Deloitte.

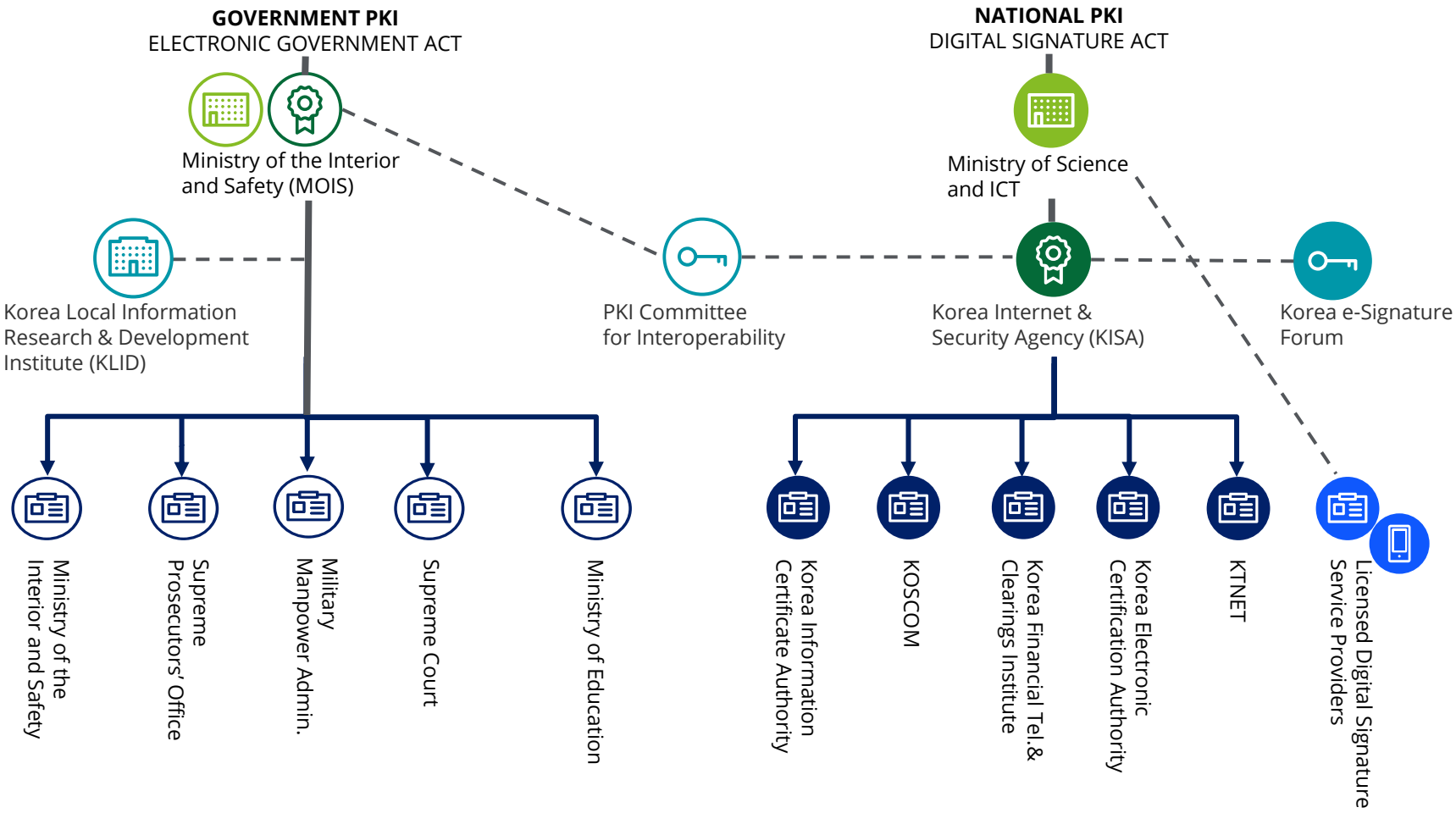

# South Korean Public Key Infrastructure (PKI), Compliance and Assessment

Jinhwan Shin (jinshin@deloitte.com)
Director, Deloitte Korea
November 2023

# South Korean Public Key Infrastructure

# South Korean Public Key Infrastructure

## National PKI and Government PKI



# South Korean Public Key Infrastructure

## Revision of Electronic Signature Act *(effective from December 10, 2020)*

- **The amended Digital Signature Act aims to introduce competition to the digital certificate market and allows consumers to choose a certificate system from an array of options provided by private firms.** For instance, South Korea's three largest telcos, SK Telecom, KT, and LG Uplus, jointly launched the identity authentication app, PASS, in 2018 and has worked with the Korean National Police Agency and Road Traffic Authority (KoRoad) to introduce a digital driver's license this year.

<source: On the Use of Digital Identity in Asia (3) – Digital Identity in Singapore & South Korea, https://international.thenewslens.com/article/147325>


- Meanwhile, the ICT Ministry would push for an amendment of the Electronic Financial Transactions Act so that more digital certificates could be developed and used in the finance industry.
- "The ICT Ministry expects **more and more digital certificates, equipped with new technologies such as blockchain and biodata, to be developed down the road**," the ministry said in its statement.

<source: New era for online ID certifications opens, The Korea Herald, http://www.koreaherald.com/view.php?ud=20201209000864>

# South Korean Public Key Infrastructure

## Korean Certificate Authorities

### 01 WebTrust

- KISA
- MOIS
- NAVER CLOUD (for SSL)
- KICA
- Other CAs (for specific purposes)
- Kakaobank
- KB Bank

### 02 New Licensed CAs after amemdment

- Kakao
- NAVER
- SKT, KT, LG
- PAYCO
- BANKSALAD
- TOSS
- SHINHAN BANK
- WOORI BANK
- HANA BANK

### 03 Accredited CAs under KICA

- KICA
- CROSSCERT
- YESKEY
- KOSCOM
- KTNET

# South Korean Public Key Infrastructure

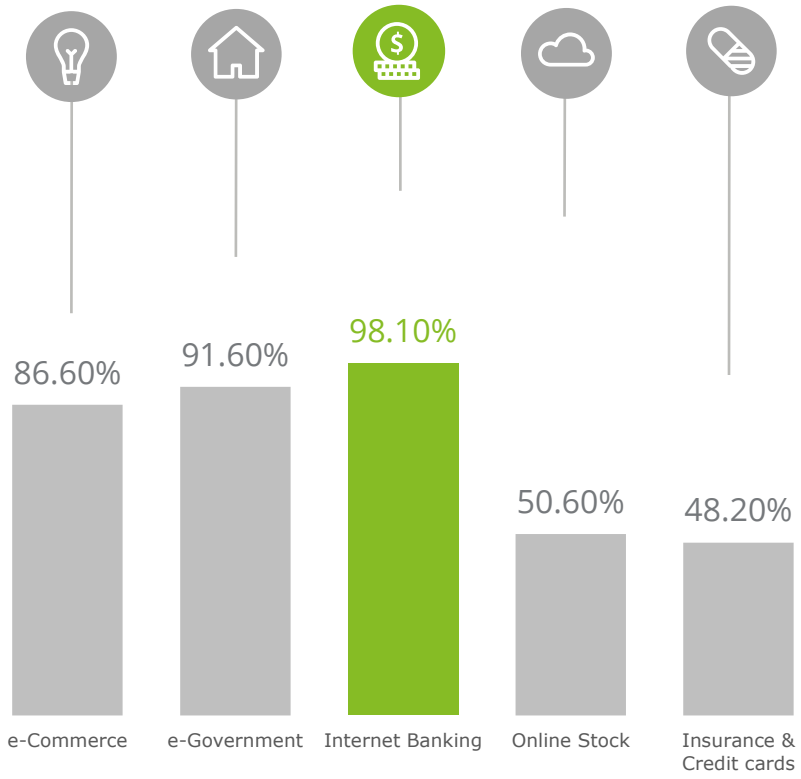
## Usage of Digital Signature

According to Digital Signature Act, in cases that a signature, signature and seal, or name and seal is, under other Acts and subordinate statutes, required to be affixed on a paper-based document or letter, it shall be deemed that such requirements are satisfied if there is a certified digital signature affixed on an electronic message.

**Online (PC-based and Mobile) Banking** has 132 million registration users in September 2017. The number of smart phone banking registration users was increased from 37 million in 2013 to 87 million in September 2017. (38.9% -> 66.2%)

**E-Government** services have 40 million registration users in 2017. 97.2% of them used the e-Government services at least once in 2017.

Usage of Digital Certificates in 2017

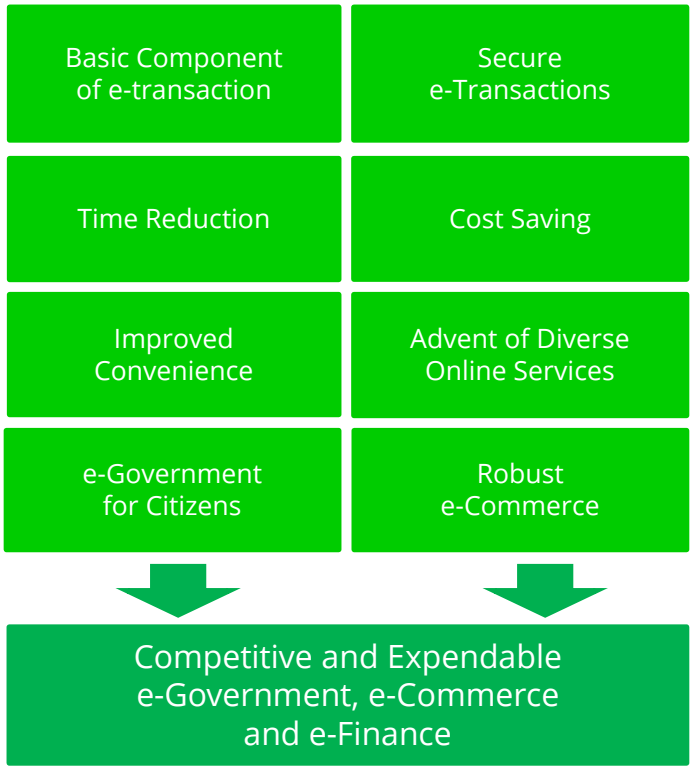



Sources: Research on the Actual Condition of Electronic Signature System Usage in Electronic Signature User (2017.12), Usage of Internet Banking – Korea Bank (2017.09), http://www.index.go.kr provided by Statistics Korea.

# South Korean Public Key Infrastructure

## Changes after the amendment of Digital Signature Act

- Rapidly increasing usage of digital certificates
- Ensuring equal security level by assessments
- Finding co-existence between accredited CAs and Licensed CAs





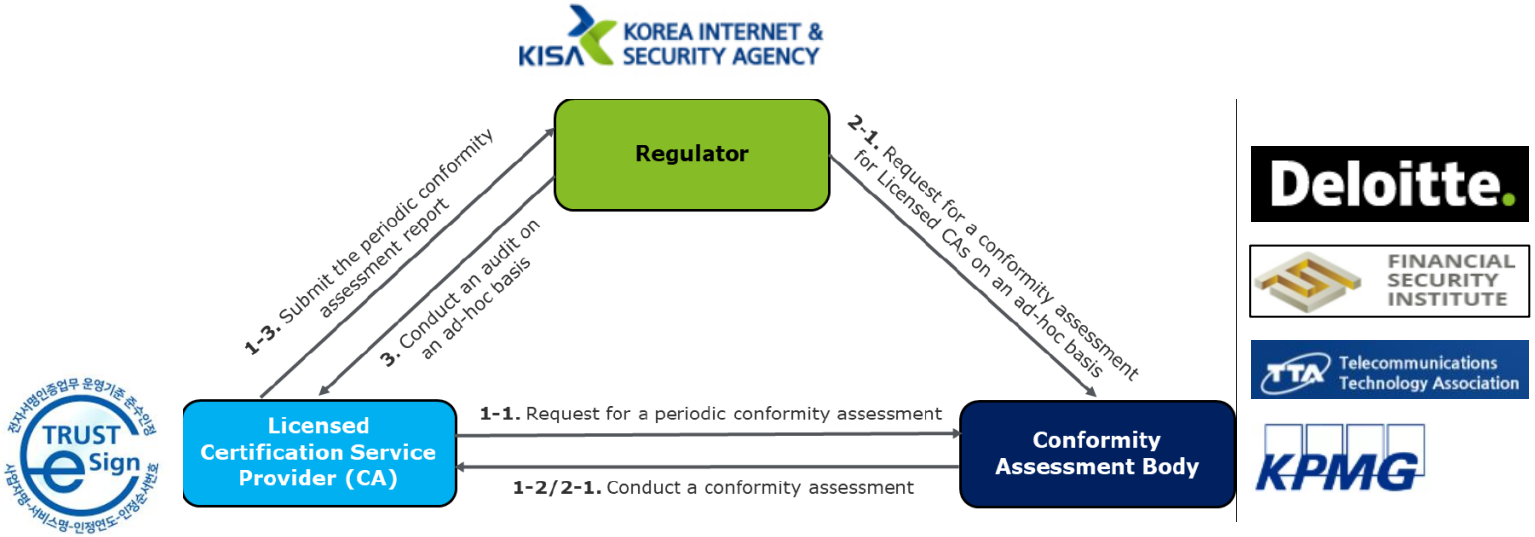
<source: KB Bank commercial>

# Compliance and Assessment

# Compliance and Assessment

## Assessment scheme for Certification Service Providers (CAs)

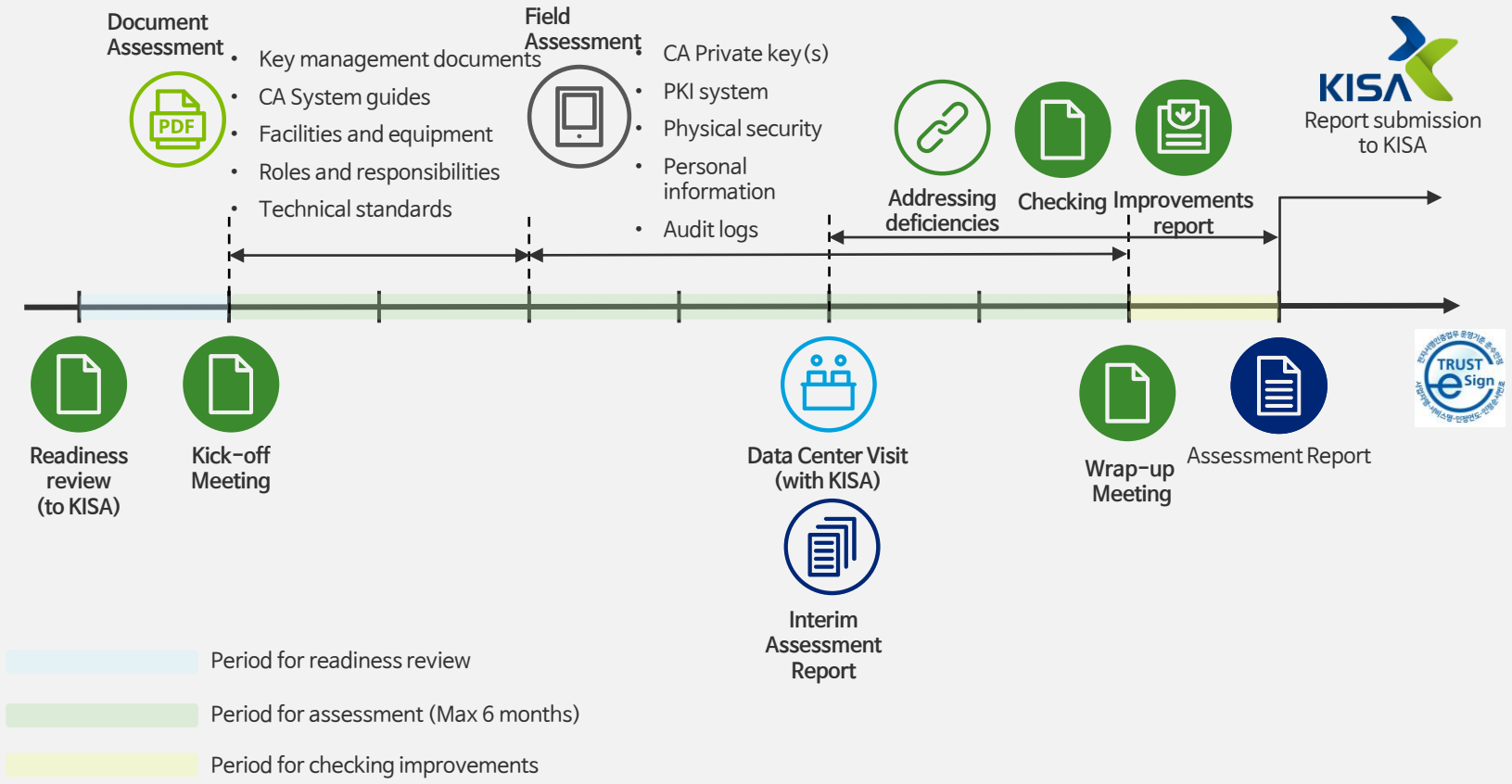
1) Ministry of Science and ICT approves the license and KISA grant a seal to a licensed digital signature service provider also known as “Certification Authority (CA)”, as their service operations and management comply with the legal requirements.
2) KISA regulates the detailed criteria for evaluation on Conformity Assessment Bodies.
3) Initial identification of applicants via no contact verification; and
4) Support on diverse of digital signature technologies




***Note:*** *The official English version of the revised Act and subordinate regulations is not published yet. The terms described as above might be changed if the English regulations are disclosed.*

# Compliance and Assessment

## Typical Process for a new Certification Service Provider (CA)




※위의 일정은 전체적인 계획이며, 업무 진행 상황에 따라 다소 변경될 수 있습니다.

# Compliance and Assessment

## Components and Criteria for Korean Assessment

### CA Components

**CP/CPS**

- Compliance with RFC 3647
- Government notification regarding making CPS

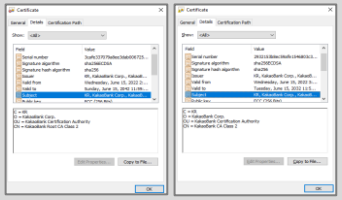
**Facilities and Equipment mgmt.**

- Information security policy and procedures
- Guidance on data center operations
- Disaster recovery procedures with DR Center

**Key and Certificate lifecycle management**

- CA key and certificate lifecycle management
- End entity certificate issuance and usage
- Technical standards for profile and validity

❖ Root certificate
❖ Issuing CA certificate
❖ End Entity certificate



### WebTrust Criteria

- P1 CA Business Practices Disclosure
- P2 CA Business Practices management
- P3 CA Environmental Controls
- P4 CA Key Lifecycle Management Controls
- P5 Subscriber Key Lifecycle Controls
- P6 Certificate Lifecycle Management
- P7 Subordinate CA and Cross Certificate Lifecycle Management

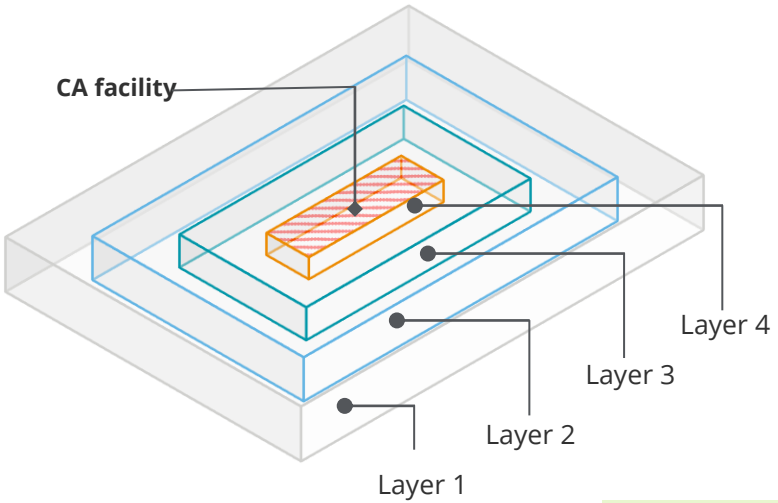
### Assessment controls

1. Independence from subscribers
2. Use of proper technology
3. CPS
4. Subscriber registration
5. Certificate Issuance, Revocation
6. Creation of Private key
7. Protection of Private key
8. Protection measures, etc.
9. Protection plan on subscribers
10. Guaranteeing the usage of digital signature

# Compliance and Assessment

## Physical Security Requirements of WebTrust

**CA's Data Center**

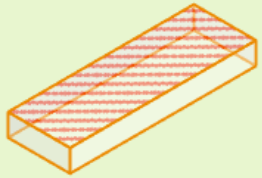



**P.3, 4. Physical Security Criteria of WebTrust for CA**

- physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control;
- CA facilities and equipment are protected from environmental hazards;
- loss, damage or compromise of assets and interruption to business activities are prevented; and
- compromise of information and information processing facilities is prevented.

- ✓ manned reception area
- ✓ wearable visible identification
- ✓ access control system
- ✓ solid walls
- ✓ fire doors
- ✓ intruder detection system (alarmed)
- ✓ monitoring / surveillance cameras
- ✓ uninterruptible power supply

**CA facility**



- should be accessible through Dual Custody Control with Multi-Factor Authentication (MFA) control
- ❖ **Dual Custody Control**: require at least two trusted people be present during the duration of the authorised activity in order to physically access CA systems.
- ❖ **MFA control**: an authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction: something you know (knowledge factor), something you have (possession factor), and something you are (inherence factor). Each factor must be independent.
- access requests and entrance/exit events are to be logged
- physical barriers (e.g. Faraday cage) are in place to prevent electromagnetic radiation emissions

Applications serving the financial services industry can be developed with digital signature and PKI capabilities.

The Certification Authority provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate.

Deloitte.