2010-1학기 현대암호학

제 10장 인증서

공개 키를 이용한 디지털 서명

박 종 혁

Tel: 970-6702
Email: jhpark1@snut.ac.kr

10.1 주요 내용

- 인증서 소개
- 인증서를 사용하는 시나리오
- 인증서 규격 X.509
- 인증서의 구체적인 내용
- 공개키기반구조(PKI; Public Key Infrastructure)
- 인증기관

10.1.1 인증서

- 인증서의 개념
- 왜 인증서를 우리가 신뢰하는가?
- 신뢰를 하기 위한 전제조건
- X.509
  - 인증서 관리와 찾기가 편리하도록 만든 인증 서비스 구조

인증서란 무엇인가?

- 공개 키 인증서에 포함되는 내용
  - 이름이나 소속
  - 메일 주소 등의 개인 정보
  - 그 사람의 공개 키

- **인증기관**(certification authority, certifying authority; CA)의 개인 키로 디지털 서명이 되어 있음

- 인증기관이 「이 공개 키는 확실히 이 사람의 것이다」라고 인정하는 수단

인증기관이란?

- 디지털 인증서를 발급할 수 있는 권한을 가지고 사용자의 요청에 따라 인증서를 발급하기관

- 인증서를 발급받은 사용자는 해당 인증서를 이용하여 인증을 요구하는 기관에 직접 출두하거나 신분증 등을 제시하지 않으면서도 온라인상에서 자신이 적법한자 임을 증명

- 인증서 속에 들어있는 것
  - 궁극적으로 사용자의 공개 키

10.1.2 X.509

- ITU-T 권고안 X.509는 디렉토리 서비스를 정의하는 권고안 X.500 시리즈의 한 부분
- X.500 디렉토리에서 사용자에게 제공되는 인증 서비스의 구조를 규정
  - 이 디렉토리를 공개키 인증서 저장소로 이용할 수도 있음
- 각 인증서 속에는 신뢰할만한 인증기관의 개인키로 서명된 사용자의 공개키가 포함되어 있음
- X.509는 공개키 인증서를 이용한 인증 프로토콜을 규정

10.1.3 인증서를 사용하는 시나리오

인증기관 트렌트를 이용해서 앨리스가 밥에게 암호문을 보내는 예

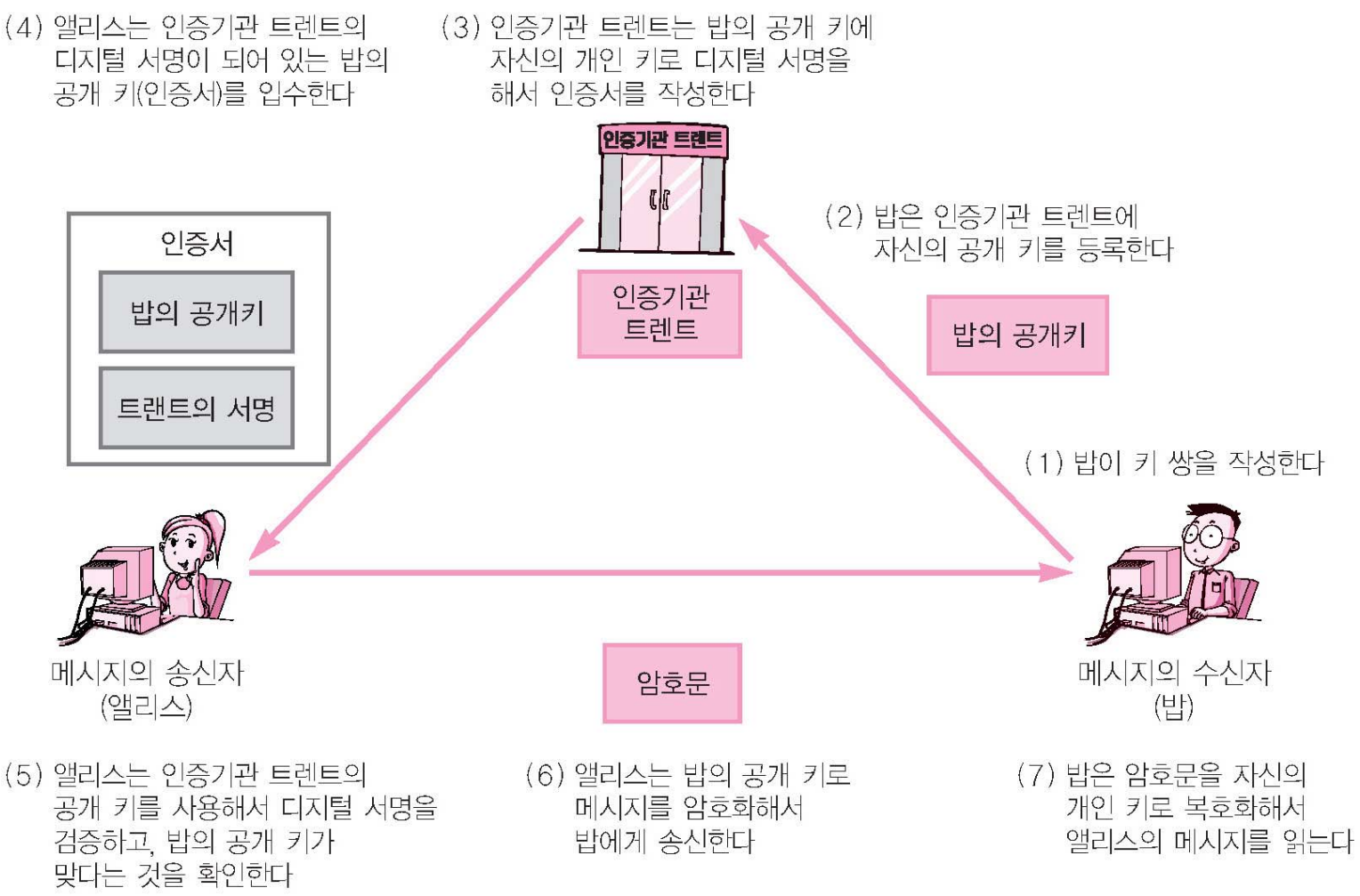


그림 10-1 인증기관 트렌트를 이용해서 앨리스가 밥에게 암호문을 보내는 예

10.2 인증서 만들기

- 한국전자인증의 무료 시험 서비스를 이용해서 클래스1에 해당되는 전자메일 인증서를 실제로 만들어 보자.

10.2.1 한국전자인증의 무료 시험 서비스

- e-메일 인증서(디지털 ID라 부르고 있다)를 60일간의 무료 시험판으로 만들어서 제공하는 서비스를 하고 있다.
- 웹 브라우저만 있으면 온라인에서 바로 발행할 수 있는 서비스이다.
- 본인 인증은 메일이 도착하는지의 여부만으로 확인한다(베리사인의 클래스1에 해당).

10.2.2 인증서의 작성

- 한국전자인증에 접속하고 글로벌인증서비스/인증서비스/e-mail 인증서/TRY IT(60일 무료)를 클릭한다.
- 다음과 같은 등록양식(그림 10-2)이 화면에 나타나게 된다.

한국전자인증의 e-mail 인증서 등록 양식

이름: * (필수사항) (예-GilDong)	
성: * (필수사항) (예 -- Hong)	
E-mail 주소: * (필수사항) (예 -- help@crosscert.com)	
구/군: * (예 -- Kangnamgu, Seochogu)	
시/도: * (예 -- Seoul, Pusan)	
국가: * (예 -- KR)	KR
주민등록번호: * (예 -- 7205051025427) "-"는 생략해 주십시오.	
연락가능 전화번호: * (예 -- 02-3019-5500)	

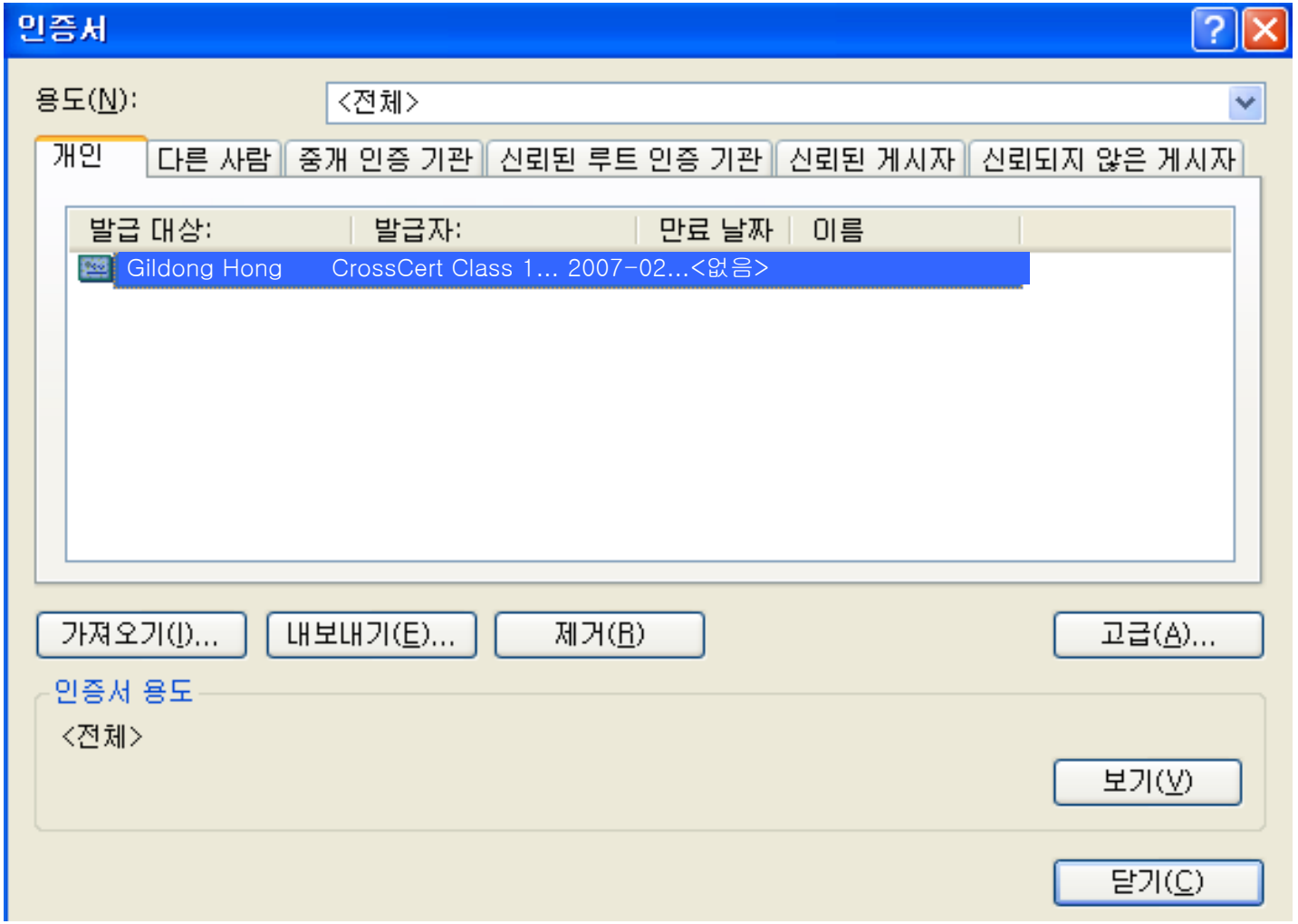
암호 이것은 디지털 ID를 처음 등록했을 때 선택했던 암호입니다. 이 암호는 귀하의 디지털 ID를 불법적인 행위로부터 보호하며, 다른 사람과 공유되지 않아야 합니다. 절대로 분실해서는 안됩니다! 이 암호는 귀하의 디지털 ID를 폐지(Revoke), 갱신(Renew)하는 데 필요합니다.	
암호를 입력하십시오.(필수사항) 특수문자를 사용해서는 안됩니다.	

그림 10-2 한국전자인증의 e-mail 인증서 등록양식

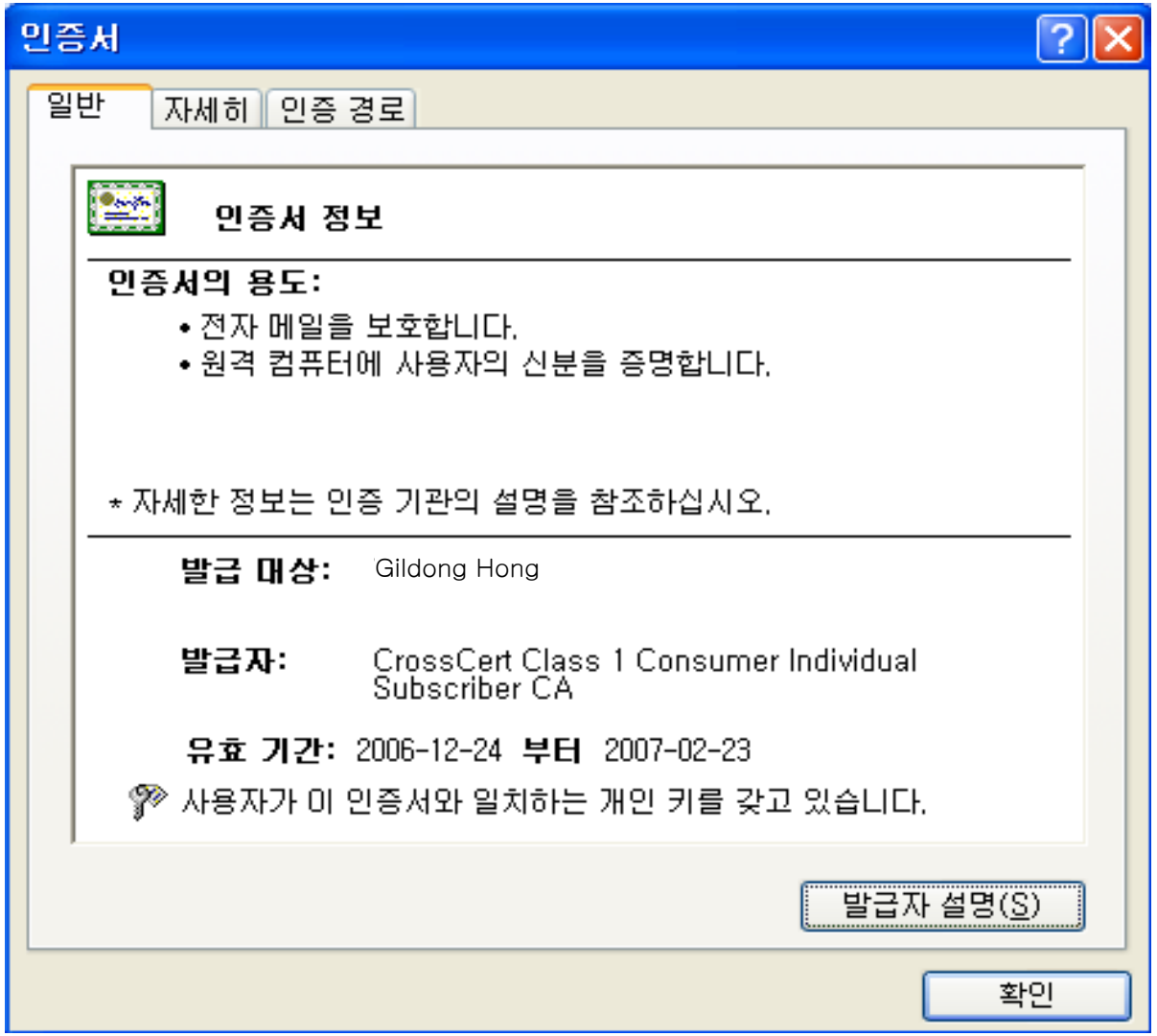
웹브라우저에 표시되는 내용

- Organization = KECA, Inc.
- Organizational Unit = CrossCert Class 1 Consumer Individual Subscriber CA
- Organizational Unit = Terms of use at www.crosscert.com/rpa (c)01
- Organizational Unit = Authenticated by CrossCert
- Organizational Unit = Member, VeriSign Trust Network
- Organizational Unit = Persona Not Validated
- Organizational Unit = Digital ID Class 1 - Netscape
- Common Name = GilDong Hong
- Email Address = gildong@novel.ac.kr

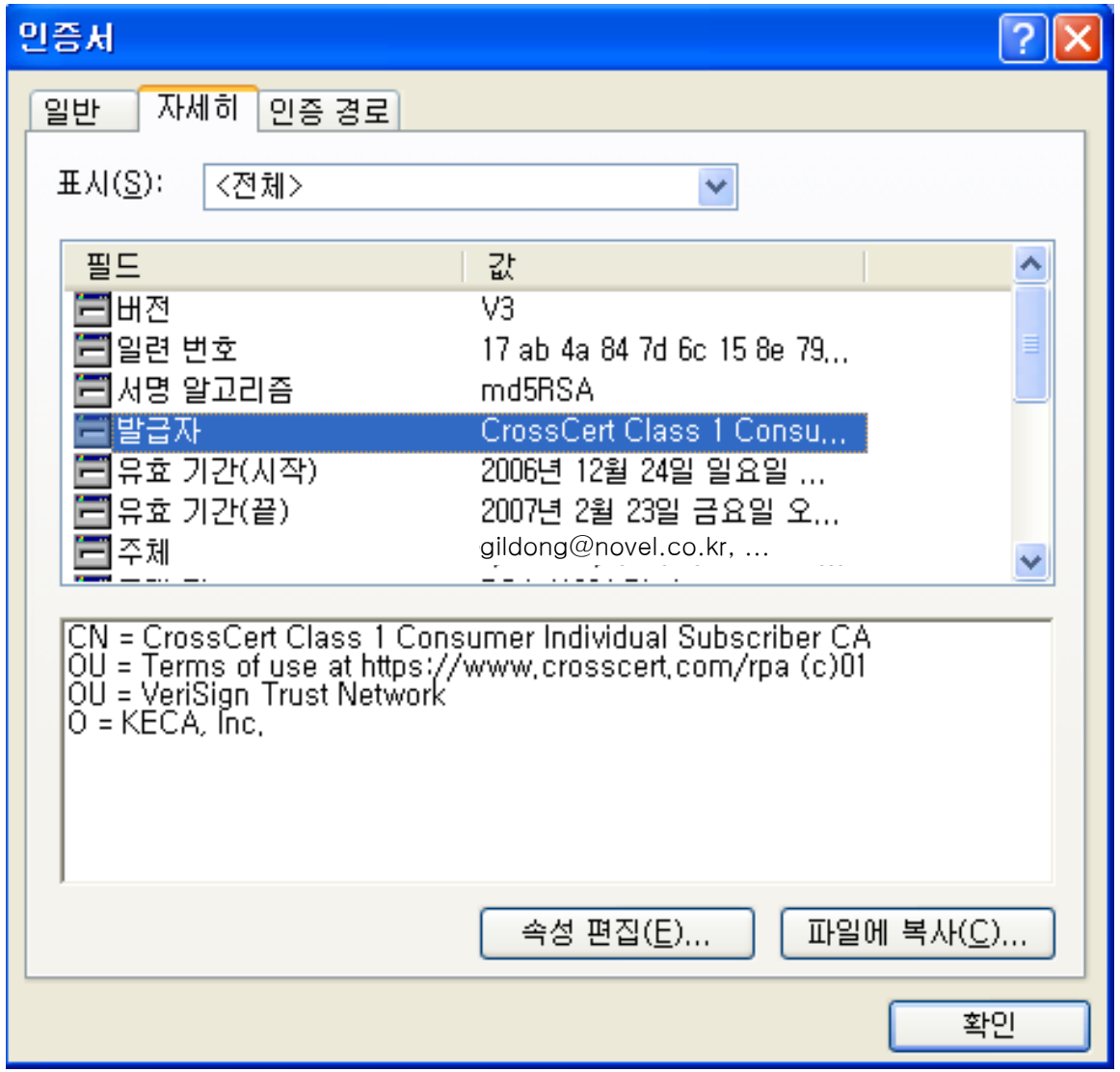
개인용 인증서


인증서
용도(N):
<전체>
개인
다른 사람
중개 인증 기관
신뢰된 루트 인증 기관
신뢰된 게시자
신뢰되지 않은 게시자
발급 대상:
발급자:
만료 날짜
이름
Gildong Hong
CrossCert Class 1... 2007-02...<없음>
가져오기(I)...
내보내기(E)...
제거(R)
고급(A)...
인증서 용도
<전체>
보기(V)
닫기(C)

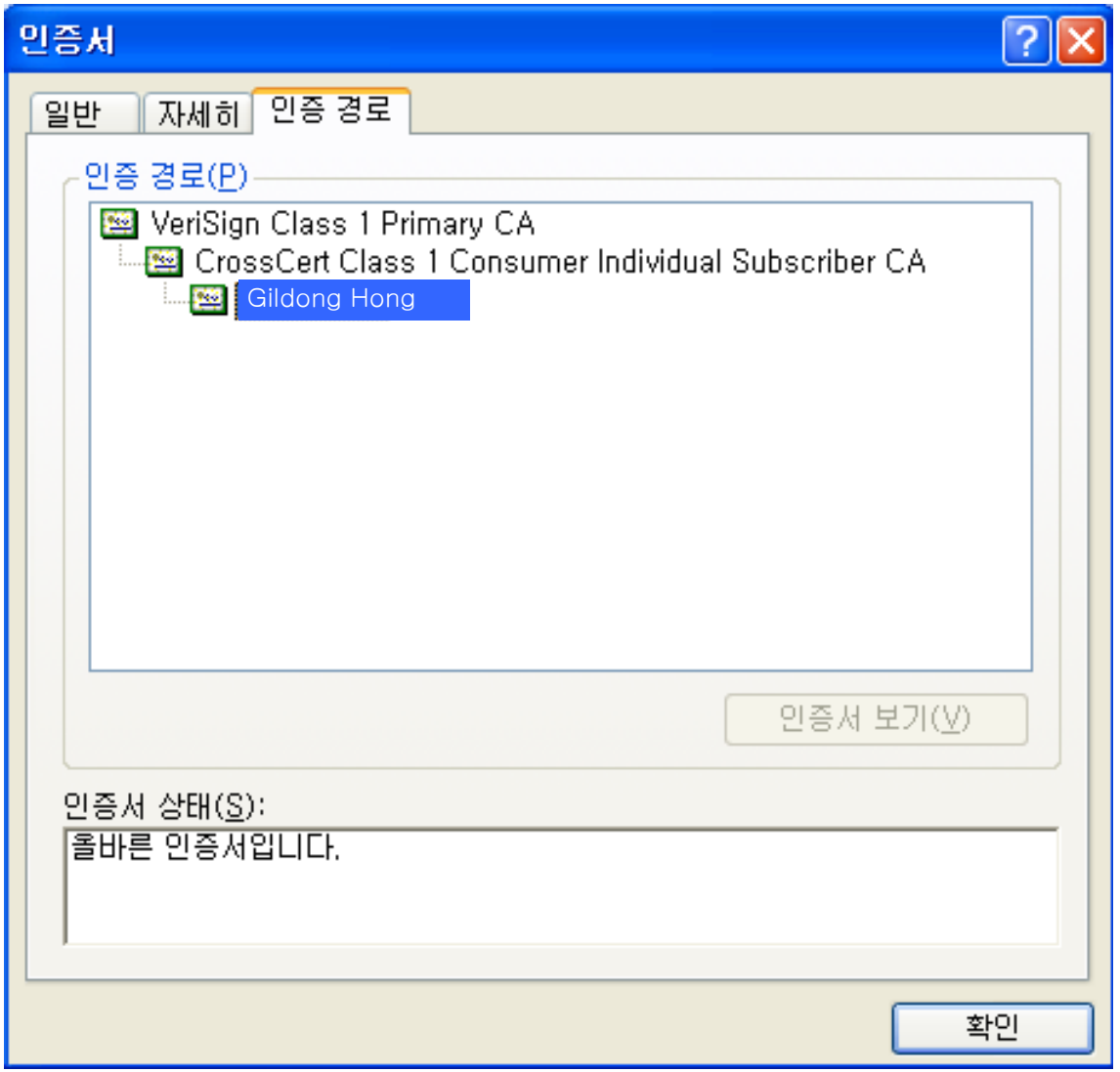
자세하게 내용을 표시


인증서
일반
자세히
인증 경로
인증서 정보
인증서의 용도:
• 전자 메일을 보호합니다.
• 원격 컴퓨터에 사용자의 신분을 증명합니다.
* 자세한 정보는 인증 기관의 설명을 참조하십시오.
발급 대상: Gildong Hong
발급자: CrossCert Class 1 Consumer Individual Subscriber CA
유효 기간: 2006-12-24 부터 2007-02-23
사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다.
발급자 설명(S)
확인

보다 자세하게 내용을 표시



인증서의 계층 표시


인증서
일반
자세히
인증 경로
인증 경로(P)
VeriSign Class 1 Primary CA
CrossCert Class 1 Consumer Individual Subscriber CA
Gildong Hong
인증서 보기(V)
인증서 상태(S):
올바른 인증서입니다.
확인

10.2.3 인증서 내보내기

- 홍길동의 인증서를 웹 브라우저로부터 내보내기를 하면 단독 파일로서 인증서를 꺼낼 수 있음
- 그 다음 인증서를 일반 편집기에서 읽어보면 다음과 같음

한국전자인증이 작성한 홍길동의 인증서

-----BEGIN CERTIFICATE-----
MIIE5TCCBE6gAwIBAgIQF6tKhH1sFY55TC7o6CZ9IzANBgkqhkiG9w0BAQQFADCBsjETMBEGA1UEChM
KS0VDQSwgSW5jLjEfMB0GA1UECxMWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazE8MDoGA1UECxMzVGV
ybXMgb2YgdXNlIGF0IGh0dHBzOi8vd3d3LmNyb3NzY2VydC5jb20vcnBhIChjKTAxMTwwOgYDVQQDEzN
Dcm9zc0NlcnQgQ2xhc3MgMSBDb25zdW1lciBJbmRpdmlkdWFsIFN1YnNjcmliZXIgQ0EwHhcNMDYxMjI0
MDAwMDAwWhcNMDcwMjIyMjM1OTU5WjCCAVUxEzARBgNVBAoUCktFQ0EsIEluYy4xPDA6BgNVBAsU
M0Nyb3NzQ2VydCBDbGFzcyAxIENvbnN1bWVyIEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTE0MDIGA1UE
CxMrVGVybXMgb2YgdXNlIGF0IHd3dy5jcm9zc2NlcnQuY29tL3JwYSAoYykwMTEjMCEGA1UECxMaQXV0
aGVudGljYXRlZCBieSBDcm9zc0NlcnQxJzAlBgNVBAsTHk1lbWJlciwgVmVyaVNpZ24gVHJ1c3QgTmV0d2
9yazEeMBwGA1UECxMVUGVyc29uYSBOb3QgVmFsaWRhdGVkMSYwJAYDVQQLEx1EaWdpdGFsIElEIElE
NsYXNzIDEgLSBOZXRzY2FwZTETMBEGA1UEAxMKVGFlSWwgSmVvbjEfMB0GCSqGSIb3DQEJARYQdG
lqZW9uQGRqdS5hYy5rcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA4whHBeppbO/ZjFmgefxKh
KVEkTuSTBwJTubG+4hnQj67/nV1uTiXNdxrIMoHLXH6+tUYUfT3taCHFx4IOsu+I/gWPakzGVM4RbfkijFIW
yas0GpGw1AttLK84Bb8lx05i72TDsGsQBA/4uhObiCIbKskucVbsfs/mhBGD6FXmyMCAwEAAaOCAVQwg
gFQMAkGA1UdEwQCMAAwbgYDVR0fBGcwZTBjoGGgX4ZdaHR0cDovL29uc2I0ZWNybC5jcm9zc2NlcN
QuY29tL0tFQ0FJbmNDcm9zc0NlcnRDbGFzczFDb25zdW1lckluZGl2aWR1YWxTdWJzY3JpYmVyQ0EvTG
F0ZXN0Q1JMMIGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsGAQUFBwIBFhx
odHRwczovL3d3dy52ZXJpc2lnbi5jb20vQ1BTMGIGCCsGAQUFBwICMFYwFRYOVmVyaVNpZ24sIEluYy4
wAwIBARo9VmVyaVNpZ24ncyBDUFMgaW5jb3JwLiBieSByZWZlcmVuY2UgbGlhYi4gbHRkLiAoYyk5NyB
WZXJpU2lnbjARBglghkgBhvhCAQEEBAMCB4AwEQYKYIZIAYb4RQEGCQQDAQH/MA0GCSqGSIb3DQE
BBAUAA4GBAGiQNr7YFsV0/FLHXrBDbgMlmuZebMvcwRHAKnDeuhlogPqb+iB/50f2ESGh5tkqPsSLg87
Z5Hc5wWEP5U8nlsHK9SlzjfBYSA51KA/2nhB2yo2NCQSE/aY4Xqn3Vi37qCPcpEVYvFQbF2fG2oprrg5x2
34gRVgMZ5feAIz7UeAE
-----END CERTIFICATE-----

10.2.4 인증서의 내용

- CertView라는 무료 소프트웨어를 사용하면 인증서의 내용을 자세히 표시할 수도 있다.

인증서의 상세한 내용 (CertView에 의한 표시)

```
Certificate :
    DATA :
        Version : 3
        SerialNumber : 17:ab:4a:84:7d:6c:15:8e:79:4c:2e:e8:e8:26:7d:23:
        Signature Algorithm: md5WithRSAEncryption
        Issuer  :
            O=KECA, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.crosscert.com/rpa (c)01,
CN=CrossCert Class 1 Consumer Individual Subscriber CA,
        Validity :
            notBefore : Dec 24 00:00:00 2006 UTC
            notAfter  : Feb 22 23:59:59 2007 UTC
        Subject :
            O=KECA, Inc., OU=CrossCert Class 1 Consumer Individual Subscriber CA, OU=Terms of use at
www.crosscert.com/rpa (c)01, OU=Authenticated by CrossCert, OU=Member, VeriSign Trust Network, OU=Persona Not
Validated, OU=Digital ID Class 1 - Netscape, CN=GilDong Hong, /Email=gildong@novel.ac.kr

        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    e3:08:47:05:ea:69:6c:ef:d9:8c:59:a0:79:fc:4a:84:a5:44:91:3b:
                    92:4c:1c:09:4e:e6:c6:fb:88:67:42:3e:bb:fe:75:75:b9:38:97:35:
                    dc:6b:20:ca:07:2d:71:fa:fa:d5:18:51:f4:f7:b5:a0:87:17:1e:08:
                    3a:cb:be:23:f8:16:3d:a9:33:19:53:38:45:b7:e4:8a:31:65:5b:26:
                    ac:d0:6a:46:c3:50:2d:b4:b2:bc:e0:16:fc:23:1d:39:8b:bd:93:0e:
                    c1:ac:40:10:3f:e2:e8:4e:6e:20:88:6c:ab:24:b9:c5:5b:b1:fb:3f:
                    9a:10:46:0f:a1:57:9b:23:
                Exponent:
                    00:01:00:01:

        X509v3 extensions:
            x509 Basic Constraints:
                CA:FALSE
                PathLenConstraint:NULL
            x509 CRL Distribution Points:
                [0] dist-point :
                    [0] fullName :
                        [6] http://onsitecrl.crosscert.com/KECAIncCrossCertClass1Consumer IndividualSubscriberCA/LatestCRL
            x509 Certificate Policies:
                policyID = 2.16.840.1.113733.1.7.1.1
                    qualifierID = pkix-id-qt CPSurl
                    qualifier = https://www.verisign.com/CPS
                    qualifierID = pkix-id-qt UserNotice
                    qualifier :
                        organization : VeriSign, Inc.
                        noticeNumbers : 1,
                        explicitText : VeriSign's CPS incorp. by reference liab. ltd. (c)97 VeriSign
Netscape Cert Type:
                SSL client, (0x80)
                2.16.840.1.113733.1.6.9:
                    01:01:ff:

                Signature Algorithm: md5WithRSAEncryption
                    68:90:36:be:d8:16:c5:74:fc:52:c7:5e:b0:43:6e:03:25:9a:
                    e6:5e:6c:cb:dc:c1:11:c0:2a:70:de:ba:12:28:80:fa:9b:fa:
                    20:7f:e7:47:f6:11:21:a1:e6:d9:2a:3e:c4:8b:83:ce:d9:e4:
                    77:39:c1:61:0f:e5:4f:27:22:c1:ca:f5:29:73:8d:f0:58:48:
                    0e:75:28:0f:f6:9e:10:76:ca:8d:8d:09:04:84:fd:a6:38:5e:
                    a9:f7:56:2d:fb:a8:23:dc:a4:45:58:bc:54:1b:17:67:c6:da:
                    8a:6b:ae:0e:71:db:7e:20:45:58:0c:67:97:de:00:8c:fb:51:
                    e0:04:
```

그림 10-8 인증서의 상세한 내용(CertView에 의한 표시)

인증서의 상세한 내용

- 버전(Version)
- 일련번호(Serial number)
- 서명 알고리즘 식별자(Signature algorithm identifier)
- 발행자 이름(Issuer name)
- 유효기간(Period of validity)
- 소유자 이름(Subject name)
- 소유자의 공개키 정보(Subject's public-key information)
- 발행자 유일 식별자(Issuer unique identifier)
- 소유자 유일 식별자(Subject unique identifier)
- 확장(Extensions)
- 서명(Signature)

10.2.5 인증서의 표준 규격 X.509

- 인증서의 형식 통일
  - 인증서는 인증기관에서 발행하고, 이용자가 그것을 검증하는 것이 되기 때문에 인증서의 형식이 서로 다르면 매우 불편

- 가장 널리 사용되고 있는 인증서의 표준 규격 ITU(International Telecommunication Union)나 ISO(International Organization for Standardization)에서 정하고 있는 X.509 규격

- X.509는 인증서의 작성/교환을 수행할 때의 표준 규격으로서 많은 애플리케이션에서 지원되고 있음

X.509의 인증서의 주요 세 부분

- 서명 전 인증서
  - 디지털 서명의 대상이 되는 정보
- 디지털 서명 알고리즘
  - 서명 전 인증서에 서명할 때에 사용하는 알고리즘
- 디지털 서명 본체
  - 서명 전 인증서에 한 디지털 서명 그 자체

인증서 규격 X.509 개요

표 10-1 인증서의 규격 X.509 개요(그림 10-7의 밥의 인증서와 대응)

서명 전 인증서	
규격의 버전	3
인증서의 일련 번호	17:ab:4a:84:7d:6c:15:8e:79:4c:2e:e8:e8:26:7d:23:
디지털 서명의 알고리즘	md5WithRSAEncryption
인증서의 발행자	CrossCert Class 1 Consumer Individual Subscriber CA
유효 기한의 개시	Dec 24 00:00:00 2006 UTC
유효 기한의 종료	Feb 22 23:59:59 2007 UTC
공개 키의 소유자	GilDong Hong, /Email=gildong@novel.ac.kr
공개 키의 알고리즘	rsaEncryption
공개 키 본체	RSA Public Key: (1024 bit) Modulus (1024 bit): e3:08:47:05:ea:69:6c:ef:d9:8c:59:a0:79:fc:4a:84:a5:44:91:3b: 92:4c:1c:09:4e:e6:c6:fb:88:67:42:3e:bb:fe:75:75:b9:38:97:35: dc:6b:20:ca:07:2d:71:fa:fa:d5:18:51:f4:f7:b5:a0:87:17:1e:08: 3a:cb:be:23:f8:16:3d:a9:33:19:53:38:45:b7:e4:8a:31:65:5b:26: ac:d0:6a:46:c3:50:2d:b4:b2:bc:e0:16:fc:23:1d:39:8b:bd:93:0e: c1:ac:40:10:3f:e2:e8:4e:6e:20:88:6c:ab:24:b9:c5:5b:b1:fb:3f: 9a:10:46:0f:a1:57:9b:23: Exponent: 00:01:00:01:
확장 항목(생략)	
디지털 서명 알고리즘	md5WithRSAEncryption
디지털 서명 본체	68:90:36:be:d8:16:c5:74:fc:52:c7:5e:b0:43:6e:03:25:9a: e6:5e:6c:cb:dc:c1:11:c0:2a:70:de:ba:12:28:80:fa:9b:fa: 20:7f:e7:47:f6:11:21:a1:e6:d9:2a:3e:c4:8b:83:ce:d9:e4: 77:39:c1:61:0f:e5:4f:27:22:c1:ca:f5:29:73:8d:f0:58:48: 0e:75:28:0f:f6:9e:10:76:ca:8d:8d:09:04:84:fd:a6:38:5e: a9:f7:56:2d:fb:a8:23:dc:a4:45:58:bc:54:1b:17:67:c6:da: 8a:6b:ae:0e:71:db:7e:20:45:58:0c:67:97:de:00:8c:fb:51: e0:04:

10.3 공개 키 기반구조(PKI)

- PKI: Public Key Infrastructure

- 인증서의 규격만으로는 공개 키의 실제로 운용하기에 불충분
  - 인증서를 누가 어떻게 만들었는지
  - 인증서를 무효는 어떻게 해야 하는지
  - 컴퓨터끼리 데이터를 교환할 때의 형식은 어떻게 하는 것인지

- 이 절에서는 공개 키를 효과적으로 사용하기 위한 PKI에 대해 설명 필요

10.3.1 공개 키 기반(PKI)

- 공개 키 기반구조(public-key infrastructure)
  - 공개 키를 효과적으로 운용하기 위해 정해진 많은 규격이나 선택 사양의 총칭
- 문서 RFC 2822(Internet Security Glossary)참조
- 이 문서는 공개키 기반구조(PKI: Public-Key Infrastructure)를 비대칭 암호시스템에 기초해서
  - 디지털 인증서 생성, 관리, 저장, 배분, 취소

  에 필요한 하드웨어, 소프트웨어, 사람, 정책 및 절차라고 정의

PKI를 개발하게 된 주요한 목적

- 안전하고, 편리하고, 효율적으로 공개키 획득

10.3.2 PKI 구성 요소

- 이용자
  - PKI를 이용하는 사람
- 인증기관
  - 인증서를 발행하는 사람
- 저장소
  - 인증서를 보관하고 있는 데이터베이스

PKI 구성 요소

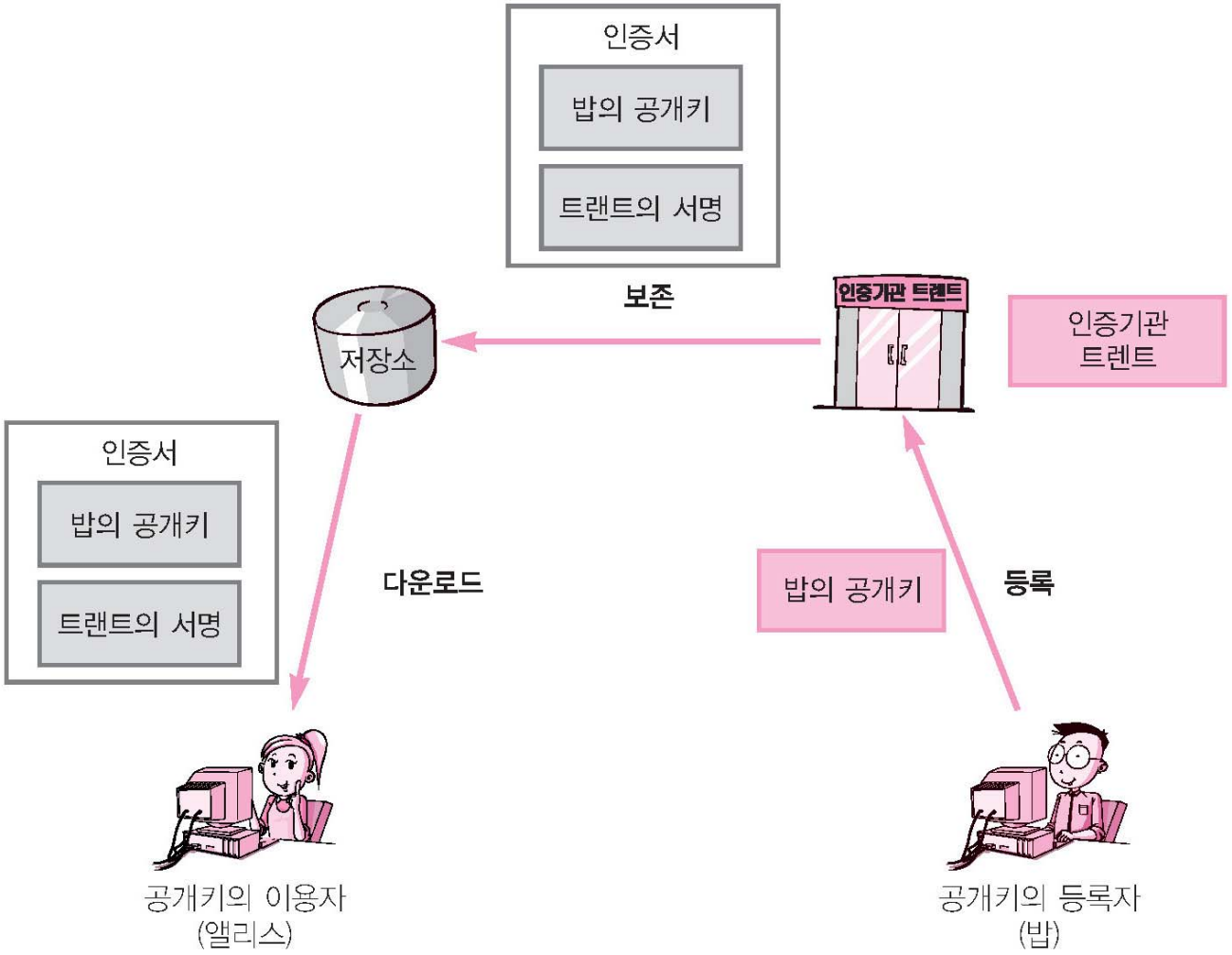


그림 10-9 PKI 구성 요소

이용자

- 공개 키를 등록하는 이용자가 행하는 것
  - 키 쌍 생성(인증기관이 작성하는 경우도 있음)
  - 인증기관에 공개 키를 등록
  - 인증기관으로부터 인증서를 발행
  - 필요할 경우 인증기관에 신청해서 등록한 공개 키를 무효로 함
  - 수신한 암호문을 복호화
  - 메시지에 디지털 서명

이용자

- 등록되어 있는 공개 키를 사용하는 이용자가 수행하는 것
  - 메시지를 암호화해서 수신자에게 송신
  - 디지털 서명을 검증

한국의 전자서명 인증관리 체계도

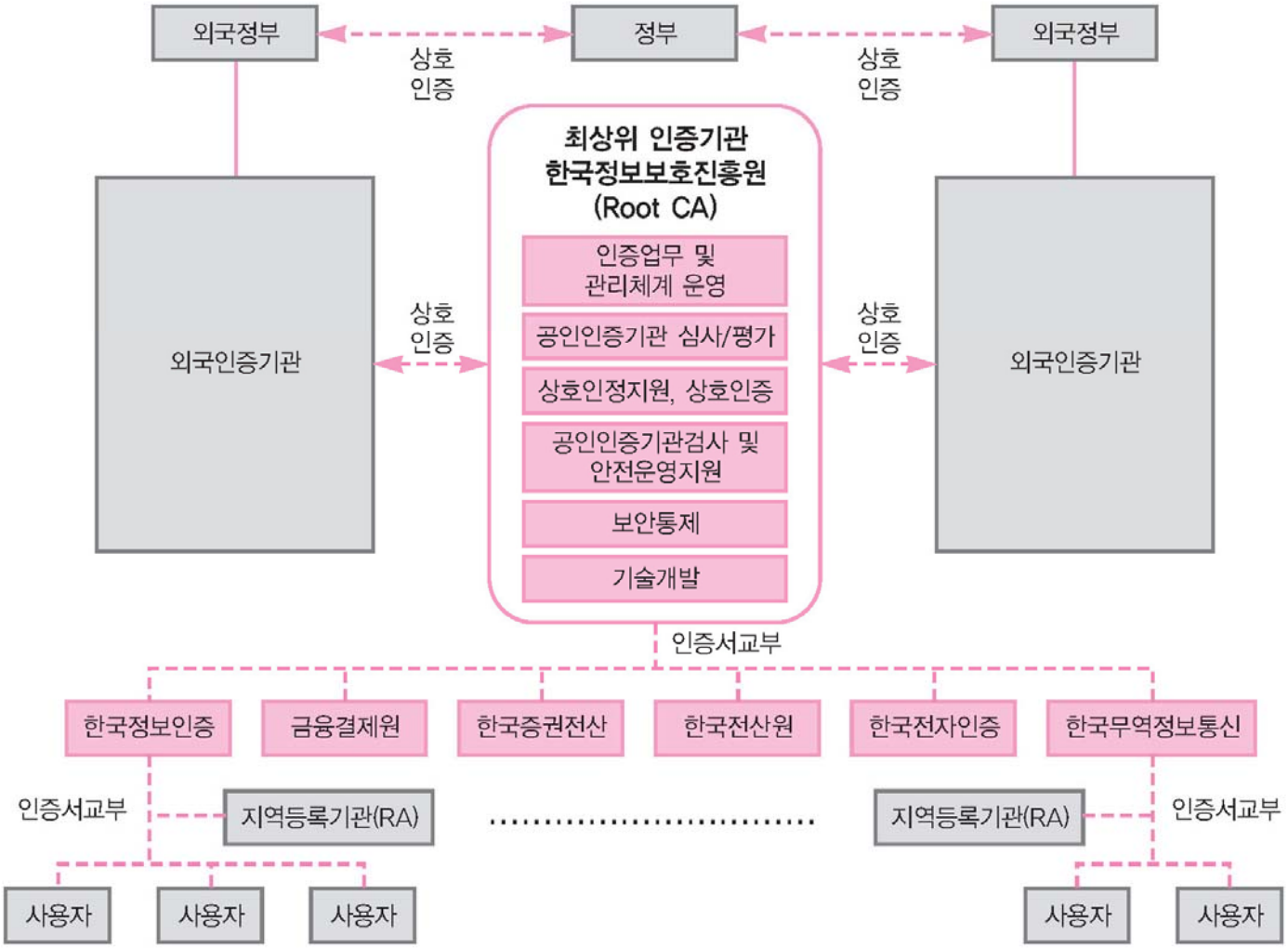


그림 10-10 한국의 전자서명 인증관리 체계도

인증기관(CA)

- 키 쌍의 작성
  - 이용자가 작성하는 경우도 있다
- 공개 키 등록 때 본인에 대한 인증
- 인증서 작성 및 발행
- 인증서 폐지

등록기관(registration authority; RA)

- 장점:
  - 인증기관의 일 중 「공개 키의 등록과 본인에 대한 인증」 대행을 분담
  - 등록기관에 일을 분담하면 인증기관은 인증서 발행에만 주력
  - 인증기관의 부담을 경감

- 단점
  - 인증기관은 등록기관 자체에 대한 추가 인증필요
  - 구성 요소확대로 주고받는 것이 복잡
  - 공격의 대상이 되는 지점의 수의 확대로 보안상 취약

저장소

- 인증서를 보존해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 한 데이터베이스
- 전화에 있어서 전화번호부와 같은 역할
- 앨리스가 밥의 인증서를 입수할 때 저장소를 이용할 수 있음
- 저장소는 인증서 디렉토리라 부르기도 함
  - Certificate Directory
  - Certificate Repository

10.3.3 PKIX 관리 기능

- 등록(Registration):
  - CA가 사용자에게 인증서를 발급하기 전에 사용자가 (직접적으로 혹은 RA를 통해서)최초로 CA에게 자신을 알리는 절차

- 초기화(Initialization):
  - 클라이언트 시스템을 안전하게 작동하기 전에 기반구조의 다른 곳에 저장된 키와 적절한 관계를 가지고 있는 키를 설치하는 것

PKIX 관리 기능

- 인증(Certification):
  - CA가 사용자에게 사용자의 공개키를 발급하고 인증서를 사용자의 클라이언트 시스템에 알려주고 자신의 저장소에 저장하는 절차

- 키 쌍 복구(Key pair recovery):
  - 한 쌍의 키를 이용해서 암호/복호화를 할 경우에 부득이하게 정상적인 키를 사용하는 것이 불가능 할 경우, 복호화 키를 획득할 수 있는 메커니즘 제공

PKIX 관리 기능

- 키 쌍 갱신(Key pair update):
  - 모든 키 쌍은 정기적으로 갱신하고 새로운 인증서를 발급받아야 함
  - 갱신은 인증서 유효기간이 종료될 때나 인증서가 취소될 경우에 필요한 절차
- 폐지 요청(Revocation request):
  - 사용자들은 공개 키 인증서를 사용하는 도중에 자신의 공개 키 인증서를 폐지해야 할 상황이 발생
  - 폐지 이유는
    - 개인키가 침해를 받았거나 가입 상태가 변경되었거나 이름이 변경될 경우 등
  - 이 경우에 폐지를 원하는 사용자는 CA로 하여금 인증서를 폐지하도록 요청할 수 있음

PKIX 관리 기능

- 교차 인증(Cross certification):
  - 두 개의 CA는 교차인증을 위해 정보를 교환
  - 교차인증이란 한 CA1이 다른 CA2에게 인증서를 발급해주는 것
  - CA1 자신의 공개 키를 CA1자신의 개인 키로 서명하여 보내는 것

PKIX 관리 프로토콜

- 관리 기능들을 지원하기 위해서 두 개의 대체가 가능한 PKIX 개체 사이의 관리 프로토콜을 정의
  - RFC 2510 문서에서는 인증서 관리 프로토콜(CMP: Certificate management protocol)을 정의
  - RFC 2797은 CMS 위에서 인증서 관리 메시지를 정의
    - CMS는 RFC 2630인 암호 메시지 구문(Cryptographic message syntax)을 나타낸다

10.3.4 인증기관의 역할

- 키 쌍의 작성
- 인증서 등록
- 인증서 폐지와 CRL

키 쌍의 작성

- 키 쌍을 작성 두 가지 방법
  - PKI의 이용자 스스로가 수행하는 경우
  - 인증기관이 수행하는 경우
    - 인증기관은 한 쌍의 공개 키와 개인키를 작성
    - 안전한 방법으로 「개인 키를 이용자에게 보내는」 일을 할 필요가 있다.
    - 그 방법은 PKCS #12(Personal Information Exchange Syntax Standard) 규격

인증서 등록

- 이용자 스스로가 키 쌍을 만들었을 경우
  - 이용자는 인증기관에 공개 키를 등록하기 위해서 해당 공개 키를 인증기관에 보내고 인증서 작성을 의뢰
- 인증서를 신청할 때의 규격
  - PKCS #10(Certification Request Syntax Standard)

인증서 폐지와 CRL

- 개인 키의 분실, 도난 등의 경우 인증기관은 인증서를 **폐지**(revoke)해서 무효화

- 개인 키가 제대로 관리되고 있어도 인증서를 폐지할 경우
  - 퇴직 등으로 인해 본인이 개인 키를 사용할 권한 상실
  - 이름이 바뀌어 인증서의 기재 내용과 맞지 않게 되었을 경우 등

인증서 폐지 목록(CRL)

- Certificate Revocation List (CRL)
  - 인증기관이 폐지한 인증서 목록

- 폐지된 인증서의 일련 번호의 목록에 대해 인증기관이 디지털 서명을 붙인 것
  - 인증서의 일련 번호:
    - 그 인증기관이 발행한 인증서에 붙여진 순서 번호
    - 인증서 속에 반드시 기재되어 있음

10.3.5 계층 구조를 갖는 인증서

- 디지털 서명 검증에 사용하는 인증기관의 공개 키는 어떻게 하면 「바르다」라고 판단할 수 있는 것일까?

- 이를 위해 인증기관의 공개 키에 대해 다른 인증기관이 디지털 서명을 하는 것으로 인증기관의 공개 키를 검증할 수가 있음

  ➔ 인증기관의 공개 키 인증서를 작성

인증서 체인(Chain of Certificate)

- 한 사용자가 다른 사용자의 인증서를 얻기 위해서는 연속된 인증절차를 거침

- 인증절차의 기본적인 요건
  - 각각의 CA가 발행한 다른 CA들에 대한 인증서들이 모두 디렉토리에 있어야 함
  - 사용자는 다른 사용자의 공개키 인증서에 이르는 경로를 따라가기 위해 어떻게 CA들이 연결되어 있는지를 알 필요가 있음

- X.509는 CA들을 계층구조(트리구조)로 만들어놓았기 때문에 탐색이 간단함

계층 구조를 갖는 인증기관

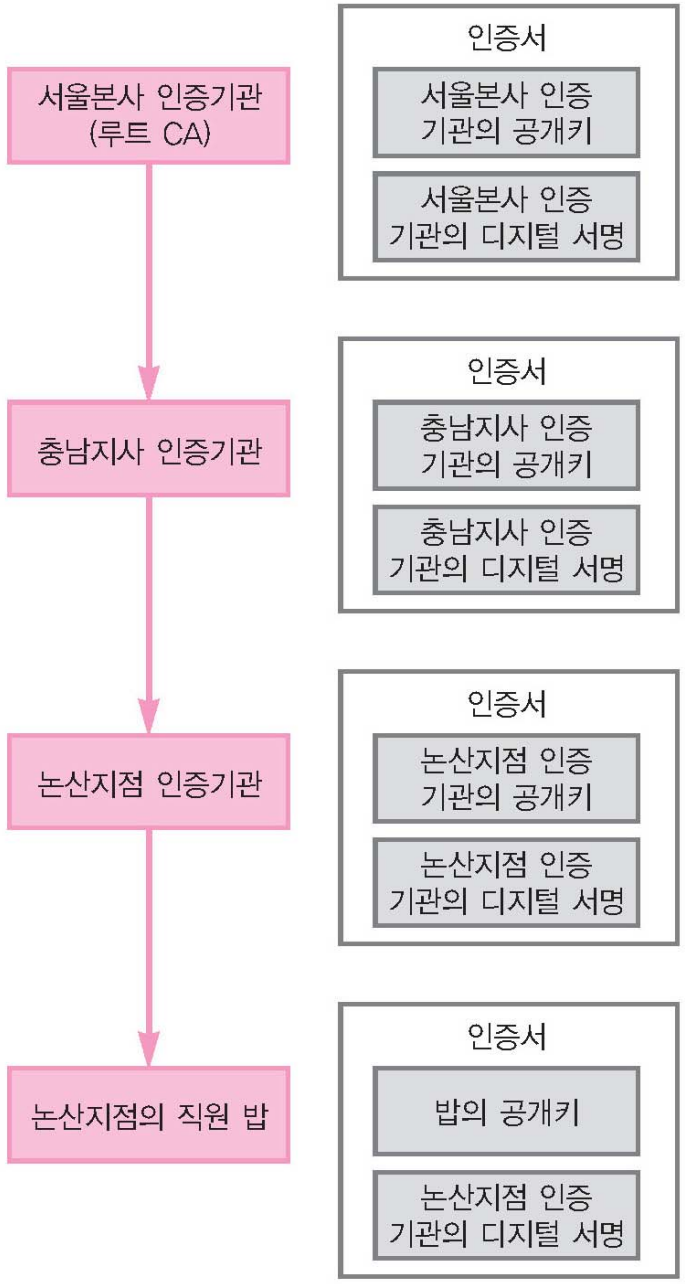


그림 10-11 계층 구조를 갖는 인증기관

10.3.6 다양한 PKI

- PKI라는 명칭으로부터 우리들은 종종 「권위 있는 인증기관이 공적으로 하나만 존재하고 있다」라고 생각
- 「전 세계의 공개 키는 단 하나의 루트 CA 하에서 인증된다」라고 생각하기 쉽다.
- 그러나 그것은 잘못된 생각이다.
- 실제로 세계에는 무수히 많은 인증기관이 있음

10.4 인증서에 대한 공격

- 인증서에는 디지털 서명이 사용되고 있기 때문에 디지털 서명에 대한 공격은 모두 인증서에 대해서도 위협이 됨

10.4.1 공개 키 등록 이전 공격

- 디지털 서명이 되기 전에 공개 키를 공격
  - 디지털 서명이 행하여진 후에는 공격하기 어려움

- 공격방법
  - 밥은 키 쌍을 만들어 공개 키를 인증기관에 등록하려고 한다.
  - 인증기관이 디지털 서명을 수행하기 이전에 적극적 공격자 맬로리가 공개 키를 자신의 것과 살짝 바꿔치기 한다.

- 방어방법
  - 밥이 공개 키를 인증기관에 등록할 때
    - 인증기관의 공개 키를 사용해서 밥의 공개 키를 암호화
  - 인증기관이 밥 본인을 확인할 때
    - 공개 키의 message digest도 함께 받아 밥을 확인

10.4.2 닮은 사람이 등록하는 공격

- 예를 들면 밥의 사용자 정보의 이름 부분이 다음과 같이 되어 있다고 하자.

  Name = Bob　　(첫 글자만 대문자)

여기에서 맬로리가

  Name = BOB　　(전부 대문자)

이라는 다른 사용자 정보를 갖는 공개 키를 인증기관에 등록

10.4.3 인증기관의 개인 키를 훔쳐 내는 방법

- 인증기관의 개인 키를 훔쳐내기
- 인증기관의 개인 키가 손에 들어오면 누구라도 그 인증기관이 발행하는 인증서를 만들 수 있게 된다.

10.4.4 공격자 자신이 인증기관이 되는 공격

- 적극적 공격자 맬로리는 자신이 인증기관이되어 인증서를 발급
- 인증기관이 된 맬로리는 자신의 공개 키라도 「이것은 밥의 공개 키이다」라고 주장하는 인증서를 자유롭게 발행
  - 그 인증서를 앨리스에게 보낼 수도 있음
- 인증기관을 신뢰할 수 없으면 인증서가 아무리 바르더라도 그 공개 키를 사용해서는 안됨

10.4.5 CRL의 허점을 찌르는 공격 (1)

- 공개 키가 무효가 되고나서 인증서 폐지 목록(CRL)이 앨리스에게 도착하기까지는 시간이 걸림

- 적극적 공격자 맬로리는
  - CRL이 도착할 때까지의 시간차를 이용한 빠른 공격을 시도

이런 공격에 대한 대책

- 공개 키가 무효가 되면 가능한 한 빨리 인증기관에 전한다(밥)
- CRL은 신속하게 발행한다(트렌트)
- CRL은 정확히 갱신한다(앨리스)
- 공개 키를 이용하기 전에는 공개 키가 무효가 되지 않았나를 재확인한다(앨리스)

10.5 인증서에 대한 Q&A

- 여기에서 인증서에 대한 이해를 높이기 위해 Q&A 형식으로 정리해 보자.

10.5.1 인증서의 필요성

- 의문
  - 인증서의 필요성을 모르겠다. 인증기관의 인증서를 사용해서 공개 키를 입수하는 것과, 공개 키만을 받는 것과는 같은 것이 아닌가?
- 답
  - 신뢰할 수 없는 경로(예를 들면 메일)로 공개 키를 입수하는 경우에는, 앞에서 말한 것 같은 중간자(man-in-the-middle)공격이 가능해 진다.
  - 앨리스는 밥의 공개 키라고 생각했는데, 실은 입수한 것이 적극적 공격자 맬로리의 공개 키일지도 모른다.

- 신뢰할 수 있는 공개 키를 입수할 수 있다면 인증기관은 불필요하다.

- 신뢰할 수 있는 인증기관의 공개 키를 가지고 있고, 인증기관의 본인 확인을 신뢰한다면, 그 인증기관이 발행한 인증서에 의해 입수한 공개 키는 신용할 수 있다.

10.5.3 인증기관에 대한 신뢰

- 의문
  - 인증기관의 기능은 대강 이해를 했지만, 결국 맴도는 것 같은 느낌이 든다.
  - 공개 키를 신뢰하기 위해서는 인증서를 발행한 인증기관을 신뢰해야 하는데, 그렇다면 인증기관은 어떻게 신뢰하는 것일까?
  - 다른 인증기관에 의한 인증서가 있다고 하더라도, 이번에는 그 인증기관을 어떻게 신뢰할까라고 하는 문제가 생기는 것은 아닌가?

- 답
  - 이 의문은 정당하다.
  - 어떻게 해서 우리들이 은행에 돈을 맡길 수 있는 것인가, 지갑에 들어있는 지폐를 가게에서 사용할 수 있다고 생각하는 것은 왜인가, 레스토랑에서 나오는 음식을 먹어도 안전하다고 생각하는 것은 왜인가와 같은 질문이다.
  - 인증기관을 신뢰하는 이유는 복수의 신뢰할 수 있는 정보원으로부터 얻은 정보에 근거하고 있는 것이다.

질의 및 응답

– 끝–