Deloitte.

South Korean Public Key Infrastructure and the Compliance World

Korean digital signature services assessment and WebTrust updates

Jinhwan Shin (jinshin@deloitte.com)
Director, Deloitte Korea
October 2024

Korean digital signature services assessment

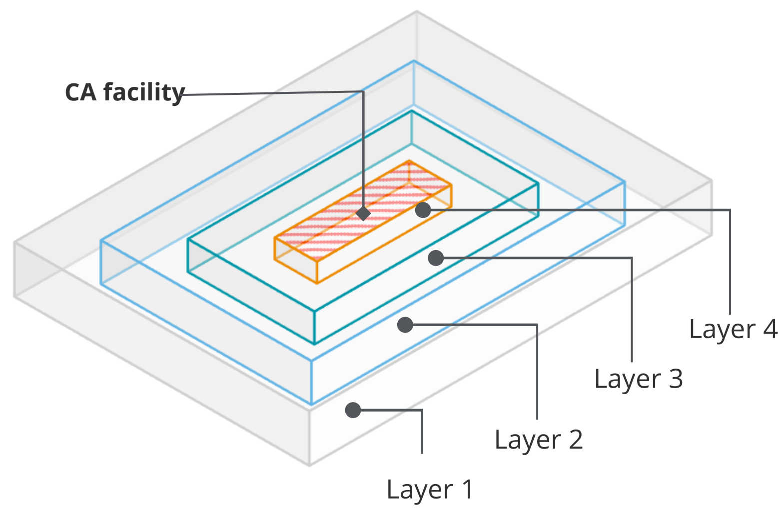
South Korean Public Key Infrastructure (from 2023 APKIC Symposium)

Digital Certificates and Physical Security Requirements in Korea

Digital Certificate advertisement at YouTube

Digital Certificate
on mobile phone

Physical security requirements



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.

Korean digital signature services assessment

List of 23 Digital Signature Service Providers (as of October 2024)

5 accredited
Certificate Authorities (CAs)

3 telecommunication
companies

7 mobile service
provid7rs

7 Banks (8 service providers)
**KB Bank provides 2 services*

Korean digital signature services assessment

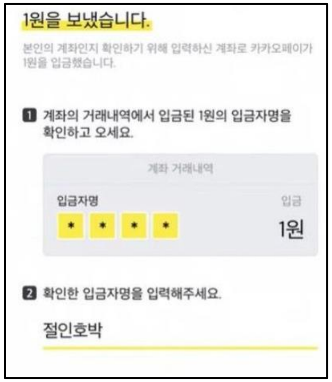
Allowed Identification Methods (“KYC”)

Individuals

- Legal name must be included in the Subject DN of the certificate.
- The information provided by a requester must be verified by a trusted third-party DB.

Resident Registration Card
**only in case of service providers who are licensed by the government on collecting and managing resident registration numbers*

Mobile Phone-based identity verification



Bank account identity verification

Legal Entities

- Legal name must be included in the Subject DN of the certificate.
- The information provided by a requester must be verified by a trusted third-party DB.
- The existence of the organization should be verified by the relevant government DB.

Hometax. 국세청홈택스

Legal entity’s status checking *provided by National Tax Service*

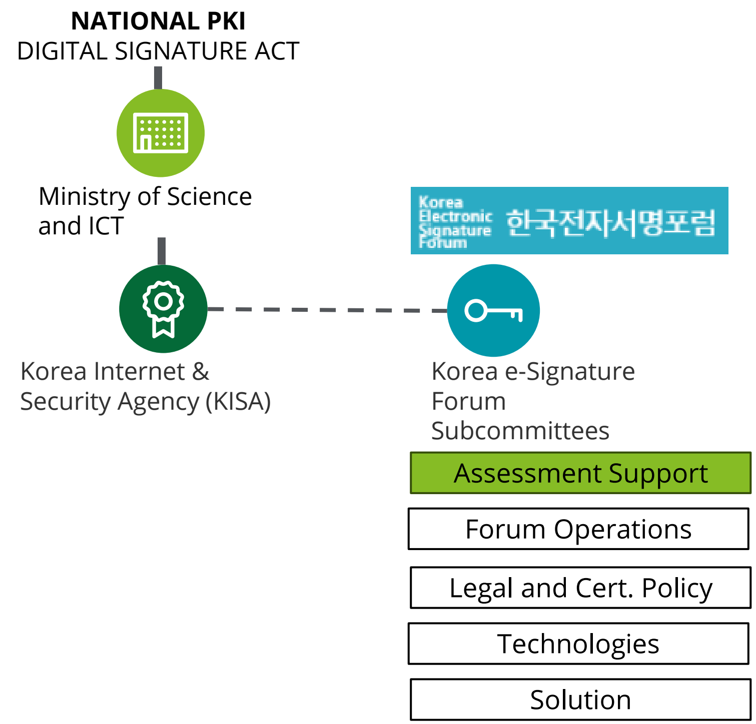
정부 전자문서지갑

Korea Government’s e-Document Wallet

Korean digital signature services assessment

Future Work in 2025

- ✓ Subordinate regulations and guidelines revision (Ministry of Science and ICT and KISA are responsible bodies to amend them)
- ✓ Discussions on updates of assessment criteria on digital signature service providers through Korea Electronic Signature Forum
- ✓ Additional KYC methods analysis if necessary
- ✓ Digital signature service expansion (e.g., money transfer to other countries, issuing digital certificate to expatriates)
- ✓ Ensuring the interoperability among digital signature service providers



WebTrust Updates

WebTrust Updates
History of WebTrust

- WebTrust was developed jointly by the AICPA and CICA in 1997 to increase consumer confidence with the internet/ecommerce.
  - Version 1.0 Baseline assurance service developed in 2000
  - 2002 became part of trusted Microsoft Root Program
  - March 2006 CA Browser Chair invited chair of WebTrust to be included in triannual in-person events and participate in committees.
- Once all the browsers became part of the CA/B Forum, WebTrust requirements were incorporated into all trusted root programs.
- Today, the ownership of the WebTrust program and practitioner enrollment sits with CPA Canada.
- **The WebTrust Task Force (WTTF) was created to support CPA Canada's WebTrust for Certification Authorities Program.**
- **CPA Canada runs the WTTF with a team of global practitioners who provide advice.**

WebTrust Updates

WebTrust Task Force (WTTF)

The Task Force is committed to sharing knowledge, experience, and expertise, building relationships with stakeholders and advising on the strategic direction for the development of the WebTrust program. Specifically, the Task Force is responsible for:

- Setting, developing and modifying the WebTrust Principles and Criteria for a Certification Authority (CA) based on developments in PKI control models (such as ISO, NIST) and processes and controls promulgated by the CA/Browser Forum
- Developing and updating assurance engagement reporting templates and non-authoritative guidance to practitioners
- Collaborating with and supporting the Browser Community as it pertains to their trusted root programs
- Liaising and participating in deliberations by the CA/Browser Forum related to principles and criteria, controls, and impact on service offerings
- Advising CPA Canada on potential new information technology-based assurance services
- Discussing potential compliance gaps, areas for enhancement and potential bad actors within the cryptographic ecosystem and WebTrust process.

WebTrust

CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

WebTrust Updates

WebTrust Seals Brief Description

WebTrust for Certification Authority (WTCA)
seal for digital certificates for secure online transactions and communications

BR SSL
Cryptographic protocols used to secure communication over the internet

Network Security
CA site has implemented appropriate measures to safeguard its network and protect sensitive information from security threats

Code Signing
Process of digitally signing software or code to verify its authenticity and integrity. Seal demonstrates commitment to security and trustworthiness in the CS process

Extended Validation
Process used to authenticate and verify the identity of a website owner before issues an SSL certificate

Secure/ Multipurpose Internet Mail Extensions (S/MIME)
Protocol for securing email messages using encryption and digital signatures

Registration Authority
RA responsible for verifying the identity of certificate applicants and processing certificate requests before they are issued by the CA

Mark Certificate
digital certificate that allows organizations and individuals to display a trademarked logo in the list view of recipients' email inboxes next to the sender field

Qualified Seal
New seal(s) created by CPA Canada after consultation with WTTF and Browsers. Rolled out in 2023

WebTrust Updates

Future Work in 2025

- ✓ WebTrust for CA Supporting X9, which is a standard setting organization for financial institutions and supporting organizations.
- ✓ WebTrust for CA Supporting IOT which will Evaluate large IOT program requirements and assurance requirements.
- ✓ Hosting CA/Browser Forum F2F meeting in Toronto, Canada in 2025
- ✓ Updates of WebTrust Principles and Criteria through WTTF regular meetings
- ✓ WebTrust Practitioner Portal (continued)

Members of the Task Force are:

- Timothy Crawford, *BDO USA, PC* (co-Chair)
- Dan Adam
- Donoghue Clarke, *Ernst & Young LLP*
- Chris Czajczyc, *Deloitte LLP*
- Adam Fiock, *BDO USA, PC*
- David Lachmansingh, *Richter LLP*
- Eric Lin, *Ernst & Young LLP*
- Zain Shabbir, *KPMG LLP*
- Jinhwan Shin, *Deloitte LLP (Korea)*