The Status of Korea PKI

Digital Signature Certification Team

KISA

2025. 11.

KISA Korea Internet & Security Agency

Agenda

1. **What the** Digital Signature Certification **Team Does**
2. Review of Changes in **the Past 5 Years**
3. **Key Focus** Areas for **This Year**

1 **What the** Digital Signature Certification **Team Does**

KISA(Korea Internet & Security Agency)

❖ **(Vision)** Information Security & Digital Trust Agency

- (Supervising Ministries) MSIT, MOIS, PIPS, KMCC, etc.

❖ **(Organization)** 5 Headquarters and 2 Offices

- Korea Internet Security Center(KISC), Personal Data Secure Usage Group, Information Security Industry Group, Digital Safety Group, etc.

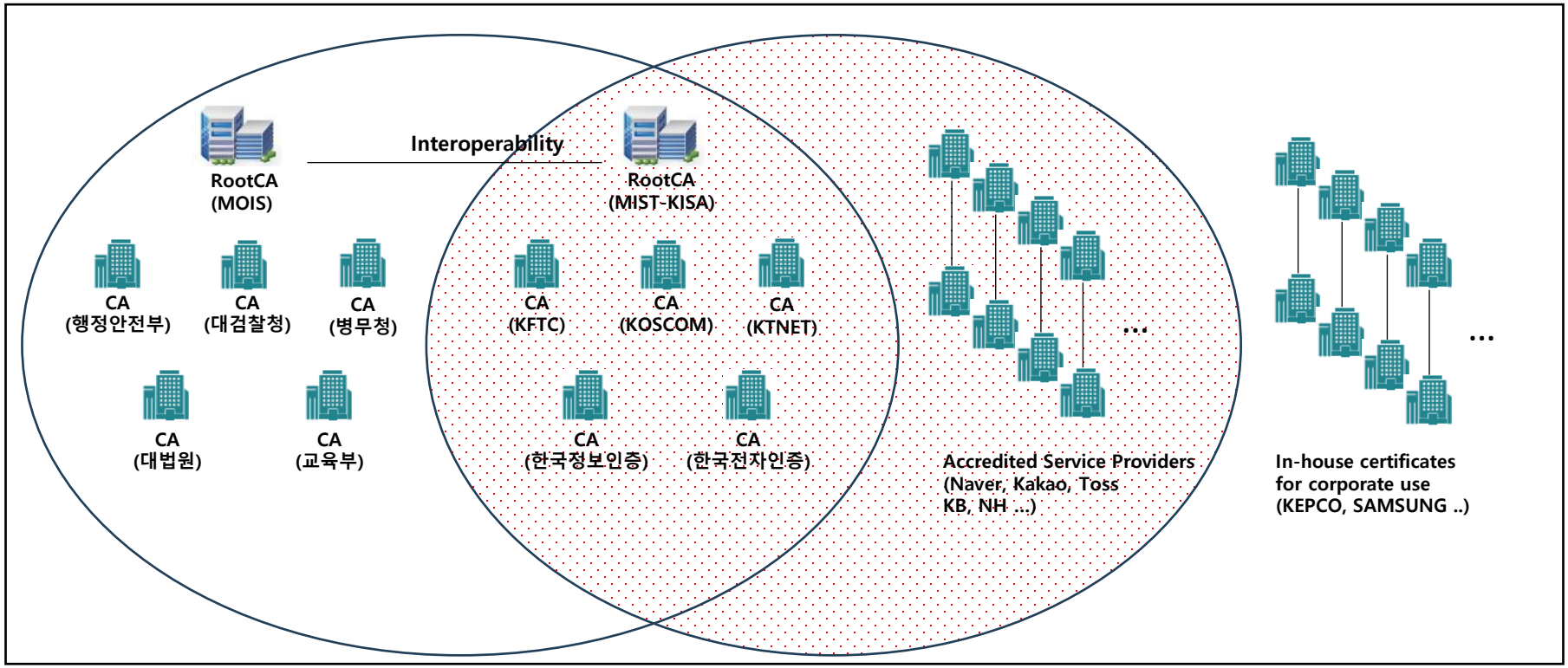
❖ **Teams of Interest to APKIC**

Team	Main Responsibility
Digital Signature Cerfitication Team (디지털서명인증팀)	Operation of **eSignature Act-based systems**
E-Document Team (전자문서확산팀)	Management of **e-document** services & certification
LBS Policy Team (위치정보팀)	Operation of **identity verification** services
Blockchain Technology Policy Team (블록체인정책팀)	**Blockchain-related events** & policy operations
MyData Promotion Center (마이데이터추진센터)	Operation of **MyData** initiative
Next Generation Cryptography Technology Team (차세대암호기술팀)	Management of **cryptographic** policy & standards

Korea's PKI

❖ Three Major Categories

: Managed by Our Team (KISA)

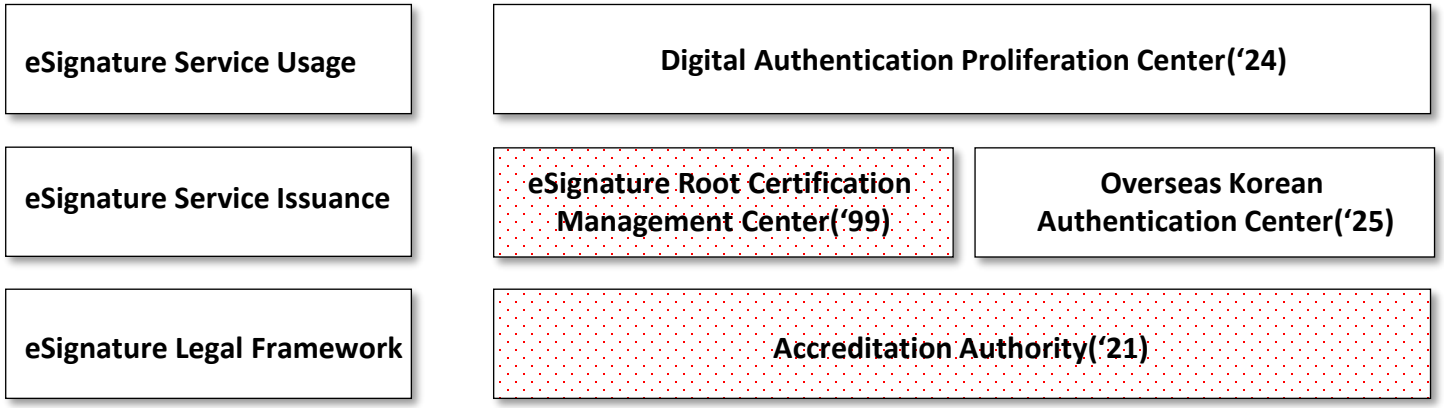


[Government-operated Root CA] [PKI under the Electronic Signature Act] [Private / In-house PKI Systems]

What the Our Team Does

❖ According to the **Electronic Signature Act**

- Operates **1 system** with **3 major centers**
  - **Root CA** interoperable with the Government eSignature system
  - Operates the **Accreditation System** for eSignature service providers



1 Key Changes Over the **Past 5 Years**

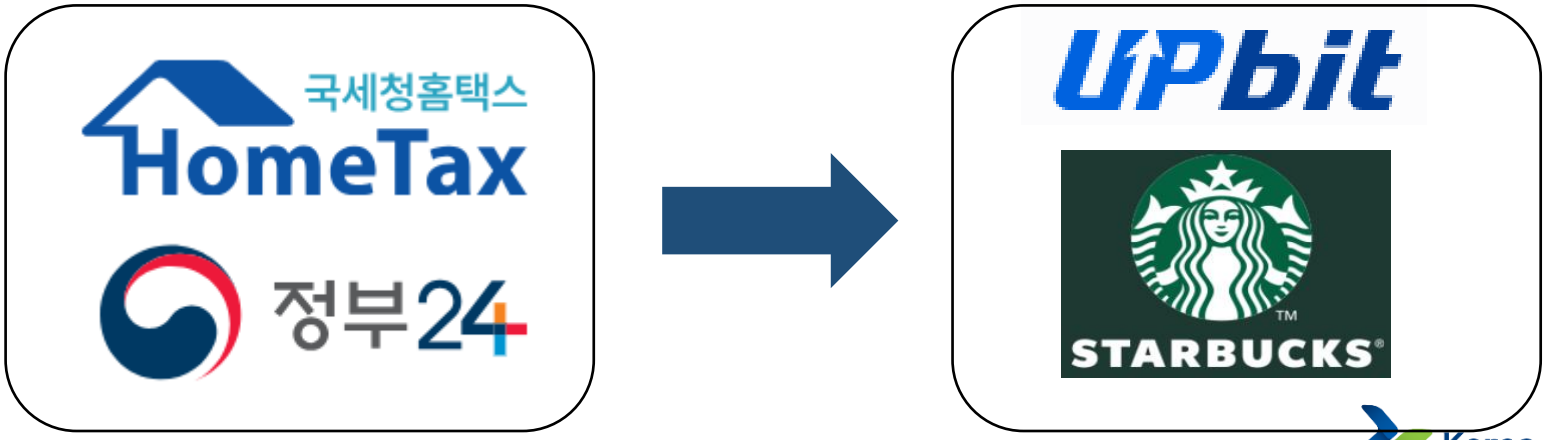
Milestones of Our Team

❖ Chronological Overview

Year	Key Event	Details / Achievements
2020	**Abolition** of the “Public Certification” system	Established fair competition and encouraged private authentication providers to emerge
2021	**Launch of the new Accreditation System** for eSignature service providers	21 providers accredited to date
2022	Establishment of **Device PKI Root** System	Expanded from public use to include **EV charging certificates**
2023	Establishment of **Digital Authentication Proliferation Center**	Created easy integration interfaces (SDKs, APIs) to promote wider adoption
2024	Establishment of **Overseas Korean Authentication Center**	Enabled certificate issuance abroad **using e-passports**
2025	**Migration** of Root Certification System	**Upgrading cryptographic structure** for stronger security

Key Outcomes of These Changes

- **(Increase in accredited service providers)** 5 -> **21** providers (as of Nov 2025)
- **(identity verification)** Certificates can be issued **without face**-to-**face** verification
- **(storage methods) PC file**-based certificates -> **mobile**, cloud-based certificates
- **(Higher adoption and usage)** On average, **each citizen** holds **six certificates**
- **(Expansion into private sectors)** Usage expanded from public services to finance, healthcare, and commercial platforms



1 Surrounding Trends and Developments

Summary

❖ Expansion of Mobile ID

- Rapid deployment of DID-based digital identity across major mobile platforms

❖ Application of MyData Across All Sectors

- Extending trusted data usage from finance to telecom, retail, and healthcare

❖ Announcement of PQC Transition Policy

- National roadmap released for migration to post-quantum cryptography

Mobile ID

❖ **(Roadmap)** DID-based Mobile ID. This year, Korea begins issuing the Mobile Resident Registration Card

('21) Mobile Civil Service Certificate
('22) mobile driver's license
('23) Mobile National Veterans Registration Card
('24) Mobile Overseas Citizen Identity Verification Card
('25) **Mobile Resident Registration Card**, Mobile Alien Registration Card

❖ **(Significance)** Diversification of identity verification methods

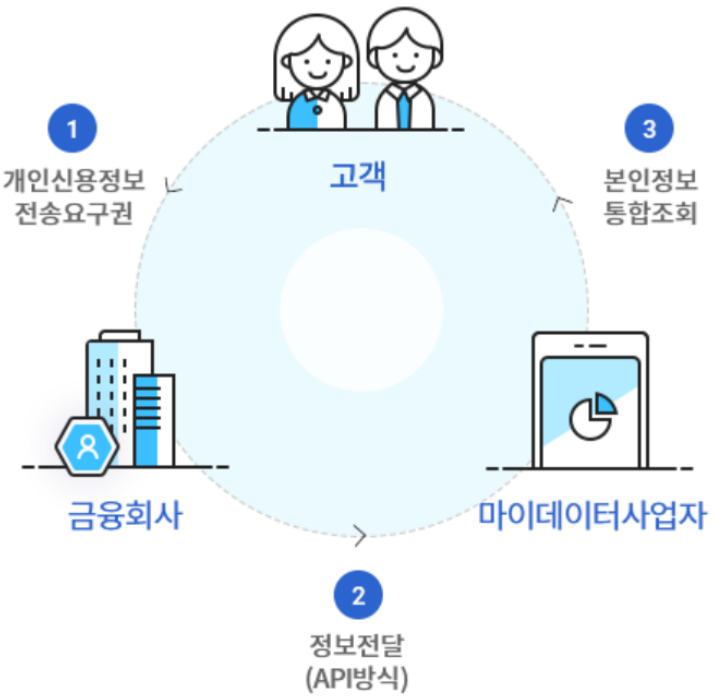
- I-Pin , Cellular Phone, Credit Card, Certificate… + **Mobile ID**

❖ **(Key Focus in 2025)** Issuing Mobile IDs through **multiple private apps** frequently used by citizens

- Users can store and share IDs across apps such as Samsung Wallet, Naver, KakaoBank, Toss, NH All-One Bank, and KB StarBanking.

MyData Expansion Across All Sectors

❖ As the **MyData** initiative **expands from finance to telecom, retail, and healthcare**, the use of eSignatures and **certificates is increasing** significantly.



Definition	• The Right to Data Portability allows individuals to request the transfer of their personal data. • MyData operators strengthen data sovereignty and provide convenient services based on user consent.
Flow	• [1] The user requests data transfer via a MyData app. • [2] The company sends user data to the MyData operator through an API. • [3] The user can view integrated data through the MyData platform.
Examples of Use	• Receiving telecom usage data and getting personalized **mobile plan recommendations**. • Analyzing financial spending patterns to suggest **credit scores or investment options.**
Relation to PKI	• eSignature certificates are used for user authentication within MyData apps. • Digital signatures ensure legal consent for each data transfer request.

KISA Korea Internet & Security Agency

축소

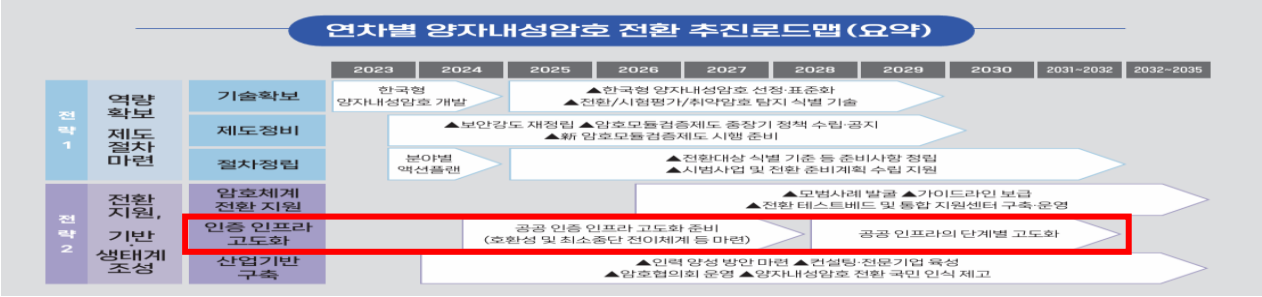
Transition to Post-Quantum Cryptography (PQC)

❖ **(Policy)** The Master Plan for PQC transition was released in July 2023, followed by the **Action Plan announced in September 2025**.

❖ **(Standardization & Certification)** Korea's national PQC project (K-PQC) has selected the following algorithms (2025):

- **Digital Signatures**: AI Mer, HAETAE, Key Exchange: NTRU+, SMAUG-T
- The KCMVP cryptographic validation program will include PQC algorithms by 2028.

❖ **(Implication)** All PKI cryptographic infrastructures in Korea will migrate to quantum-resistant algorithms according to this roadmap.



Contact Us

❖ If you would like more detailed information,

❖ If you are interested in collaboration,

❖ Or if you would like to support or contribute,

👉 Please feel free to contact us anytime.

📧 **rootca@kisa.or.kr**

🌐 **Korea Internet & Security Agency (KISA)**

Internet On, Security In!

Thank you

KISA Korea Internet & Security Agency