4.4 X.509 인증서

4장. 키 분배와 사용자 인증

개요

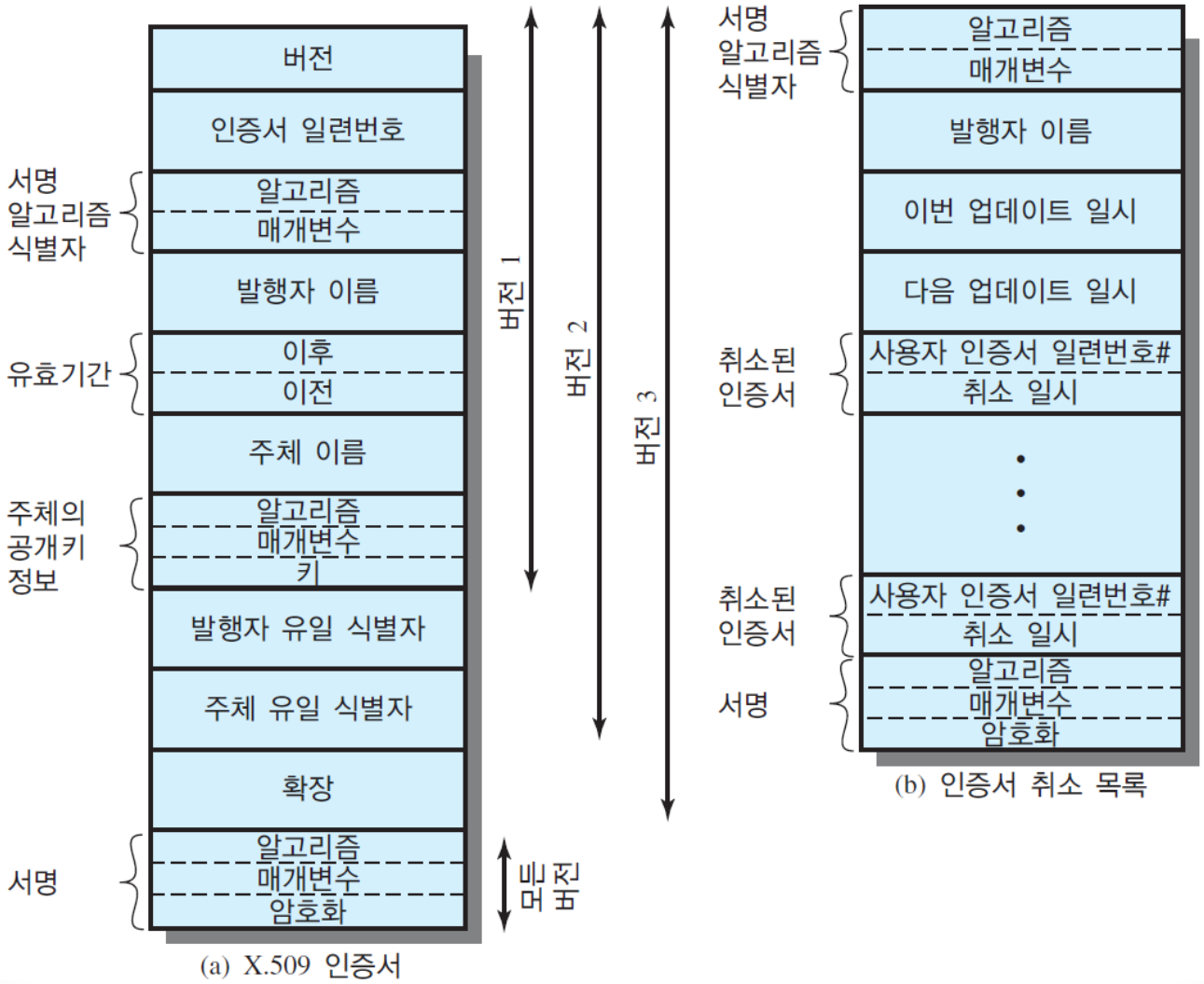
- ITU-T 권고안 X.509는 디렉터리 서비스를 정의하는 권고안 X.500 시리즈의 한 부분
- 디렉터리(Directory)
  - 사용자 정보 데이터베이스를 관리하는 하나의 서버 또는 분산 서버 집단
- X.509는 X.500 디렉토리에서 사용자에게 제공되는 인증 서비스의 구조를 규정
- 디렉토리를 공개키 인증서의 저장소로 이용
- 공개키 인증서를 이용한 인증 프로토콜 정의

X.509 인증서 형식 사용처

- 사용처
  - S/MIME(5장)
  - IP Security(6장)
  - SSL/TLS, SET(7장)

- 소개
  - 1988년 최초 소개
  - 1993년 수정권고
  - 1995년 버전3
  - 2000년 수정안

X.509 형식



(a) X.509 인증서

(b) 인증서 취소 목록

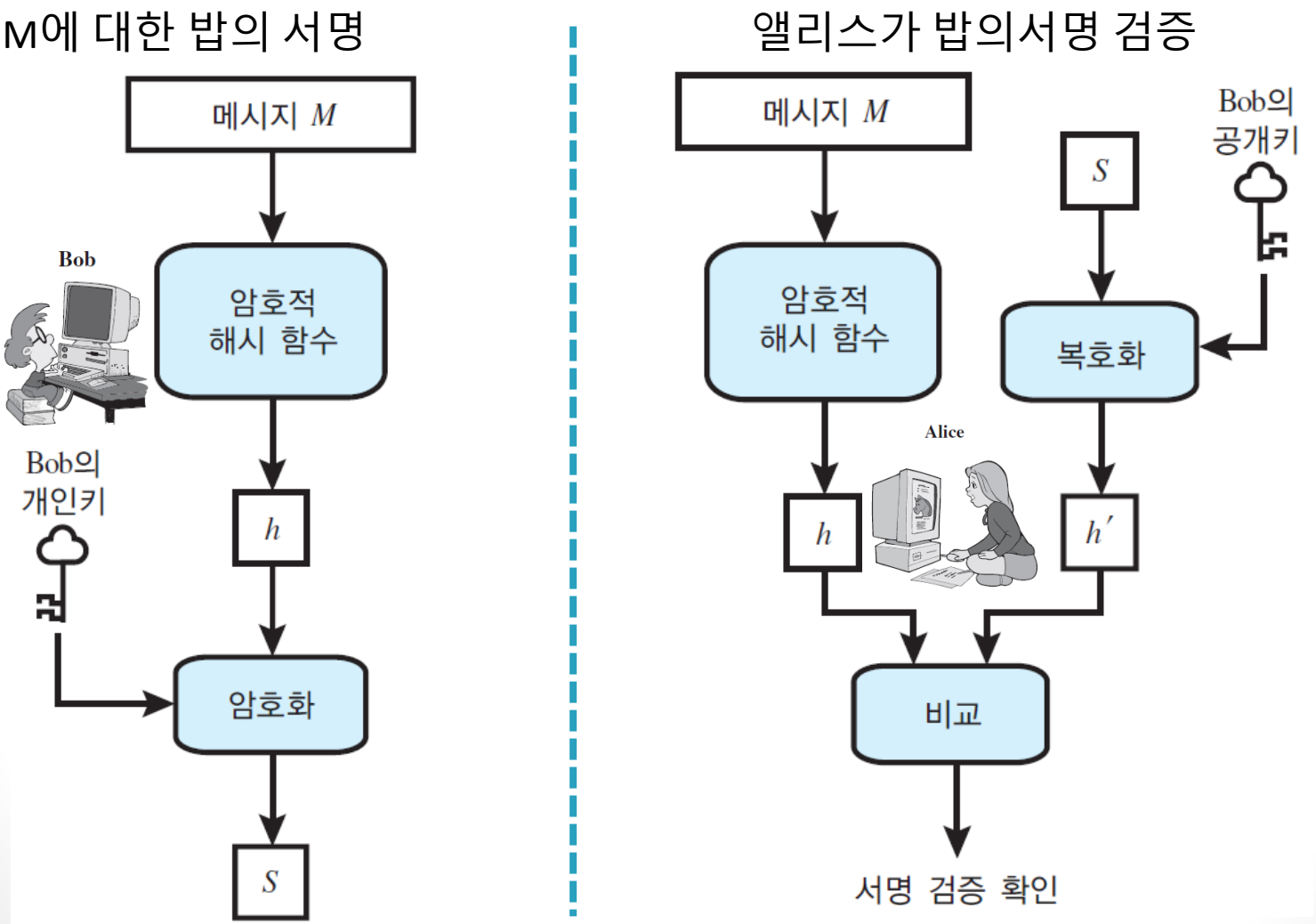
인증서

- 인증서를 정의: 표현을 이용한다:
- CA<<A>>= CA {V, SN, AI, CA, UCA, A, UA, Ap, TA}
- 여기서
  - Y<<X>> = 인증기관 Y 가 발행한 사용자 X 의 인증서
  - Y{I} = I 에 대한 Y 의 서명. I 에 암호화된 해시 코드를 붙여 작성
  - V = 인증서 버전
  - SN = 일련번호
  - AI = 서명에 사용된 알고리즘 식별자
  - CA =인증기관명
  - UCA = CA 식별자(옵션)
  - A = 사용자 A의 이름(옵션)
  - UA = 사용자 A 식별자(옵션)
  - Ap = 사용자 A의 공개키
  - TA= 유효기간

사용자 인증서 얻기

- CA가 발행한 사용자 인증서 특성
  - CA의 공개키를 얻을 수 있는 어떤 사용자도 특정 사용자의 인증된 공개키를 확인할 수 있다.
  - 인증기관을 제외한 어느 누구도 들키지 않게 인증서를 변경할 수 없다.

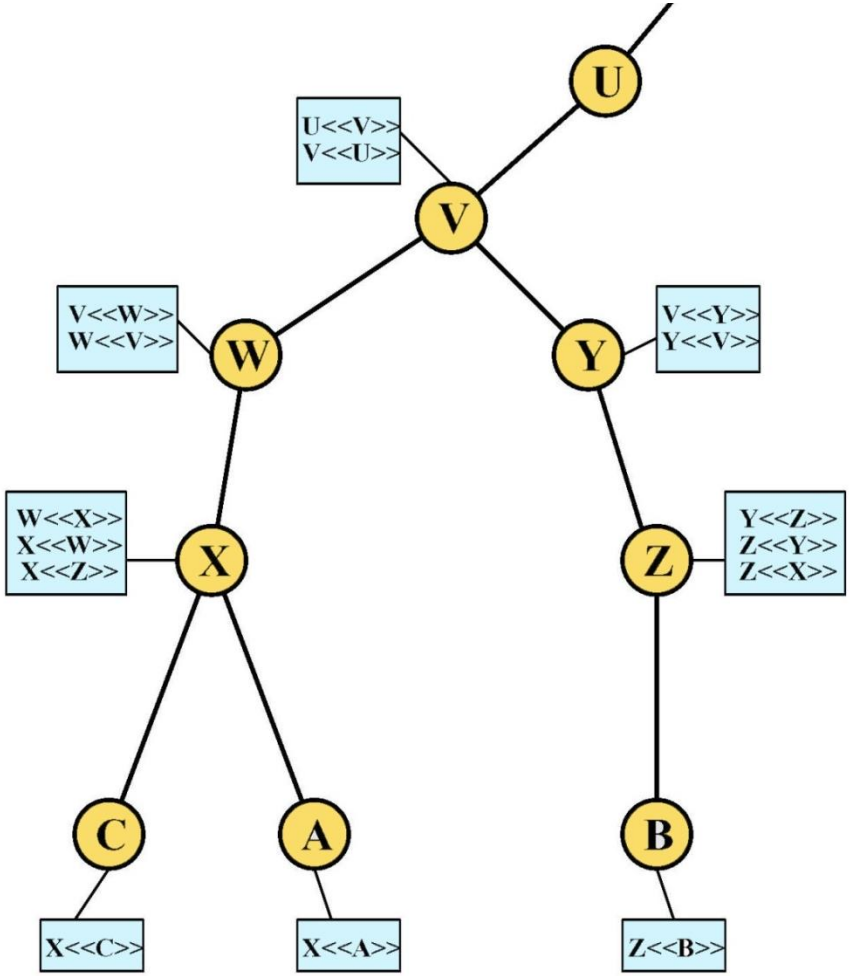
디지털 서명 프로세스


M에 대한 밥의 서명
메시지 M
Bob
암호적
해시 함수
Bob의
개인키
h
암호화
S
앨리스가 밥의서명 검증
메시지 M
Bob의
공개키
S
암호적
해시 함수
복호화
Alice
h
h′
비교
서명 검증 확인

인증서 체인 (chain of certificate)

- A가 X.509 형식에 따라 B의 공개키 구하기
  - X1<<X2>>X2<<B>>
- N개의 요소로 구성된 체인
  - X1<<X2>>X2 <<X3>>…XN <<B>>
- 체인 (Xi, Xi+1) 안 쌍방은 상호 인증서 발행

X.509 계층구조

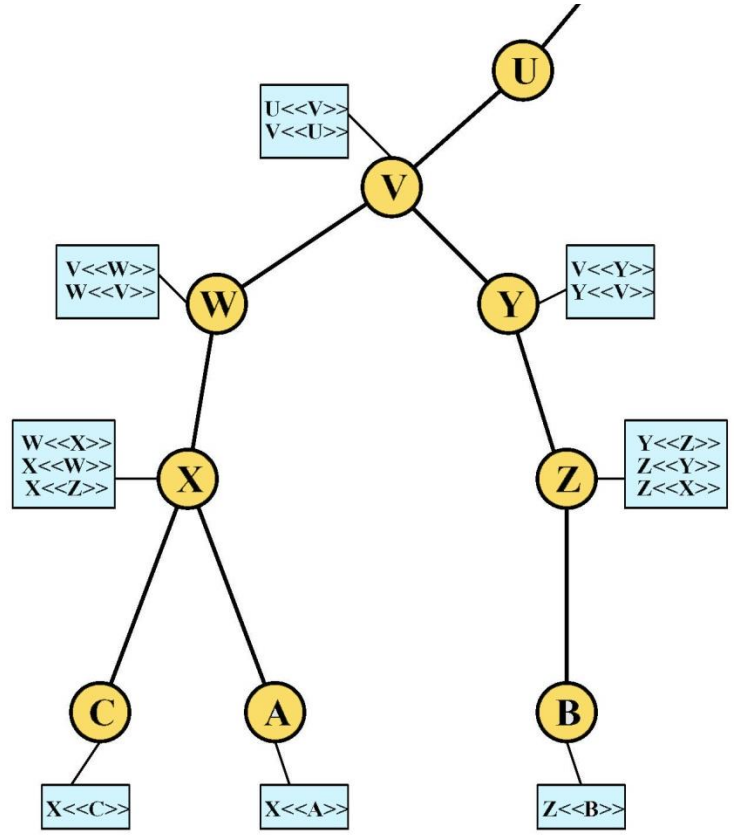


CA의 디렉터리 내 두 종류 인증서

- 순방향 인증서(Forward certificates):
  - 다른 CA에 의해서 생성된 X의 인증서
- 역방향 인증서(Reverse certificates):
  - X가 생성한 다른 CA의 인증서

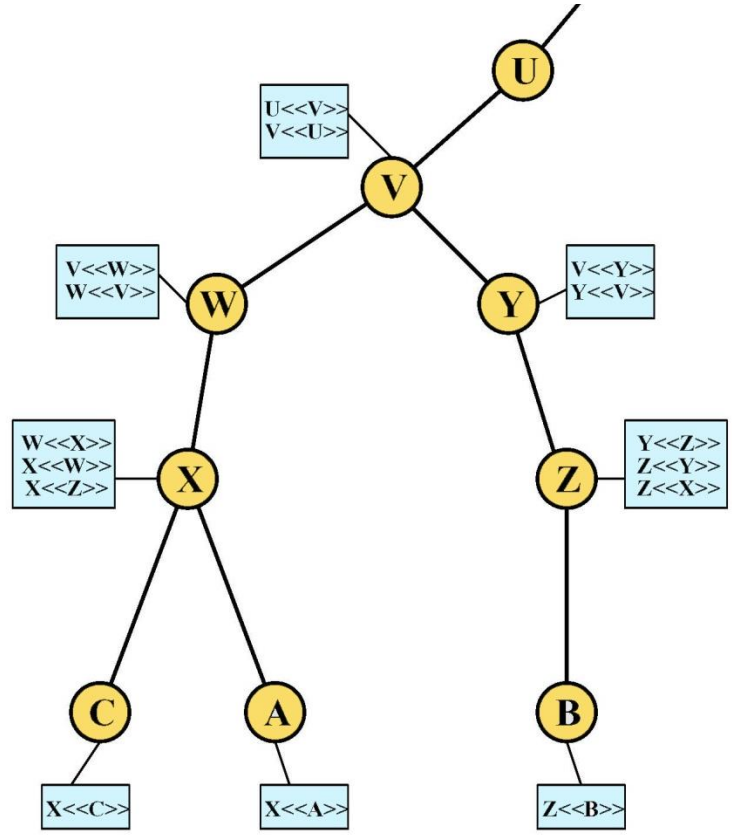
A가 B의 인증서를 얻는 체인

X<<W>>W<<V>>V<<Y>>Y<<Z>>Z<<B>>



B가 A의 인증서를 얻는 체인

Z<<Y>>Y<<V>>V<<W>>W<<X>>X<<A>>



인증서 취소 (1)

- 취소해야 하는 경우
  1. 사용자 개인키가 노출, 훼손 시
  2. CA가 사용자를 더 이상 인증해줄 수 없을 때
  3. CA의 인증서가 노출, 훼손 시

- 취소 인증서 목록 (CRL: Certificate Revocation List)
  - 각 CA 는 취소했지만 유효기간이 아직 끝나지 않은 인증서 목록을 보관
  - 취소된 인증서들은 사용자에게 발행한 것과 다른 CA 들에게 발행한 것 모두를 포함
  - 취소목록을 디렉토리에 공개

인증서 취소 (2)

- 취소인증서목록 사항
  - 발행자 이름
  - 목록 작성 일자
  - 다음 번 CRL을 발표할 일자
  - 취소된 인증서 항목

X.509 버전 3 (1)

- 버전 2의 약점
  - 신원정보 결여
    - 주체 필드 크기가 키 소유자 신원을 전달하기에 부적합
    - 자세한 신원정보가 결여
  - 주체 필드의 수용능력 부족
    - 개체를 이메일 주소, URL 혹은 다른 형태의 인터넷 관련 신원을 통해 인식하기에 부적합
  - 보안 정책 정보 표시 필요
    - IPSec 같은 보안 응용프로그램이나 보안 기능이 X.509 인증서를 주어진 정책에 이용가능

X.509 버전 3 (2)

- 버전 2의 약점(계속)
  - CA에 대한 견제기능 필요
    - 특정 인증서 사용에 제약조건을 설치하여 악의가 있는 CA에 의해 유발되는 피해를 줄인다
  - 시간별로 달리 사용하는 키 구별 필요
    - 키 소유자가 다른 시간에 사용하는 다른 키를 구별하는 능력필요
    - 이 기능은 키의 수명 관리를 지원
    - 특히 사용자와 CA의 키 쌍을 정기적, 예외적인 환경하에서 갱신 가능
- 보다 유연한 접근방법 필요
  - 선택사항으로 많은 확장 포함
  - 확장식별자, 위험성 표시자(확장을 안전하게 무시할 수 있는지 표시), 확장값으로 구성

인증서 확장

- 키와 정책정보
- 인증서 주체와 발행자 속성
- 인증경로 제약조건

키와 정책정보

- 주체와 발행자 키에 관한 추가적인 정보,인증서 정책 표시자를 처리
- 인증서를 특정 집단이나 일상적인 보안 사항을 요구하는 응용 프로그램 집단에 적용할 수 있는지 없는지를 판단
- 포함된 내용
  - 기관 키 식별자(Authority key identifier):
  - 주체 키 식별자(Subject key identifier):
  - 키 용도(Key usage):
  - 개인키 유효기간(Private-key usage period):
  - 인증서 정책(Certificate policies):
  - 정책 매핑(Policy mapping):

인증서 주체와 발행자 속성

- 주체 대체 이름(Subject alternative name):
- 발행자 대체 이름(Issuer alternative name):
- 주체 디렉터리 속성(Subject directory attributes):

인증경로 제약조건

- 기본 제약(Basic constraints):
- 이름 제약(Name constraints):
- 정책 제약(Policy constraints):