

The Status of Korea PKI

Cryptography & Electronic Signature Team

KISA

2019. 6.





Agenda

1 Overview

2 PKI Business Models in Korea

3 Future Work



1 Overview



NPKI & GPKI

• National PKI

- | Established in 1999 under the Electronic Signature Act
- | Competent Authority : MSIT
- | Root CA : KISA (Korea Internet Security Agency)
- | Main Customer : Individual, Company

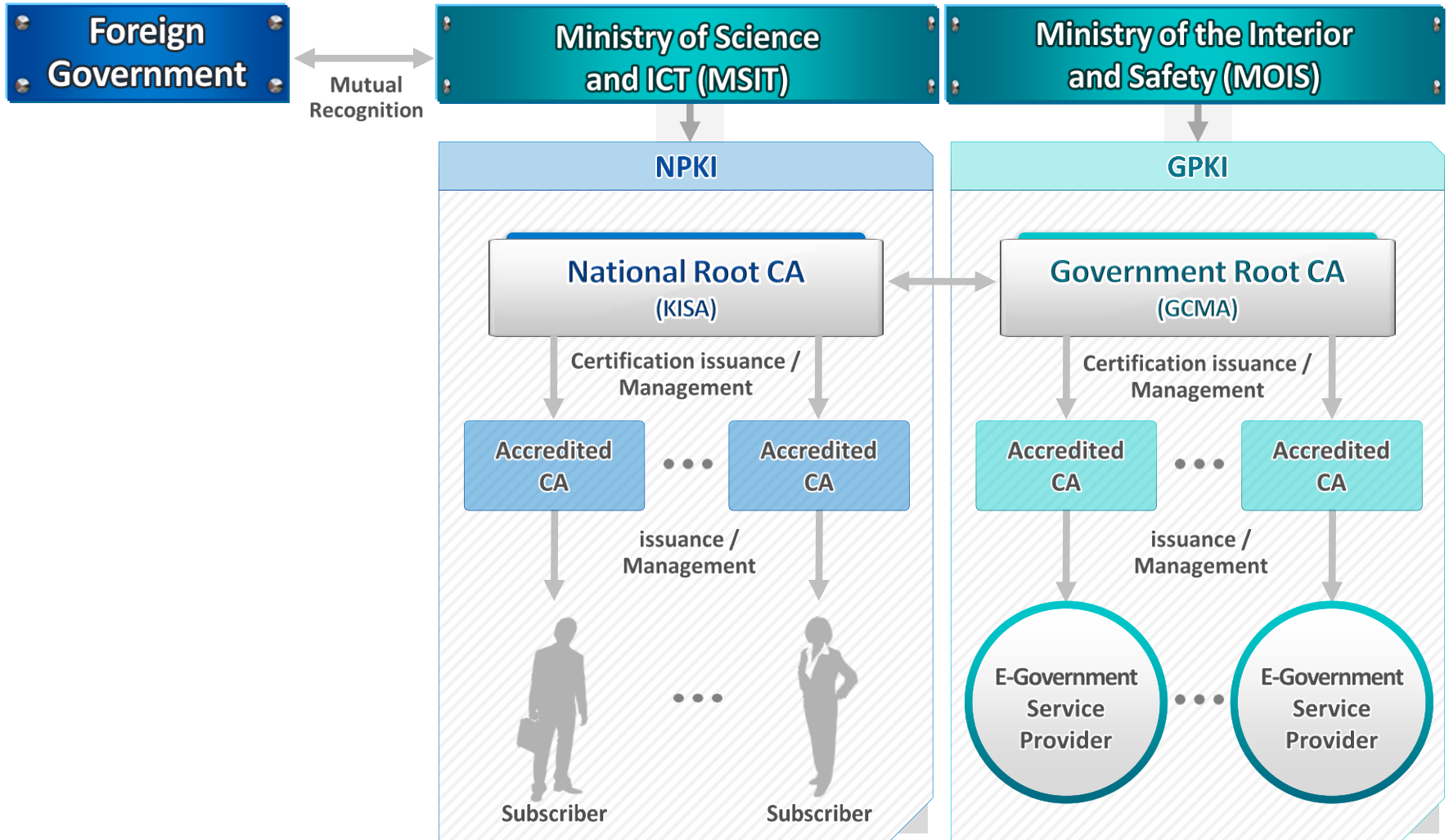
※ MSIT(Ministry of Science and ICT)

• Government PKI

- | Established in 2001 under the E-Government Act
- | Competent Authority : MOIS
- | Root CA : GCMA (Government Certification Management Authority)
- | Main Customer : Public Servants







※ MOIS(Ministry of the Interior and Safety)

PKI Scheme



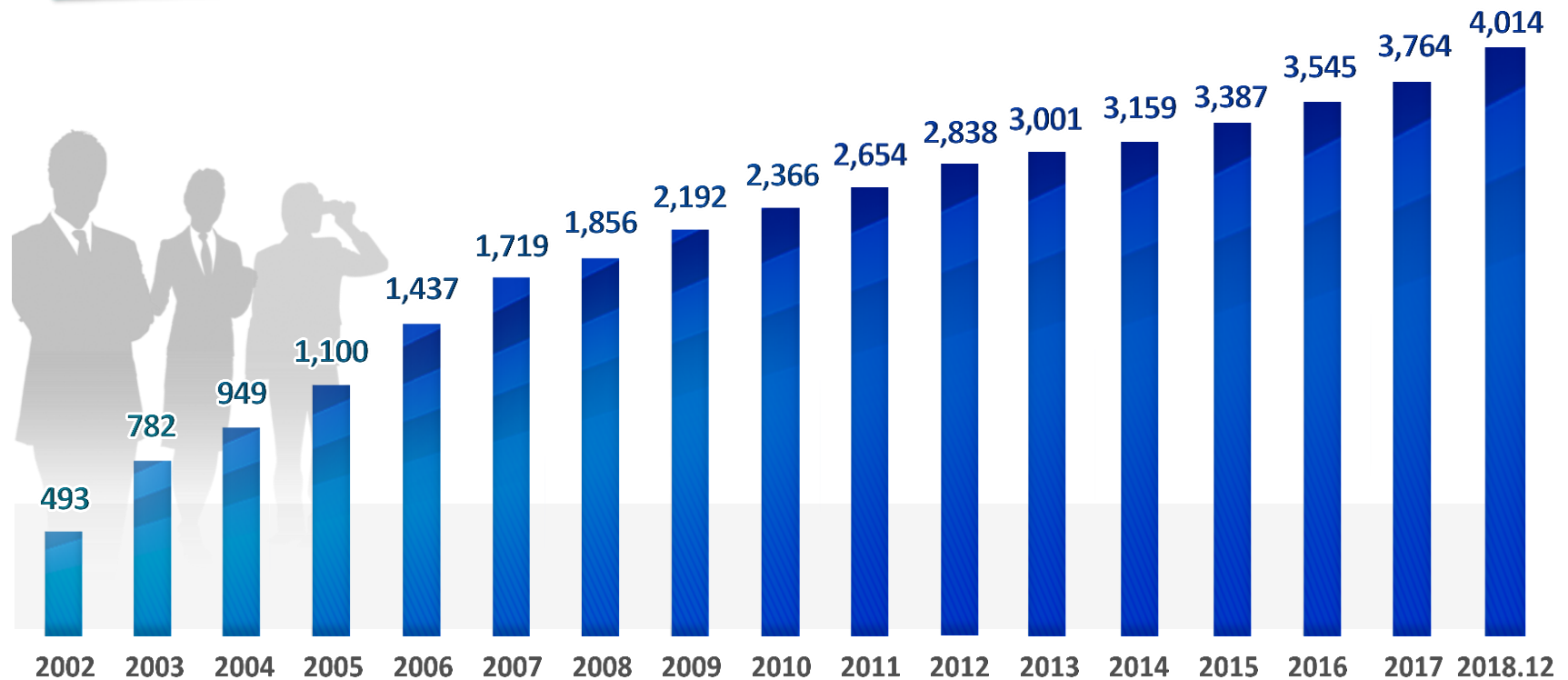
Accredited CA

- 6 CA are accredited by MSIT until now

Accredited CA	Accredited Date	Website
 KICA Korea Information Certificate Authority Inc.	2000. 02. 10	http://www.signgate.com
 SIGNKOREA Certification Authority	2000. 02. 10	http://www.signkorea.co.kr
 yes sign	2000. 04. 12	http://www.yessign.com
 CROSSCERT	2001. 11. 24	http://www.crosscert.com
 TRADE Sign	2002. 03. 11	http://www.tradesign.net
 INITECH	2019. 06. 14	http://www.inipass.com

Accredited CA

- 6 Accredited CAs issued accredited certificate to subscriber around 40 million in total



Accredited Certificate Subscriber (Unit : 10 thousand)

2

PKI Business Model in Korea



Online Banking

- All the Banks and Post Office provide internet banking service using accredited certificate



Online Stock trading

- Security corporations provide online stock service based on using the accredited certificate
- Online stock trading services recommend using accredited certificates for secure online transaction ('03. 3)



Public Service

- | Housing subscription deposit system, Education, Medical information, e-bidding ('06)
- | Housing subscription, the year-end tax adjustment, NEIS, National health Insurance, etc.



HomeTax National Tax Service



NEIS (National Education Information System)

Smart Phone Banking

Smart Phone Banking service with certificate ('10~)

- Transferring a certificate from PC to smart phone
- Generating electronic signature in smart phone



HANA N
Bank



IBK Corporate
Banking



SHIN HAN
Smartphone Banking

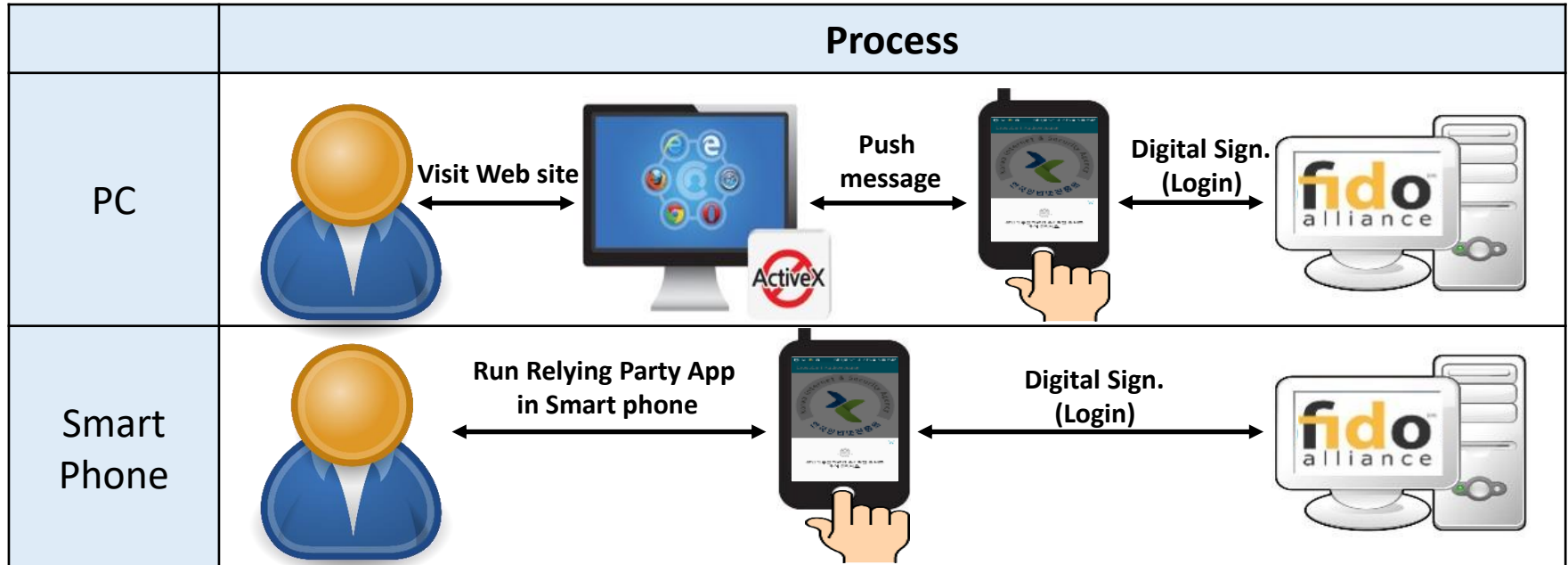


Mirae Asset
M-Stock



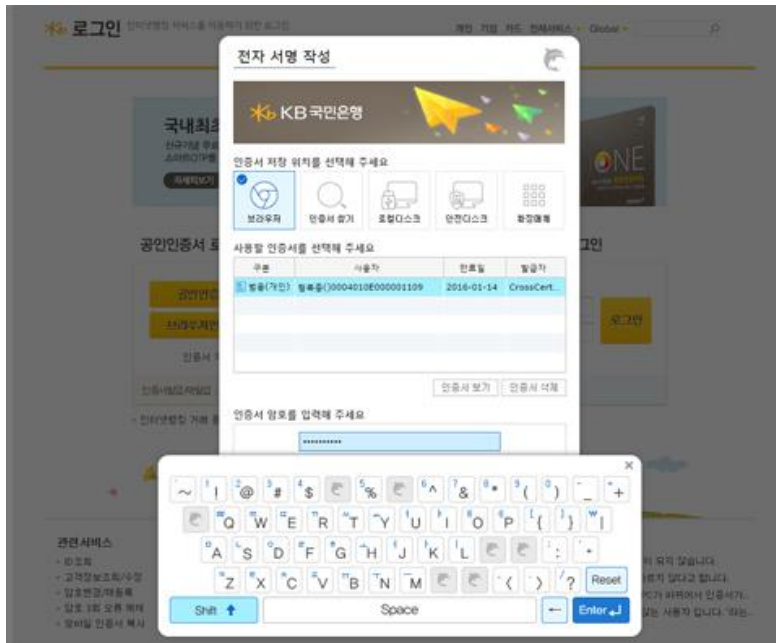
FIDO + PKI services

- FIDO authenticator(Fingerprint, Iris, etc) replaces the entering password of NPKI private key
- Store NPKI private key in Trust Zone embedded in the Smart phone
- No ActiveX in PC, Sensitive information is encrypted in Smart phone TEE

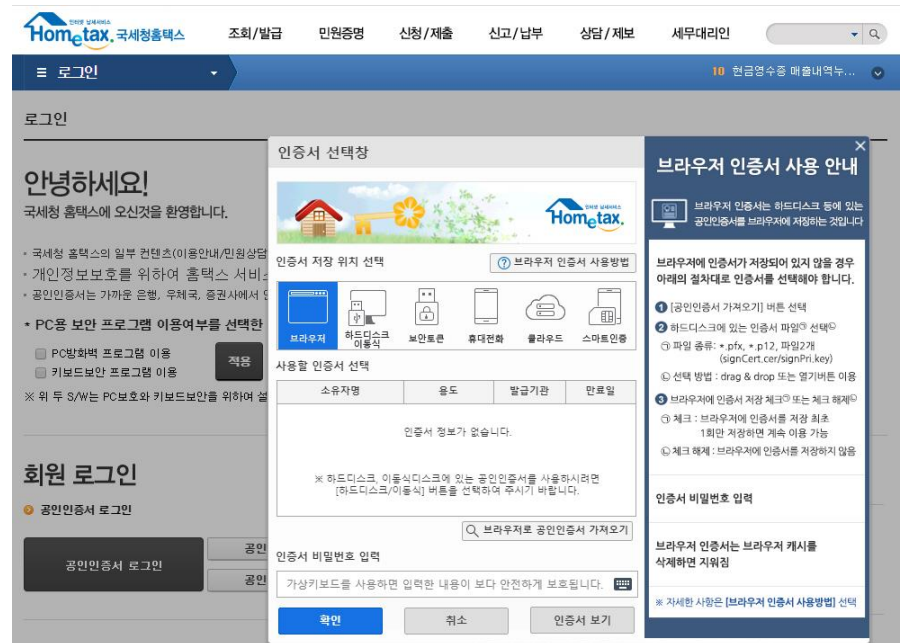


HTML5 Web Standard PKI Technology

- | Store PKI private key in Web browser that supports HTML5
- | HTML5 based PKI technology without downloading and installing any plugins



Kookmin Bank (Online Banking)



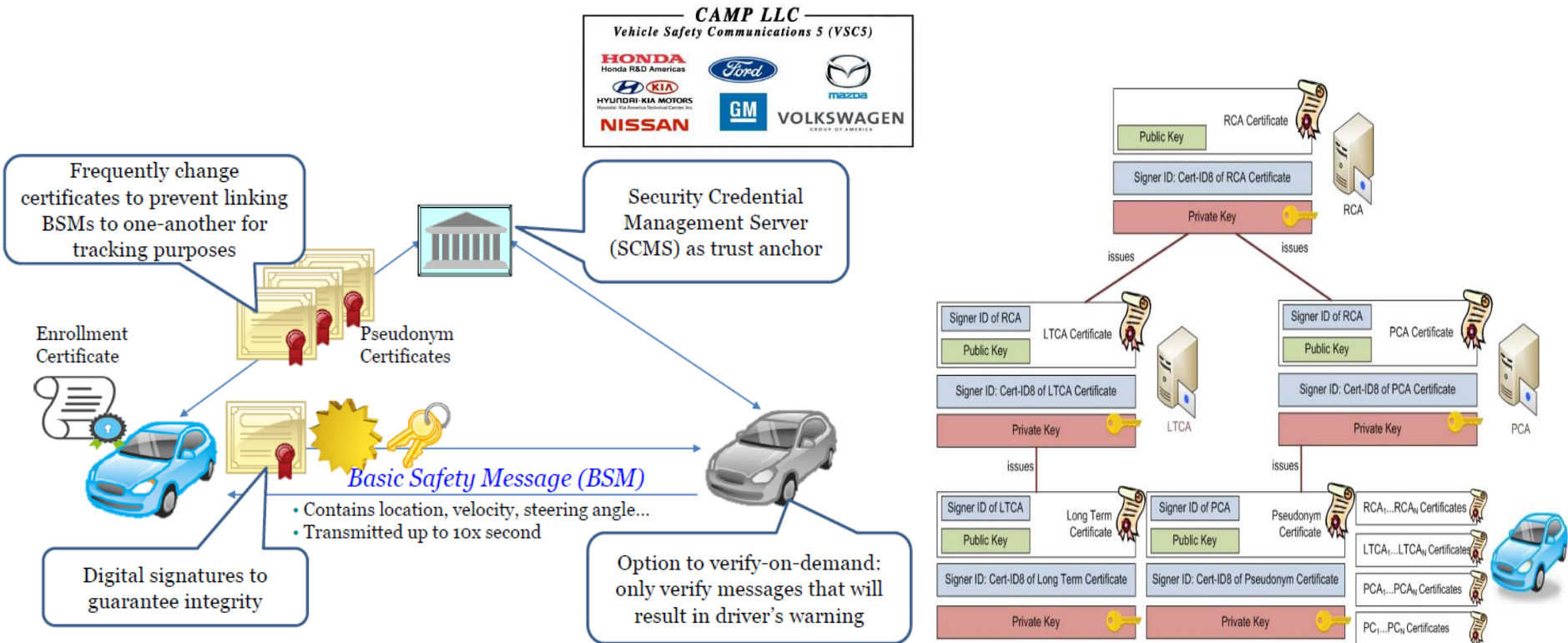
HomeTax (National Tax Service)

3 Future Work



IoT Smart device authentication

- IEEE 1609.2, CAMP VSC5
(Crash Avoidance Metrics Partnership Vehicle Safety Communications 5)
- Digital signature and encryption based on PKI certificate



BlockChain + PKI services

- | A single integrated application provides various PKI services by 6 different CAs
- | Installing additional browser plug-ins is NOT required

BlockChain solution for accredited certificate (40 million certificates)



Internet On, Security In!

Thank you

