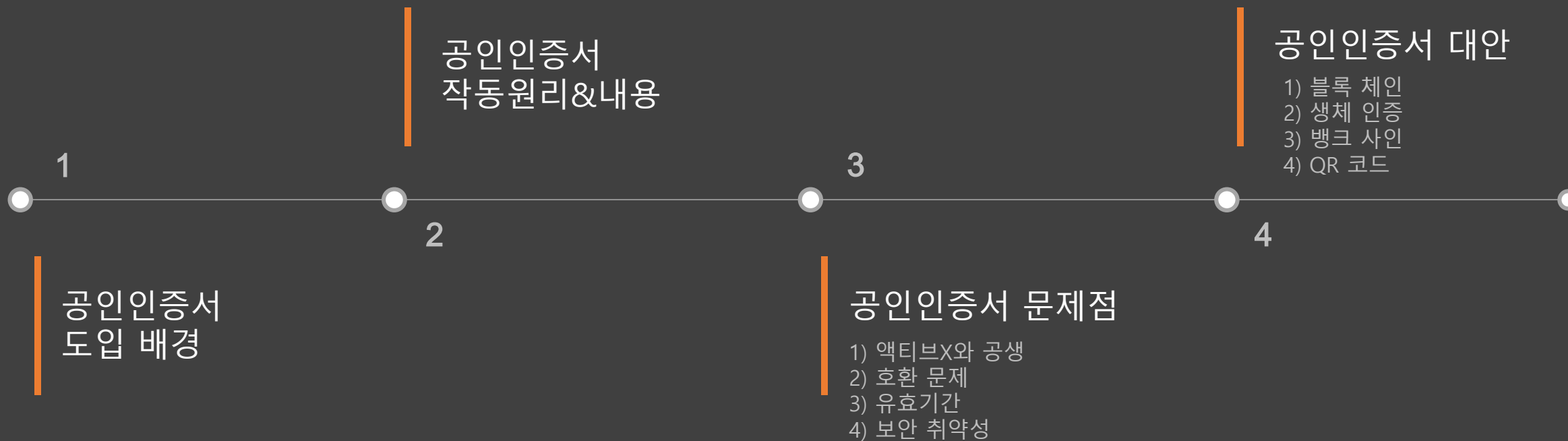


공인인증서의 폐지 및 대안

1495037 유원상



Certificate 목차





Certificate

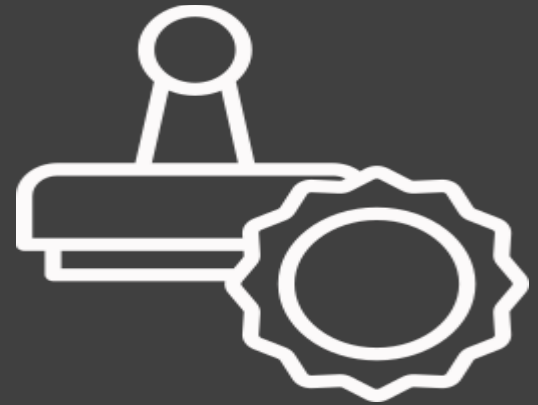
공인인증서 도입 배경



1. 거래 당사자 간 신원확인



2. 거래 내용의 변경 여부 확인



3. 거래 사실에 대한 증명

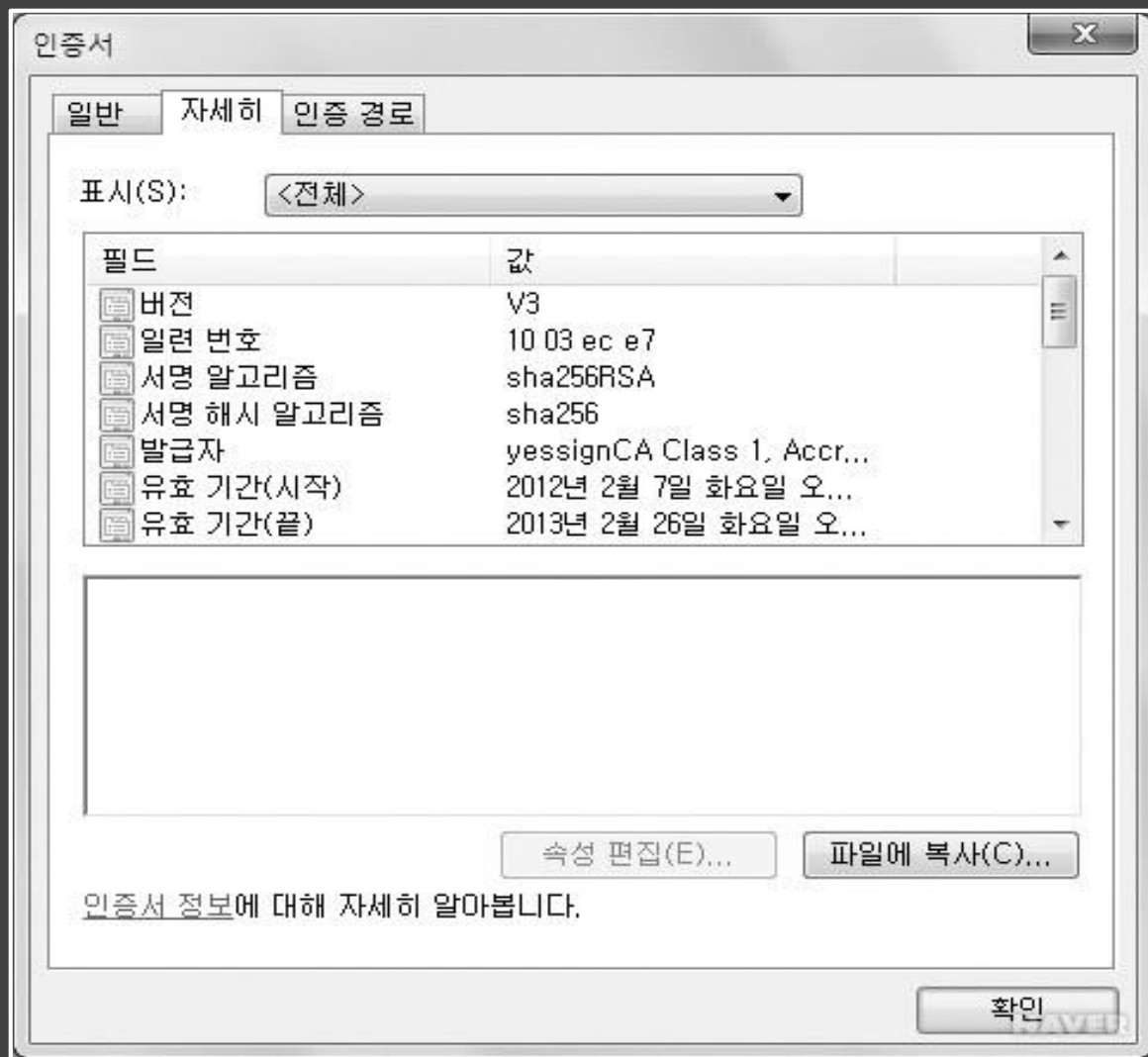
Certificate 공인인증서 작동원리



공인인증서는 파일에 대한 전자서명을 파일형태로 나타내어 전자 신분증 형태로 관리하는 것이다.

Certificate

공인인증서 내용



인증서 기본영역

버전
일련번호
서명 알고리즘
발급자
유효기간(시작, 끝)
주체
공개키

+

인증서 확장영역

기관 키 식별자
주체 키 식별자
주체 대체 이름
CRL 배포 지점
기관 정보 액세스
키 사용 용도



Certificate 공인인증서 문제점

액티브X와 공생

사이트마다 다른
액티브X 설치 필요함



호환 문제

인터넷 익스플로러 외에 다른
인터넷 브라우저와 호환 안됨



짧은 유효기간

1년의 유효기간이
지나면 갱신 필요함



보안 취약성

DDOS 등의 좀비PC
악성코드의 주 감염경로

Certificate 공인인증서 대안

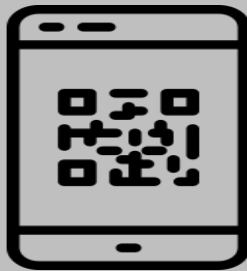


뱅크사인

은행권 주도로 만들어졌지만, 여전히 별도 앱 설치/실행 필요해 불편.

QR코드

스마트폰으로 QR코드를 스캔하면 각종 결제 가능




블록체인

컴퓨터마다 분산된 장부를 통해 개인정보, 데이터 변조 등을 최소화시켜 정보 유출 예방

생체인증

정맥인식, 홍채인식, 안면인식, 음성인식, 지문인식 등을 통해 자신임을 증명



A person is sitting at a desk, writing in a notebook with a pen. A laptop is open in the background. The image is dimmed, and the text '감사합니다' and 'Thank You' is overlaid in the center.

감사합니다
Thank You