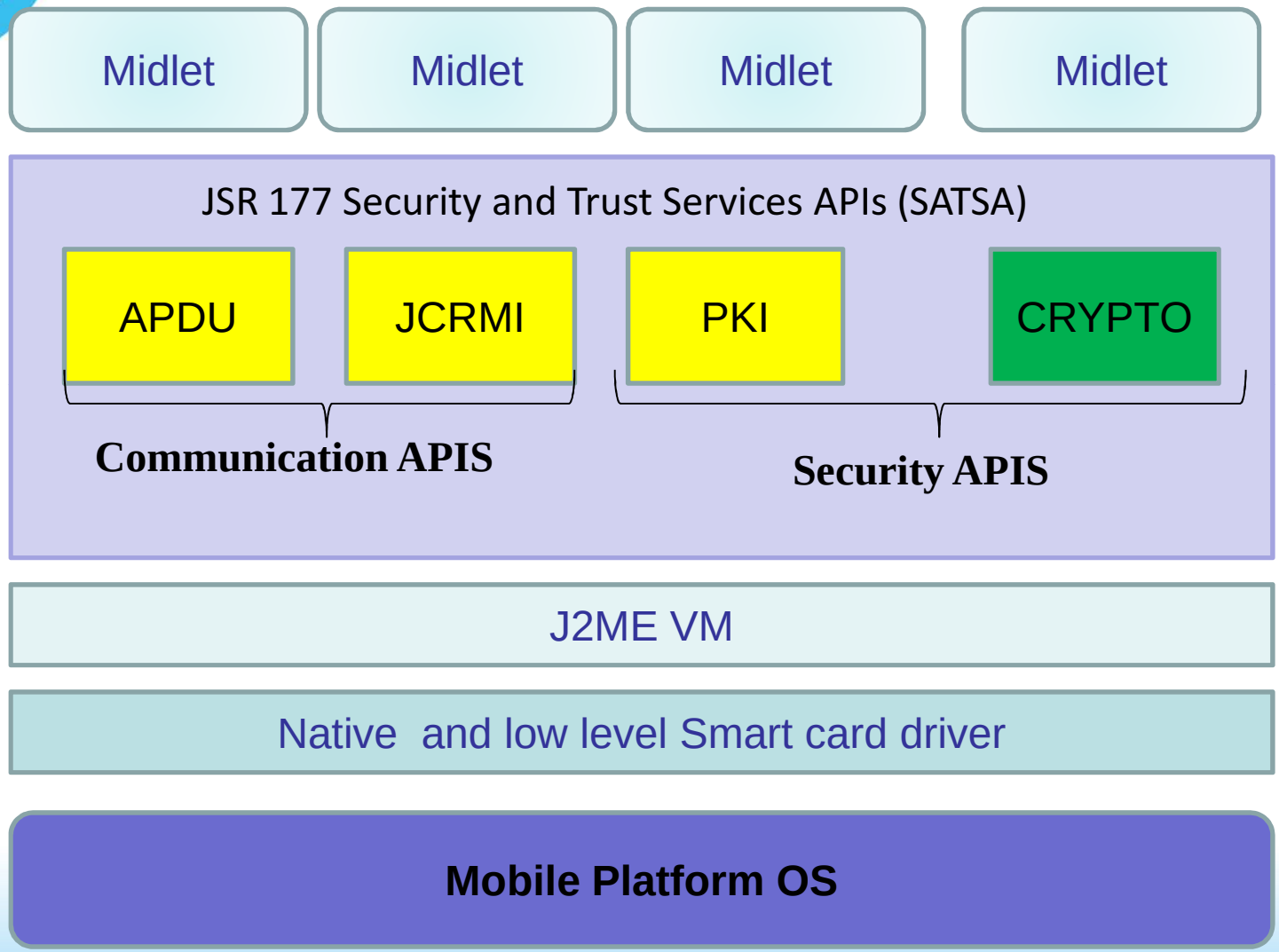


SE in uSD

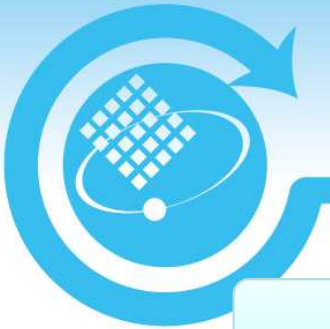


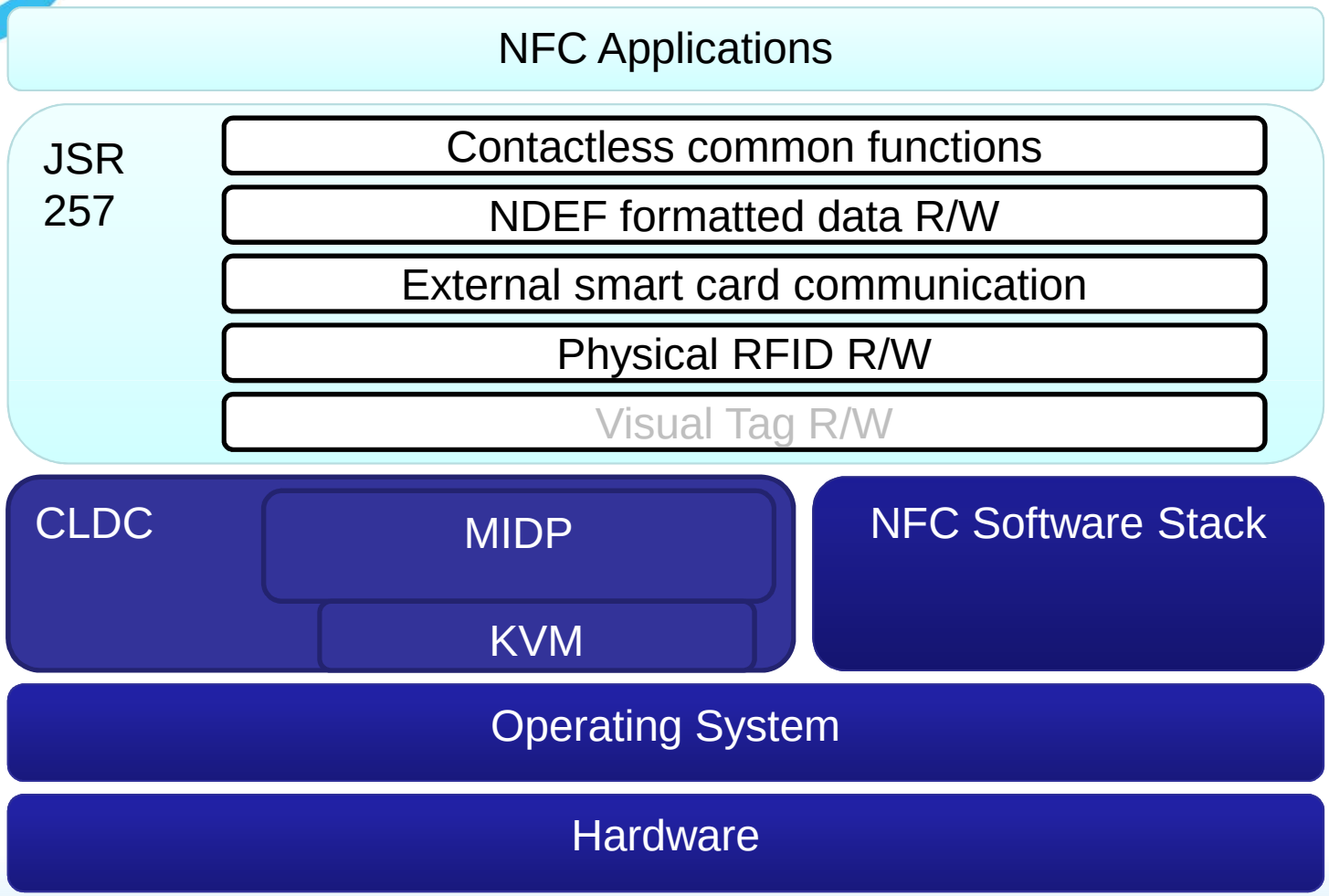
SE in Stack SIM

JSR 177 Architecture

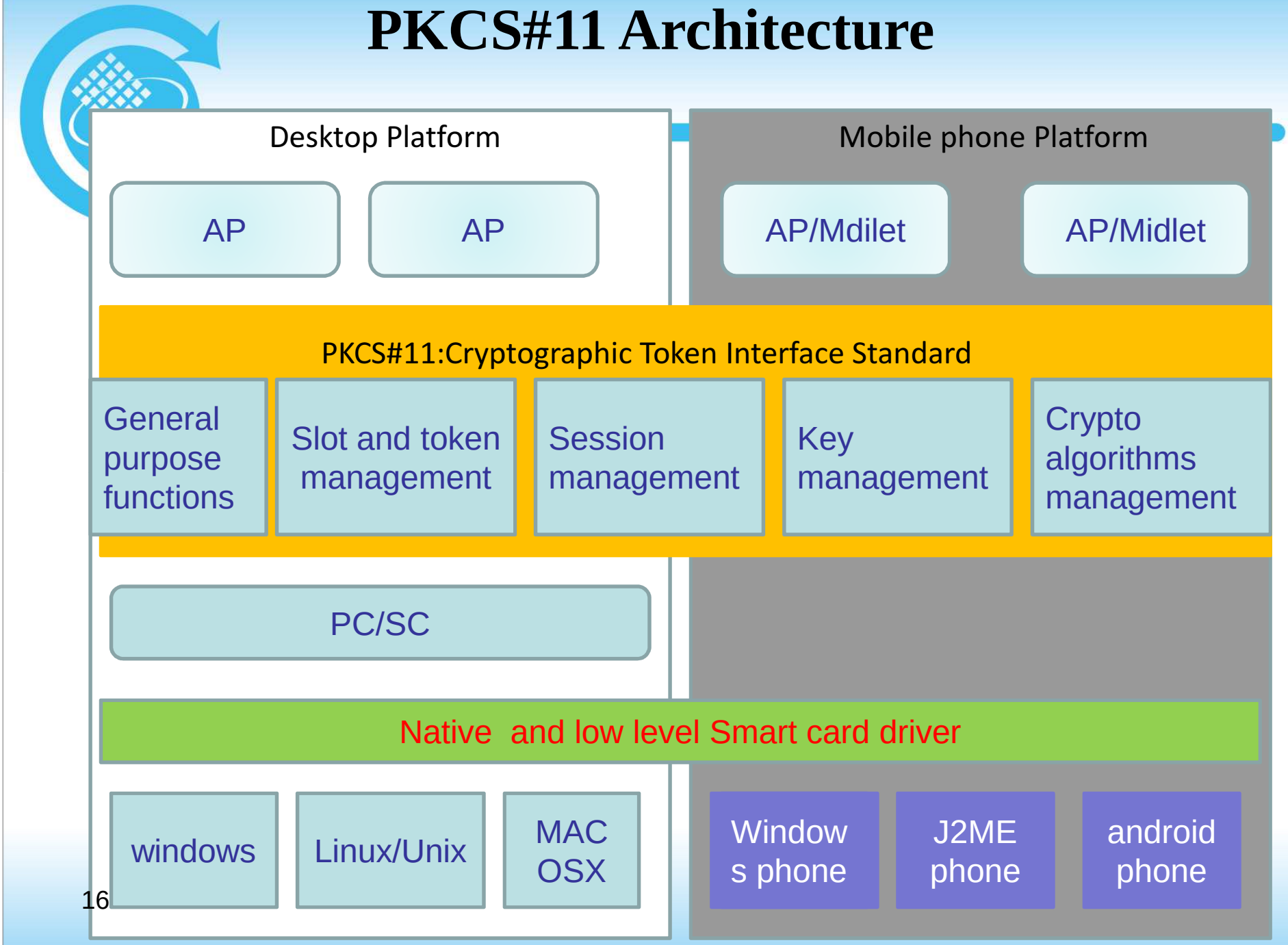


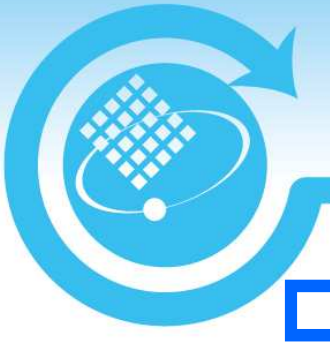
JSR-257




NFC Applications
JSR 257
Contactless common functions
NDEF formatted data R/W
External smart card communication
Physical RFID R/W
Visual Tag R/W
CLDC
MIDP
KVM
NFC Software Stack
Operating System
Hardware

PKCS#11 Architecture





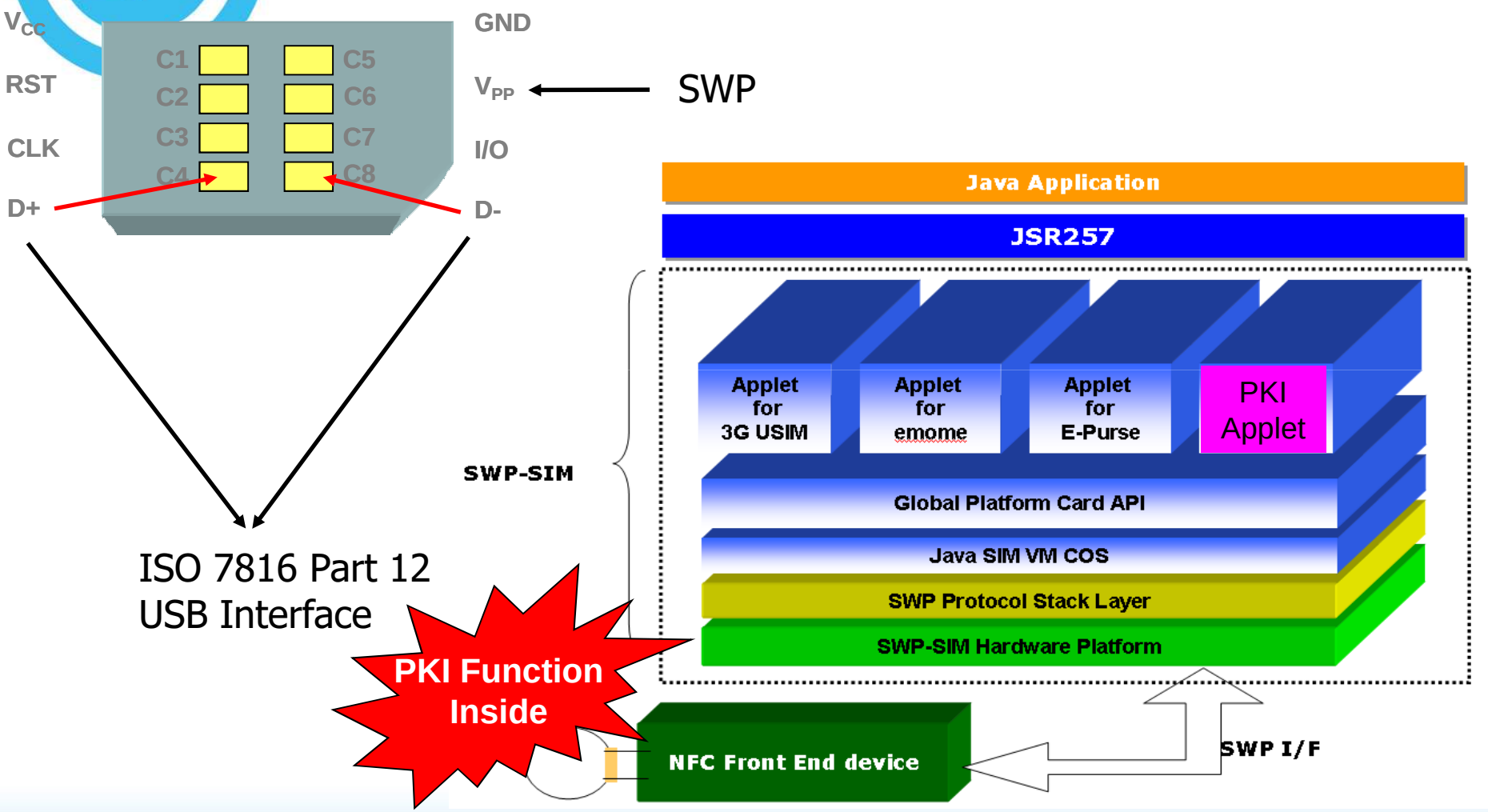
- Problems and current status
- Approach for the Mobile Security Application
- **Mobile PKI and Mobile NFC**
- Case Study
- Conclusions

What is NFC ?

- NFC (Near Field Communication) Provides the way information and services are distributed, paid for and accessed by the connected consumer

- NFC is a wireless technology enabling convenient short-range communication between electronic devices with secure way

SWP SIM Architecture



Defined by GSMA Standard