

# 전자인증서 및 공개키 기반구조

## (Digital Certificate, Public Key Infrastructure)

2024. 10.

컴퓨터·소프트웨어공학과

이 형 효

(hlee@wku.ac.kr)

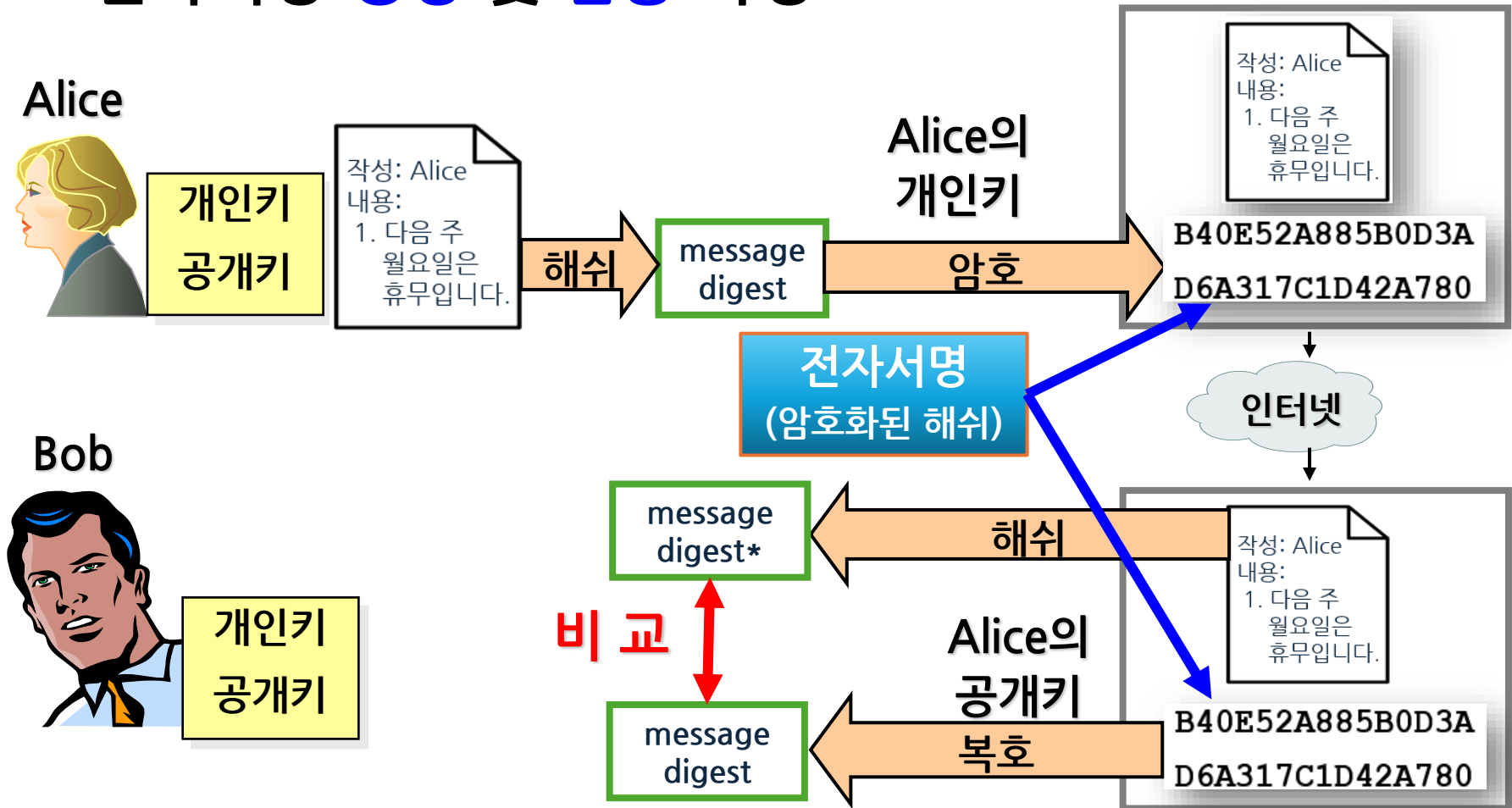
# 전자서명과 공개키(1)

## ■ 전자서명 제공 기능(서비스)

전자서명 목적	질 문	이유?
① 서명자 신원 확인	Q1. Alice가 전자서명한 사용자가 맞는가?	
② 위조 불가 (Unforgeable)	Q2. 제3자가 메시지를 작성하고 Alice가 작성한 것처럼 속일 수 있을까?	
③ 변조 불가 (Unalterable)	Q3. Alice가 작성한 메시지를 제3자가 수정하여 보내고 검증 절차를 마칠 수 있을까?	
④ 재사용 금지 (Unreusable)	Q4. 제3자가 현재 메시지의 전자서명을 다른 메시지에 붙여 보내 검증 절차를 마칠 수 있을까?	
⑤ 부인 봉쇄 (Non-repudiation)	Q5. Alice가 나중에 자신이 이 메시지를 보낸 사실이 없다고 부인할 수 있을까?	

# 전자서명과 공개키(2)

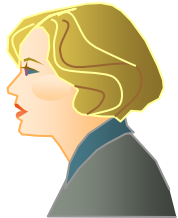
## 전자서명 생성 및 검증 과정



# 전자서명과 공개키(3)

- 전자서명 검증키(송신자 공개키) 속임 공격

Alice



Bob



Hi, Bob! This is Alice.  
This is my new public  
key [가짜 공개키]

Alice의 가짜 키쌍 생성

개인키  
공개키

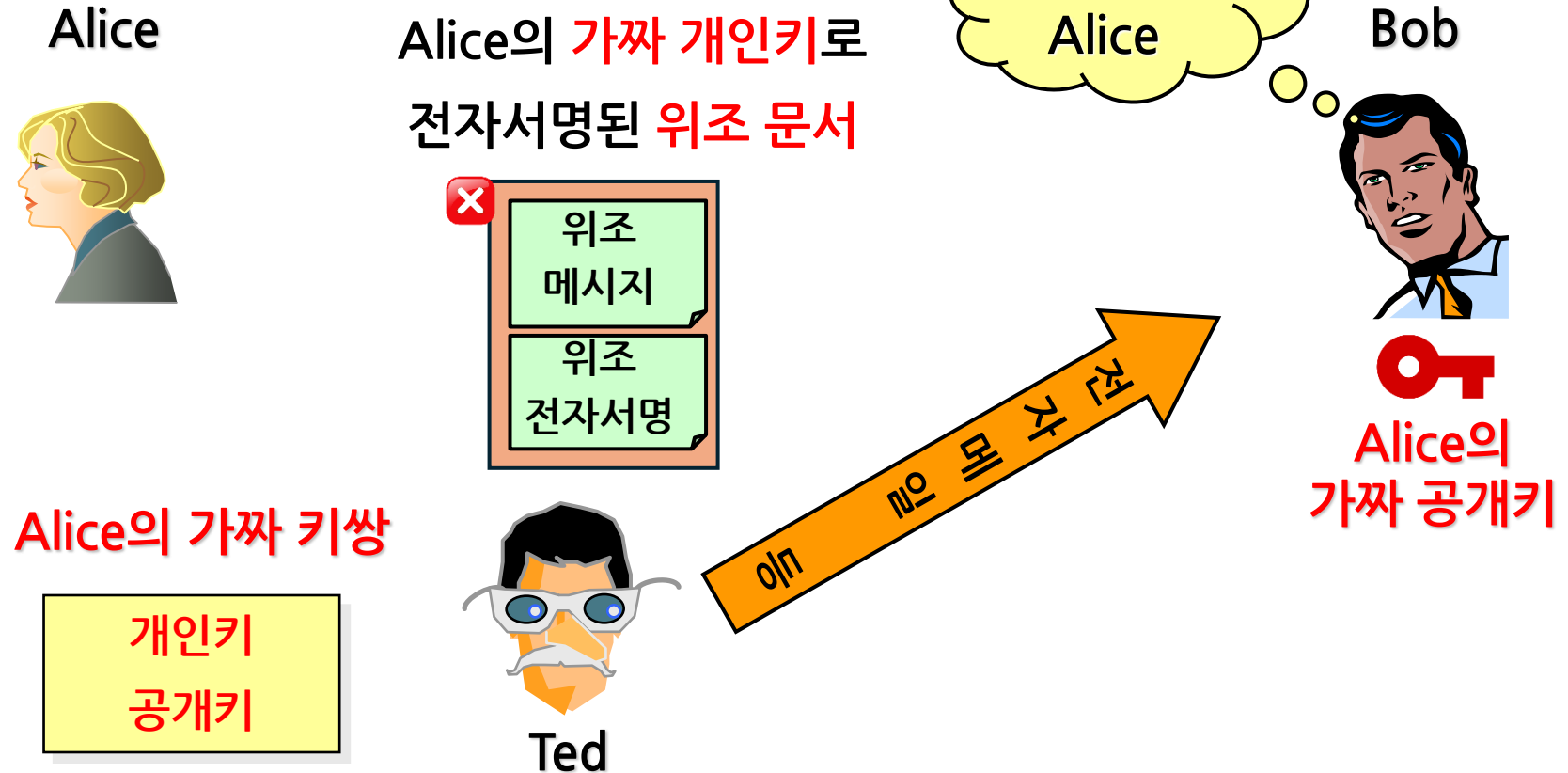


Ted

이  
의  
문  
전

# 전자서명과 공개키(4)

- 전자서명 **검증키**(송신자 공개키) **속임** 공격



# 전자서명과 공개키(5)

## ■ (중요)

- 사용자 Alice가 전자서명한 문서를 검증할 때
  - 검증과정에 사용되는 검증키(Alice의 공개키)가
  - Alice의 진짜 공개키가 맞는지 확인 중요!!!
- 
- 어떤 공개키가 Alice의 공개키가 맞다는 사실을 신뢰할 수 있는 제3의 기관이 보증하는 방법 필요
    - 전자인증서(digital certificate)
    - 인증기관(CA: Certificate Authority)

# 현실 속 인증서(Certificate)

## ■ 인증(認證)이란?

- 어떤 문서나 행위가 **정당한 절차**로 이루어졌다는 것을 **공적 기관**이 **증명**함

## ■ 사례



**가족관계증명서 (일반)**

등록기준지	서울특별시 영등포구 여의도동 1번지의 1234				
-------	---------------------------	--	--	--	--

구분	성명	출생연월일	주민등록번호	성별	본
본인	김본인(金本人)	1965년 01월 01일	650101-1*****	남	金海

가족사항

구분	성명	출생연월일	주민등록번호	성별	본
부	김영철(金鏗徹)	1940년 04월 01일	400401-1*****	남	金剛
모	이은미(李恩美)	1942년 04월 02일	420402-2*****	여	全州
배우자	박여인(朴予仁)	1968년 02월 02일	680202-2*****	여	博仁
자녀	김상민(金上敏)	2003년 02월 01일	030201-3*****	남	金海

위 가족관계증명서(일반)는 가족관계등록부의 기록사항과 일치함을 증명합니다.

2020년 11월 04일

법원행정처 전산정보중앙관리소 전산운영책임관 홍길동

※ 위 증명서는 「가족관계의 등록 등에 관한 법률」 제15조제2항에 따른 등록사항을 현출한 일반증명서입니다.

# 전자인증서(Digital Certificate)(1)

- 사용자 공개키의 진위여부를 확인할 수 있는 방법 필요
- 인증서(Certificate) (眞僞)
  - 사용자 정보와 해당 사용자의 공개키를 포함
  - 신뢰된 인증기관에 의해 보증 필요
- 인증기관(CA: Certificate Authority)
  - 사용자 신원, 사용자의 공개키를 보증하는 믿을 수 있는 기관
    - ✓ TTP: Trusted Third Party
  - 인증서의 내용을 자신(인증기관)의 개인키로 서명
  - 인증서 발급, 관리, 폐지 업무 수행



# 전자인증서(Digital Certificate)(2)

## ■ 인증서 주요 구성요소 (일부)

Name: Individual, organization	발급대상자(subject)
Owner's public key	발급대상자 공개키
Certificate expiration date	인증서 유효기간
Certificate serial number	인증서 발급번호
Name of issuing CA	인증기관
Issuing CA's digital signature	인증기관 전자서명

# 전자인증서(Digital Certificate)(3)

## ■ 인증서 구성 요소

- 사용자 이름, 주소
- 인증서 유효 기간
- 인증서 일련 번호
- 사용자 공개키
- 인증기관(CA) 이름, 인증기관의 전자서명
- 확장 필드
  - ✓ 사용자 접근권한
  - ✓ 사용자의 위치 정보 등

# 전자인증서(Digital Certificate)(4)

## ■ 공동인증서, 금융인증서 차이

구분	공동인증서(구. 공인인증서)	금융인증서
발급기관	한국인터넷진흥원, 금융결제원, 한국정보인증(주), (주)코스콤, 한국전자인증(주), 한국무역정보통신, 한국정보사회진흥원	금융결제원
인증서 보관	사용자 기기 (PC, 스마트폰, USB 등)	클라우드
유효기간	1년 (수동갱신)	3년 (자동갱신)
비밀번호 형식	영문+숫자+특수문자 혼합	6자리 숫자
PC 보안 프로그램 설치	필요	불필요

# 인증기관(1)

## ■ 기능

- 전자인증서 발행 및 관리
- 전자인증서 취소목록(CRL) 발행
  - ✓ Certificate Revocation List

## ■ 전자인증서를 발행할 수준의 신뢰도 필수적

- 공동인증서 발급기관 (7개 기관)
  - ✓ 한국인터넷진흥원, 금융결제원, 한국정보인증(주), (주)코스콤, 한국전자인증(주), 한국무역정보통신, 한국정보사회진흥원
- 금융인증서 발급기관 - 금융결제원

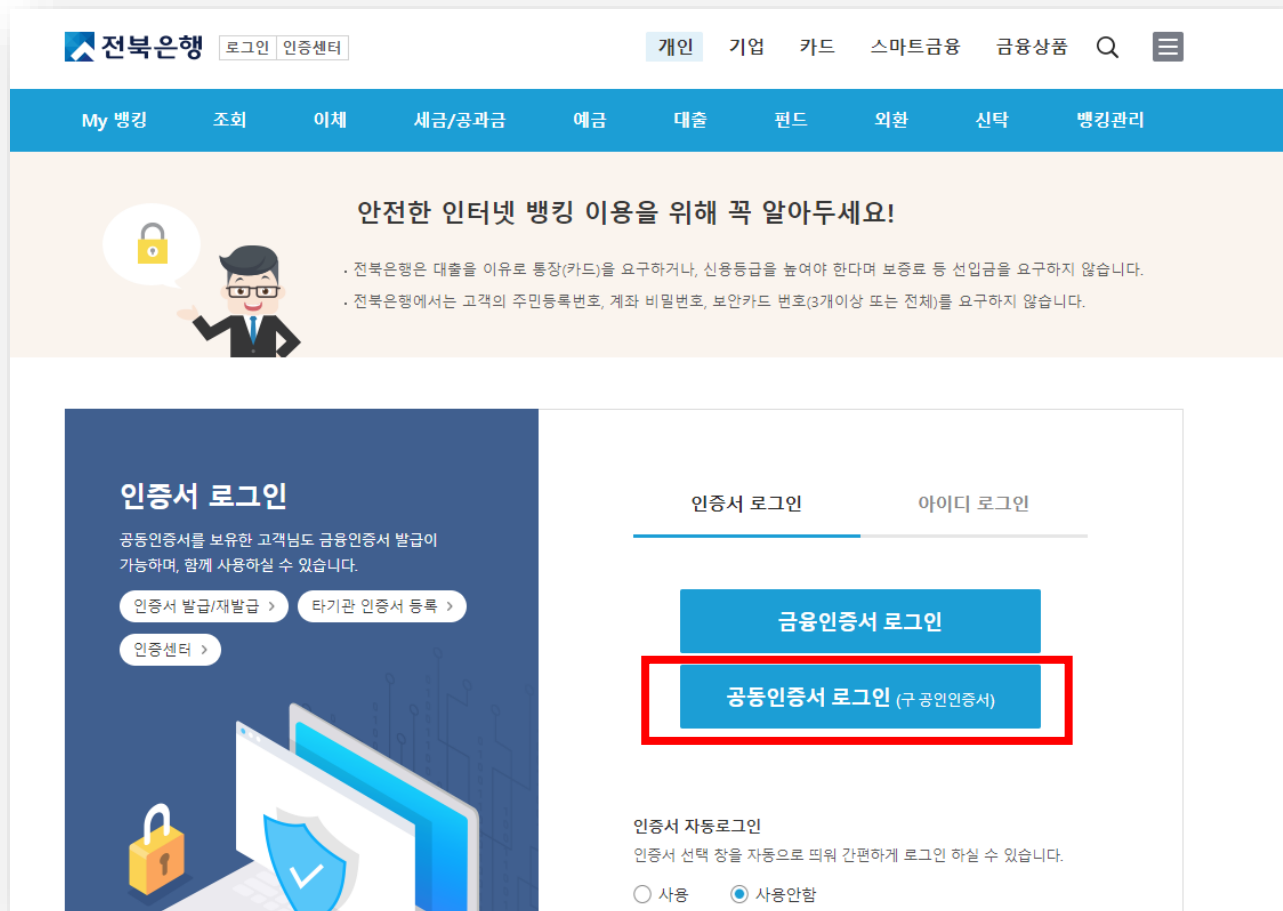
# 인증기관(2)

## ■ 공동인증서 발행 절차

- CA에 전자인증서 발행 신청
  - ✓ 사용자의 인적사항
- CA에 의한 사용자 확인
  - ✓ 주민등록, 지문 등 정보 요청, 확인
  - ✓ 확인 절차와 내용은 전자인증서의 내용에 따라 달라짐
- 사용자 확인이 성공적으로 완료된 사용자에 대해  
CA의 비밀키로 전자서명된 전자인증서 발급

# 인증기관(3)

## ■ 공동인증서 사용 사례 (예: 전북은행)



# 인증기관(4)

- 공동인증서 사용 사례 (예: 전북은행)

공통인증서

전북은행

인증서 위치

하드 디스크 이동식디스크 브라우저 인증서찾기 저장토큰

구분	사용자	마료일	발급자
범용개인	이형호(LEE HYUNG HYO)0...	2025-03-08	yesignCA ...

인증서 보기 인증서 암호는 대소문자를 구분합니다.

인증서 삭제 인증서 암호 ..... 마우스 입력>

인증서 복사 ! 인증서 선택 후 암호를 입력하세요.

확인 취소


# 인증기관(5)

## ■ 공동인증서 사용 사례 (예: 전북은행)

인증서 정보

일반 자세히

일반

 인증서 정보

이 인증서의 전자서명이 올바릅니다.

[발급대상]  
이형호(LEE HYUNG HYO)003701520040214000059

[발급자]  
yesignCA Class 3

[구분]  
범용개인 - 전북은행

[유효기간]  
2024-03-08 00:00:00 ~ 2025-03-08 23:59:59

[PC Time]  
2024-10-14 19:46:12

사용자 알림

발급대상자  
(subject)

발급자  
(인증기관,CA)



# 인증기관(6)

## ■ 공동인증서 사용 사례 (예: 전북은행)

인증서 정보	
일반	자세히
자세히	
필드	값
버전	3
일련번호	852972637 (0x32D7545D)
서명 알고리...	SHA256 + RSA
발급자	cn=yessignCA Class 3,ou=AccreditedCA,o=yesign,c...
다음부터 유...	2024-03-08 00:00:00
다음까지 유...	2025-03-08 23:59:59
주체	cn=이형효(LEE HYUNG HYU)00370152004021400005...
공개키 알고...	RSA (2048 Bits)
공개키	3082010a028201010090c87b532ee1f84c808a4d9f38d...
서명	417676b2db452510ea03939e667305b9486fa47d476d...
CA 키 고유...	f287a3e6d95e1616724ed8c2bc853903375990c4
인증서 정책	1.2.410.200005.1.1.1
키사용	digitalSignature,nonRepudiation

# 공개키 기반 구조(PKI)

- Public Key Infrastructure

- 정의

- 공개키 사용을 위한 표준들
  - ✓ 암호, 해시 알고리즘
- CA, CA들간의 복합 구조 및 인증 경로
  - ✓ Certificate, Certificate Revocation List(CRL)
- 운영/관리 규약 및 관련 법규 들의 집합

# X.509 인증서(1)

## ■ 정의

- ITU-T에 의해 제안된 인증서 형식 정의
- 인증서를 이용한 공개키의 효율적인 분배 방법 정의
- 1988년 X.509 v1에서 1996년 v3까지 발전
  - ✓ 인증서 취소 목록(CRL)은 v1, v2가 있음
  - ✓ 인증서에 필요한 항목이 증가하면서 v1부터 v3까지 발전함

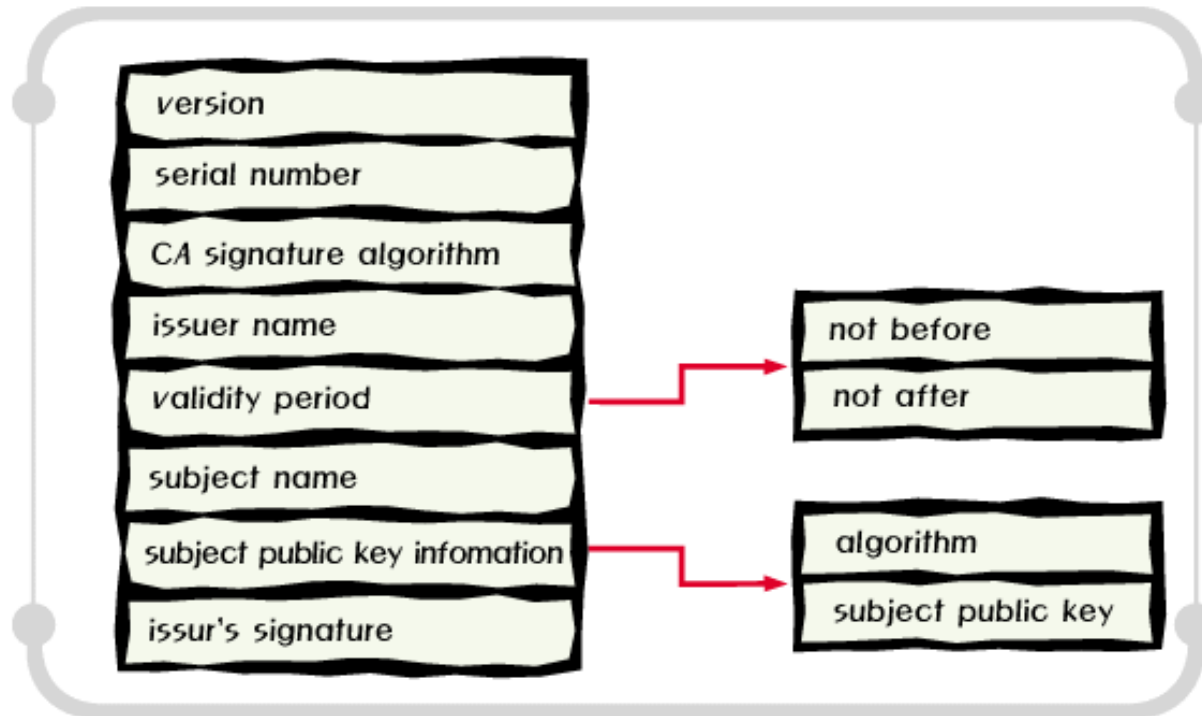
## ■ CA가 최종 개체에 발급함

- 인증서에는 **공개키**와 **신분정보**가 포함됨
- **CA의 개인키**를 사용하여 **인증서의 내용 보증**

# X.509 인증서(2)

## ■ X.509 v1

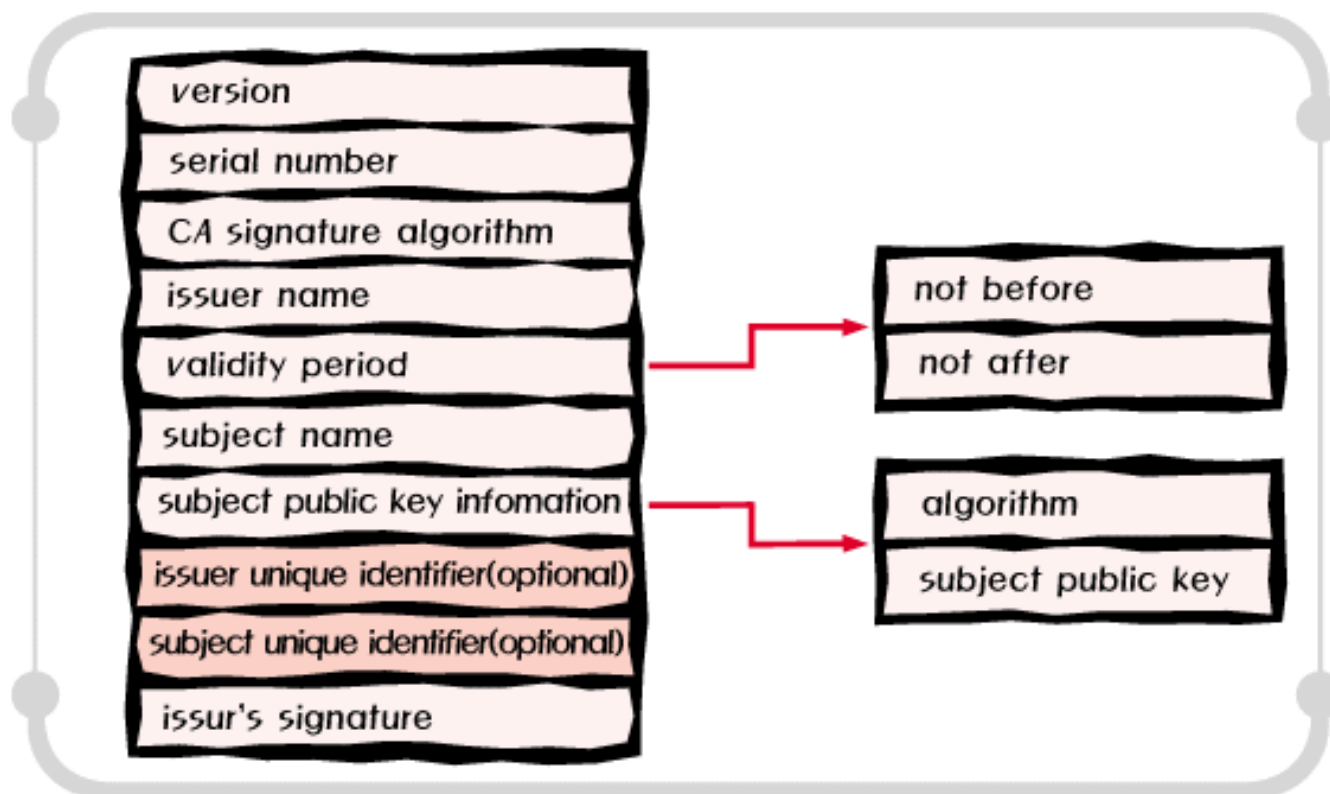
- CA signature algorithm : 인증서 서명 생성시 사용된 **서명/해시 알고리즘**에 대한 표시



# X.509 인증서(3)

## ■ X.509 v2

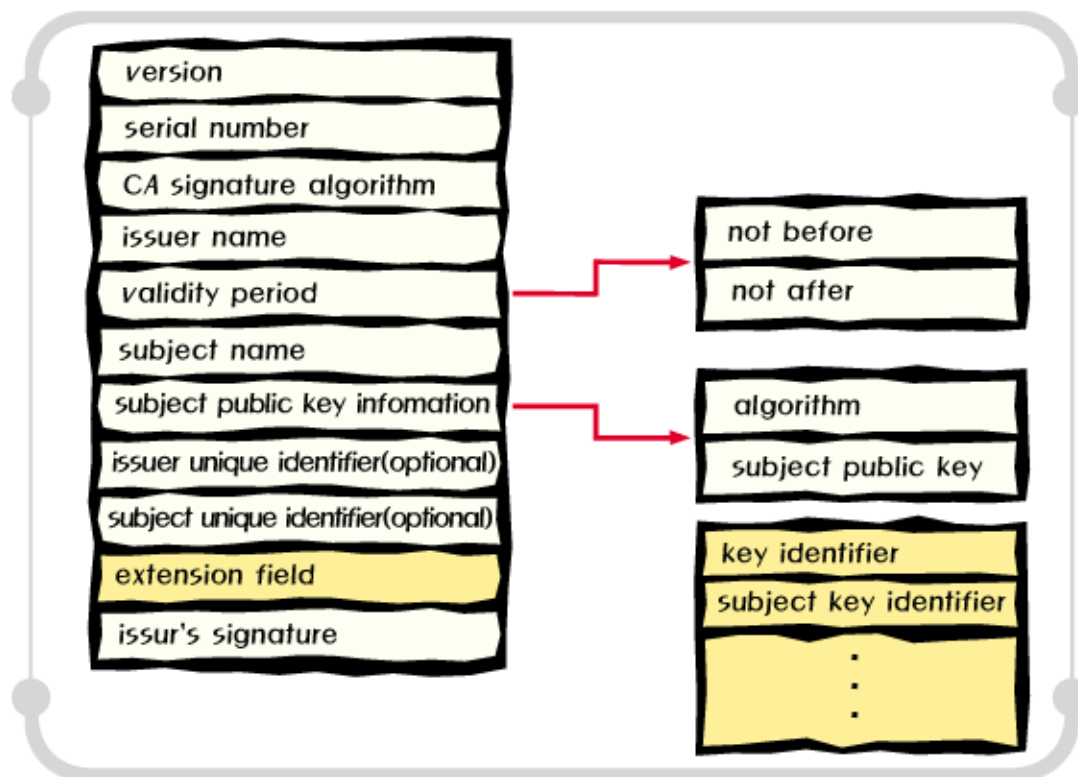
- Issuer/Subject Unique Identifier 추가



# X.509 인증서(4)

## ■ X.509 v3

- 확장 필드 추가(예: Key Identifier, ...)



# 인증서 인증 경로(1)

## ■ 사용자, 중간 인증기관, 루트 인증기관

(Q1) Alice 전자서명 검증 시  
필요정보와 출처는?

(Q2) Alice 전자인증서  
검증 시 필요정보와 출처는?

Alice 전자서명  
문서



Alice 전자인증서

버전정보
주체이름(Alice)
Alice 공개키
CA이름(CA-1)
CA-1 전자서명

CA-1 전자인증서

버전정보
주체이름(CA-1)
CA-1 공개키
CA이름(CA-2)
CA-2 전자서명

CA-3 전자인증서

**끝없는 반복**

CA-2 전자인증서

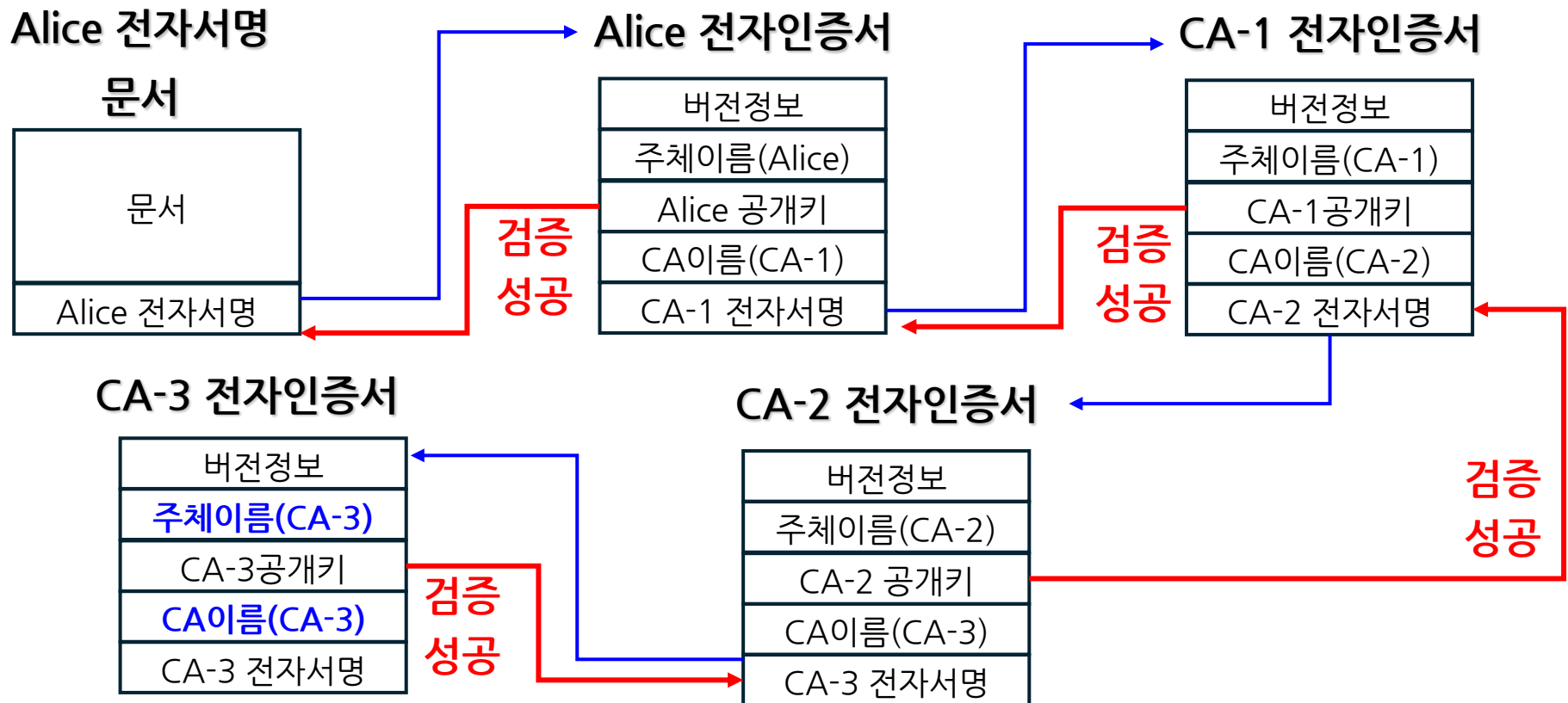
버전정보
주체이름(CA-2)
CA-2 공개키
CA이름(CA-3)
CA-3 전자서명

(Q4) CA-2 전자인증서  
검증 시 필요정보와 출처는?

(Q3) CA-1 전자인증서  
검증 시 필요정보와 출처는?

# 인증서 인증 경로(2)

- 사용자, 중간 인증기관, 루트 인증기관
  - 중간 인증기관(CA-1, CA-2), 루트 인증기관(CA3)





# Chrome 관리 전자인증서 확인(1)

## ■ Chrome 브라우저

- [설정] - [개인 정보 보호 및 보안] - [보안] - [인증서 관리]

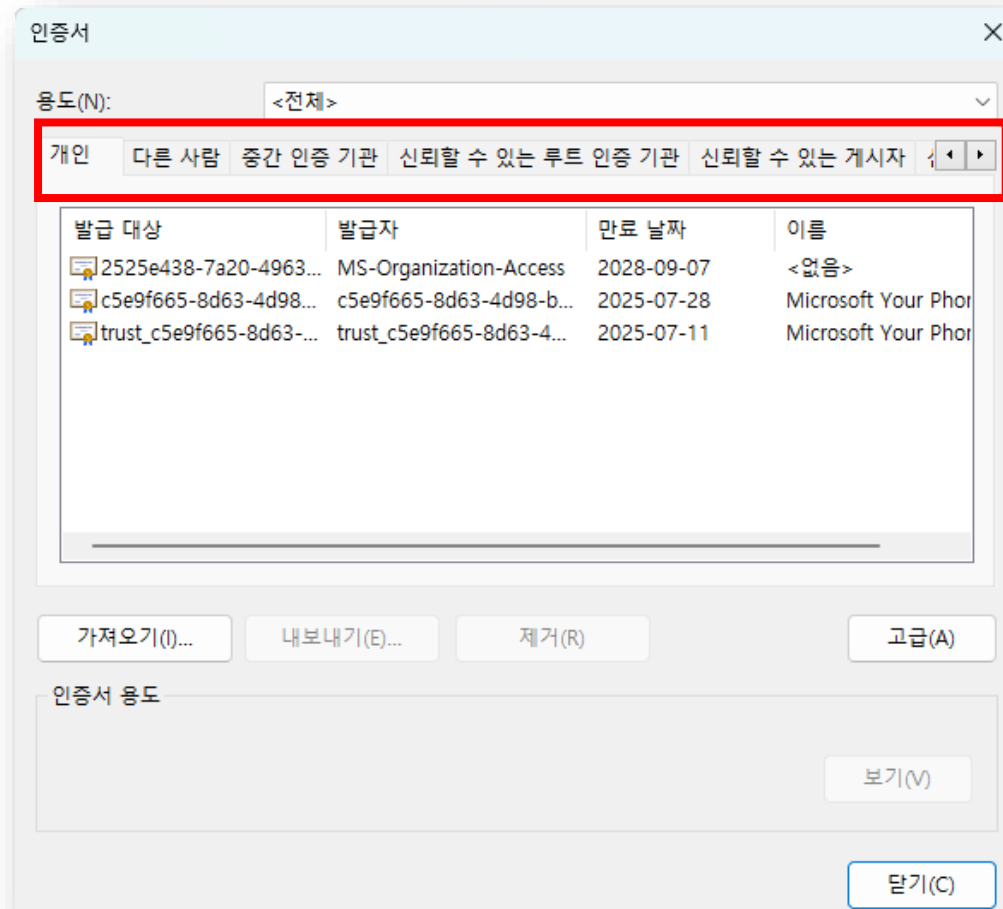


# Chrome 관리 전자인증서 확인(2)

## ■ Chrome 브라우저

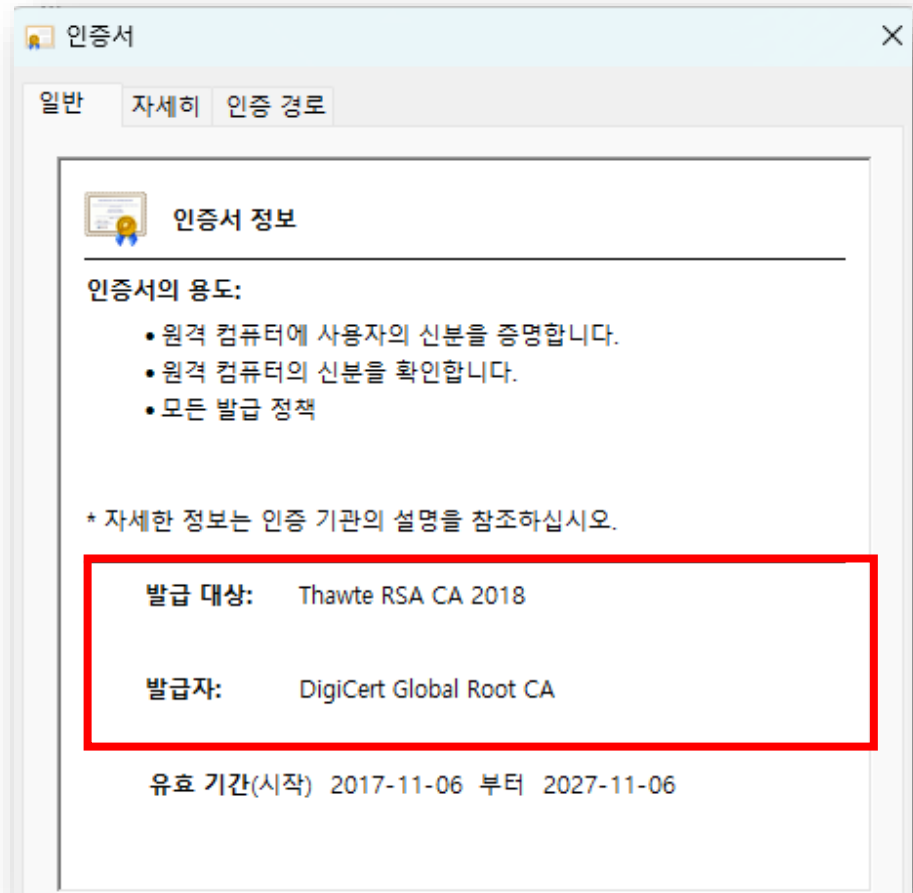
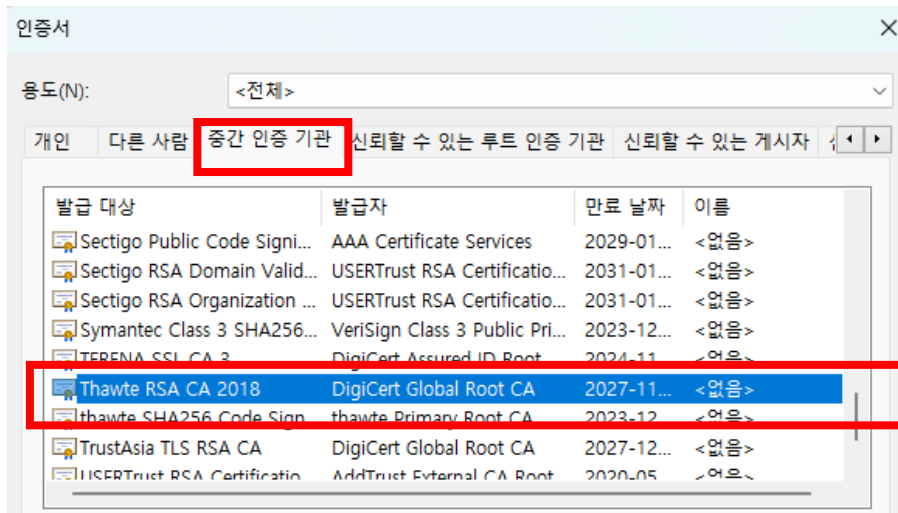
### • [인증서] 관리 창

- ✓ 개인
- ✓ 다른사람
- ✓ 중간 인증 기관
- ✓ 신뢰할 수 있는 루트 인증 기관
- ✓ 신뢰할 수 있는 게시자



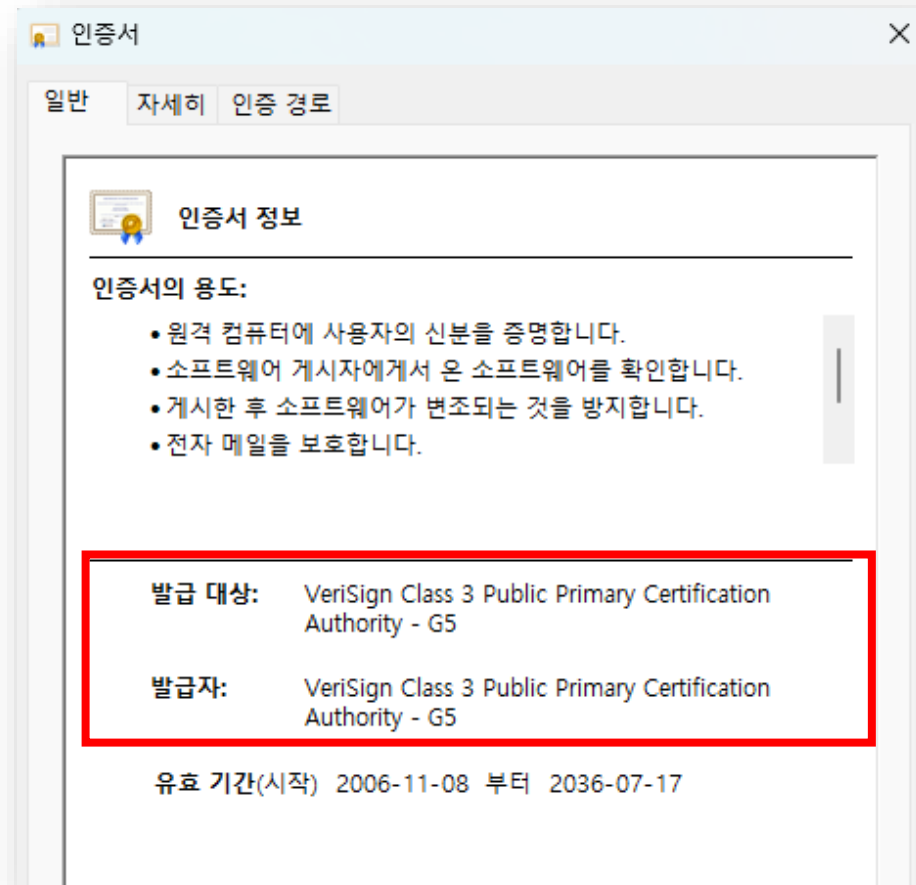
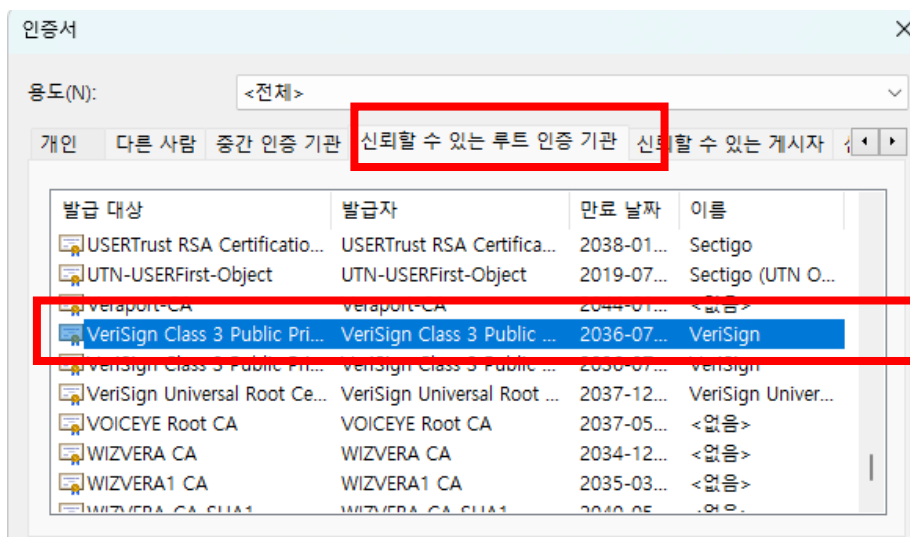
# Chrome 관리 전자인증서 확인(3)

## ■ Chrome 브라우저 - 중간 인증 기관



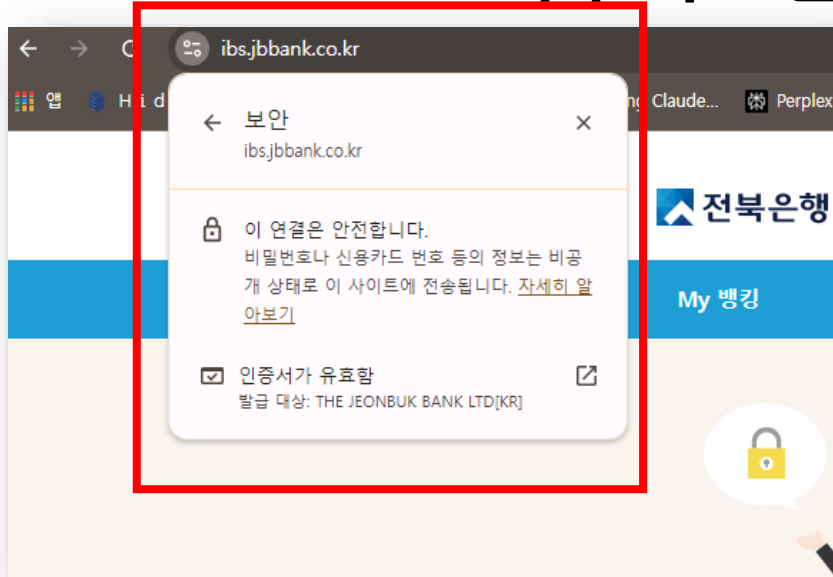
# Chrome 관리 전자인증서 확인(4)

## ■ Chrome 브라우저 - 신뢰할 수 있는 루트 인증 기관



# Chrome 관리 전자인증서 확인(5)

## ■ Chrome 브라우저 - 전북은행 전자인증서 확인



**Q & A**