Development of smart authentication and identification in Asia

Asia PKI Consortium

Dr. Wei-Chung Hwang

weichung.hwang@gmail.com

Nov 16 , 2017

Agenda

- About APKIC
- Background
- Current Development
- New trends
- Way forward

Background of APKIC (1)

- Asia PKI Forum was founded in 2001, and transform to **Asia PKI Consortium** in 2007, with leading organizations from Asia area supported by government and industrial sectors
- Objectives:
  - Promote the applications of PKI in e-commerce, e-government, e-financial, etc.
  - Advance the interoperability among PKIs in countries in the Asia region
  - Collaboration with global community to deliver a comprehensive framework of e-authentication

Background of APKIC (2)

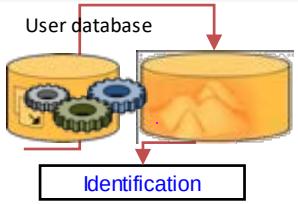
Policy and Technology	Promotion and Awareness
✓ Asia PKI Interoperability Guideline ✓ CA Responsibilities and Liability ✓ Legal Issues on New Security Technologies ✓ Mutual Recognition of National PKIs (Greater China, ASEAN) ✓ Cross Border Applications(Trade, Financial)	✓ Asia PKI Case Study ✓ Asia PKI Company List and Total Solutions ✓ Asia PKI Best Practice Award ✓ Asia PKI Innovation Award ✓ PKI Market Survey ✓ International Collaboration(PAA, AFACT, APSCA, FIDO, etc.)

It’s all about…

(e)-Authentication

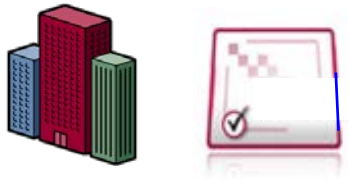
Authenticate the token
Authorization access
Accounting usage

(e)-Identification



The process of presenting an identity to a system

(e)-Signature



PKI service issues certificates for strong authentication, encryption and digital signing

Portal of Service、Critical to Security、Key for User Behavior

Enterprise

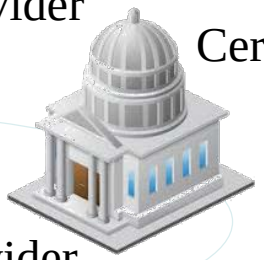
eCommerce

Government

Financial Services

Authentication and Identification: the key to Digital Economy

Service Provider



Certificate Authority

User

Identity Provider

Biometrics

Devices

Token

Password

Public Key Infrastructure

Public Key Cryptography

Cryptography

Identity Management

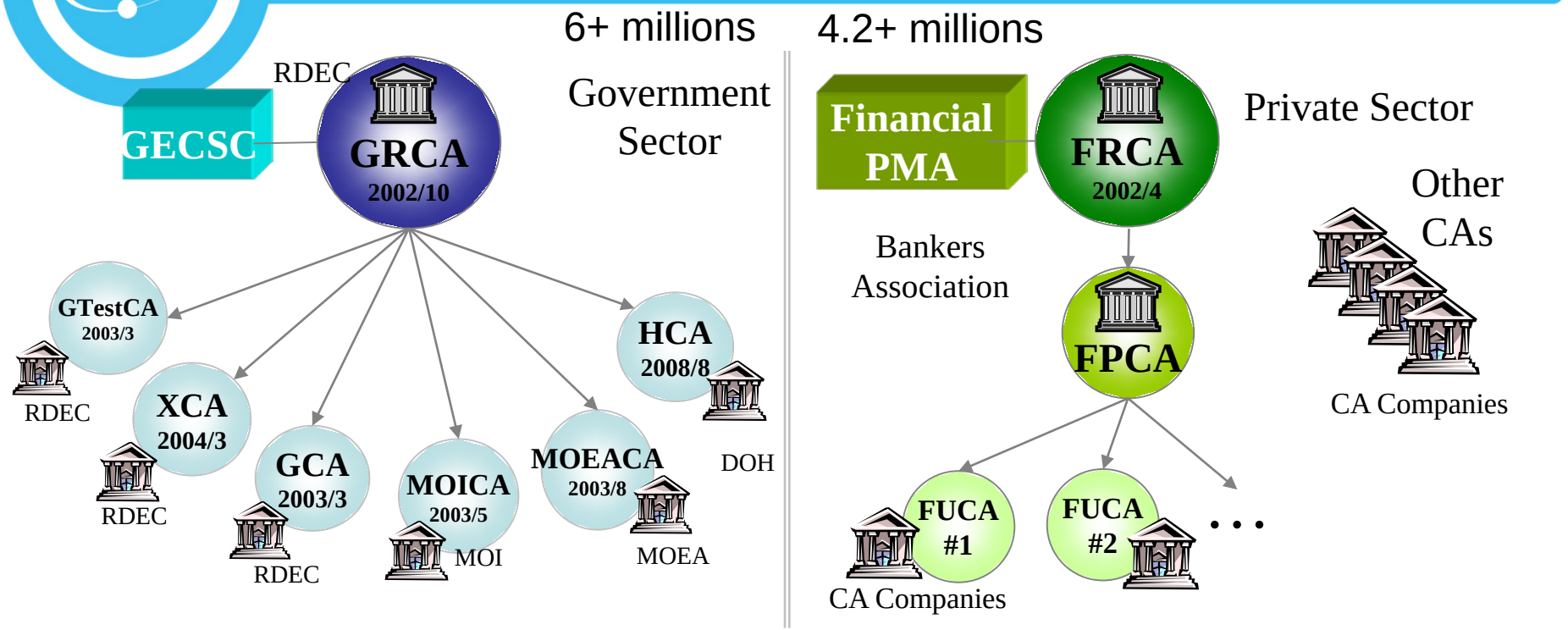
Legal Compliance / Certification

PKI: The infrastructure for digital signature and electronic transactions

Country/ Region	Digital Signature Legislation	National/ Regional PKI	Financial Transaction**	Others**
Korea	✓ (ESA, 1999)	✓ (NPKI, GPKI)	O (mandatory ~ '14)	eID (Optional without PKI) e-Government, e-Commerce
China	✓ (ESL-16, 2005)	✓ (some regions)	✓ (bank-high-risk) ~17	eID (Optional, with PKI), e-Government, e-Commerce, etc.
India	✓ (ITA-CCA, 2000)	✓ (CCA)	✓ (bank-high-risk)	eID (Mandatory, signed by PKI), e-Government, e-Commerce, etc.
Taiwan	✓ (ESA-10~11, 2002)	✓ (GPKI, FPKI)	✓ (bank-high-risk) (stock-trading)	eID (Optional, with PKI), e-Government, e-Commerce, etc.
Thailand	✓ (ETA-28, 2001)	✓ (NRCA)	O	eID, e-Government, e-Commerce
Hong Kong	✓ (ETO, 2000)	✓ (HKPost)	O	eID (Mandatory, with PKI option), e-Government, e-Commerce, etc.
Macau	✓ (EDSL, 2005)	✓ (eSignTrust)	O	eID (Mandatory, with PKI option), e-Government, e-Commerce, etc.
Japan	✓ (ESaCBA, 2000)	✓ (JPKI)	O	eID (Optional, with PKI option), e-Government, e-Commerce, etc.

** ✓: Mandatory, O: Optional with some use cases

Taiwan's Public Key Infrastructure



Government Applications

Financial Applications

B2B Applications

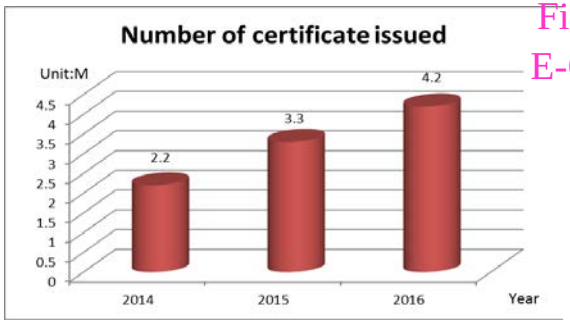
B2C Applications

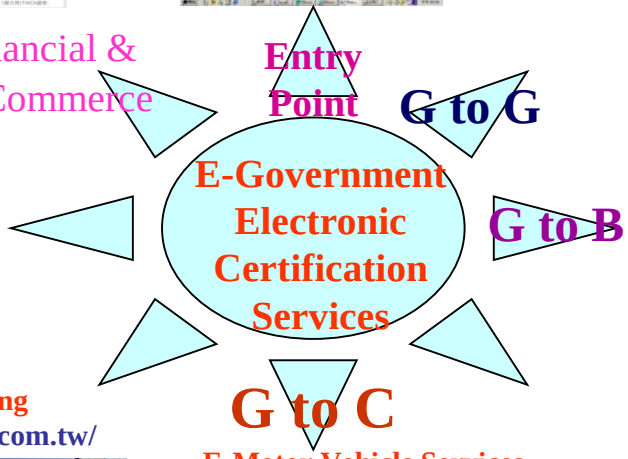
Enterprise Applications

Major Applications of Taiwan's GPKI

E-Government Portal
http://www.gov.tw/ENGLISH/

E-Official Document Interchange
http://www.rdec.gov.tw/mis/eg/edoc.htm





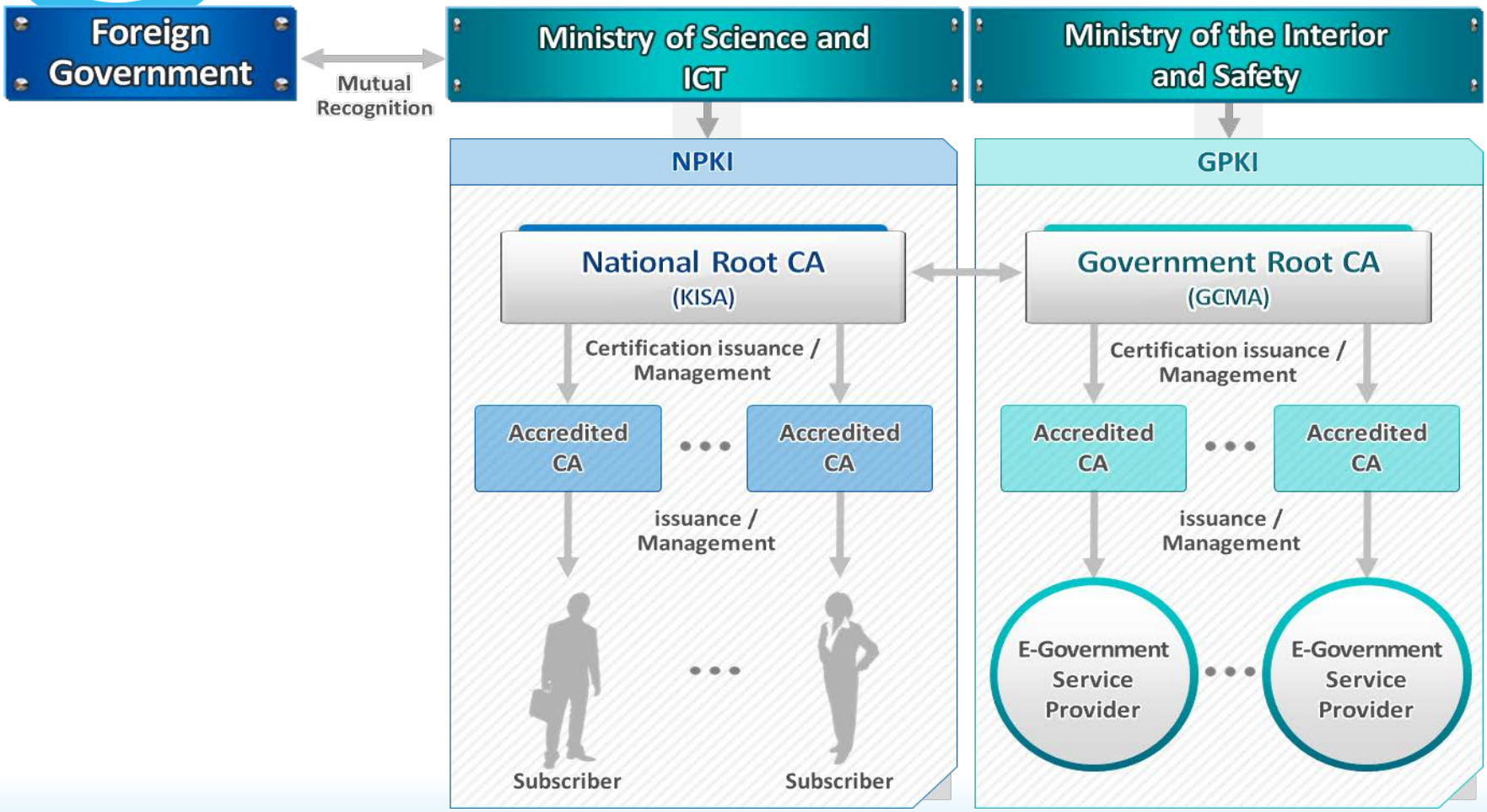
E-Procurement
http://www.geps.gov.tw/

E-Tax Filling
http://www.itax.com.tw/

E-Motor Vehicle Services
http://www.mvdis.gov.tw/

E-Health Insurance
http://202.39.225.21/

Korea's Public Key Infrastructure



Applications of Korea's NPKI

<Internet banking>

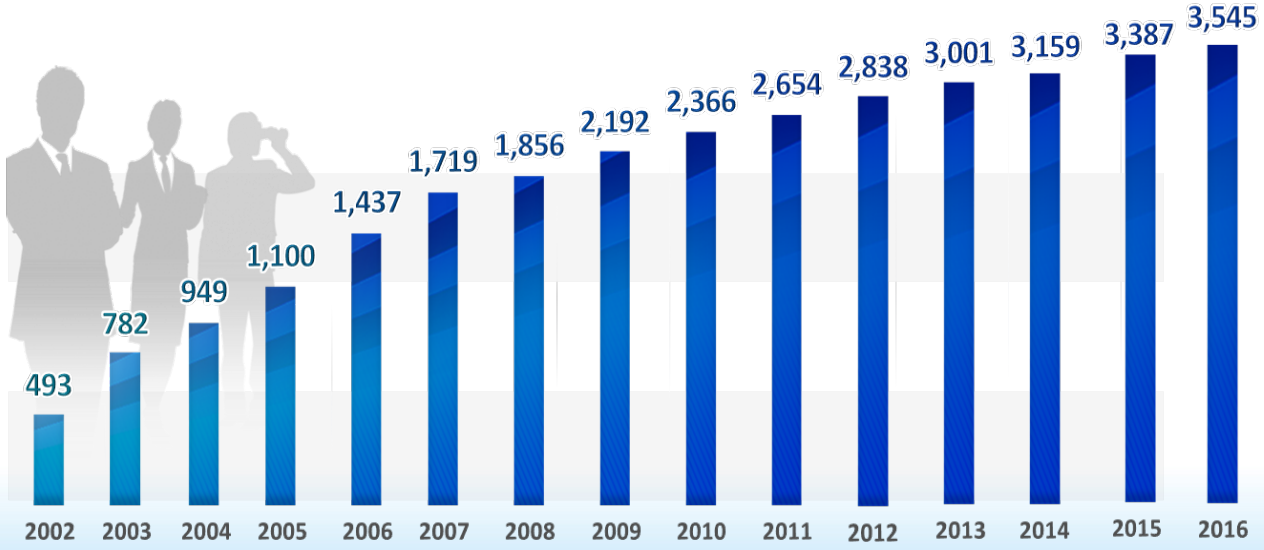
No. of transactions (daily average): 87,500 thousand
Amount (daily average): 42,400 billion Won

<smartphone banking>

No. of transactions (daily average): 52,900 thousand
Amount (daily average): 3,100 billion Won

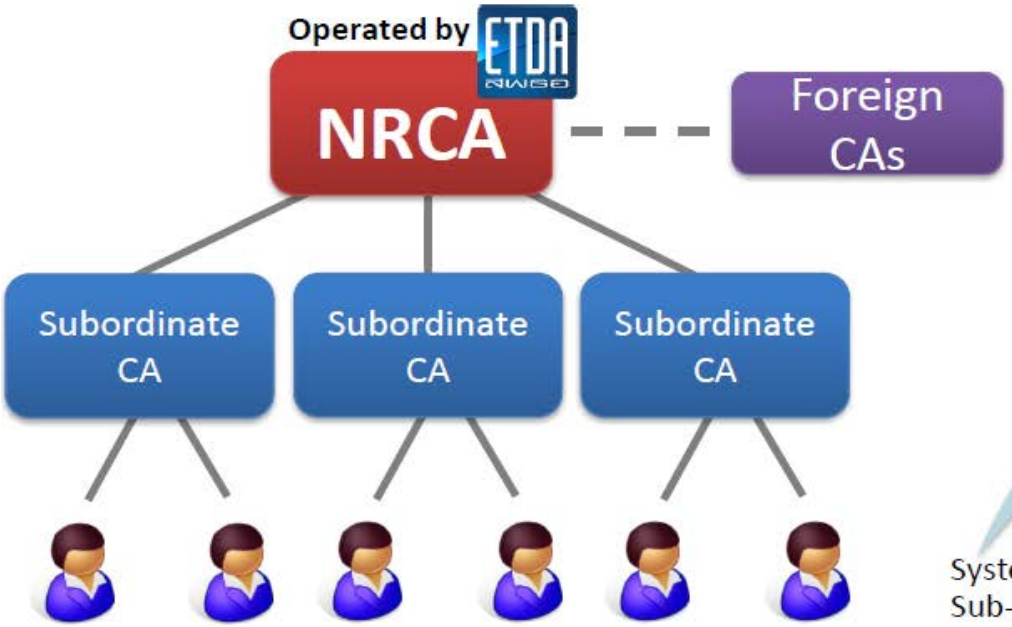
<E-civil petition service>

No. of applications: 58,460 thousand
No of issues: 58,700 thousand
No. of readings: 7,780 thousand



Accredited Certificate Subscriber (Unit : 10 thousand)

Thailand's Public Key Infrastructure



Missions

2013

System Setup
Sub-CA Issuance
Compliance with Intl. Standards

2014

Link with Foreign CAs in ASEAN

PKI Application Promotion & Training

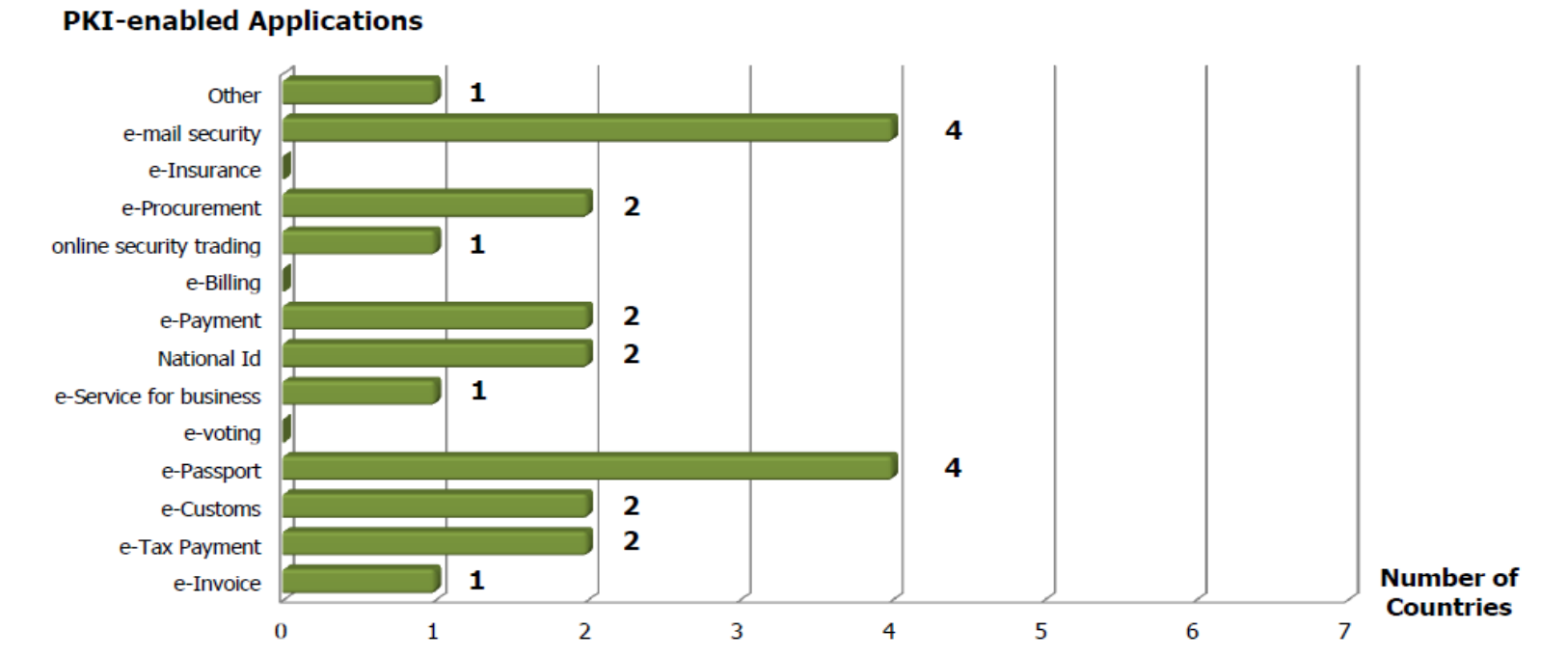
2015

Extend link to other regions

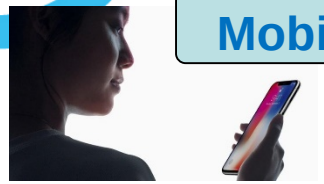
PKI applications in ASEAN

PKI Survey in ASEAN

PKI-enabled Applications



The world is changing…



Mobile + **Biometrics** ? **PKI**

- eID Card (with PKI)
  - ✓Estonia, Italy, German, Span, Finland, Belgium
- BankID (with PKI)
  - ✓Norway, Sweden, Denmark(NemID with 2nd token)
- Netherland DigiD with PKI

mobile connect

NIST National Institute of Standards and Technology Technology Administration U.S. Department of Commerce

IETF W3C OpenID

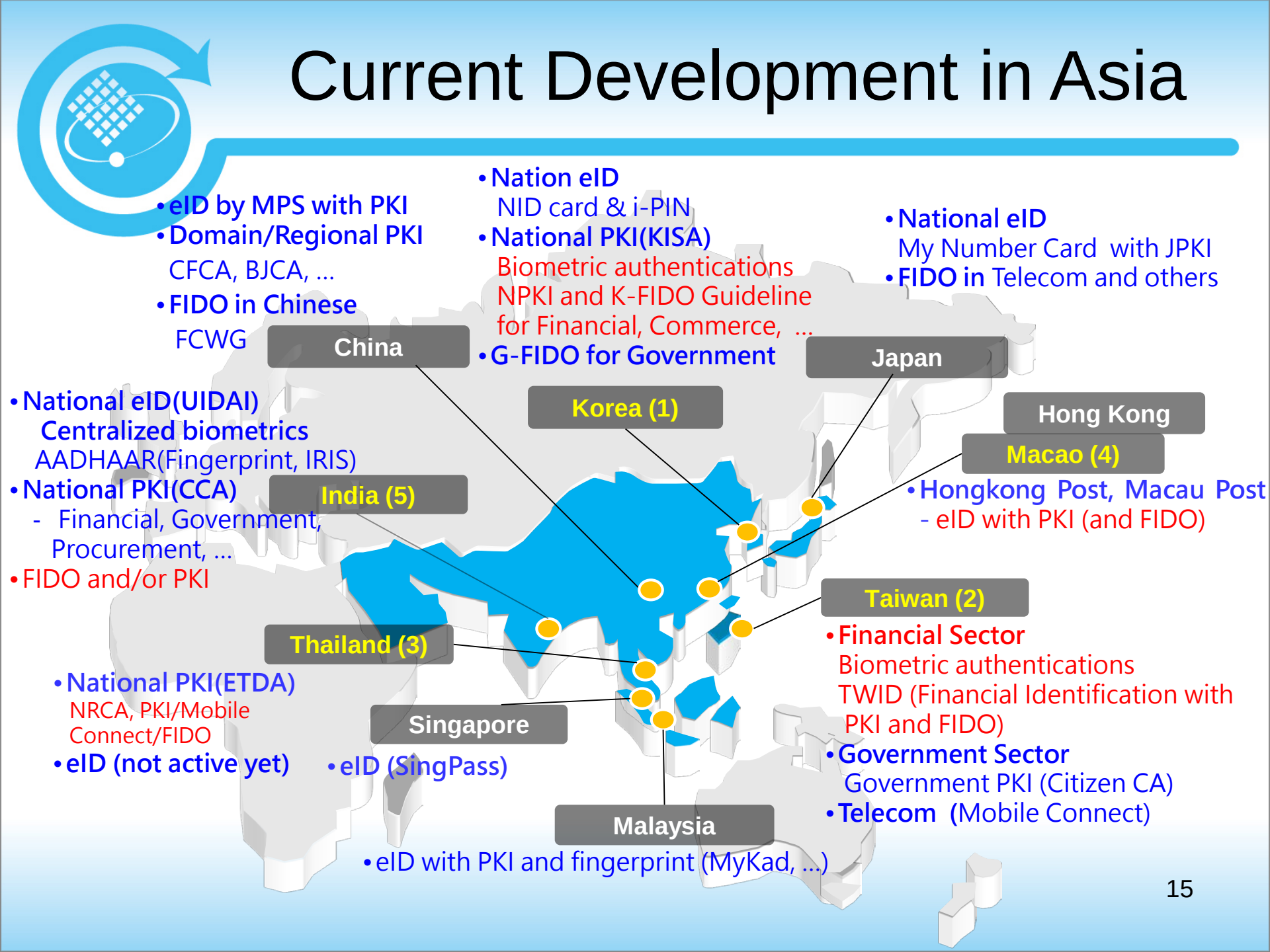
fido alliance simpler stronger authentication

eID.AS

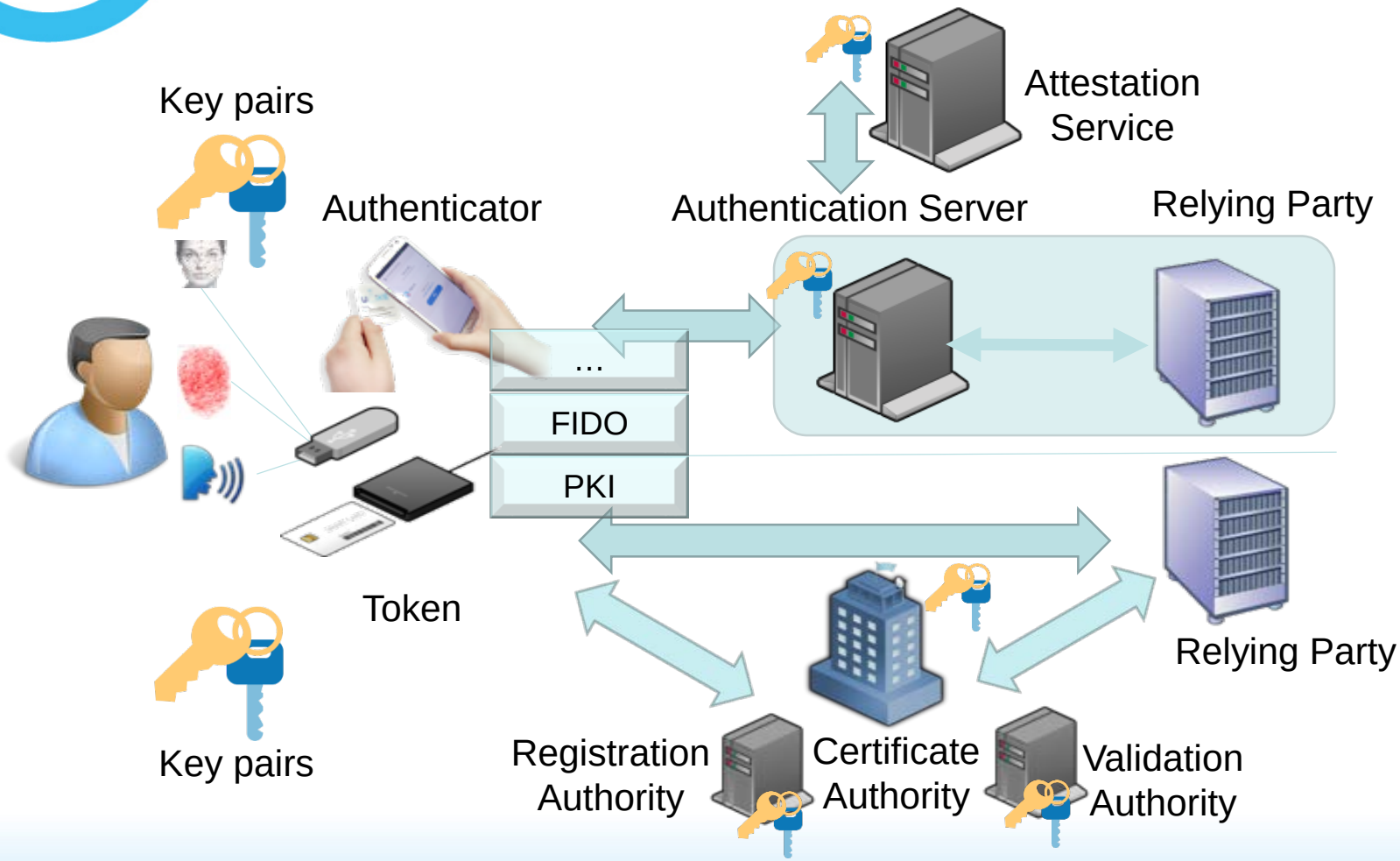
Google Bank of America ebay facebook salesforce GitHub AVAILABLE TO PROTECT 3 BILLION ACCOUNTS WORLDWIDE docomo PayPal Dropbox BCcard dashlane

ITU ICAO · OACI · ИКАО 国际民航组织 · ايكاو ISO

Current Development in Asia

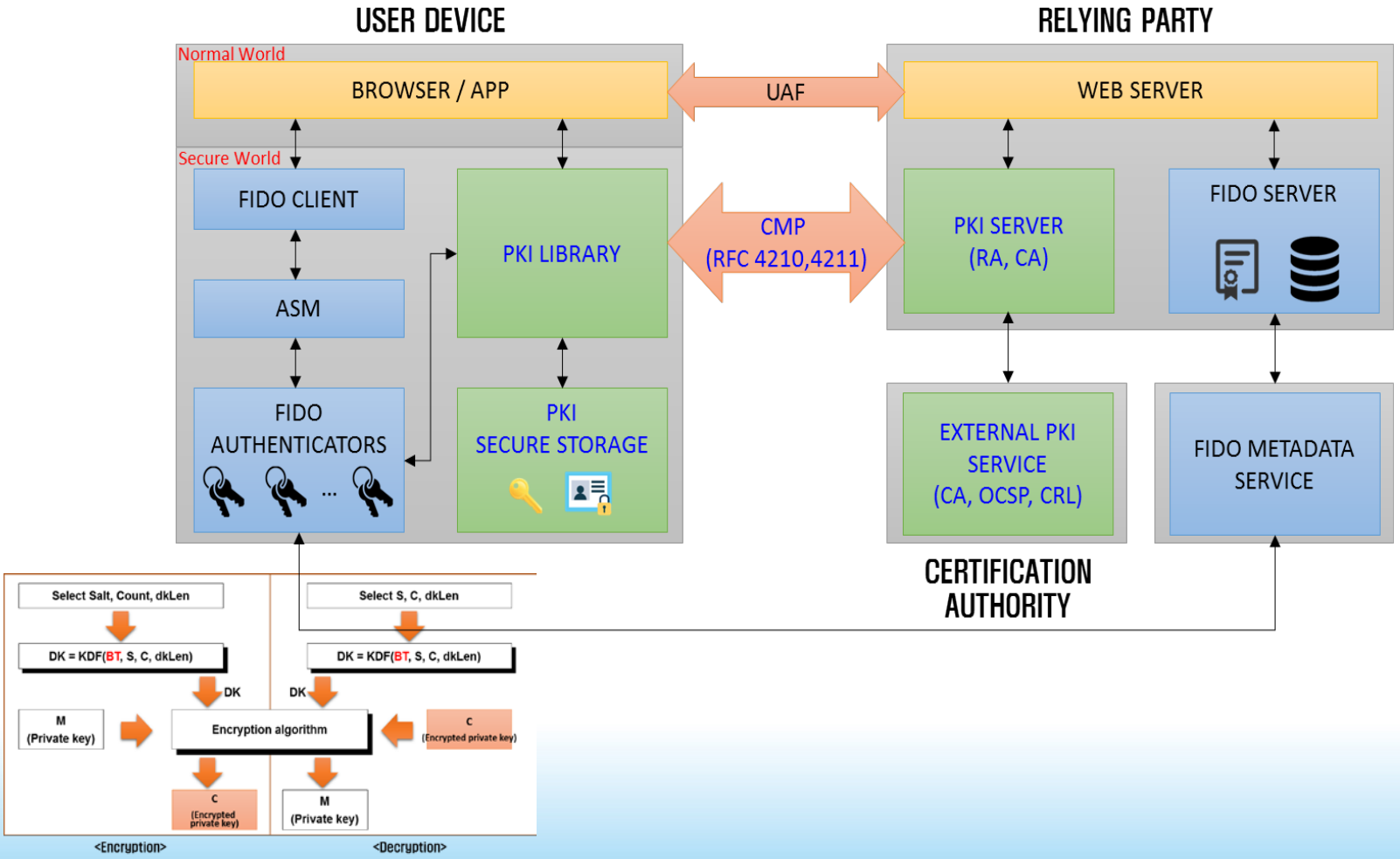


FIDO meets PKI



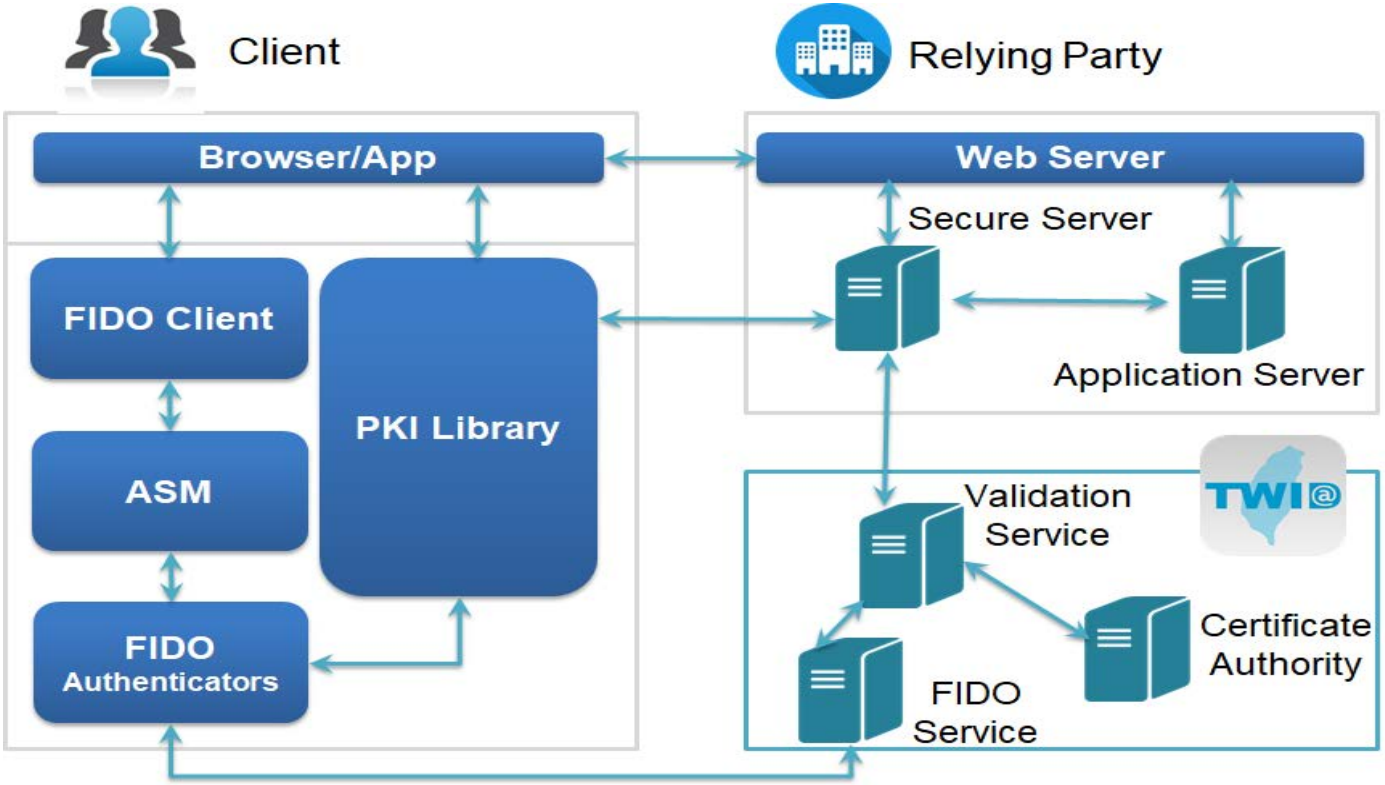
Case Study (1)

K-FIDO (FIDO + NPKI certificate) by KISA



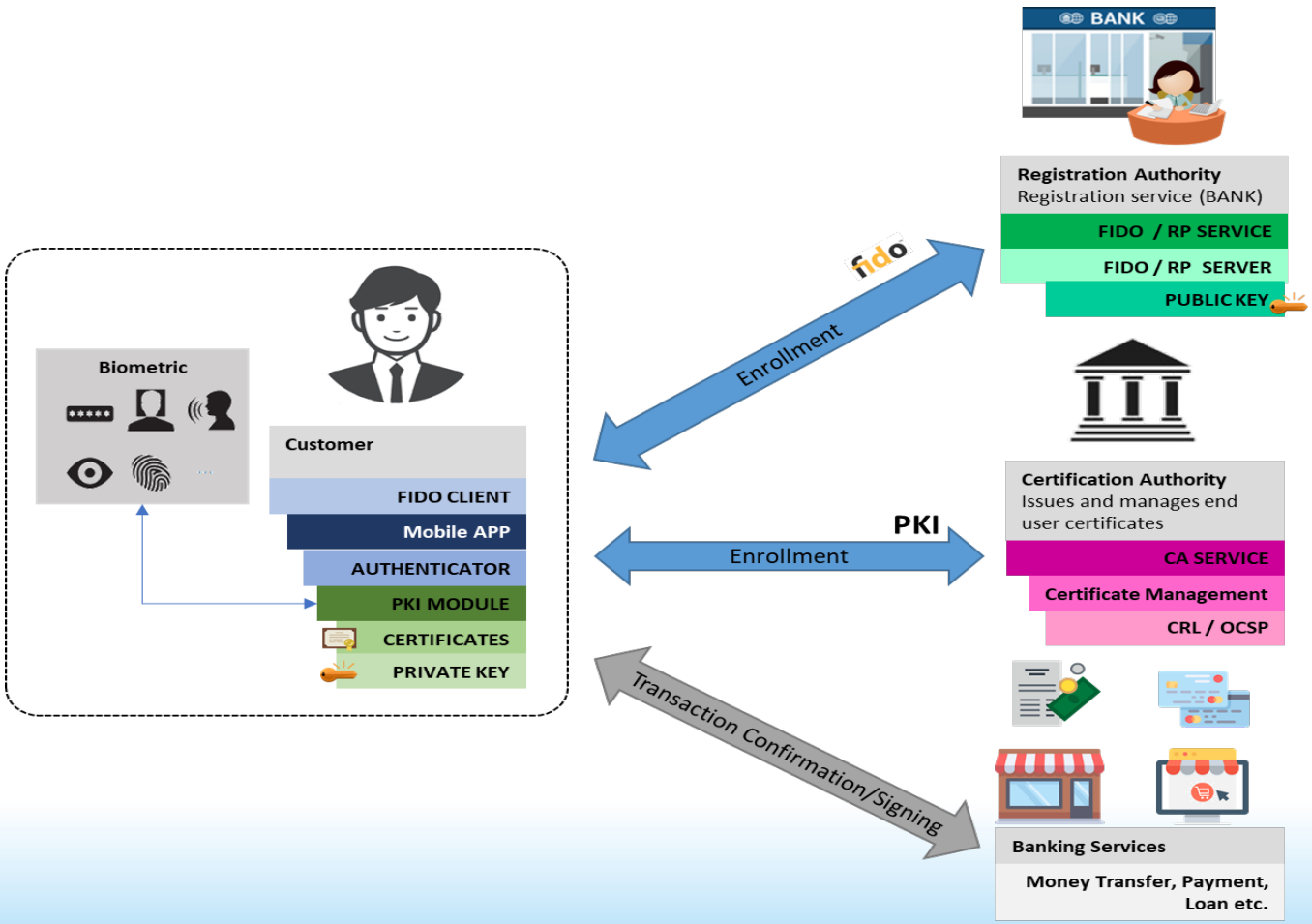
Case Study (2)

- **Taiwan Identification Center (FIDO + PKI) by TWCA**



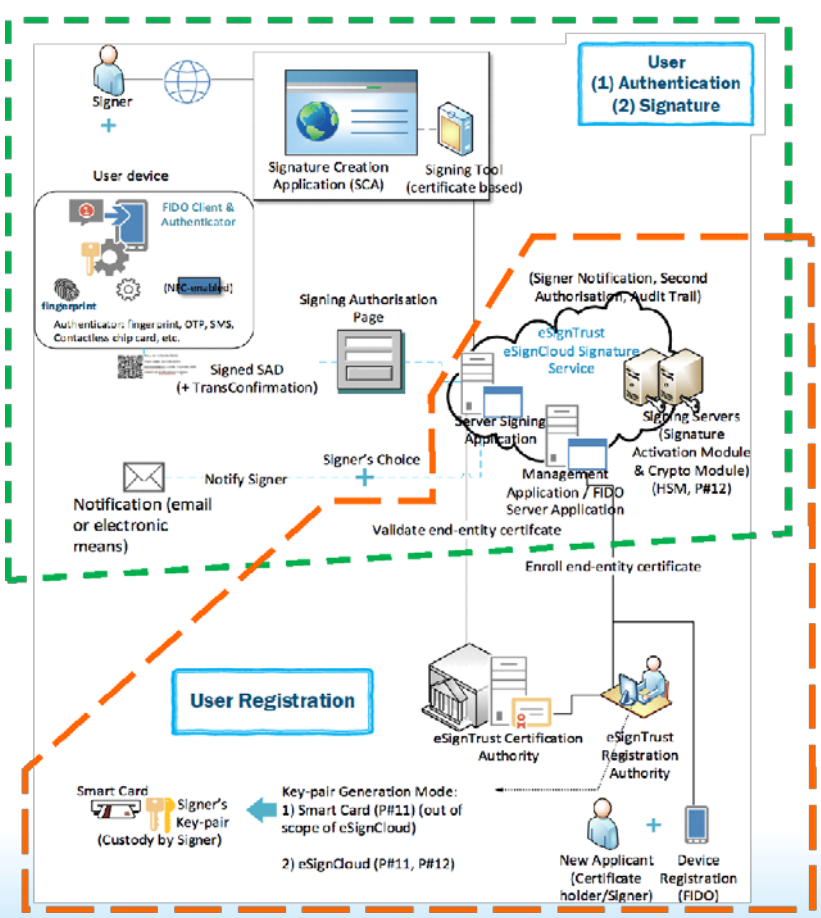
Case Study (3)

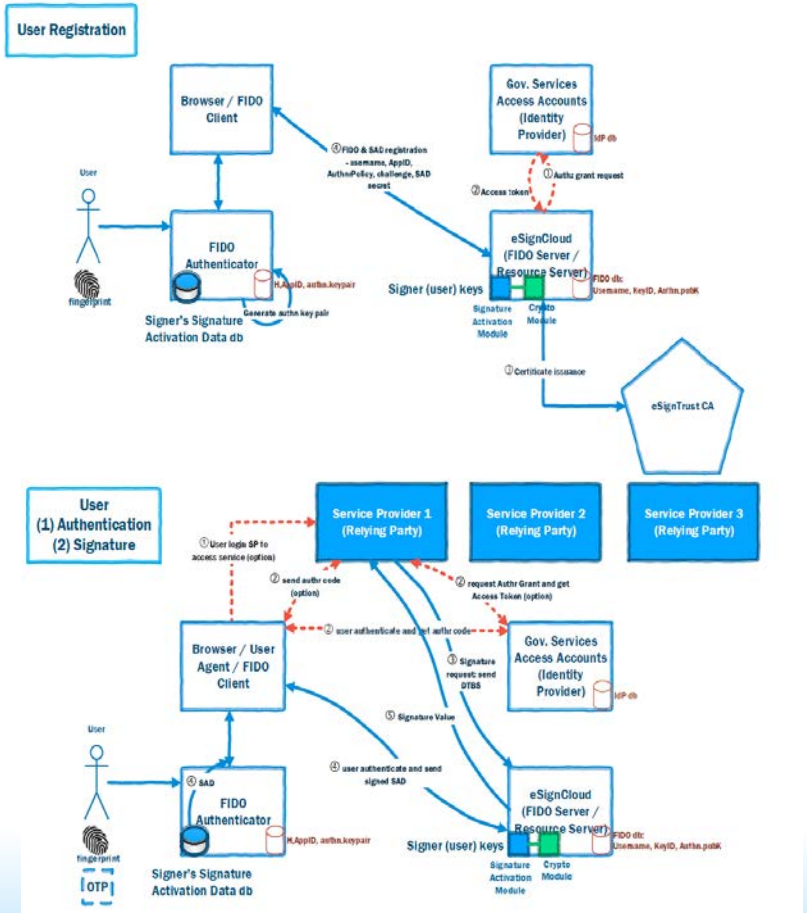
Thailand Banking Service with PKI and FIDO



Case Study (4)

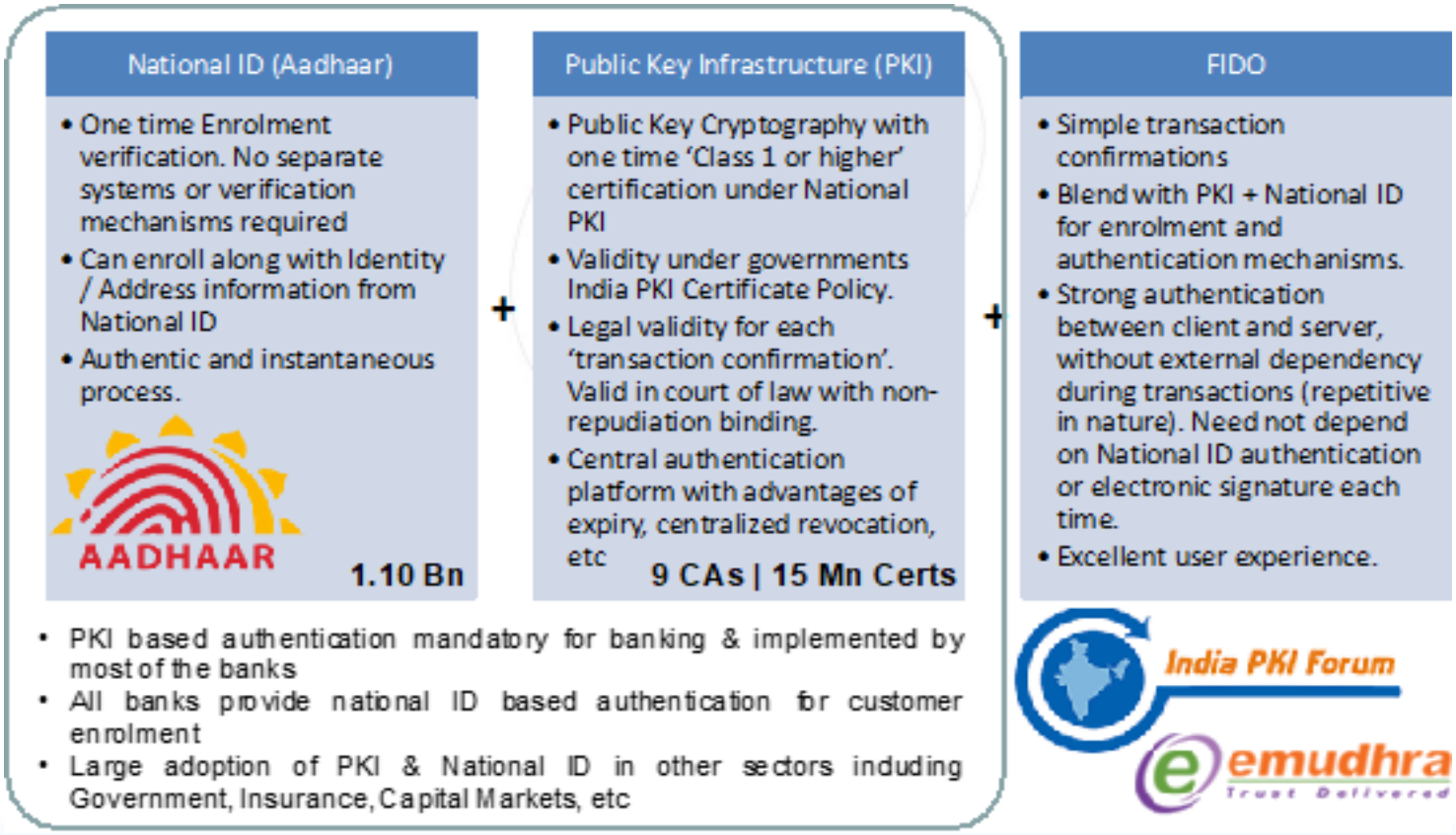
Macao eSignTrust eSignCloud with FIDO





Case Study (5)

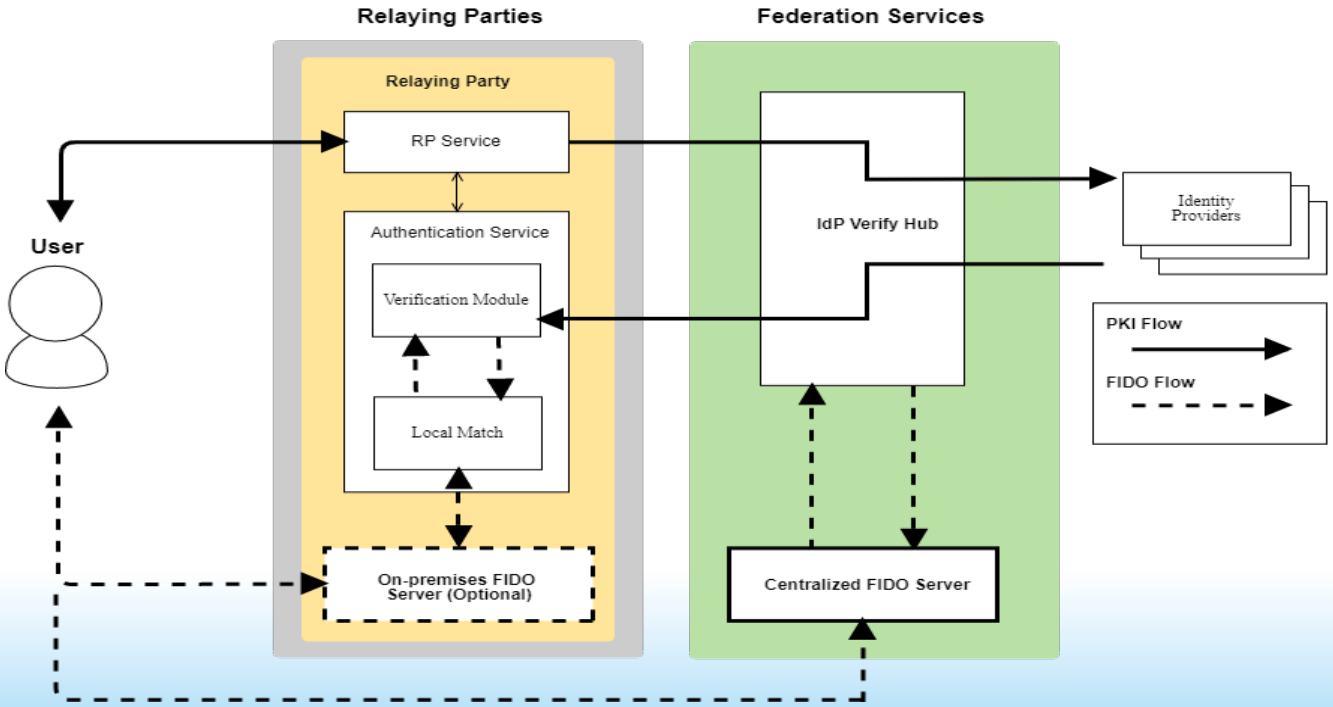
India Aadhaar, PKI, and FIDO



Basic Ideas

FIDO and PKI are complement to each other

- With a “Federation”-like approach to provide comprehensive mechanism to leverage the strength of FIDO and PKI
- Enhance the overall experience and performance for authentication and digital signature



Recommendations for PKI+FIDO

- **Three classes to integrate FIDO and PKI**
  - Class 1: Shared authenticator/token
  - Class 2: Synchronized key pairs
  - Class 3: Shared key pair

    (1) FIDO reuse PKI's key pair

    (2) PKI reuse FIDO's key pair

    (3) Generate new FIDO+PKI key pair
- **Class 1 and 2 could be implemented by extension of FIDO specifications**
- **Class 3 may conflict with FIDO Security Guideline and UAF specification**
  - Not recommended in current deployment

Way forward

- **Collaboration between Digital Society!**
- **PKI implementation in Web Browsers**
  - Web Cryptography API
  - Local Server
  - PKI with FIDO W3C Web Authentication(TBD)
- **PKI vs Blockchain**
  - Make it clear the relations between PKI and Blockchain
- **PKI vs IoT**
  - Explore the opportunity of PKI in IoT applications and how PKI can be deployed in IoT

Asia PKI Consortium

weichung.hwang@gmail.com

INNOVATING
A BETTER FUTURE