

전자증명서 발급·유통 시스템

전자증명서 발급·유통 시스템은 주민등록초본 등 민원증명서를 스마트폰 앱에서 전자문서로 발급받아 제3자에게 제출할 수 있는 디지털 문서 생성, 유통, 증명 기술이다.

대한민국에서는 블록체인 기술이 적용된 '전자문서지갑(정부 플랫폼)'만 있으면 간단한 개인 인증으로 쉽고 편리하게 모바일 전자증명서를 발급받아 기관에 바로 제출할 수 있다.



▲ 스마트폰에서 증명서 발급신청, 열람, 제출이 가능하다.

해결과제

- ☑ 각종 증명서가 종이로 발급·출력되어 이후 절차가 모두 오프라인으로 처리되고 있어 개선 필요
- ☑ 증명서류 접수 시 증명서의 진위확인을 위해 별도 노력과 시간 필요

기대 효과

- ☑ 증명서 발급, 수령, 제출에 소요되는 사회적 비용 절감
- ☑ 디지털 기반 증명 문서의 진위 확인, 데이터 활용 등 보안성과 편의성 증대

💡 주요 서비스

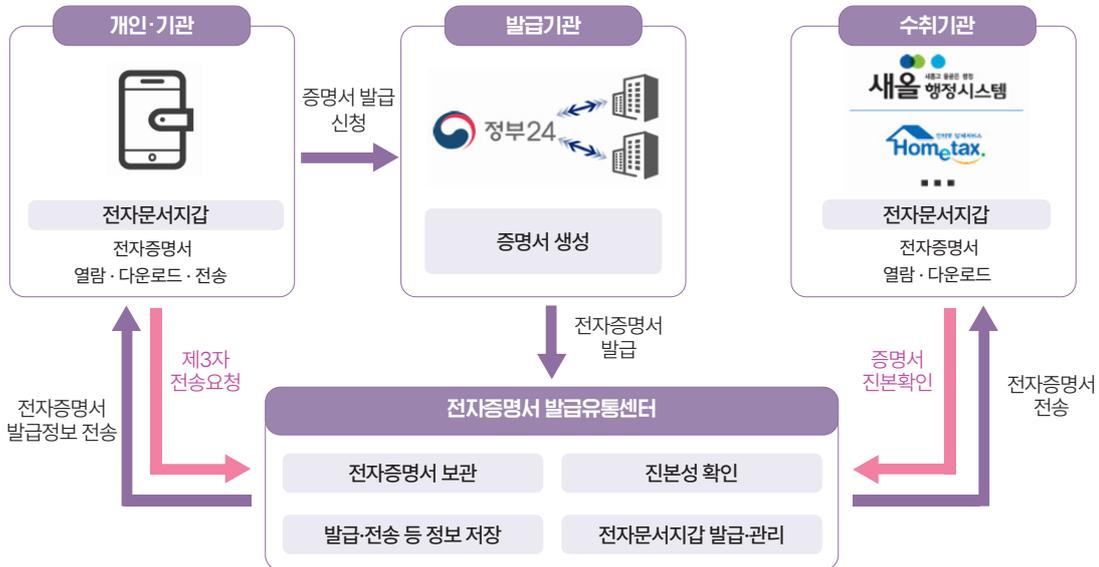
- 주민등록초본 등 공공부문에서 발급하는 증명서를 전자문서로 발급받아 내 전자문서지갑에 보관
- 필요 시 내 전자문서지갑의 전자증명서를 은행, 공공기관 등 제3자에게 제출
- 전자문서지갑에서 증명서 발급 수령, 열람, 제출 및 증명서 진위 확인
- 증명서가 보관되는 자기정보 저장소는 암호화, 접근 차단, 접속기록 등 보안조치가 적용되며 증명서의 위·변조를 차단 및 진본 여부 확인은 블록체인 보안 적용

📍 도입 사례

- 2024년 기준 전자증명서 서비스는 주민등록등·초본, 가족관계증명서 등 민원서류 435종을 전자증명서로 발급 가능, 민간앱(네이버, 카카오, 토스, 이니셜 등)에서도 70종의 전자증명서를 손쉽게 발급신청 가능
- 카카오톡에서 '카톡사원증'으로 이용자의 재직 및 경력을 증명할 수 있어 온라인과 오프라인에서 직장 인증 수단으로 활용
- 그 외에도 국민연금공단, 보건복지부의 복지료, 중소기업벤처기업부 중소기업벤처24, 경찰민원포털 등에서 도입

주요 구성

구성도



주요 기술

1. 하드웨어 보안 모듈(HSM, Hardware Security Module)

· 암호키를 생성, 보호, 관리하고 디지털 서명 및 인증서를 생성하여 암호화 프로세스를 보호하는 강화된 변조 방지 하드웨어 장치

2. 보안 소프트웨어 개발 키트 (SDK, Software Development Kit)

· 지갑인증키의 관리 및 전자증명서의 복호화와 진본성 검증값 추출
POINT 열람키, 전자증명서, 지갑인증키, 지갑인증키 비밀번호를 입력 받아 전자증명서 복호화 기능 제공

3. 블록체인 기반 디지털 아이디(DID)

· 블록체인의 해시기술(임의 데이터를 해시값으로 변환하는 암호 알고리즘) 및 블록 간 체인기술(블록의 해시값 연결)을 적용
POINT 증명서 유효성 검증, 위변조 방지, 증명서 진위증명

4. 공개 키 기반 구조(PKI, Public Key Infrastructure)

· 공개키를 이용하여 송수신 데이터를 암호화하고 개인키로 사용자를 인증하는 시스템
POINT X.509 표준 PKI 기술 준수

5. 시점 확인 기술(TSA, Time Stamping Authority)

· 증명서의 위변조 차단을 위해 발급 시 시점확인기술 연동으로 무결성 검증
POINT 행정안전부 전자문서진본확인센터(GTSA)의 타임스탬프 사용



전자증명서 위·변조방지를 위한 정부표준인영 주입

· 타임스탬프를 주입하여 전자증명서가 생성된 시각을 증명하고 이후 전자증명서가 변경되지 않았음을 기술적으로 증명할 수 있는 기술



기술기업

정부 전자문서지갑
 www.dpaper.kr

