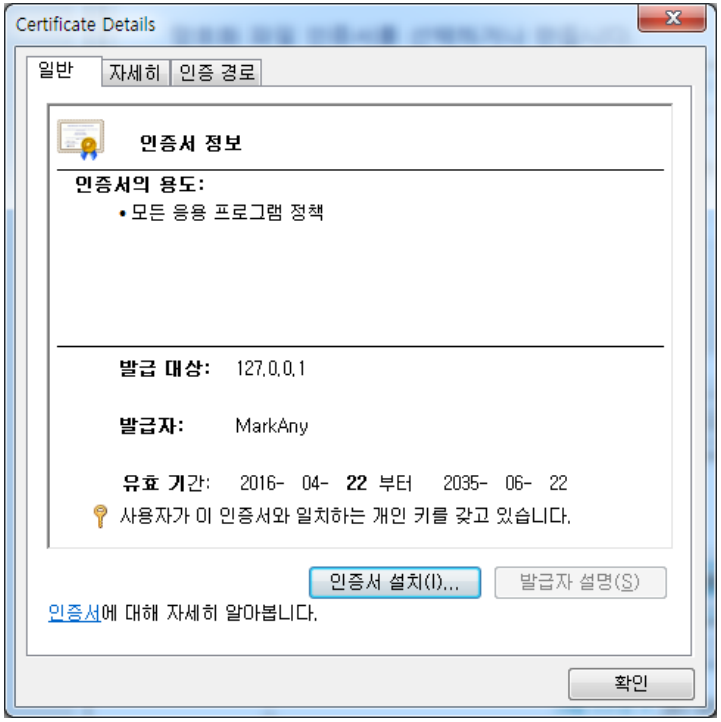
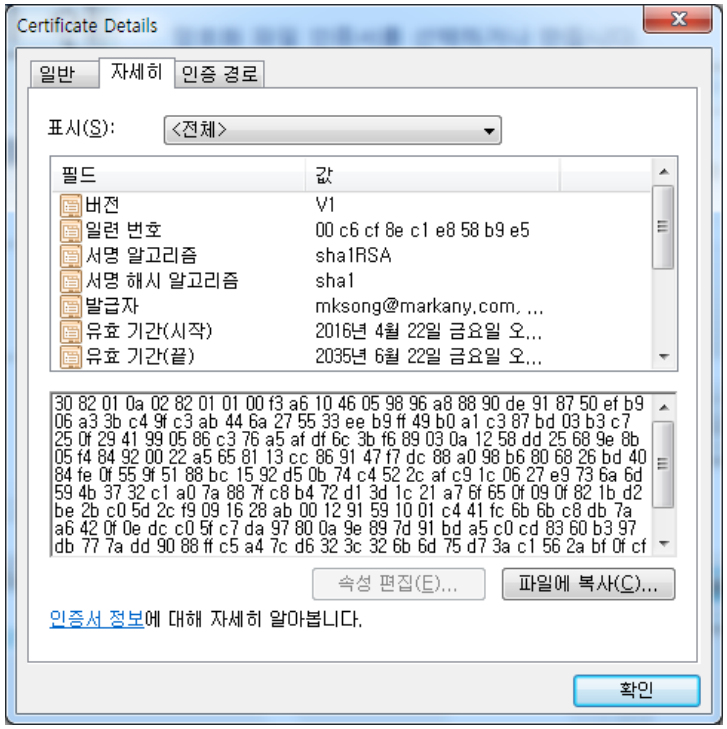
정 보 보 안
실습3
인증서와 openssl

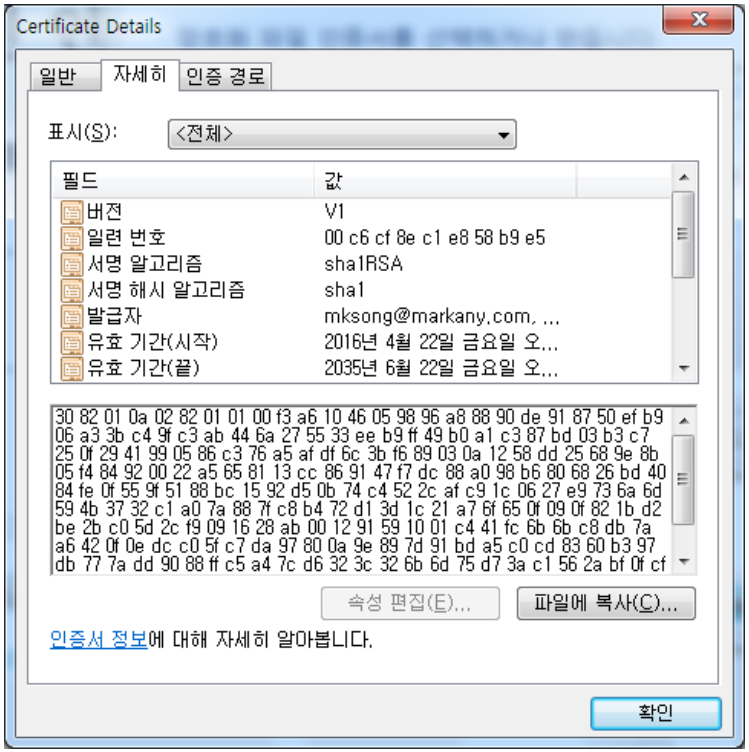
- 인증서란?
  - 공개 키 인증서(public-key certificate; PKC)
    - 사용자의 공개 키에 사용자의 식별 정보를 추가하여 만든 일종의 전자 신분증
    - 일명 : 공개키 증명서, 디지털 증명성, 전자 증명서





– 인증서의 내용

- 이름이나 소속, 메일 주소 등의 개인 정보
- 당사자의 공개키가 기재
- 인증기관(CA; Certification Authority, certifying authority)의 개인키로 디지털 서명



– 인증서를 사용하는 시나리오

- 예) 인증기관(CA)를 이용해서 앨리스가 밥에게 암호문을 보내는 예

1)밥이 키 쌍을 작성한다

2)밥은 인증기관(CA)에 자신의 공개 키를 등록한다

3)인증기관은 밥의 공개 키에 자신의 개인 키로 디지털 서명을 해서 인증서를 작성한다

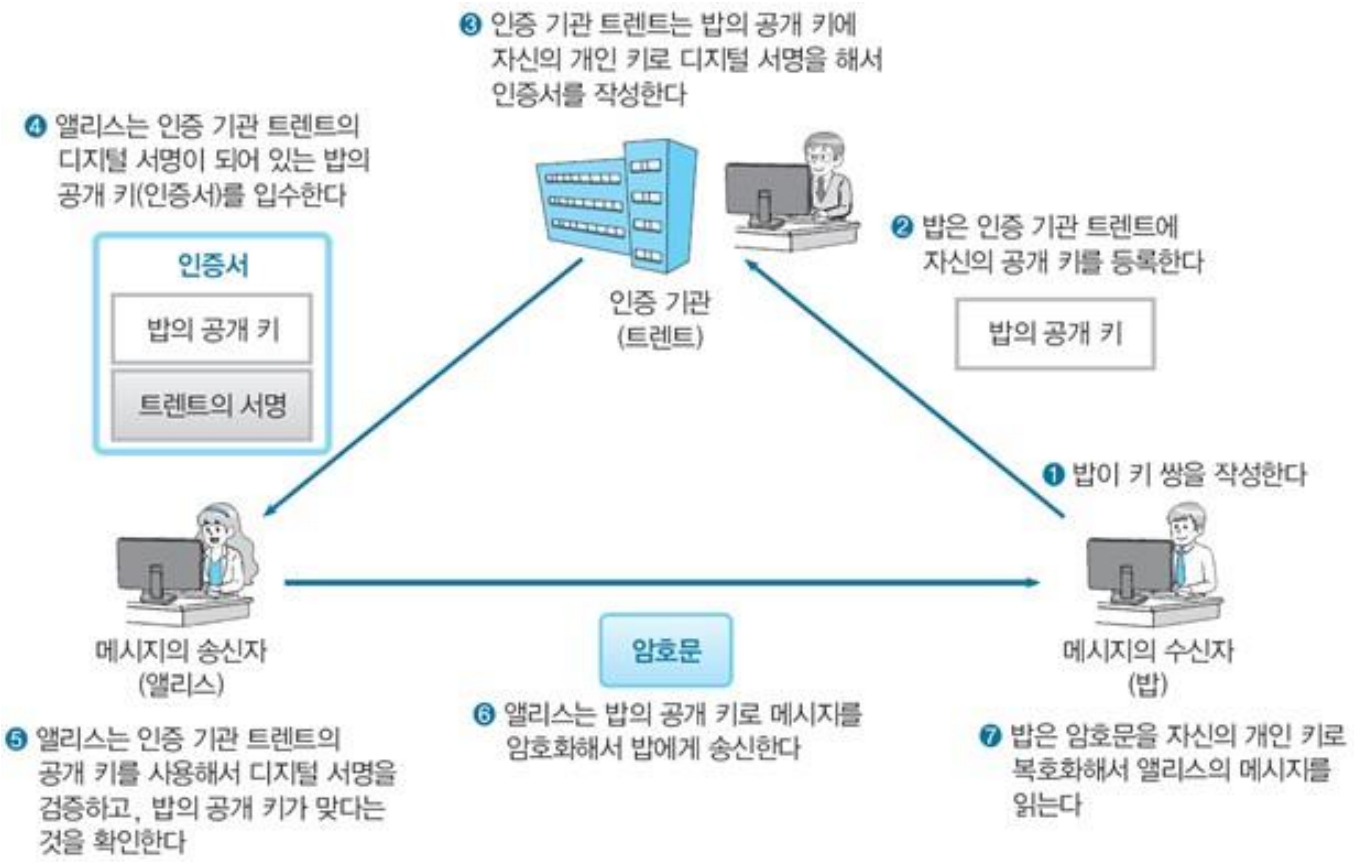
4)앨리스는 인증기관의 디지털 서명이 되어 있는 밥의 공개 키(인증서)를 입수한다

5)앨리스는 인증기관의 공개 키를 사용해서 디지털 서명을 검증하고, 밥의 공개 키가 맞다는 것을 확인한다

6)앨리스는 밥의 공개 키로 메시지를 암호화해서 밥에게 송신한다

7)밥은 암호문을 자신의 개인 키로 복호화해서 앨리스의 메시지를 읽는다

– 예) 인증기관(CA)를 이용해서 앨리스가 밥에게 암호문을 보내는 예



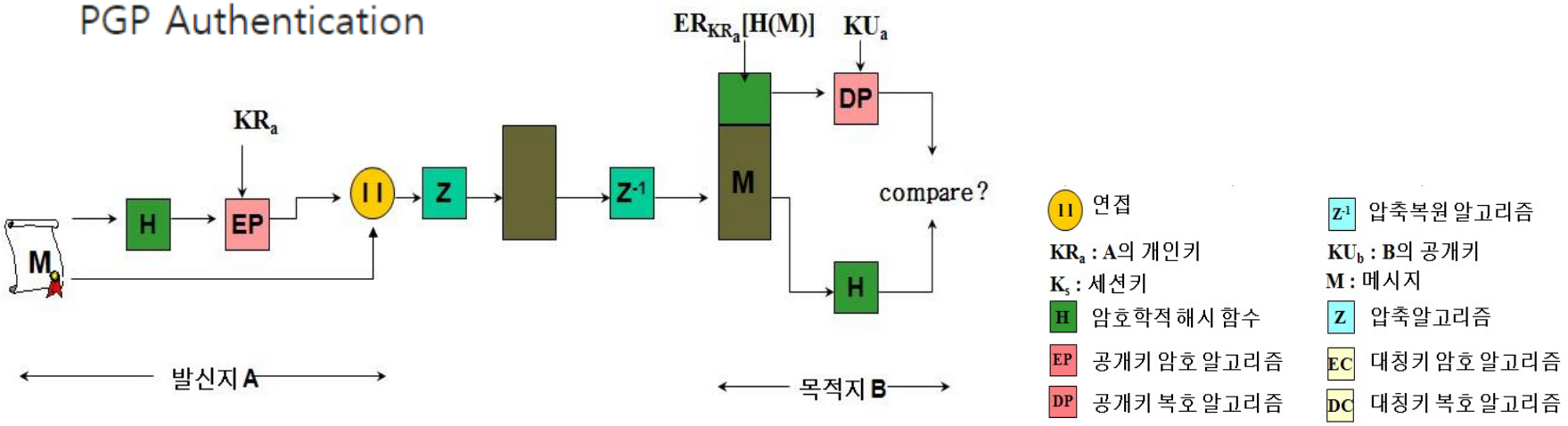
• 인증기관 트렌트를 이용해서 앨리스가 밥에게 암호문을 보내는 예

- 공인 인증서 종류
  - 범용 공인인증서
    - 모든 분야에서 이용
    - 인터넷뱅킹, 온라인증권, 전자상거래, 전자정부 민원서비스, 4대 사회보험, 국세청 홈텍스, 전자세금계산서, 전자입찰/조달, 온라인교육, 예비군 등 다양한 분야에서 활용
    - 소정의 수수료
  - 용도제한 공인인증서
    - 은행 및 보험, 신용카드 업무, 정부 민원업무 등 특정분야에서만 이용
    - 해당 기관이 고객에게만 발급
    - 무료

- 인증서 표준 규격
  - X.509
    - 가장 널리 사용
    - ITU(International Telecommunication Union, 국제전기통신연합)나 ISO(International Organization for Standardization, 국제 표준화기구)에서 규정한 규격
    - 인증서의 생성・교환을 수행할 때 사용
    - 많은 애플리케이션에서 지원
  - SPKI(Simple Public Key Infrastructure)
  - PGP(Pretty Good Privacy)

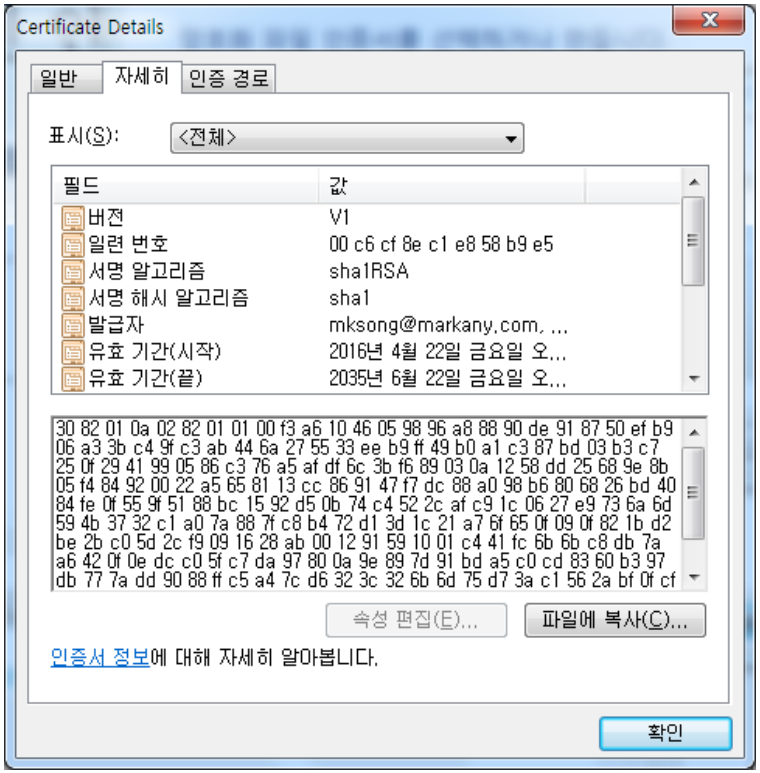
– PGP(Pretty Good Privacy)

- 필 짐머맨(Phil Zimmermann)이 독자적으로 개발한 것
- 인터넷에서 사용되고 있는 전자 우편 보안 시스템의 하나
- 비밀성(confidentiality), 메시지 무결성, 사용자 인증, 송신 부인 방지, 수신 부인 방지, 메시지 반복 공격 방지 등의 기능을 지원
- 또 다른 전자 우편 방식 : PEM(Privacy Enhanced Mail)



- 개인 인증서

  - 버전
  - 일련번호
  - 서명 알고리즘
  - 발급자
    - 인증서를 발급한 인증기관의 DN(Distinguish Name)이름
    - DN : 어떤 개인 또는 조직의 이름을 정의하는 방식
      - X.500 표준에서 정의
      - DN : C(country), O(Organization), OU(Organization Unit, 조직 하위)
  - 유효 기간
  - 주체 : 인증서 소유자의 DN 이름
  - 공개키



– 개인 인증서 세부 필드

필드	값
버전	V3
일련 번호	03 5a 89 ef
서명 알고리즘	sha256RSA
서명 해시 알고리즘	sha256
발급자	CN = yanGATE CA4 OU = AccreditedCA O = KICA C = KR
유효 기간(시작)	2016년 12월 28일 수요일 오후 8:26:16
유효 기간(끝)	2017년 12월 27일 수요일 오후 11:59:59
주체	CN = 홍길동 OU = 용양우체국 OU = 우체국 OU = 등록기관 OU = licensedCA O = KICA C = KR
공개 키	30 82 01 0a 02 82 01 01 00 c2 8d 87 01 d0 3b 50 d7 a3 ea 72 b4 f3 a5 cf 1e 45 45 7b ac c0 58 6f f1 7b a9 87 18 72 71 c3 b6 d7 8f a8 b9 b8 97 d7 d4 ea aa 1b 00 34 b2 4b c8 b5 5e 45 93 84 54 e7 62 5d d3 2c 7b d2 43 c4 ed a5 7a d5 87 e0 c9 04 a0 aa 98 ae b9 8c 29 62 f8 58 22 46 9b 95 9c 80 d7 fc ab 45 08 91 fc 0c 54 95 74 6f 35 bc 90 47 59 b0 a6 3a 24 64 f3 bc b8 cf 5c 1f b4 3e 16 7c d4 15 a7 01 e0 59 6f ca e3 a5 52 0f 2f 92 db ca 3d a9 9a 3e 95 43 72 f0 26 b3 58 8a 27 74 9b 1c 35 a6 8e 9e eb 96 7e 3c 31 17 59 34 17 90 03 95 5a 5e 35 ef be e7 c9 97 44 1b c8 88 20 2a 98 6a 2f 1f 50 ae c9 e0 c5 2b 50 31 bd 89 6a d6 7e d1 64 13 3e 23 a5 06 eb 64 33 42 1f ed 1f 90 b7 9a 63 c1 3f 0a 8f 04 62 32 b9 76 e0 7f fa e9 1c c5 e2 be c2 01 b9 7f e5 13 26 8d be a9 ba d6 9a 5c 56 89 ef 78 fb f9 3c f1 21 02 03 01 00 01
기관 키 식별자	KeyID=ae 52 fd 0e 0e 01 f8 30 86 37 7e f6 18 c6 49 25 4a 60 09 70 Certificate Issuer: 디렉터리 주소: CN=KISA RootCA 4 OU=Korea Certification Authority Central O=KISA C=KR Certificate SerialNumber=10 0a
주체 키 식별자	67 10 1f 3d 04 47 97 c7 79 22 a2 68 4e a4 77 af 78 04 ad 0d
인증서 정책	[1]Certificate Policy: Policy Identifier=1.2.410.200004.5.2.1.7.1
주체 대체 이름	Other Name: 1.2.410.200004.10.1.1=30 4e 0c 09 ec a0 84 ed 83 9c ec 9d bc 30 41 30 3f 06 0a 2a 83 1a 8c 9a 44 0a 01 01 01 30 31 30 0b 06 09 60 86 48 01 65 03 04 02 01 a0 22 04 20 e9 36 22 bd d2 4a 61 02 d1 e5 84 f2 76 83 d7 cf 20 dc b2 54 f3 a2 41 af 07 d4 61 6f f9 6b 4c 72
CRL 배포 지점	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.yanggate.com:389/ou=dp6b26866,ou=crldp,ou=AccreditedCA,o=KICA,c=KR
기관 정보 액세스	[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.yanggate.com:9020/OCSPServer
키 사용	Key Encipherment (20)
지문 알고리즘	sha1
지문	d3 1f 49 f5 73 28 16 ee e3 3d bd 90 f5 ee 75 95 94 84 f2 e6

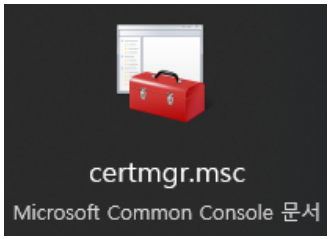
– 인증서 세부 필드

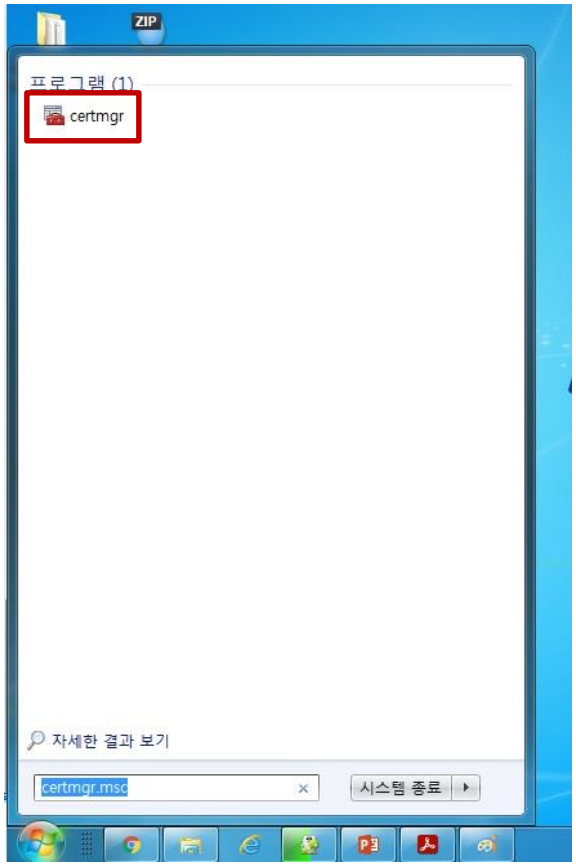
- 최상위 인증기관 인터넷진흥원의 인증서

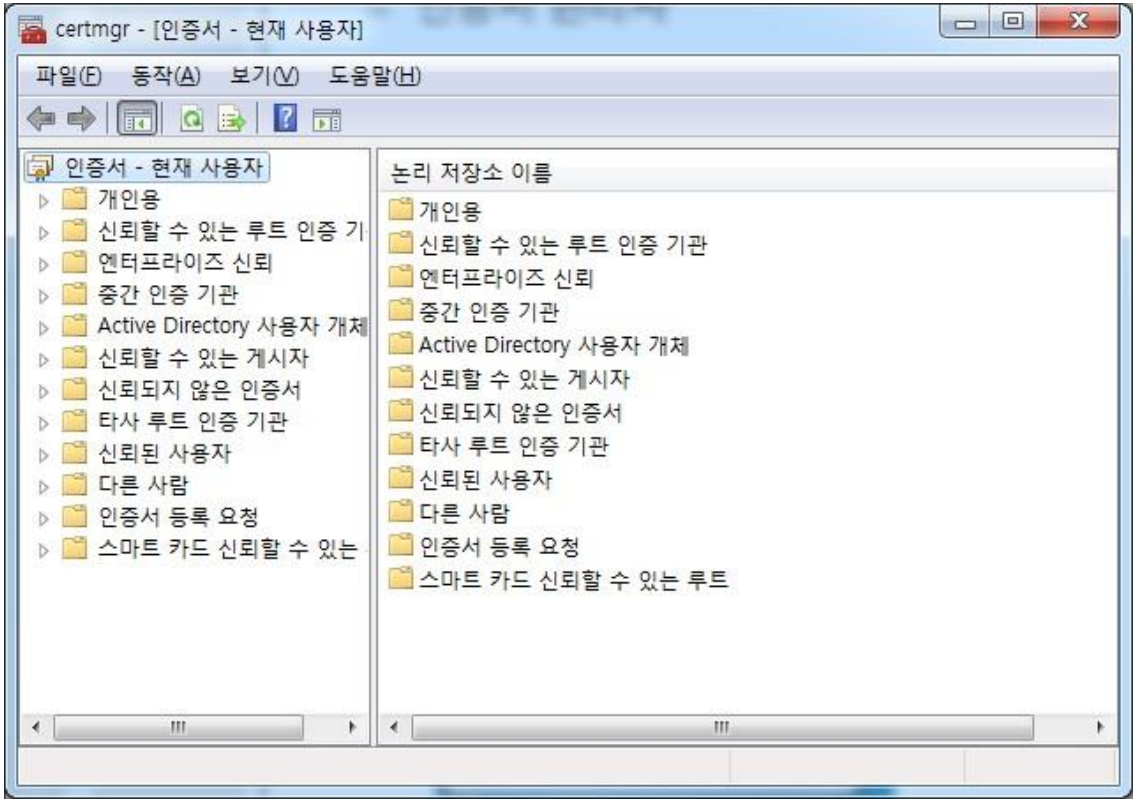
```
Data:
Version: 3 (0x2)
Serial Number: 4 (0x4)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=KR, O=KISA, OU=Korea Certification Authority Central,
CN=KISA RootCA 1
Validity
Not Before: Aug 24 08:05:46 2005 GMT
Not After : Aug 24 08:05:46 2025 GMT
Subject: C=KR, O=KISA, OU=Korea Certification Authority Central,
CN=KISA RootCA 1
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:bc:04:e4:fa:13:39:f0:34:96:20:6b:6c:68:bb:fa:db:77:ff:27:f7:ac:ec:2f:e7:fd:f0:7f:6d:
6f:8c:2a:cd:25:09:5b:24:f4:a1:68:fc:28:ec:c9:25:e2:ac:ed:de:c8:33:84:f5:b0:a5:09:3a:a7:
b1:47:48:c5:cc:4f:8c:79:9c:f9:06:57:7d:dd:ee:38:f6:cf:14:b2:9c:ea:d3:c0:5d:77:62:f0:47:
0d:b9:1a:40:53:5c:64:70:af:08:5a:c0:f7:cf:75:f9:6c:8d:64:28:1e:20:fe:b7:1b:19:d3:5a:66:
83:72:e2:b0:9b:bd:d3:25:15:0d:32:6f:64:37:94:85:46:c8:72:be:77:d5:6e:1f:28:2f:c7:69:ed:e7:
83:89:33:58:d3:de:a0:bf:40:e8:43:50:ee:dc:4d:6b:bc:a5:ea:a6:c8:61:8e:f5:c3:64:af:06:15:dc:
29:8b:3f:75:8c:bc:71:44:db:fc:ad:b5:17:1d:6d:89:83:cf:c6:33:bd:bf:45:a2:fe:0a:9f:a3:11:
5f:0f:b9:1f:9c:1a:c2:46:cc:9c:28:66:9f:70:26:3c:2e:df:aa:80:fe:8c:c5:04:09:25:
4f:cd:93:47:3c:37:ea:02:67:92:fe:fc:22:24:5c:ac:d2:2c:e0:5c:01:33:8a:c1:19:db
```

– 인증서 관리자

- certmgr.msc : 관리자 권한으로 실행

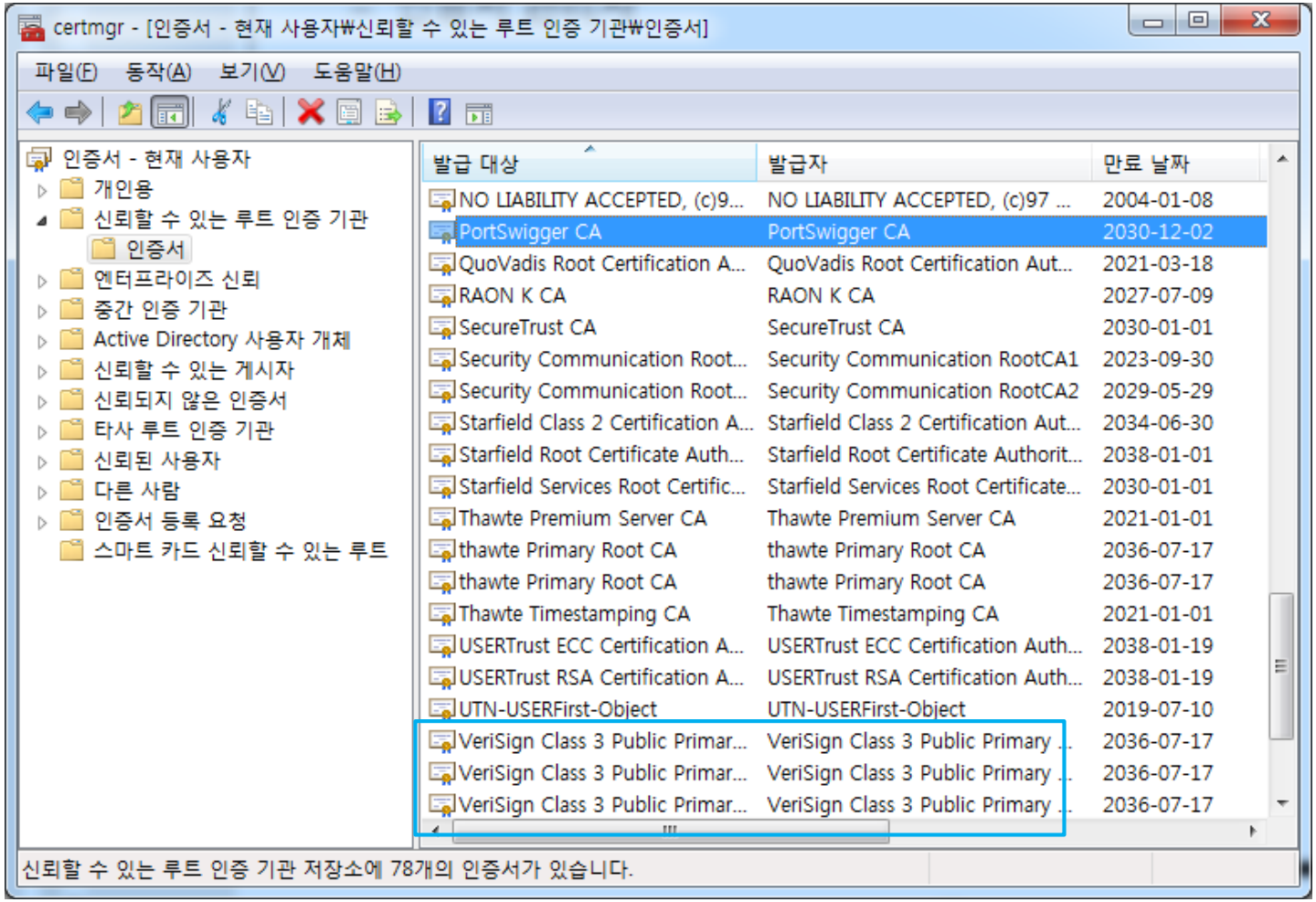




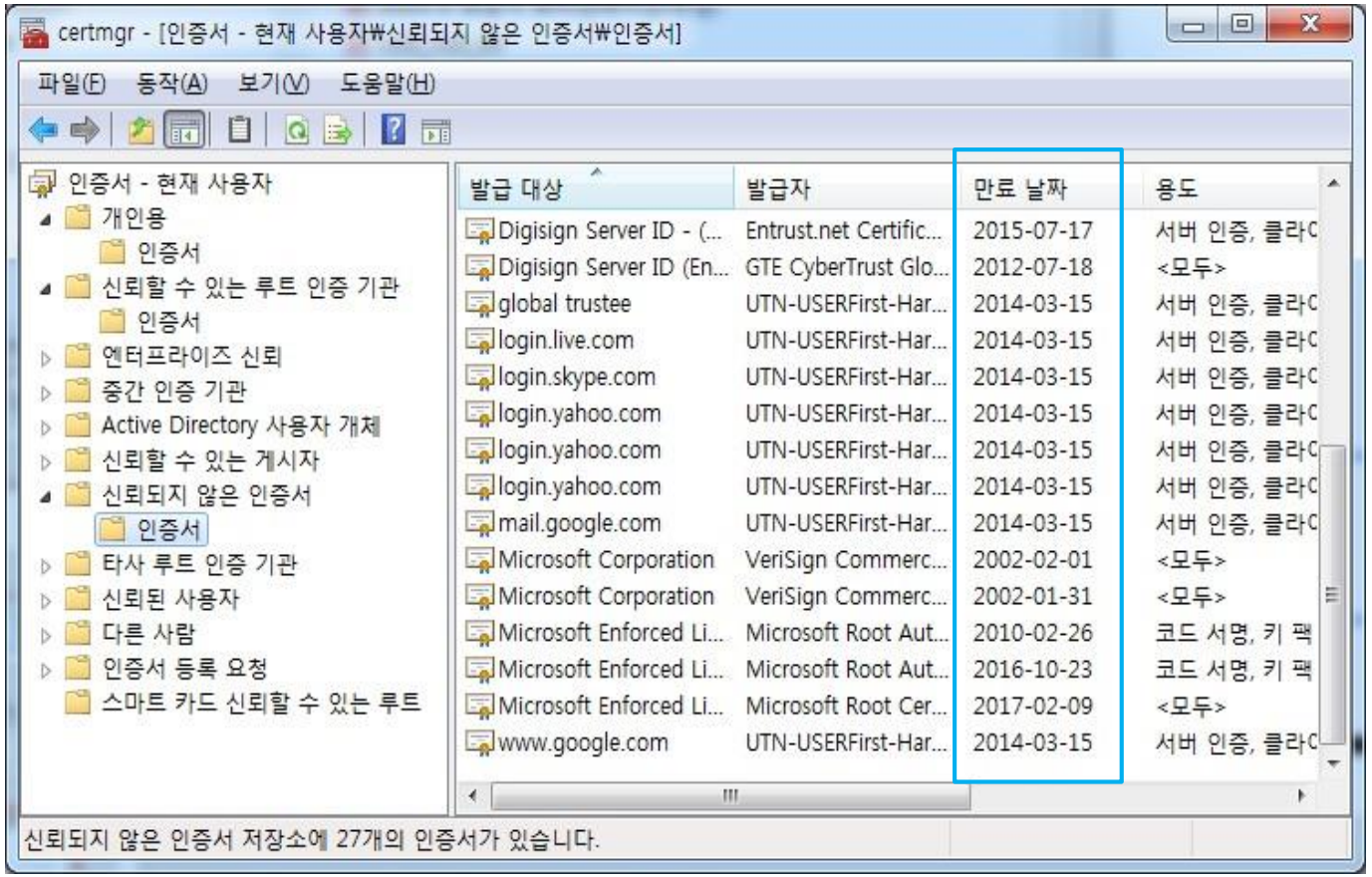


– 인증서 관리자

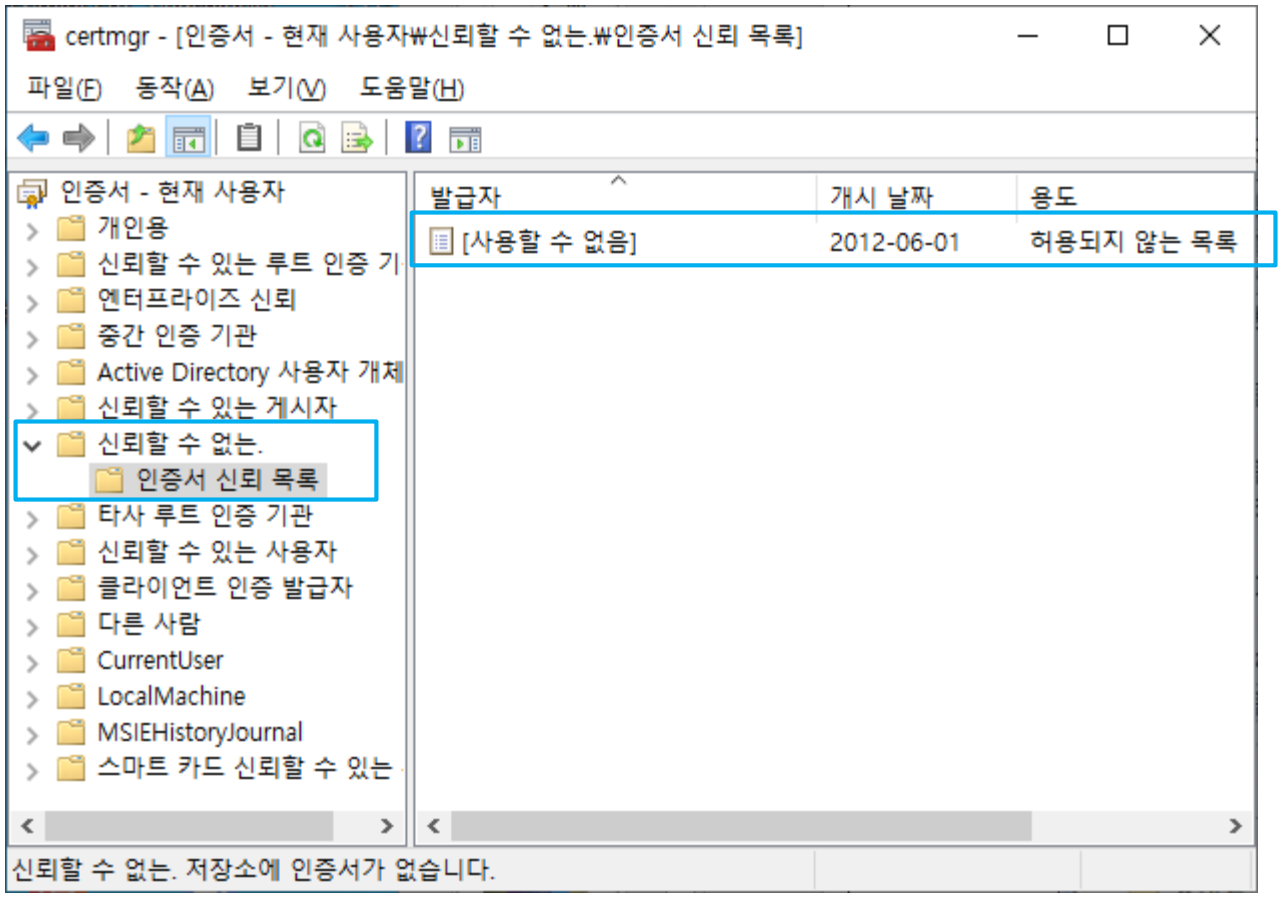
- ‘신뢰할 수 있는 루트 인증기관‘ – ‘인증서’ 선택



- ‘신뢰되지 않은 인증서‘ - ‘인증서’ 선택
  - [Q] 이 인증서들의 공통점은?

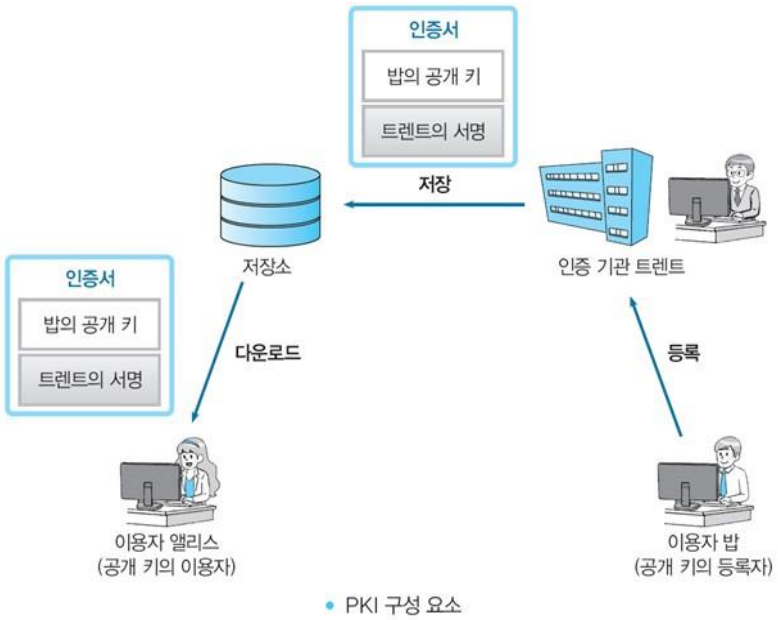


- ‘신뢰되지 않은 인증서‘ -> ‘신뢰할 수 없는’



- 공개 키 기반(Public-Key Infrastructure, PKI)
  - 공개 키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택 사양의 총칭
  - PKCS(Public-Key Cryptography Standards, 공개키 암호 표준)
    - 공개키 암호의 통신 규약
  - RSA사가 정하고 있는 규격의 집합
  - RFC(Requests for Comments) 중에도 PKI에 관련된 문서
  - 인터넷의 선택 사양을 정한다
  - X.509
  - API(Application Programming Interface) 사양서

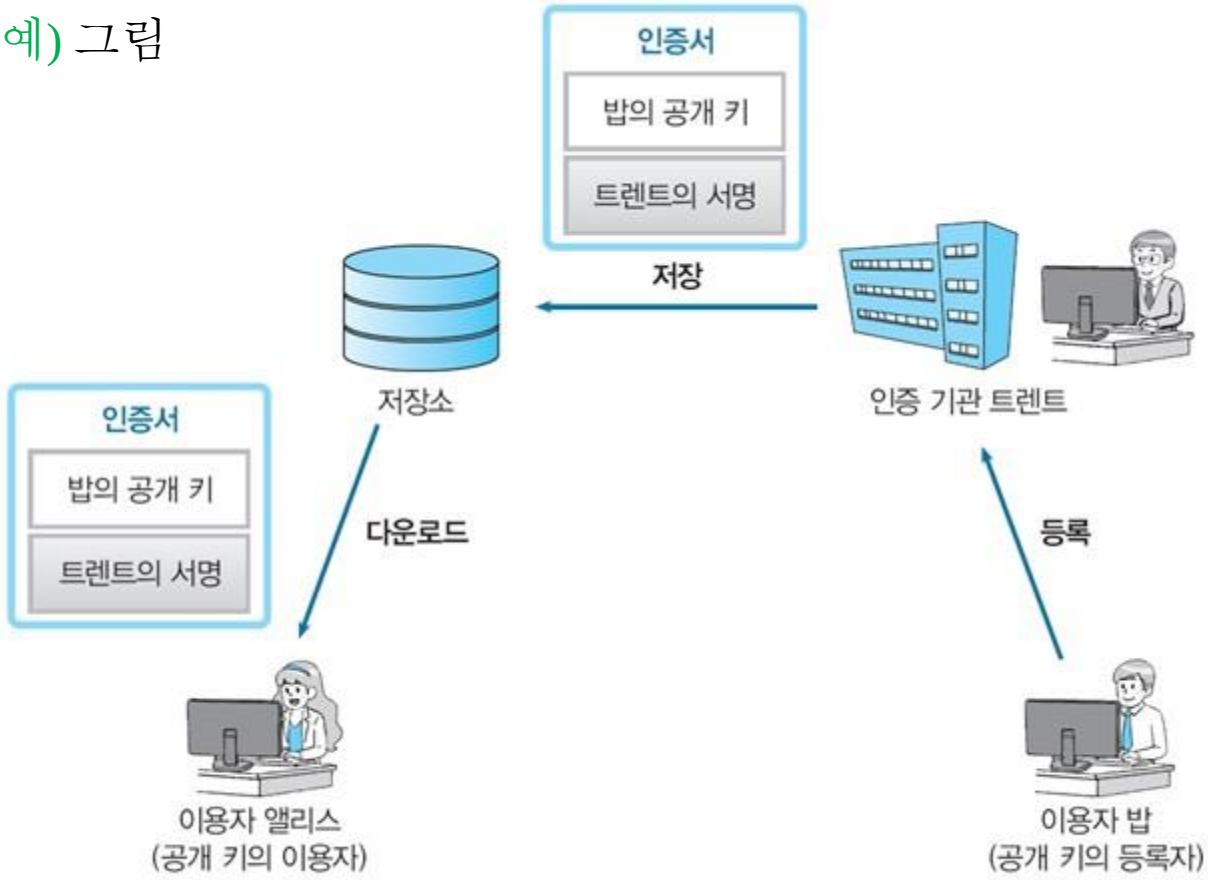
- PKI 구성 요소
  - 이용자
    - PKI를 이용하는 사람
    - PKI를 사용해서 자신의 공개 키를 등록하고 싶어 하는 사람과
    - 등록되어 있는 공개 키를 사용하고 싶어 하는 사람
  - 인증기관(CA) : 인증서를 발행하는 사람
  - 저장소 : 인증서를 보관하고 있는 데이터베이스
  - 예) 그림



PKI 구성 요소

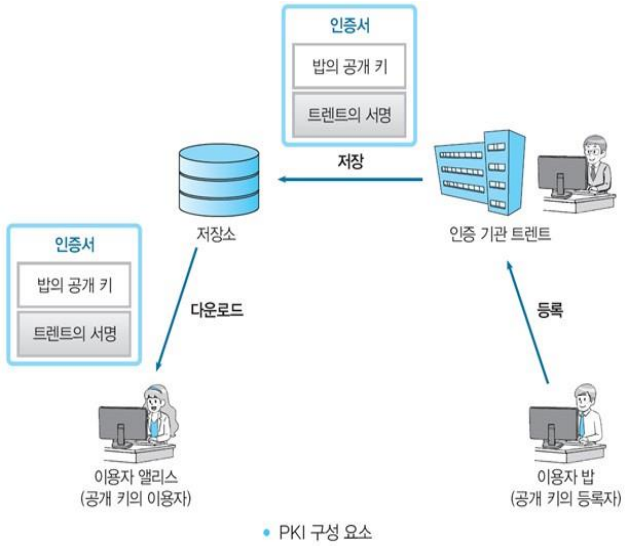
– PKI 구성 요소

- 예) 그림



• PKI 구성 요소

- 이용자가 하는 일
  - 키 쌍을 작성한다(인증기관이 작성하는 경우도 있다)
  - 인증기관에 공개키를 등록한다
  - 인증기관으로부터 인증서를 발행받는다
  - 필요할 경우 인증기관에 신청해서 등록한 공개 키를 무효로 한다
  - 수신한 암호문을 복호화한다
  - 메시지에 디지털 서명을 한다
- 공개키 사용자가 하는 일
  - 메시지를 암호화해서 수신자에게 송신
  - 디지털 서명을 검증

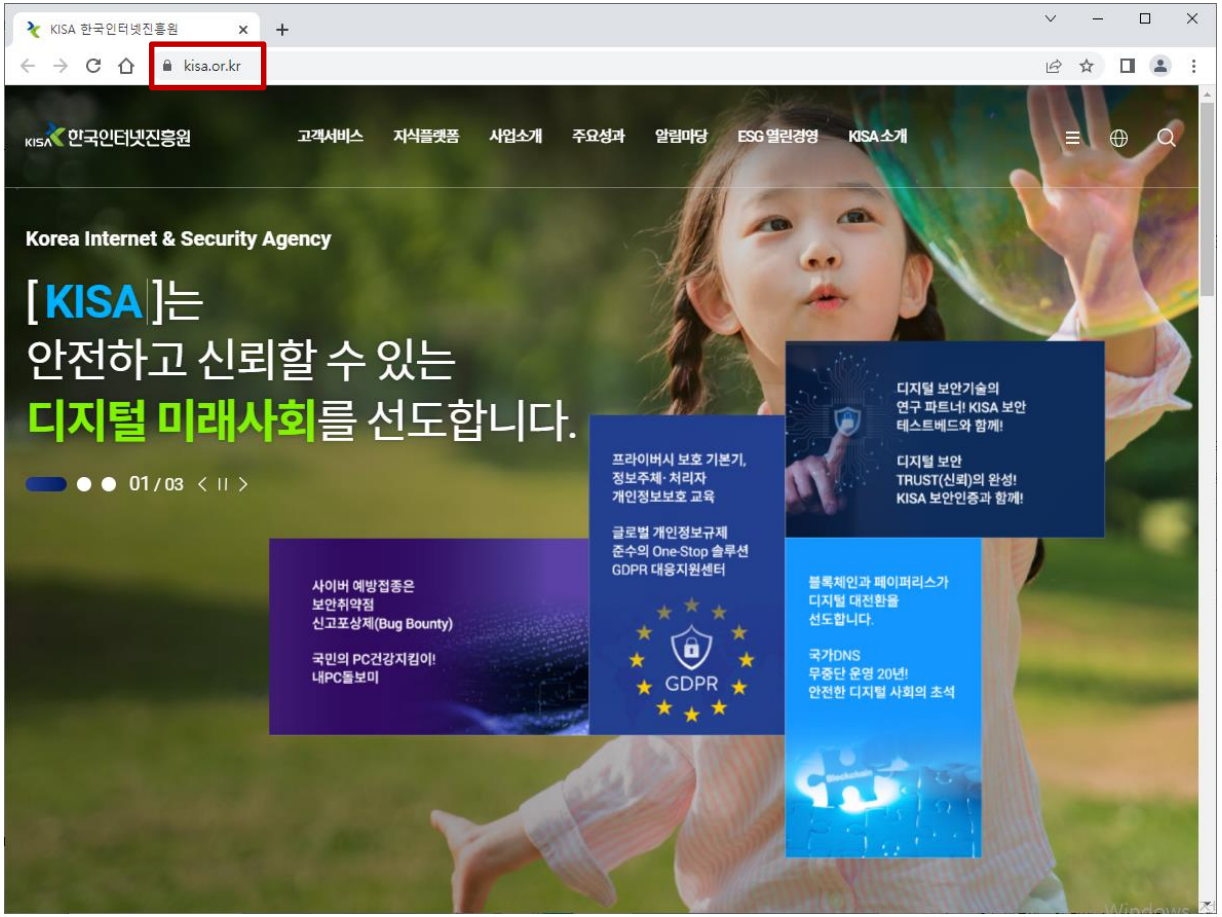


- 인증기관(Certification Authority; CA)
  - 인증서의 관리를 행하는 기관
  - 키 쌍을 작성한다(이용자가 작성하는 경우도 있다)
  - 공개키 등록 때 본인을 인증
  - 인증서를 작성해서 발행
  - 인증서를 폐지

- 등록기관(RA; registration authority)
  - 인증기관의 일 중 「공개 키의 등록과 본인에 대한 인증」을 대행하는 기관

– 공인 인증기관

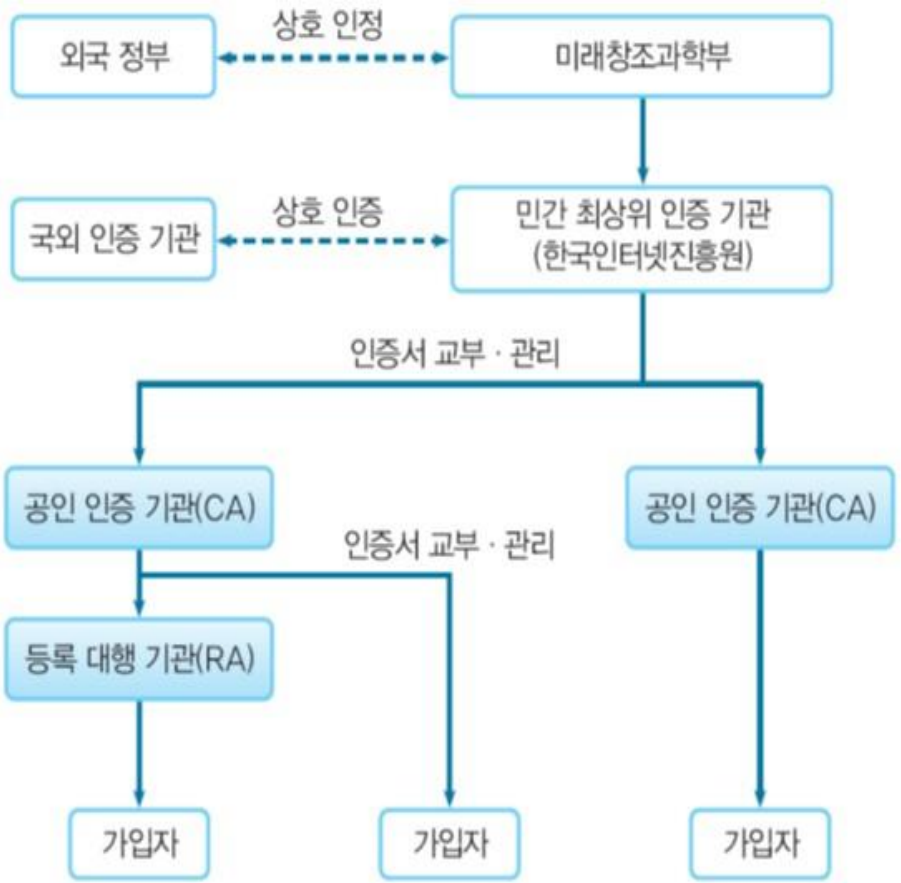
- 미래창조과학부 산하에 민간 최상위 인증기관인 한국인터넷진흥원(KISA)이 있음



- 전자서명법 제 4조의 규정에 의해 지정된 공인 인증기관은 5개가 있음
  - 개인 또는 기업 등의 요청에 따라 공인인증서를 발급
  - 철저한 심사 절차를 통해 발급
  - 법적 효력과 안전성 보장

공인 인증기관	웹페이지	전화번호
한국정보인증(주)	http://www.signgate.com	1577-7337
(주)코스콤	http://www.signkorea.com	1577-7337
금융결제원	http://www.yessign.or.kr	1577-5500
한국전자인증(주)	http://www.crosscert.com	1566-0566
한국무역정보통신	http://www.tradesign.net	1566-2119

– 한국의 인증관리 체계도



• 한국의 전자서명 인증관리 체계도

- 저장소(repository)
  - 인증서를 보존
  - PKI 이용자가 인증서를 입수할 수 있도록 한 데이터베이스
  - 인증서 디렉토리
- 인증기관의 역할
  - 키 쌍의 작성
  - 인증서 등록
  - 인증서 폐지와 CRL(Certificate Revocation List)

- 키 쌍의 작성
  - PKI의 이용자가 작성하기
  - 인증기관이 작성하기
    - 「개인 키를 이용자에게 보내는」 추가 업무
    - 방법은 PKCS #12(Personal Information Exchange Syntax Standard)로 정의
- 인증서 등록
  - 이용자는 인증기관에 인증서 작성을 의뢰
    - 규격은 PKCS #10(Certification Request Syntax Standard) 등으로 정의
  - 운용 규격(certification practice statement; CPS)에 근거해서 이용자를 인증하고, 인증서를 작성
    - 인증서 형식은 PKCS #6(Extended-Certificate Syntax Standard)나 X.509로 정의

- 인증서 폐지와 CRL
  - 인증서를 폐지(revoke)해야 할 경우
    - 이용자가 개인 키를 분실 혹은 도난
  - 인증서 폐지 목록(CRL: certificate revocation list)을 작성
    - 인증기관의 최신 CRL을 조사해서 그 인증서 유효성 확인 필요

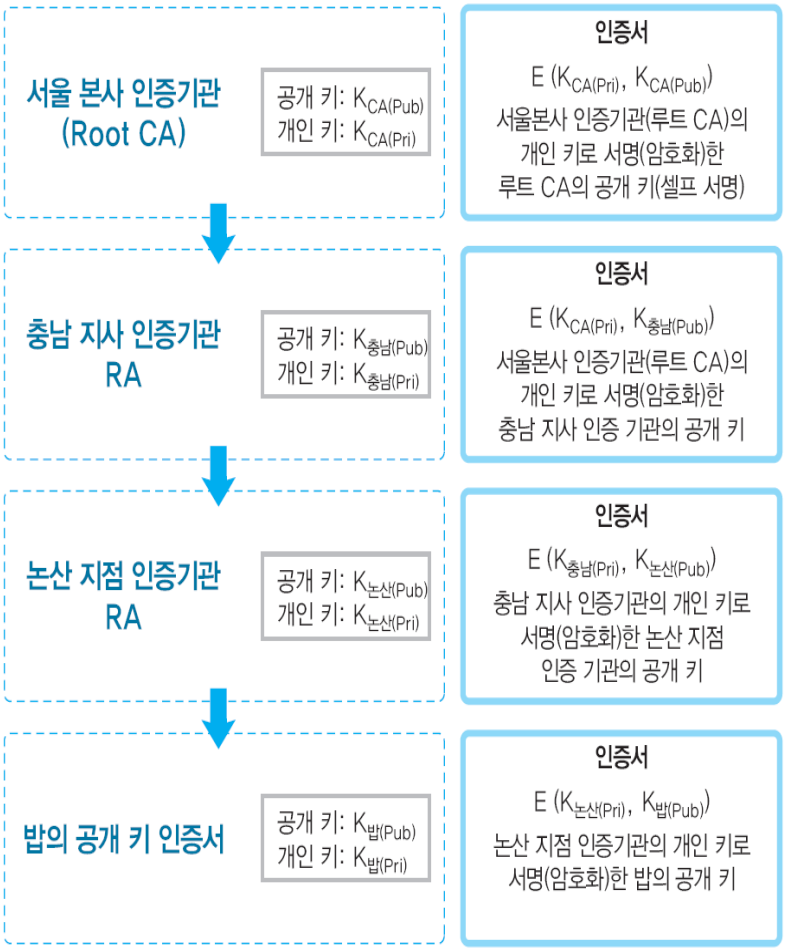
- 계층 구조를 갖는 인증서
  - 회사 내의 사내 PKI
    - 서울 본사 (서울 본사 인증기관)

      ↓

    - 충남 지사(충남 지사 인증기관)

      ↓

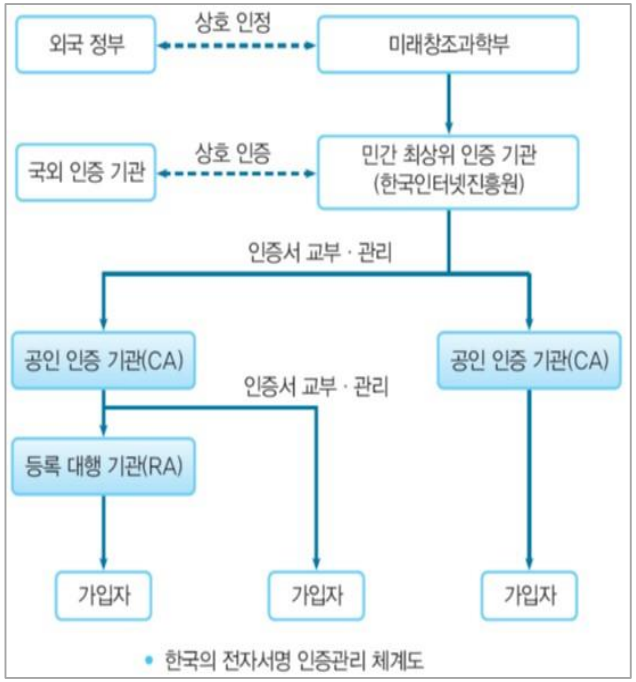
    - 논산 지점(논산 지점 인증기관)



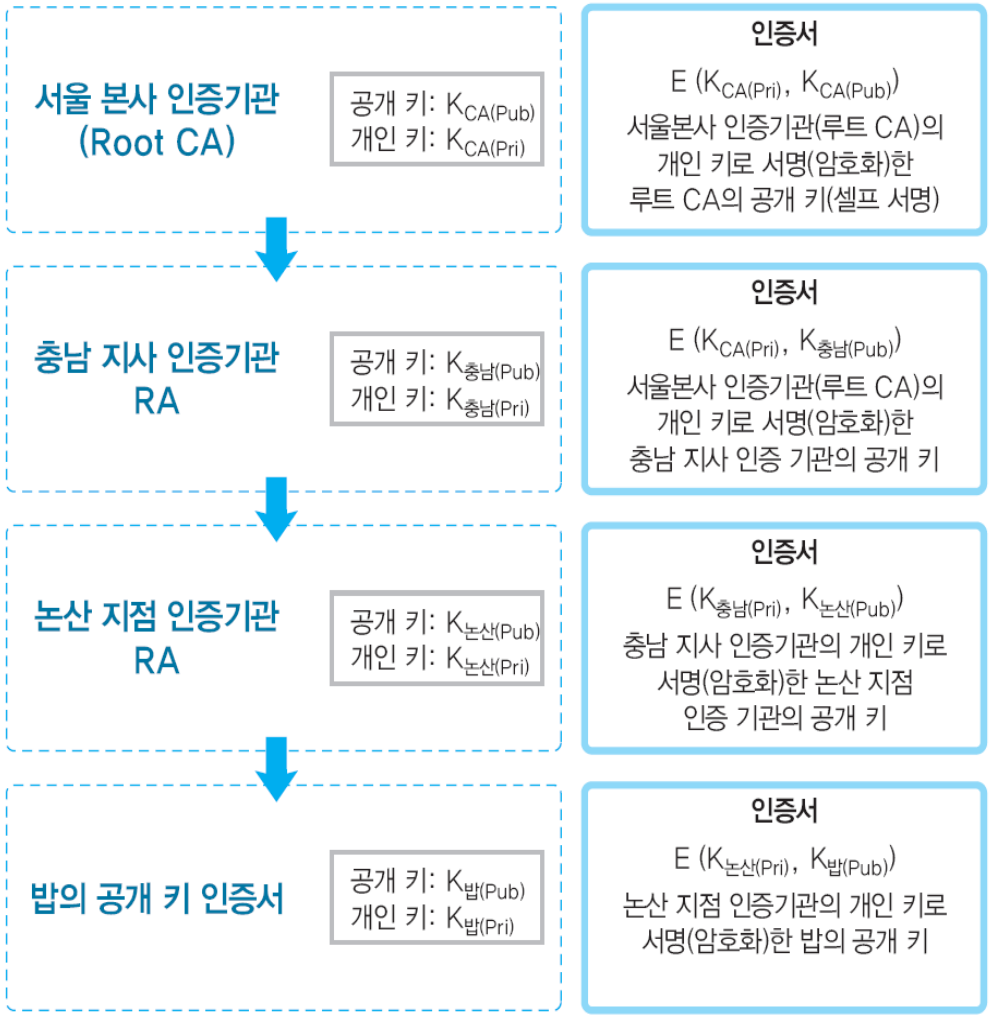
• 계층구조를 갖는 인증기관

- 루트 CA
  - 최상위 인증기관
- 셀프 서명(self-signature)
  - 자기 자신의 공개 키에 대해서 자신의 개인 키로 서명하는 디지털 서명

- 계층 구조를 갖는 인증서

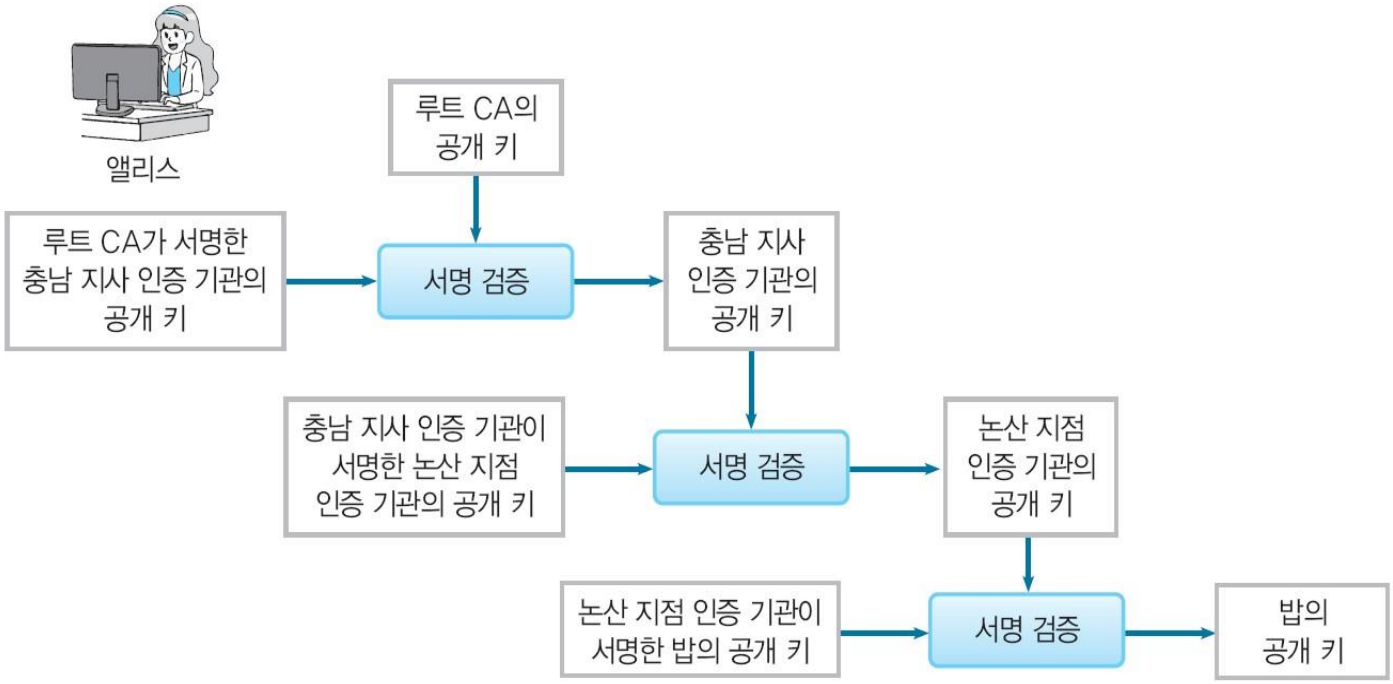


• 한국의 전자서명 인증관리 체계도



• 계층구조를 갖는 인증기관

– 예) 앨리스가 밥의 올바른 공개 키를 얻는 과정



• 앨리스가 밥의 바른 공개 키를 얻는 과정

- 다양한 **PKI**
  - 누구나 인증기관이 될 수 있고 실제로 세계에는 무수히 많은 인증기관이 존재
  - 사내 이용 방법
    - 인증기관의 계층을 회사의 조직 계층에 적용
    - 부서별로 PKI 운영하고 상호 인증
  - 우리나라 PKI
    - 한국인터넷진흥원 전자서명인증관리센터에서 관리
    - 인증기관의 계층이나, 운용 규약, 공개 키의 등록 · 인증서 발행 등을 규정