5. 공개키 기반구조

담당교수: 차 영욱
ywcha@andong.ac.kr

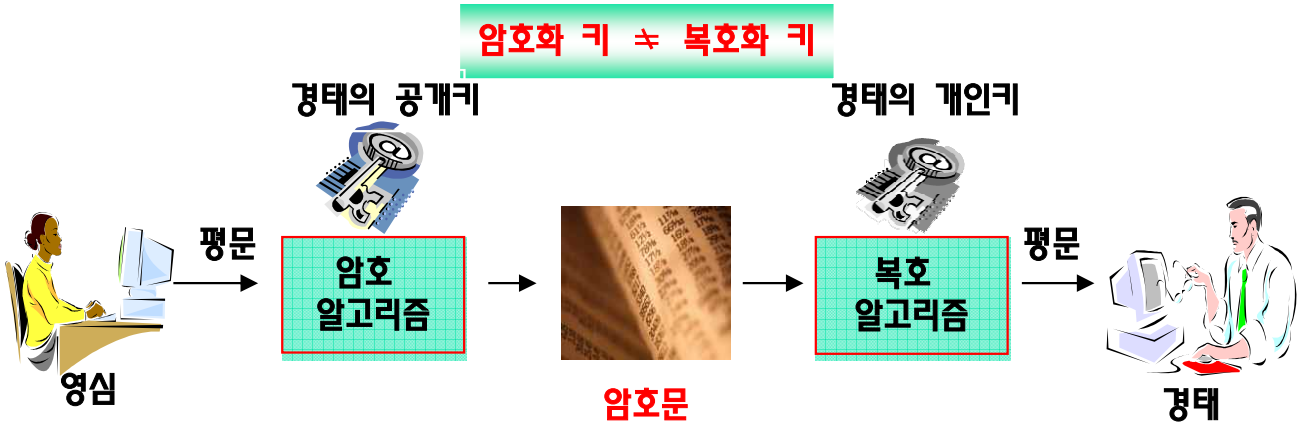
안동대학교
ANDONG NATIONAL UNIVERSITY

목 차

공개키 암호시스템 개요

❑ 암호화 및 복호화

- 영심은 네트워크에 공개되어 있는 경태의 공개키로 문서를 암호화
- 경태는 비밀리에 보관하고 있는 개인키로 암호화된 문서를 복호화

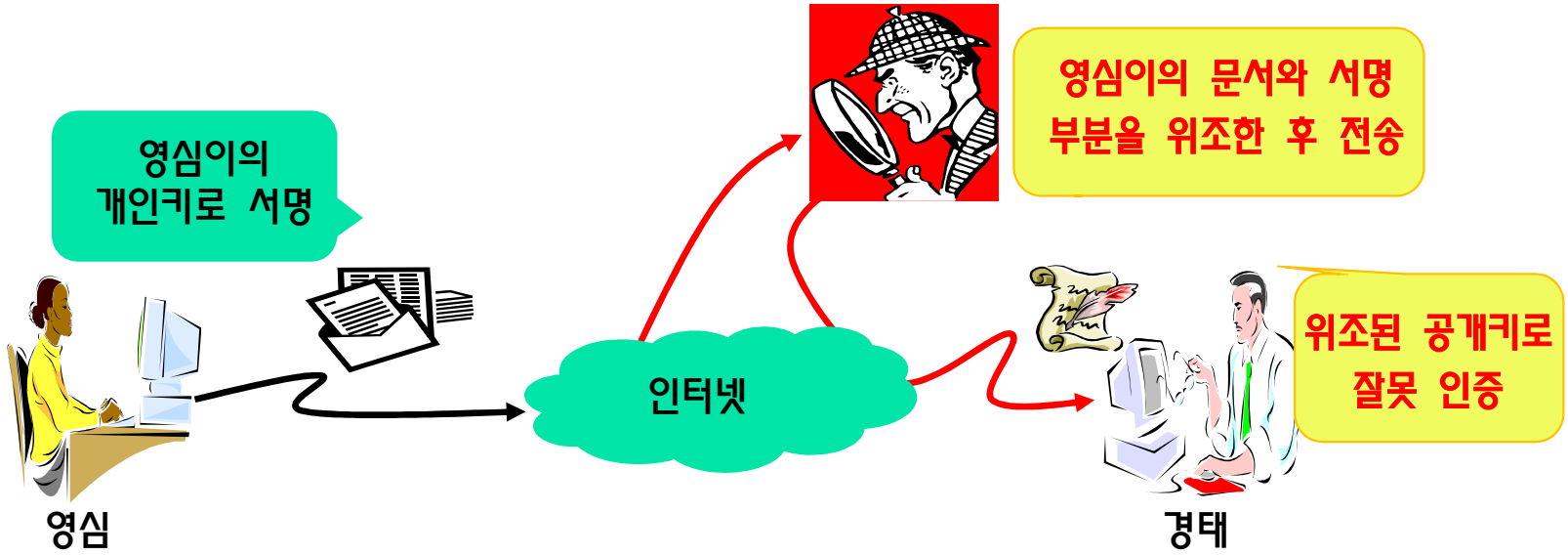


❑ 공개키 암호 시스템

- 대칭키 암호 시스템의 단점인 암호 키의 관리와 분배 문제 해결
- 인터넷 뱅킹 및 전자상거래와 같은 응용에 널리 사용

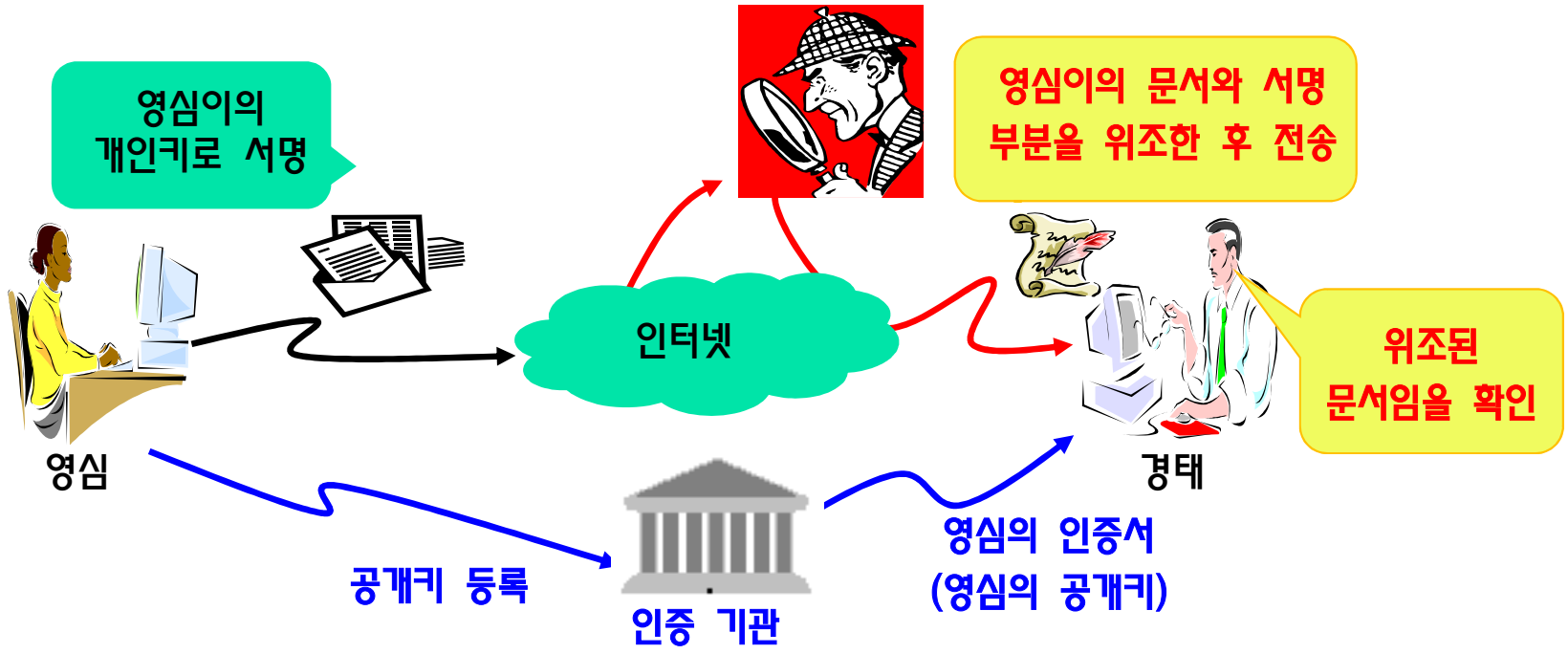
공개키 방식 메시지 인증의 취약성

- 공격자는 위조된 영심의 공개키를 사전에 경태에게 배포
- 공격자는 영심의 문서를 가로채어 문서의 내용을 위조 → 위조된 영심의 개인키로 전자서명을 생성하여 문서를 경태에게 전송
- 경태는 공격자의 위조된 공개키로 수신한 문서를 인증함으로 문서의 위조 사실을 확인하지 못함



공개키 방식에서 인증서의 필요성

- 영심: 공개키의 위조를 방지하기 위하여 자신의 공개키 및 개인 정보를 인증기관에 인증서로 등록
- 경태
  - 영심의 공개키를 가져오기 위하여 영심의 인증서를 인증기관에 요청
  - 인증서에 포함된 영심의 공개키로 수신한 문서를 인증 → 공격자가 위조한 서명을 확인



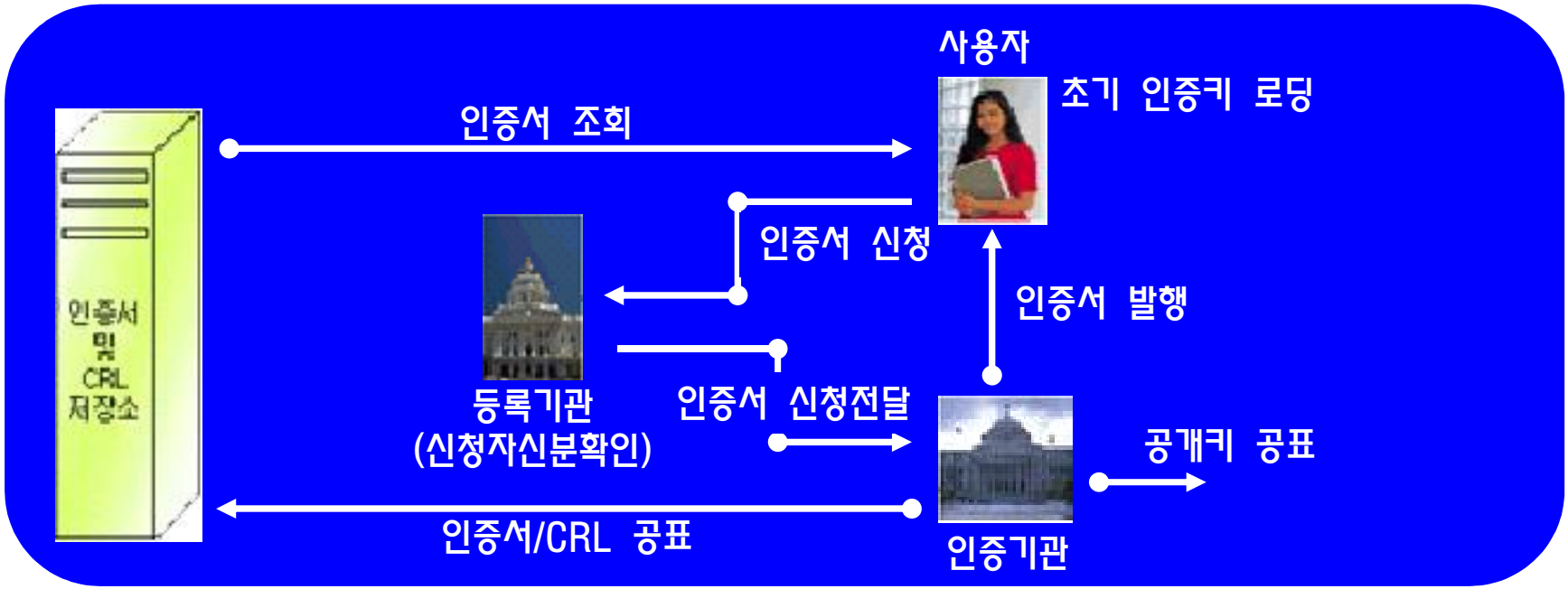
공개키 기반구조의 필요성

- 공개키 암호 시스템의 광범위한 응용
  - 인터넷 뱅킹 서비스: 예금조회, 계좌이체, 대출, 카드 등의 은행업무
  - 전자화폐 서비스: 온라인 상에서의 전자화폐 사용
  - 인터넷 쇼핑: 인터넷 쇼핑몰에 대한 안전한 거래 및 개인정보의 보호
  - 각종 예약: 항공권, 열차권, 공연의 입장권 및 호텔 예약 등
  - 전자우편의 송수신: 전자우편의 송신자 신원 확인 및 메일 내용의 암호화

- 공개키 암호 시스템의 광범위한 응용으로 공개키를 관리하고 분배하는 공개키 기반구조(PKI: Public-Key Infra-structure)가 요구됨
  - 공개키의 생성, 관리, 저장, 분배, 폐지 등에 필요한 하드웨어, 소프트웨어, 인력, 정책 및 절차

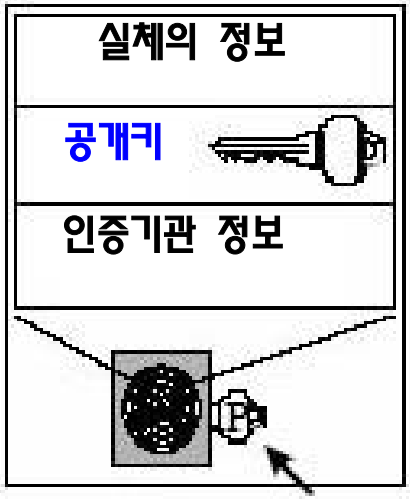
공개키 기반구조의 구성요소

- 사용자: 인증서를 발행 받아 전자상거래나 인터넷 뱅킹 등을 사용
- 등록기관: 인증서 신청자의 신원 확인 및 인증서 등록을 대행하는 기관
- 인증기관: 인증서를 발행하는 기관
- 저장소: 인증서나 인증서의 취소목록을 저장하는 장소



공개키 기반구조-인증서

- 공신력 있는 인증기관이 발행한 사이버 거래의 인감증명서
- 위조가 불가능하도록 실체(개인 또는 조직)의 정보와 공개키 그리고 인증기관의 정보가 수록된 인증서를 인증기관의 개인키로 서명하여 발급
- X.509 인증서, PGP(Pretty Good Privacy) 인증서



공개키 기반구조-인증기관

- 인증서가 진짜라는 것을 어떻게 증명할 수 있는가?
- 인증기관(CA; Certificate Authority): 인증서의 생성, 배정, 관리 등의 작업을 수행하는 기관
  - 민간분야(금융 · 증권 · 무역 · 전자입찰 등)의 NPKI(National PKI): 국내의 6개 공인인증기관이 제공하는 공인인증서비스는 1999년 7월 시행된 전자서명법에 따라 한국인터넷진흥원(KISA)이 최상위 인증기관이다.
  - 정부분야의 GPKI(Government PKI): 행정전자서명인증관리센터(www.gpki.or.kr)는 2000년 4월부터 전자문서 송 · 수신에 대한 정부차원의 정보보호 체계로 인증서비스 및 인증서관리를 제공한다.

인증기관과 인증서

- 국내 민간분야의 인증기관
  - 한국인터넷진흥원(http://www.kisa.or.kr)
  - 한국정보인증(주)(http://www.signgate.com)
  - (주)코스콤(http://www.signkorea.com)
  - 금융결제원(http://www.yessign.or.kr)
  - 한국전자인증(주)(http://gca.crosscert.com)
  - 한국무역정보통신(http://www.tradesign.net)

- 금융결재원: 국내 인터넷뱅킹 및 전자상거래에 사용하는 yessign 공인인증서 발급
  - 2004년 4월 정통부로 부터 공인 인증기관 지정

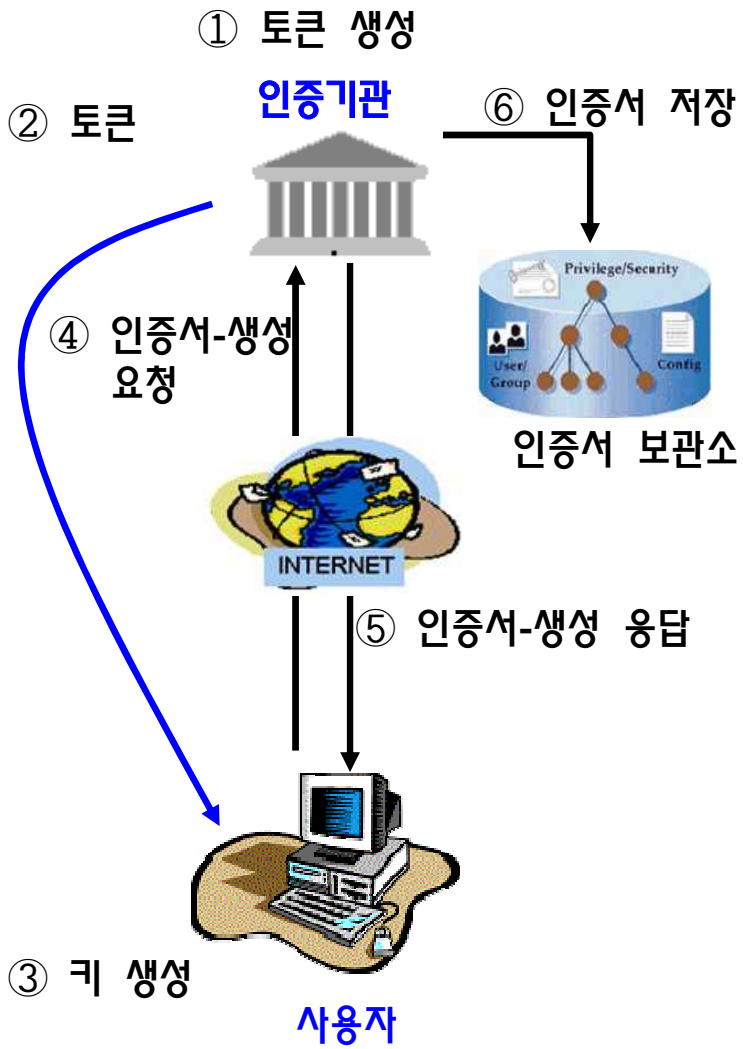
KISA의 전자서명인증관리센터

- 공인인증서를 안전하고 신뢰성 있게 이용할 수 있도록 1999년 7월 7일 업무개시 (http://rootca.kisa.or.kr/kcac/jsp/kcac.jsp)
  - 최상위인증기관 운영 및 보호대책 수립
  - 공인인증기관 관리 및 전자서명 인증기술 개발
  - 전자서명 이용환경 개선 및 국제협력

외국의 인증기관

- 인증서는 지역의 법이나 인증 스킴에 연관되어 사용되므로 인증기관의 시장은 전 세계의 각 지역으로 분할되어 있다.
- 그러나, 웹 사이트의 보안에 사용되는 SSL 인증서의 시장은 몇 개의 회사에 의하여 점유되고 있다.
  - 이는 웹 브라우저의 신뢰할 수 있는 인증기관의 목록에 포함되기 위해서는 WebTrust와 같은 기관의 평가를 통과하여야 하는 시장 진입의 장벽이 있기 때문이다.
- 대부분의 주요 웹 브라우저에 대하여 50개 이상의 신뢰할 수 있는 인증기관 목록이 등록되어 있으나, Net Craft의 2009년 보고서에 의하면 각 회사의 인증기관 시장 점유율은 다음과 같다.
  - VeriSign 및 VeriSign의 합병회사(Thawte and Geotrust): 47.5%
  - GoDaddy: 23.4%
  - Comodo:15.44%
- Verisign: 전자상거래를 위해 125,000개 이상의 웹사이트에 SSL 서버 인증서를 제공하고 있는 선도적인 인증기관

키 생성 및 관리-사용자 키 생성 방식



① 사용자의 신분확인 후, 스마트 카드 혹은 디스켓 형태의 토큰 생성. 토큰에는 사용자가 자신의 공개키/개인키 쌍을 생성할 수 있는 정보 포함

② 토큰을 안전한 채널로 전송

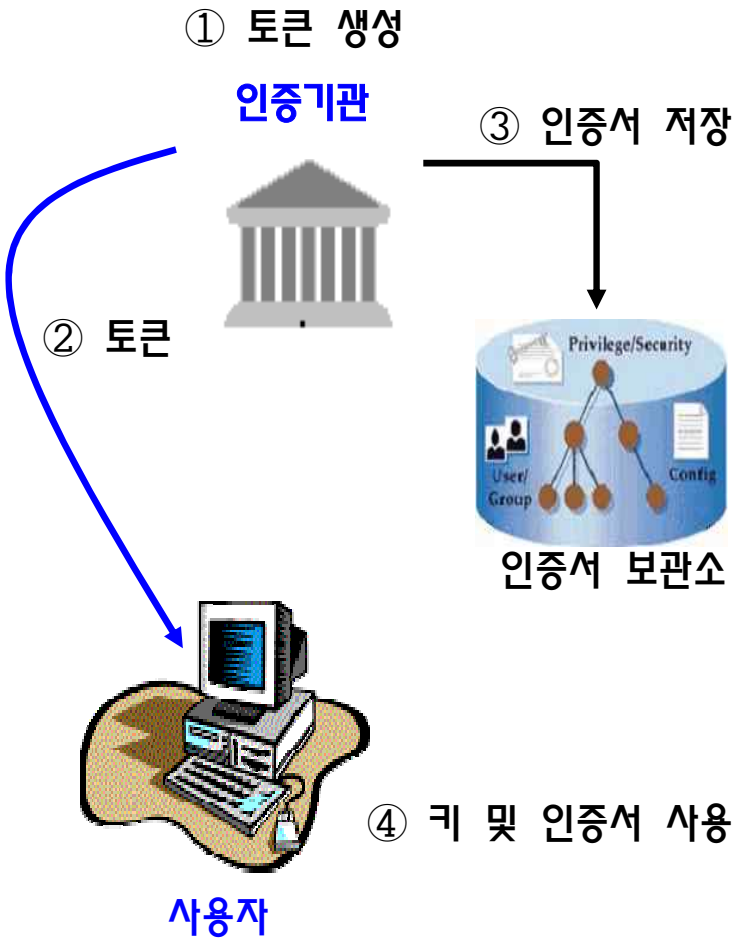
③ 사용자는 자신의 공개키와 개인키 생성

④ 공개키를 포함하고 있는 인증서-생성 요청 메시지 전송

⑤ 인증서-생성 요청 메시지의 유효성을 확인한 후, 응답 메시지를 사용자에게 전송

⑥ 발급한 인증서를 인증서 보관소에 저장

키 생성 및 관리–중앙 집중형 키 생성 방식



① 사용자의 신원확인 후 토큰 생성. 토큰에는 인증기관이 생성한 사용자의 공개키/개인키 쌍과 인증서가 포함

② 토큰을 안전한 채널로 전송

③ 발급한 인증서를 인증서 보관소에 저장

④ 사용자는 토큰에 있는 인증서와 공개키/개인키를 사용

ITU-T의 X.509

- X.509 표준 권고안은 디렉터리 서비스의 인증을 지원하기 위하여
  - 인증서의 분배와 관련된 데이터 형식과 절차 정의
  - 인증서 폐지목록(CRL: Certificate Revocation List) 메커니즘 정의
- X.509 권고안의 표준화 과정

구 분	내 용
1988	• ITU-T X.509 1판 발표 - 인증서 버전 1
1993	• ITU-T X.509 2판 발표 - 인증서 버전 2, CRL 버전 1
1997	• X.509 3판 발표 - 인증서 버전 3, CRL 버전 2
2000	• X.509 4판 발표 - 인증서 버전 3 확장, CRL 버전 2 확장

IETF의 PKIX

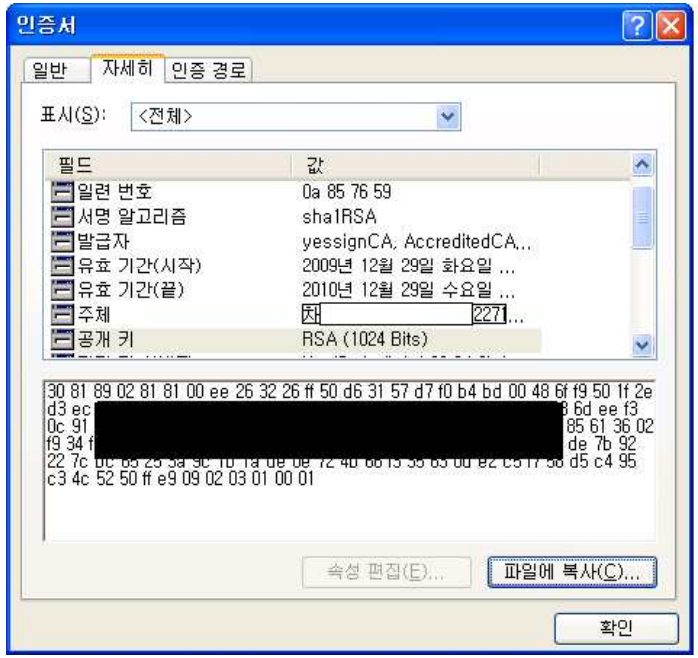
- ITU-T의 X.509는 인증서의 분배와 관련된 데이터 형식과 절차만 정의하였으며, 인증서의 내부 필드들에 대한 실제 자료구조는 정의하지 않았음

- IETF의 PKIX(Public-Key Infrastructure X.509) 작업반: X.509 기반의 PKI를 지원하기 위한 인터넷의 표준 개발을 위하여 1995년에 구성
  - 프로파일 정의: 인터넷의 공개키 기반 구조를 위하여 X.509 인증서 버전 3과 인증서 폐지목록 버전 2의 내부 필드들에 대한 실제 자료구조 및 의미 정의
  - 운영 프로토콜: 인증서와 인증서 폐지목록을 전달하기 위한 프로토콜로 LDAP, FTP, HTTP 선택
  - 관리 프로토콜: 사용자들과 PKI 관리 엔터티들 사이의 온라인 상호작용 정의
    - 키 쌍의 생성, 인증서 발행, 손실된 키의 복구
    - 만기된 인증서의 갱신, 인증서 폐기

X.509 버전 3 인증서 형식

버전(3)
일련번호(0a 85 76 59)
CA의 서명 알고리즘 (SHA-1 RSA)
발급자(yessign CA)
유효기간
주체 c = kr, o = yessign ou = SHB, cn = 홍길동
주체의 공개키(RSA 1024)
확장 필드
발급자의 서명(160비트)

- **일련 번호:** 발급된 다른 인증서들과 구분하기 위해 사용
- **발급자:** 인증서를 발급한 인증기관(CA)의 고유명
- **유효기간:** 인증서의 개시 및 만료일자
- **주체의 공개키:** 공개키 및 사용할 암호 알고리즘
- **확장:** 기관/주체 키 식별자, 주체의 대체 이름, CRL 배포지점 등
- **발급자의 서명:** 서명 값 필드를 제외한 모든 필드에 CA의 개인 키와 서명 알고리즘을 적용하여 생성

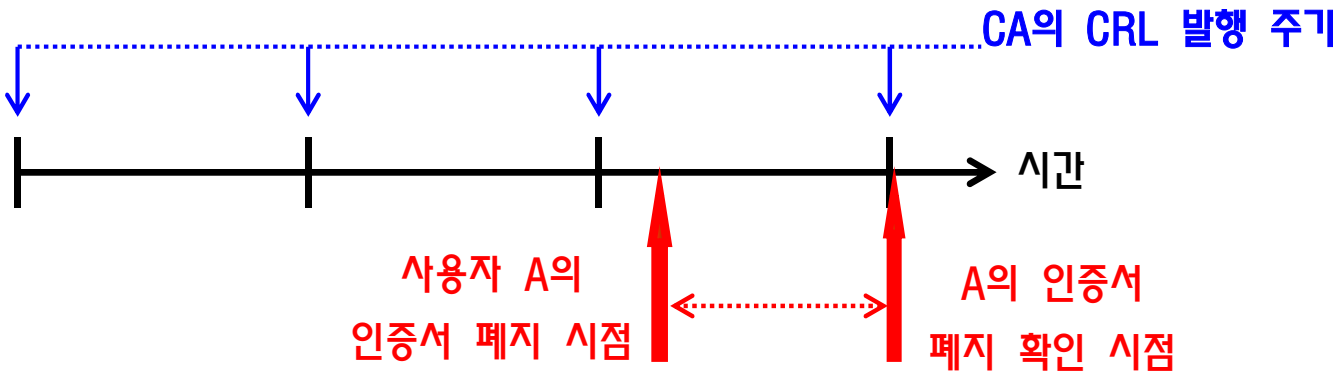


인증서의 상태 검사

- 인증서의 효력정지 및 폐지 사유
  - 인증서와 연관된 주체의 개인키 누설
  - 인증서와 연관된 주체의 소속 변경
  - 인증기관의 개인키 누설, …

- IETF의 PKIX 작업반은 X.509 인증서의 상태를 검사하기 위한 두 가지 방법 규정
  - 인증서 폐지목록(CRL)
  - 온라인 인증서 상태확인 프로토콜(OCSP)

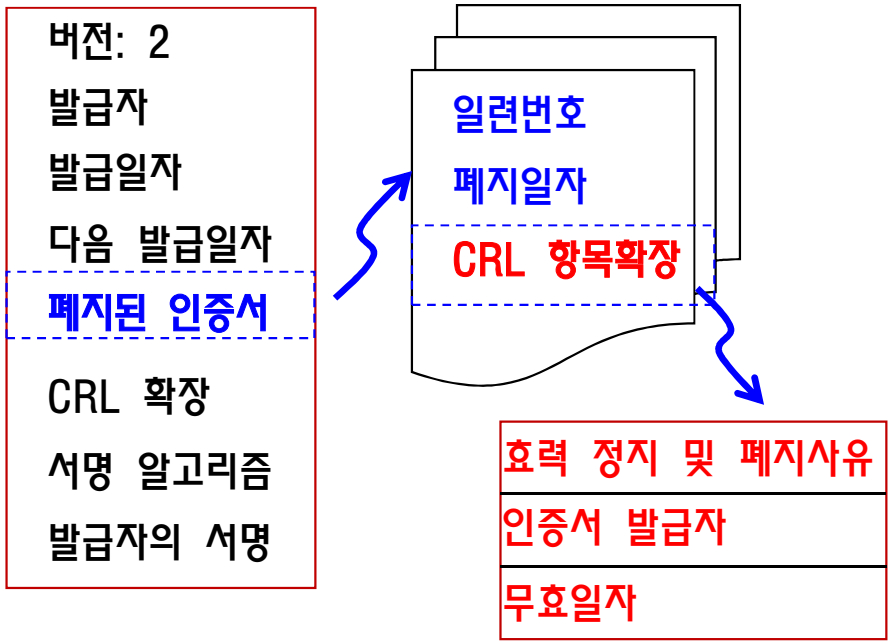
인증서 폐지목록(CRL)



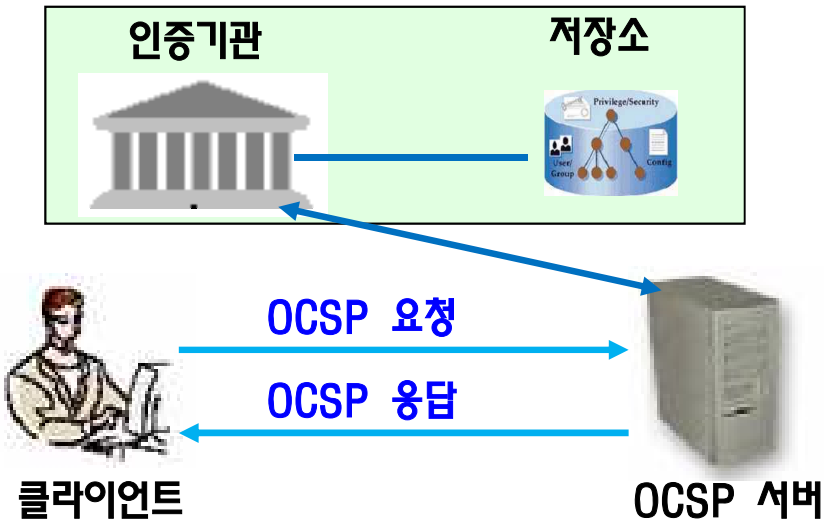
- 인증서 폐지목록(CRL: Certificate Revocation List)
- 인증기관은 일정한 시간 간격으로 CRL 발행: 일주일, 하루 또는 매시간 단위
- CRL의 발행 주기 사이에 폐지된 인증서는 다음 번 인증서 폐지목록에 나타남 → 폐지된 인증서의 상태를 실시간으로 알 수 없음

인증서 폐지목록의 필드

- 발급자: CRL 발급자인 인증기관의 고유명
- 발급일자/다음 발급일자: CRL의 현재 및 다음 발급 날짜와 시간
- 폐지된 인증서
  - 일련번호
  - 폐지 일자: 인증서가 폐지된 날짜와 시간
  - CRL 항목 확장: 폐지된 인증서의 추가 정보 제공
    - 효력정지 및 폐지 사유 코드
    - 인증서 발급자
    - 무효일자: 폐지된 인증서와 연관된 개인키가 누설되었다고 의심되는 날짜
- CRL 확장: CRL의 추가 정보 제공
- 서명 알고리즘: CA가 사용한 서명 알고리즘
- 발급자의 서명: 서명 값 필드를 제외한 모든 필드에 CA의 개인 키와 서명 알고리즘을 적용하여 생성



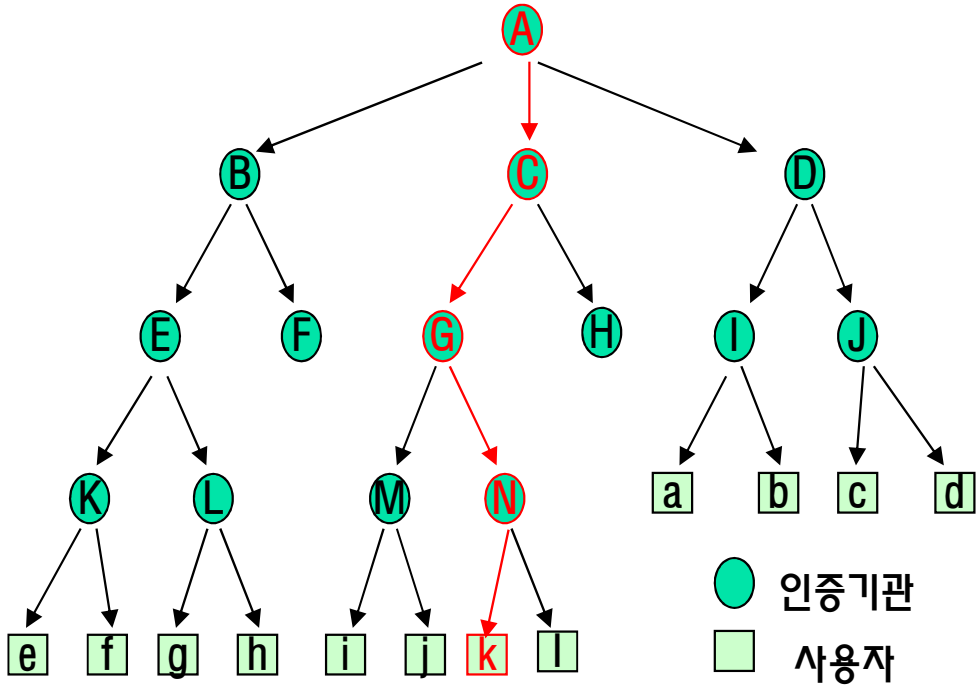
온라인 인증서 상태확인 프로토콜(OCSP)



- OCSP: Online Certificate Status Protocol
- 클라이언트-서버 모델
- 특정 인증서의 유효성을 온라인으로 언제든지 확인할 수 있는 메커니즘 제공
  - 특정 인증서의 상태를 확인하기 위하여 클라이언트는 OCSP 서버에게 상태확인 요청을 전송
  - OCSP 서버는 인증기관과의 협조하에 인증서 상태 정보를 클라이언트에게 응답

X.509 신뢰 모델

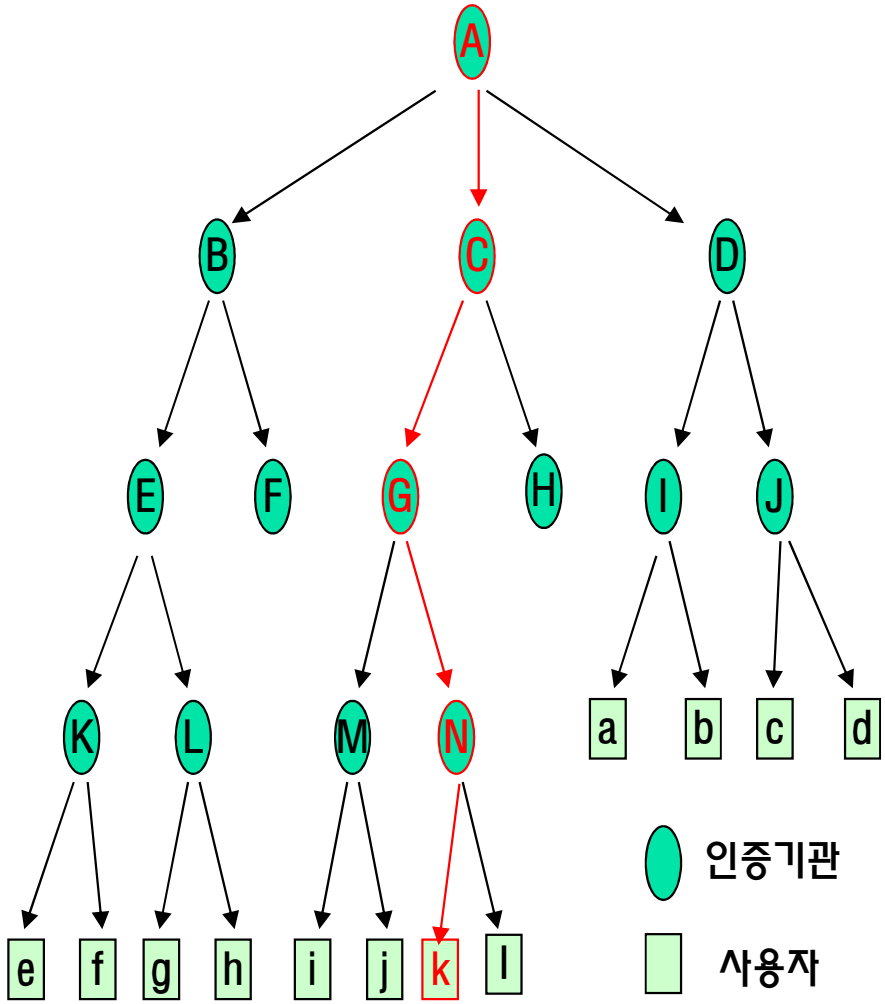
- 인증서의 유효성을 결정하기 위해 사용하는 규칙으로 계층적 신뢰를 사용
  - 사용자 k의 인증서가 유효하기 위하여서는 인증기관 N, G, C 및 A의 인증서도 유효하여야 함
- 최상위 인증기관인 A는 자체 서명한 인증서를 발행
- 최종 사용자 및 중간 인증기관의 인증서는 상위의 인증기관이 발급



사용자 K의 인증서 검증

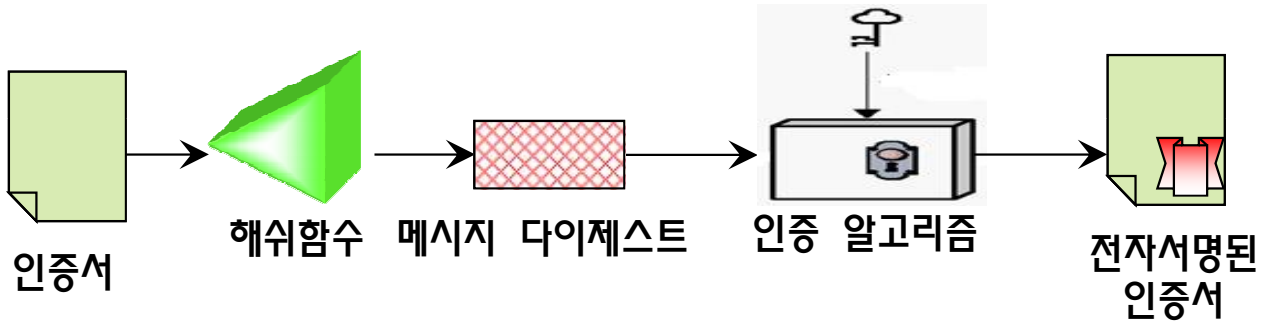
- K에서 최상위 CA A에 이르는 경로 상의 모든 인증서들에 검증 절차 수행
  - K, N, G, C, A의 인증서

- 인증서의 검증 절차
  1. 인증서의 버전 필드 확인
  2. 인증서가 주체의 인증서에 해당하는지 확인
  3. 인증서의 유효기간 확인
  4. 인증서 발급자의 공개키와 서명 알고리즘으로 서명 값의 유효성 확인
  5. 최근의 인증서 페지목록에서 해당 인증서의 폐지 유무 확인
  6. 최상위 CA 인증서가 아니면 인증서 발급자의 인증서를 구하여 단계 1-6을 반복



최상위 인증기관

- 최상위 인증기관의 개인키가 침해된 경우 최상위 인증기관의 인증서는 물론 모든 중간 인증기관과 최종 사용자의 인증서가 함께 폐지되어야 함
- 최상위 인증기관의 개인키는 엄격한 보안이 요구
  - 최소한 160비트 메시지 다이제스트를 갖는 SHA-1, RIPEMD-160 등과 같은 해쉬 함수 사용
  - 인증 알고리즘에 사용할 개인키의 길이는 최소한 2048 비트 사용



요점 정리(1/2)

- 공개키 암호 시스템의 광범위한 응용으로 공개키를 관리하고 분배하는 공개키 기반구조(PKI: Public-Key Infra-structure)가 요구됨
  - 인증서를 발행 받아 인터넷 뱅킹 등에 사용하는 사용자
  - 인증서 신청자의 신원 확인 및 인증서 등록을 대행하는 등록기관
  - 인증서를 발행하는 인증기관
  - 인증서나 인증서의 취소목록을 저장하는 저장소

- 인증서
  - 공신력 있는 인증기관이 발행한 사이버 거래의 인감증명서
  - 위조가 불가능하도록 실체(개인 또는 조직)의 정보와 공개키 그리고 인증기관의 정보가 수록된 인증서를 인증기관의 개인키로 서명하여 발급
  - X.509 인증서, PGP(Pretty Good Privacy) 인증서

- 인증기관(CA; Certificate Authority): 인증서의 생성, 배정, 관리 등의 작업을 수행하는 기관
  - 민간분야(금융 · 증권 · 무역 · 전자입찰 등)의 NPKI(National PKI)
  - 정부분야의 GPKI(Government PKI)

요점 정리(2/2)

- 외국의 인증기관
  - 인증기관의 시장은 전 세계의 각 지역으로 분할되어 있다. 그러나, 웹 사이트의 보안에 사용되는 SSL 인증서의 시장은 몇 개의 회사에 의하여 점유되고 있다.
  - VeriSign, GoDaddy, Comodo, …
- 키 생성 및 관리
  - 사용자 키 생성 방식
  - 중앙 집중형 키 생성 방식
- ITU-T의 X.509는 인증서의 분배와 관련된 데이터 형식과 절차만 정의하였으며, 인증서의 내부 필드들에 대한 실제 자료구조는 정의하지 않았음
  - IETF의 PKIX 작업반: X.509 기반의 PKI를 지원하기 위한 인터넷의 표준 개발을 위하여 1995년에 구성
- IETF의 PKIX가 규정한 X.509 인증서의 상태를 검사하는 방법
  - 인증서 폐지목록
  - 온라인 인증서 상태확인 프로토콜
- X.509 신뢰모델: 인증서의 유효성을 결정하기 위해 계층적 신뢰를 사용