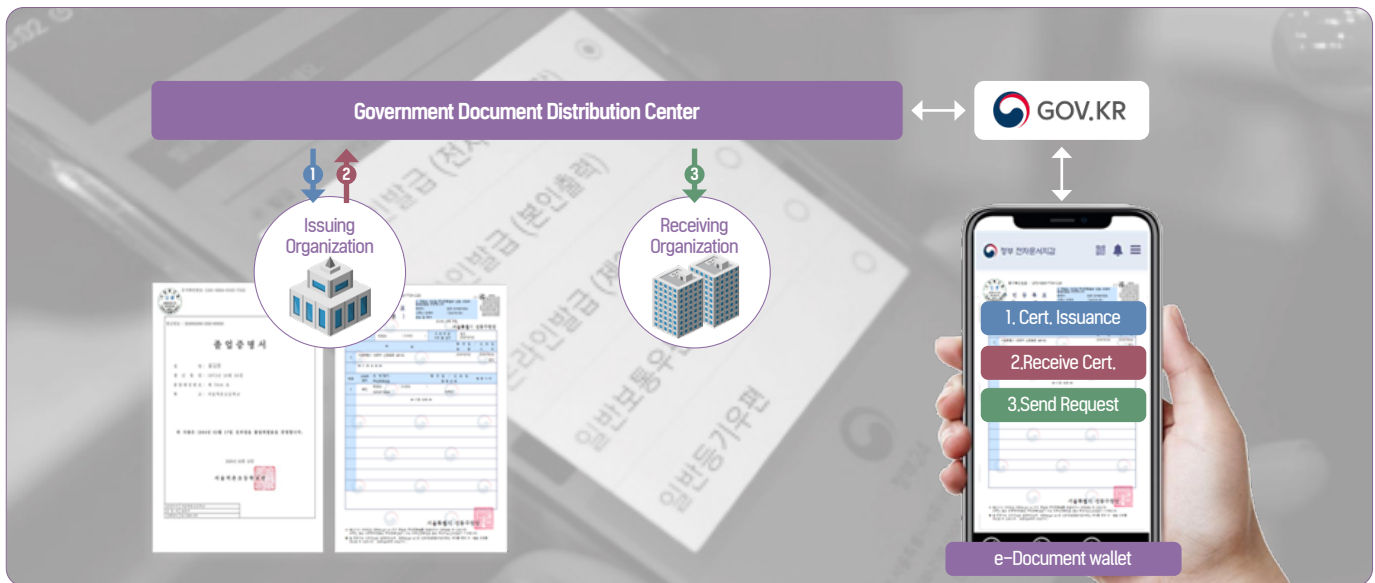


Digital Government Certificate Management System

The Digital Government Certificate Management system is a digital document creation, distribution, and verification technology. It allows citizens to issue civil certificates, such as resident registration documents, through a smartphone app and submit them to third parties in electronic form.

In South Korea, this system applies blockchain technology to the "Digital Document Vault" (Government24 platform), enabling individuals to authenticate themselves easily and conveniently. Citizens can request, issue, and submit electronic certificates directly to institutions via mobile devices.



▲ Certificates can be requested, reviewed, and submitted using a smartphone app.

Issues to Tackle

- ☑ Various certificates are issued and printed as paper documents, requiring offline processing for all subsequent steps, which needs improvement.
- ☑ Additional effort and time are required to verify the authenticity of certificates during submission.

Expected Benefits

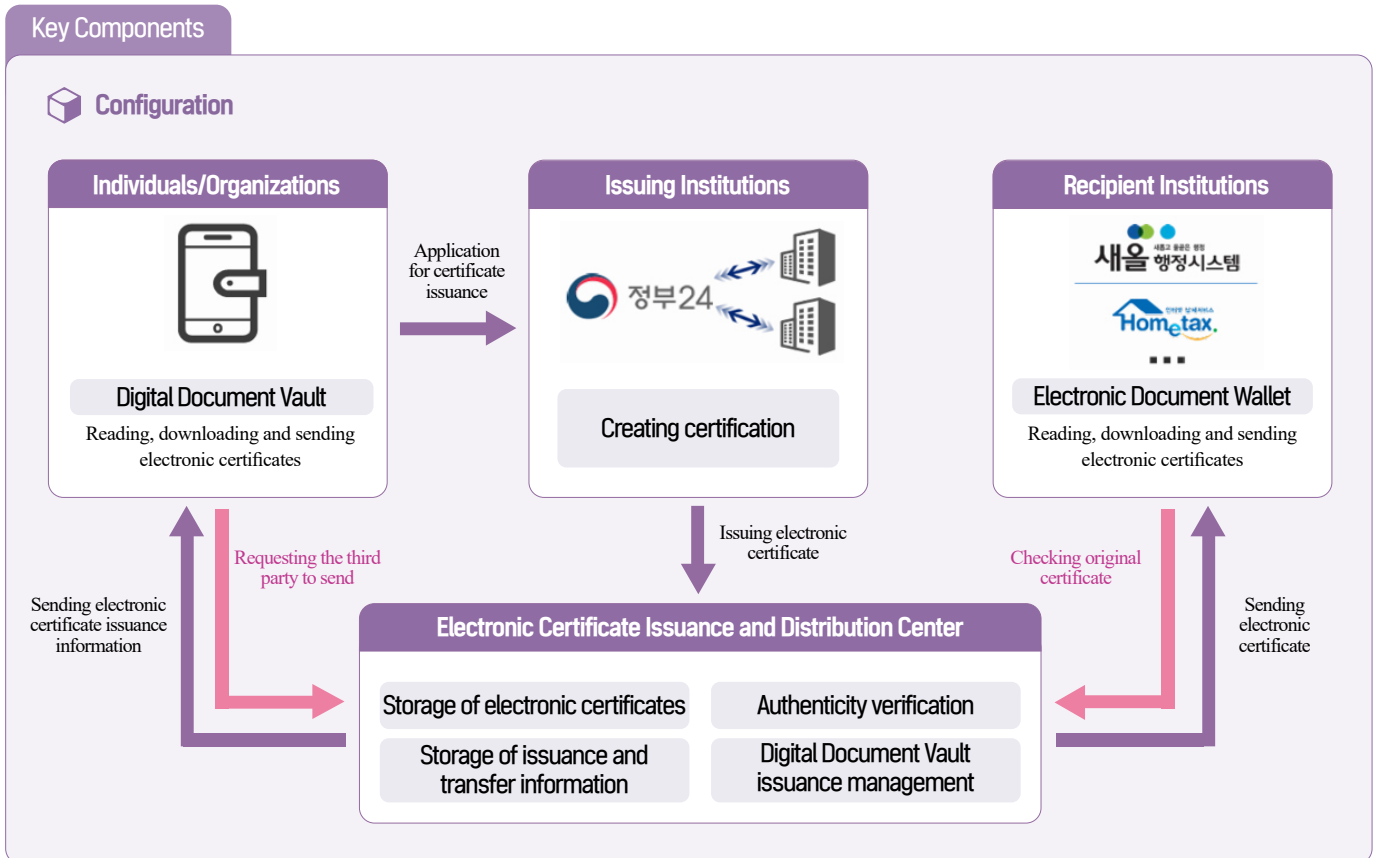
- ☑ Reducing social costs associated with issuing, receiving, and submitting certificates.
- ☑ Enhancing security and convenience through digital verification of certificates, data utilization, and streamlined processes.

💡 Key Services

- Issuance of public documents, such as resident registration certificates in electronic format and storage in the Digital Document Vault.
- Submission of electronic certificates to banks, public institutions, and other third parties as needed.
- Comprehensive management of certificate issuance, viewing, submission, and authenticity verification via the Digital Document Vault.
- Security measures, such as encryption, access control, and access logs are applied to the self-managed storage system for certificates, preventing forgery and verifying integrity using blockchain security.

⚙️ Use Cases

- As of 2024, the electronic certificate service supports the issuance of 435 types of civil documents, including resident registration certificates and family relationship certificates. Seventy types of certificates can also be conveniently requested through private apps like Naver, Kakao, Toss, and Initial.
- KakaoTalk introduced a "Kakao Certification" feature, allowing users to prove their qualifications and experience for job applications both online and offline.



Key Technologies

1. Hardware Security Module (HSM)

- Ensures secure encryption by generating, managing, and protecting encryption keys and digital certificates. This module safeguards processes against tampering.

2. Software Development Kit (SDK)

- Manages digital certificates and verifies authenticity through code extraction and validation.
- POINT** Offers features like opening certificates, inputting private keys, and restoring encrypted documents.

3. Blockchain-Based Digital Identity (DID)

- Converts input data into secure hash values using cryptographic algorithms and ensures identity verification through blockchain.
- POINT** Prevents forgery and maintains certificate integrity using advanced blockchain technologies.

4. Public Key Infrastructure (PKI)

- Encrypts data during transmission with public keys and verifies user identity for secure communication.
- POINT** Adheres to X.509 PKI standards for global encryption protocols.

5. Time Stamping Authority (TSA)

- Prevents unauthorized changes to certificates by verifying issuance time with linked secure timestamps.
- POINT** Uses timestamps provided by the Government Trusted Authentication Center (GTSA).

Securing Certificates Against Tampering

- The system guarantees that electronic certificates remain authentic and unchanged. Timestamps confirm the creation time and verify the document's integrity post-issuance.

Technology Companies

GOVERNMENT ELECTRONIC DOCUMENT WALLET
www.dpaper.kr

