# Digital Government Certificate Management System

The electronic certificate issuance and distribution system is a digital document creation, distribution, and verification technology that allows users to receive civil complaint certificates, such as resident registration abstracts, as electronic documents through a smartphone app and submit them to third parties.

In South Korea, one can easily and conveniently receive mobile electronic certificates through simple personal authentication and submit them directly to institutions with just an 'electronic document wallet (government platform)' that utilizes blockchain technology.
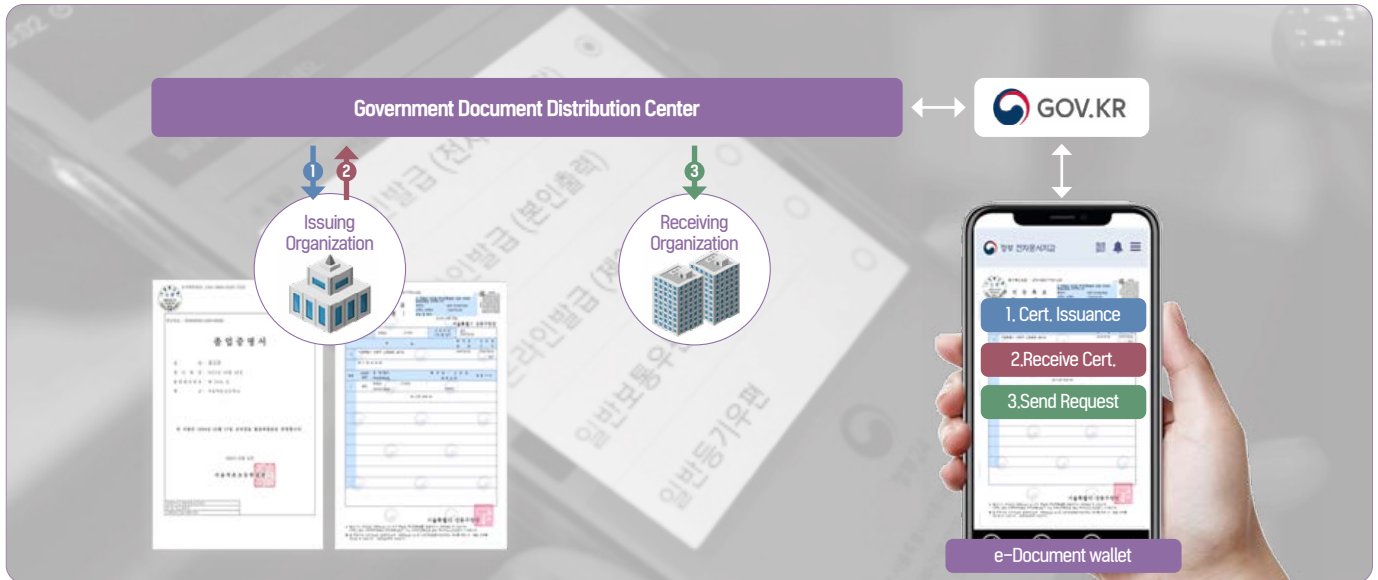
▲ It is possible to apply for, view, and submit certificates using a smartphone.

Issues to Tackle

☑ Need for improvement, as various certificates are issued and printed on paper, with subsequent procedures all processed offline.

☑ Need for separate time and effort to verify the authenticity of the certificates upon receipt.

Expected Benefits ☑

☑ Reducing social costs associated with the issuance, receipt, and submission of certificates.

☑ Enhancing security and convenience through the verification of the authenticity of digital-based certificates and the utilization of data
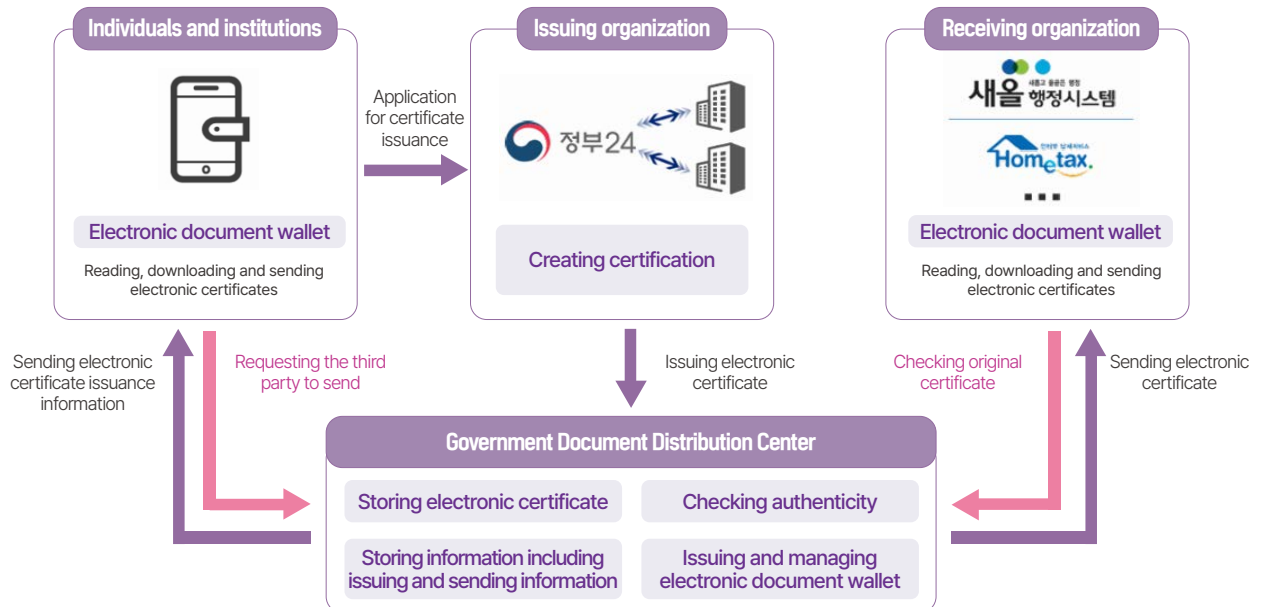
💡 Key Services

· Receiving certificates issued by the public sector, such as resident registration abstracts, as electronic documents and storing them in my electronic document wallet.

· Submitting electronic certificates from my electronic document wallet to third parties such as banks and public institutions when needed.

· Issuing, receiving, viewing, and submitting certificates, and verifying the authenticity of certificates in the 'electronic document wallet'.

· The personal information storage where the certificates are kept applies security measures such as encryption, access blocking, and access logs, and blockchain security is applied to prevent forgery and alteration of certificates and to verify their authenticity.

⚙ Use Cases

· As of 2024, the electronic certificate service allows for the issuance of 435 types of administrative documents, including Resident Registration Certificates and Family Relationship Certificates, in electronic format. Additionally, 70 types of electronic certificates can be easily applied for through private apps such as Naver, Kakao, Toss, and Initial.

· In KakaoTalk, the "KakaoTalk Employee ID" can be used to verify a user's employment and career, serving as a means of workplace authentication both online and offline.

Key Components

Configuration

Individuals and institutions

Electronic document wallet

Reading, downloading and sending electronic certificates

Application for certificate issuance →

Issuing organization

정부24

Creating certification

Receiving organization

새올 행정시스템

Hometax.

Electronic document wallet

Reading, downloading and sending electronic certificates

Sending electronic certificate issuance information

Requesting the third party to send

Issuing electronic certificate

Checking original certificate

Sending electronic certificate

Government Document Distribution Center

Storing electronic certificate	Checking authenticity
Storing information including issuing and sending information	Issuing and managing electronic document wallet

Technology

1. Hardware Security Module

· A hardware device that generates, protects, and manages cryptographic keys, creates digital signatures and certificates to protect cryptographic processes with enhanced tamper resistance.

2. Software Development Kit

· Management of wallet authentication keys, decryption of electronic certificates, and extraction of authenticity verification values.

POINT Providing an electronic certificate decryption function by receiving the viewing key, electronic certificate, wallet authentication key, and wallet authentication key password.

3. Blockchain−Based Digital ID (DID)

· Applying blockchain's hash technology and inter-block chaining technology (linking hash values of blocks).

POINT Certificate validity verification, prevention of forgery and tampering, and authentication of certificate genuineness.

4. Public Key Infrastructure

· A system that encrypts transmitted and received data using a public key and authenticates users through digital certificates.

POINT Complying with X.509 standard PKI technology

5. Time Stamping Authority (TSA)

· Verifying the integrity of certificates at the time of issuance by linking with point-in-time verification technology to prevent forgery and tampering.

POINT Using timestamps from the Ministry of the Interior and Safety's Electronic Document Authenticity Verification Center (GTSA)

Injection of government-standard seals to prevent forgery and tampering of electronic certificates.

· A technology that proves the time when an electronic certificate was created by injecting a timestamp and technically proves that the electronic certificate has not been changed since then.

Technology Companies

GOVERNMENT ELECTRONIC DOCUMENT WALLET
www.dpaper.kr