NETWORK SECURITY ESSENTIALS

- X.509 인증서 -

Ki woon Moon

Protocol **E**ngineering **L**ab. **Sangmyung** University

2015. 01. 06

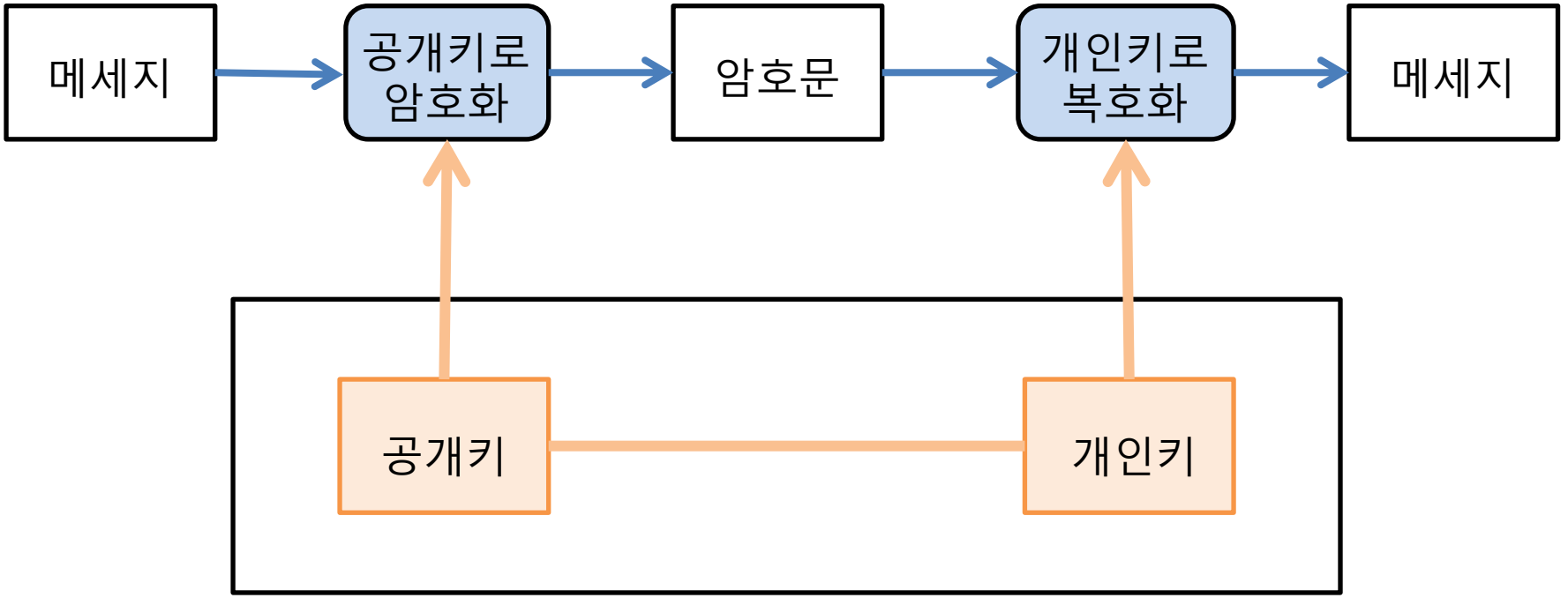
Content

- 공개키 암호와 디지털 서명
- 공개키 인증서

공개키 암호와 디지털 서명 (1/5)

- **공개키에 의한 암호화**

  - 공개키로 암호화한 암호문은 대응하는 개인키로만 올바르게 복호화 가능



공개키 암호와 디지털 서명 (2/5)

- **디지털 서명의 기능**

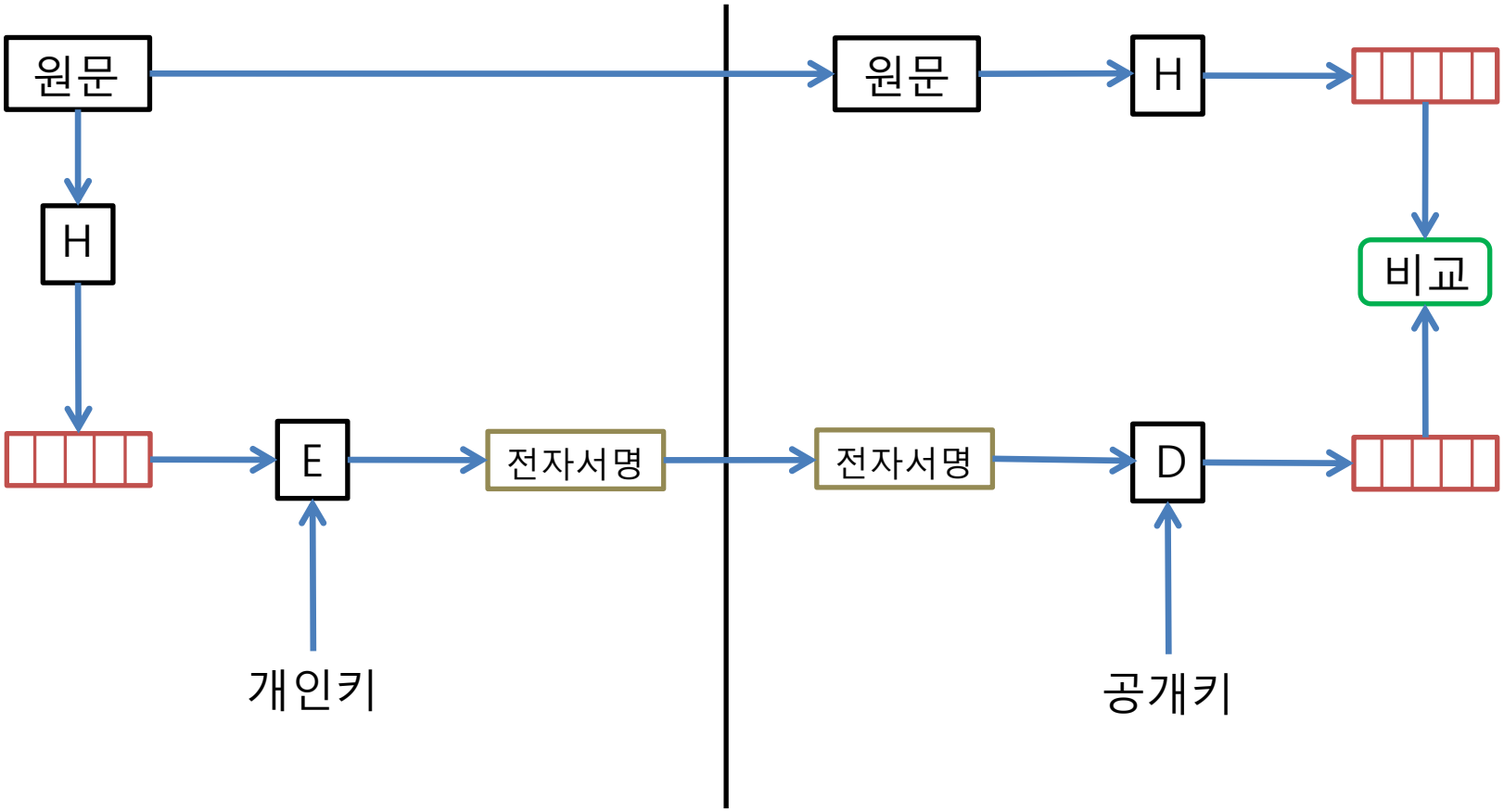
1. 본인 인증
   - 송신자 본인이 서명했음을 인증

2. 무결성 보장
   - 원문의 해쉬값과 전자서명을 복호화한 해쉬값을 비교하여 무결성을 확인

3. 부인 봉쇄
   - 송신자는 자신만이 소유한 개인키로 서명을 하였으므로 부인 불가

공개키 암호와 디지털 서명 (3/5)

- **디지털 서명**



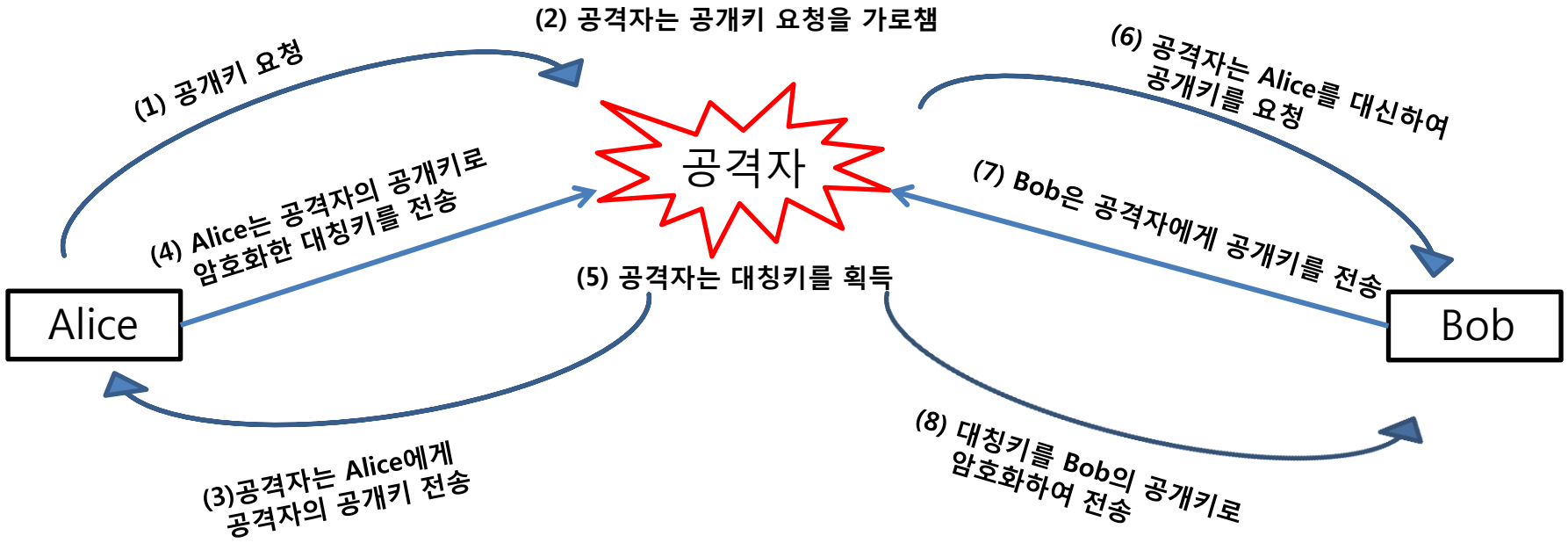
공개키 암호와 디지털 서명 (4/5)

- **키 사용 방법**

	개인키	공개키
공개키 암호	수신자가 복호화에 사용	송신자가 암호화에 사용
디지털 서명	서명자가 서명 작성에 사용	검증자가 서명 검증에 사용
키의 소유	개인이 소유	필요한 사람 누구나 소유 가능

공개키 암호와 디지털 서명 (5/5)

- 중간자 공격



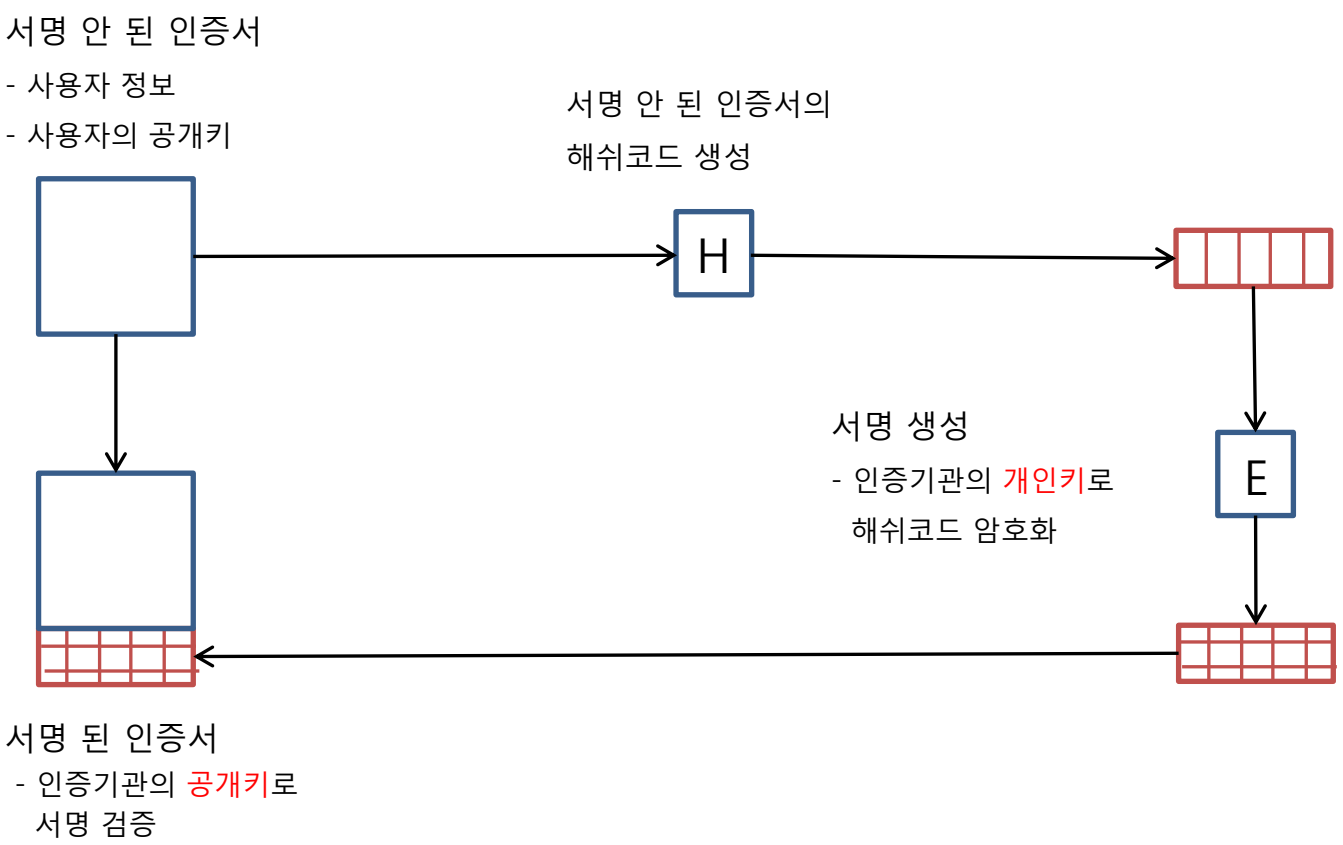
이후 Alice와 Bob의 메시지는 공격자가 모두 해독 가능

공개키 인증서 (1/12)

- **개요**
  - 사용자의 공개키와 사용자의 정보를 결합, 인증기관이 서명한 문서
  - 공개키의 인증성을 제공
  - 사용자 확인, 특정한 권한을 허가하는데 이용
  - 정보화 사회에서 개인의 신분증 역할
  - 인증기관은 자신의 개인키를 사용하여 전자서명을 생성하여 인증서에 첨부
    검증자는 인증기관의 공개키를 사용하여 인증서의 유효성 확인
  - 인증기간만이 인증서 수정이 가능

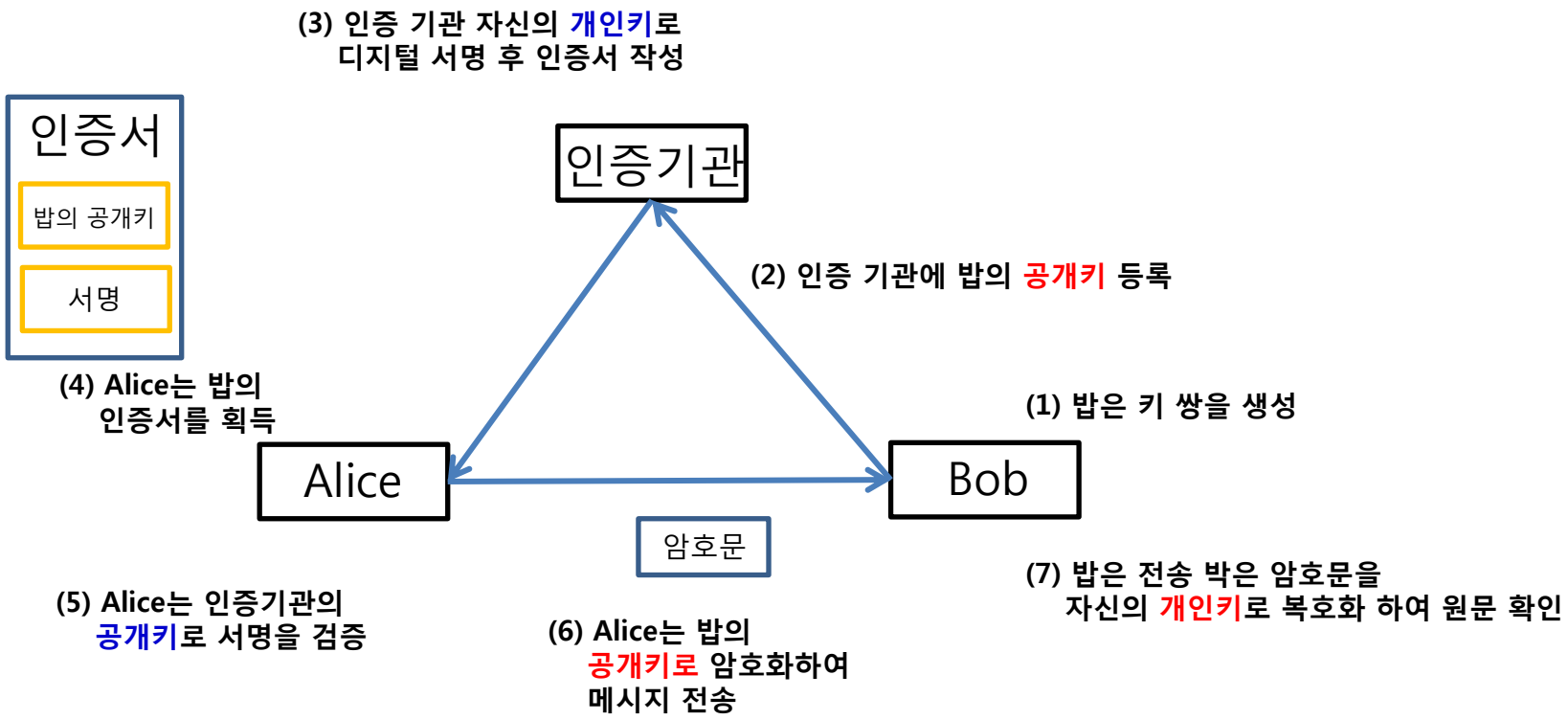
공개키 인증서 (2/12)

- **공개키 인증서 기본 프로세스**



공개키 인증서 (3/12)

- 공개키 인증서 사용 시나리오



공개키 인증서 (4/12)

- **X.509 인증서 표준**

  - ITU에 의해 제안된 인증서에 대한 기본 형식을 정의

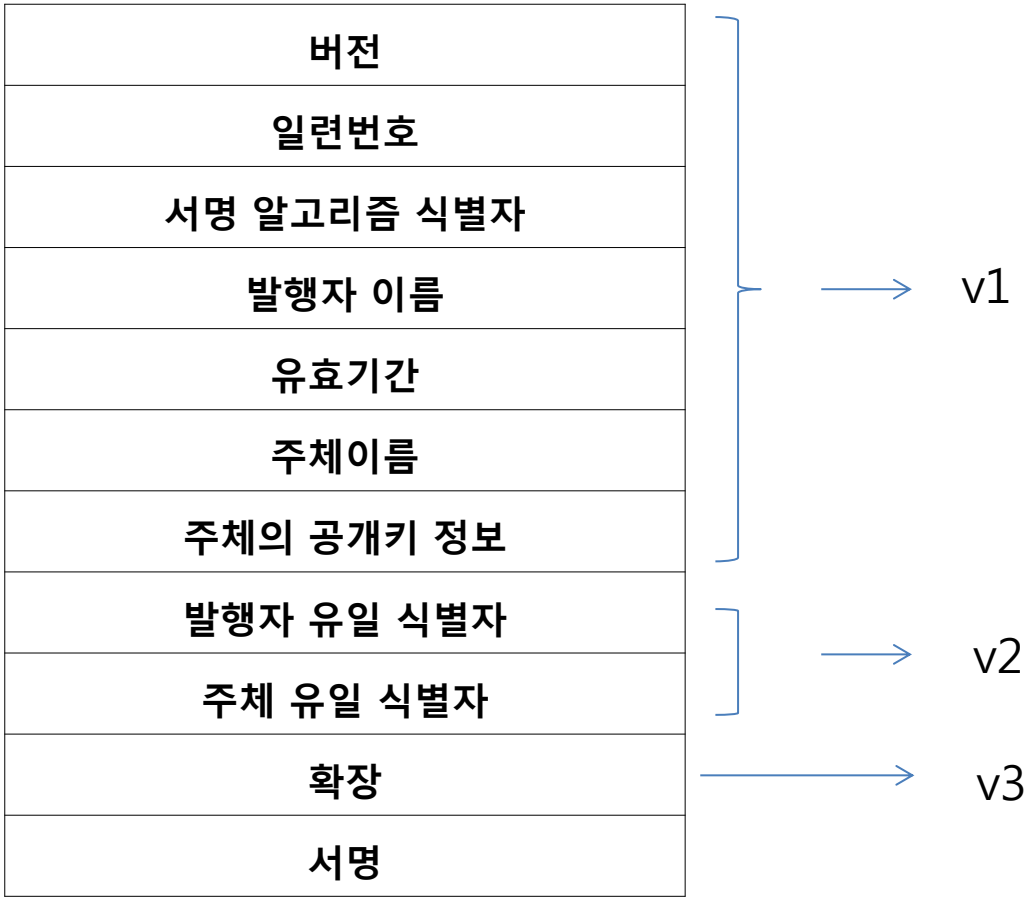
  - X.509 v1 (1988)

  - X.509 v2 (1992)
    - 인증서 취소목록 (CRL : Certificate Revocation List)을 도입
    - 유일 식별자 (Unique identifier) 도입

  - X.509 v3 (1996)
    - 인증서를 정의하는 다양한 조건과 서명 알고리즘들을 선택적으로 적용 가능하도록 확장영역 추가

공개키 인증서 (5/12)

- **X.509 인증서 구조**



공개키 인증서 (6/12)

- **X.509 인증서 예**

필드	값
버전	V3
일련 번호	12 95 32 20 03 8f 1e
서명 알고리즘	sha1RSA
서명 해시 알고리즘	sha1
발급자	jonghyouk@pel.smuc.ac....
유효 기간(시작)	2014년 7월 10일 목요일 오...
유효 기간(끝)	2024년 7월 7일 일요일 오...
주체	jonghyouk@pel.smuc.ac....
공개 키	RSA (4096 Bits)

공개키 인증서 (7/12)

- **X.509 인증서 구조**

버전
일련번호
서명 알고리즘 식별자
발행자 이름
유효기간
주체이름
주체의 공개키 정보
발행자 유일 식별자
주체 유일 식별자
확장
서명

- **버전 (Version) : 인증서의 형식을 구별, 버전 번호**
- **일련번호 (Serial Number) : 인증기관에서 발행한 인증서의 일련번호**
- **서명 알고리즘 식별자 (Signature algorithm Identifier) : 인증서 서명에 사용한 알고리즘**

  ex) sha1RSA
- **발행자 이름 (Issuer name) : 인증서를 만들고 서명한 인증기관의 이름**
- **유효기간 (Period of validity) : 인증서가 유효한 시작일과 만료일의 두 날짜로 구성**
- **주체 (Subject name) : 인증서가 인증하는 사용자의 이름**
- **주체의 공개키 정보 (Subject's public-key information) : 주체의 공개키와 인증서의 모든 영역을 해시해서 인증기관의 개인키로 서명한 값 표시**

  ex) RSA (1024비트**)**

  30 81 88 02 81 80 69 e8 a2 a6 20 55 f0 7f 90 8c 22 36 e9 37 6f 17 f0 36 0e 30 65 12
  00 2e 04 36 23 e3 ea ce 41 42 58 89 c2 12 ec 7d 1a c3 84 9d 32 20 ed f4 8a 72 6e 23
  01 b8 e8 17 b4 d4 02 39 62 4c 9a c5 d7 c2 12 b1 b6 be 8d e8 d1 79 71 49 06 4f 5a 0e
  6a 26 fe c0 d7 b8 62 55 66 a6 e6 c3 e5 b9 7d 45 a9 c3 91 c9 3d 48 42 4a 10 95 9c ef
  13 ed 53 cd 35 54 a5 a6 86 45 25 6f 9b 96 75 38 4e 26 d3 67 64 43 02 03 01 00 01

공개키 인증서 (8/12)

- **X.509 인증서 구조**

버전
일련번호
서명 알고리즘 식별자
발행자 이름
유효기간
주체이름
주체의 공개키 정보
발행자 유일 식별자
주체 유일 식별자
확장
서명

- **발행자 유일 식별자 (Issuer unique identifier) : 인증 기관을 식별하기 위한 고유 번호**
- **주체 유일 식별자 (Subject unique identifier) : 인증서 주체를 식별하기 위한 고유 번호**

- **확장 (Extensions) : v3에서 추가된 확장 영역**
- **서명(Signature) : 인증기관의 개인키로 암호화하여 서명한 서명문**

공개키 인증서 (9/12)

- **X.509 v3의 확장 영역**

- **기관 키 식별자 (Authority key identifier) : 하나의 인증기관이 여러 개의 개인키로 인증서를 서명한 경우, 서명 검증용 공개키를 식별하기 위해 사용**
- **주체 키 식별자 (subject key identifier) : 한 주체가 여러 인증서를 발급 받아 소유 하고 있을 때, 인증서에 포함된 공개키 들을 구별하는데 사용**
- **개인키 유효기간 (Private-key usage period) : 공개키에 대응되는 개인키의 사용기간**
- **주체 대체 이름 (Subject alternative name) : 주체 이름을 대체할 또 다른 이름 (DNS, IP , 메일..)**
- **발행자 대체 이름 (Issuer alternative name) : 인증 기관의 또 다른 이름**
- **키 용도 (key usage) : 해당 공개키의 용도(암호화용, 서명용)를 비트로 표시**
  - **DigitalSignature : keyCertSign, cRLSign을 제외한 서명 용도의 공개키**
  - **NonRepudiation : 부인방지를 위한 서명용 공개키**
  - **KeyEncipherment : 공유 비밀키를 암호화할 때 사용하는 공개키**
  - **DataEncipherment : 데이터 암호용 공개키**
  - **KeyAgreement : 키 분배 프로토콜에 사용할 공개키**
  - **KeyCertSign : 루트 인증서의 서명용 공개키**
  - **cRLSign : CRL 서명용 공개키**
  - **Encipheronly : keyAgreement 비트가 1일 때, 암호 전용 공개키 임을 지시**
  - **Dncipheronly : keyAgreement 비트가 1일 때, 복호 전용 공개키 임을 지시**

공개키 인증서 (10/12)

- 인증서 체인

  - 인증 기관들을 계층구조(트리구조)로 만들어 탐색에 용이

  - 한 사용자가 다른 사용자의 인증서를 얻기 위하여 연속된 인증 절차를 거침

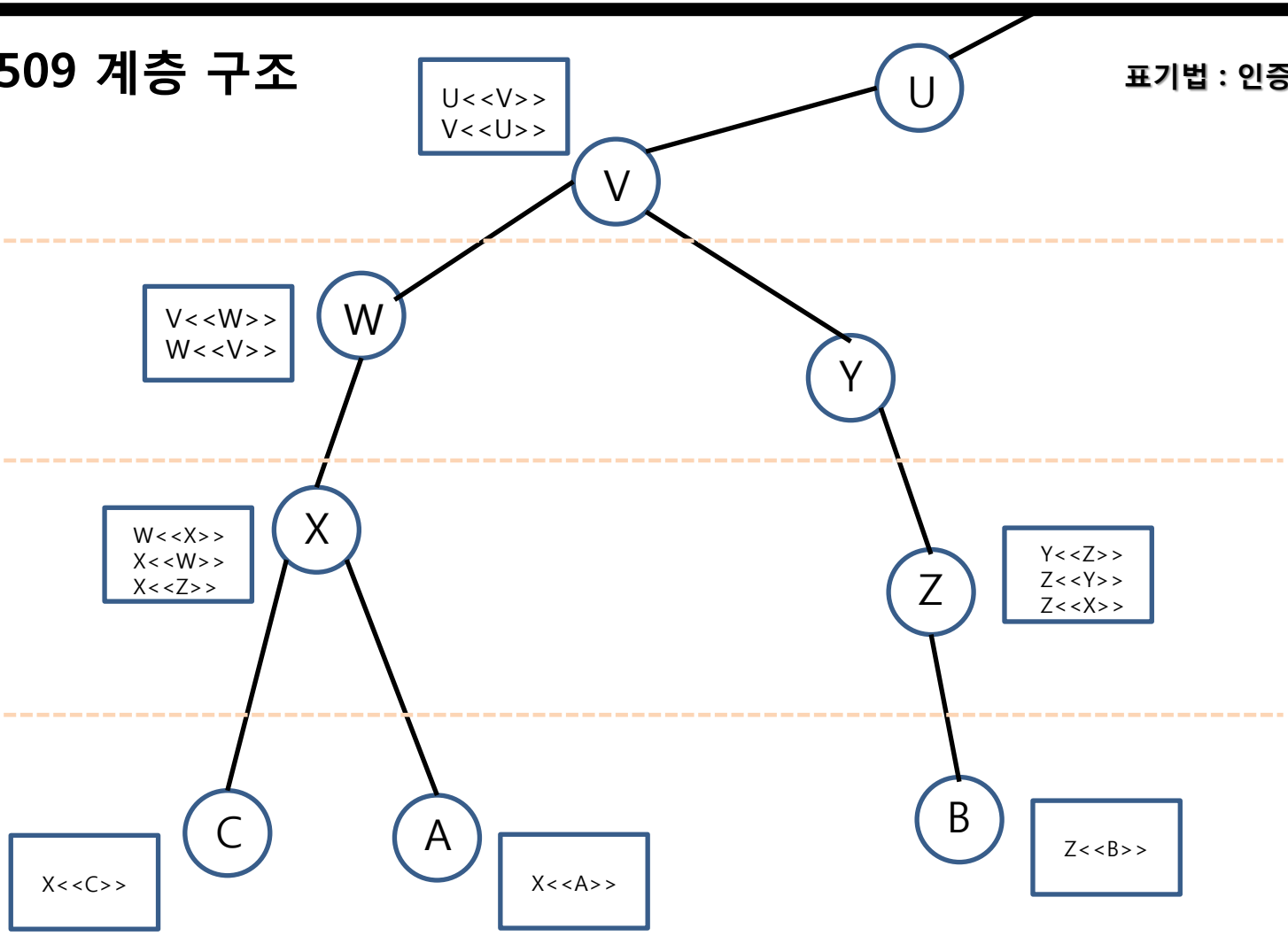
  - 각각의 인증기관이 발행한 다른 인증기관들에 대한 인증서들 모두 디렉토리에 있어야 함

  - 다른 사용자의 공개키 인증서에 이르는 경로를 따라가기 위해 어떻게 인증기관들이 연결 되어 있는지를 알 필요가 있음

공개키 인증서 (11/12)

- **X.509 계층 구조**

표기법 : 인증기관<<A>>



공개키 인증서 (12/12)

- **인증서의 취소**

인증서 유효기간 만료 이외의 취소 사유

1. 사용자의 개인키 노출되었거나 훼손 되었을 때
2. 인증기관이 사용자를 더 이상 인증해 줄 수 없을 때
3. 인증기관의 인증서가 노출되었거나 훼손 되었을 때

- CRL (Certificate Revocation List) -

버전		
서명 알고리즘 식별자		
발행자 이름		
이번 업데이트 일시		
다음 업데이트 일시		
일련번호	취소 일시	사유
1110011	2014/10/14	개인키 노출
1111001	2014/12/15	회원탈퇴
…	…	…
서명		