제 11 장
인증서

박 종 혁 교수

Tel: 970-6702

Email: jhpark1@seoultech.ac.kr

1절 인증서

2절 인증서 만들기

3절 공개 키 기반 구조 (PKI)

4절 인증서에 대한 공격

5절 인증서에 대한 Q&A

제1절 디지털 서명

1.1 인증서란 무엇인가?

1.2 인증서를 사용하는 시나리오

1.1 인증서란 무엇인가?

- 공개 키 인증서(public-key certificate; PKC)
  - 이름이나 소속, 메일 주소 등의 개인 정보
  - 당사자의 공개 키가 기재
  - **인증기관**(CA; certification authority, certifying authority)의 개인 키로 디지털 서명

1.2 인증서를 사용하는 시나리오

1) 밥이 키 쌍을 작성한다
2) 밥은 인증기관 트렌트에 자신의 공개 키를 등록한다
3) 인증기관 트렌트는 밥의 공개 키에 자신의 개인 키로 디지털 서명을 해서 인증서를 작성한다
4) 앨리스는 인증기관 트렌트의 디지털 서명이 되어 있는 밥의 공개 키(인증서)를 입수한다
5) 앨리스는 인증기관 트렌트의 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

인증기관 트렌트를 이용해서 앨리스가 밥에게 암호문을 보내는 예

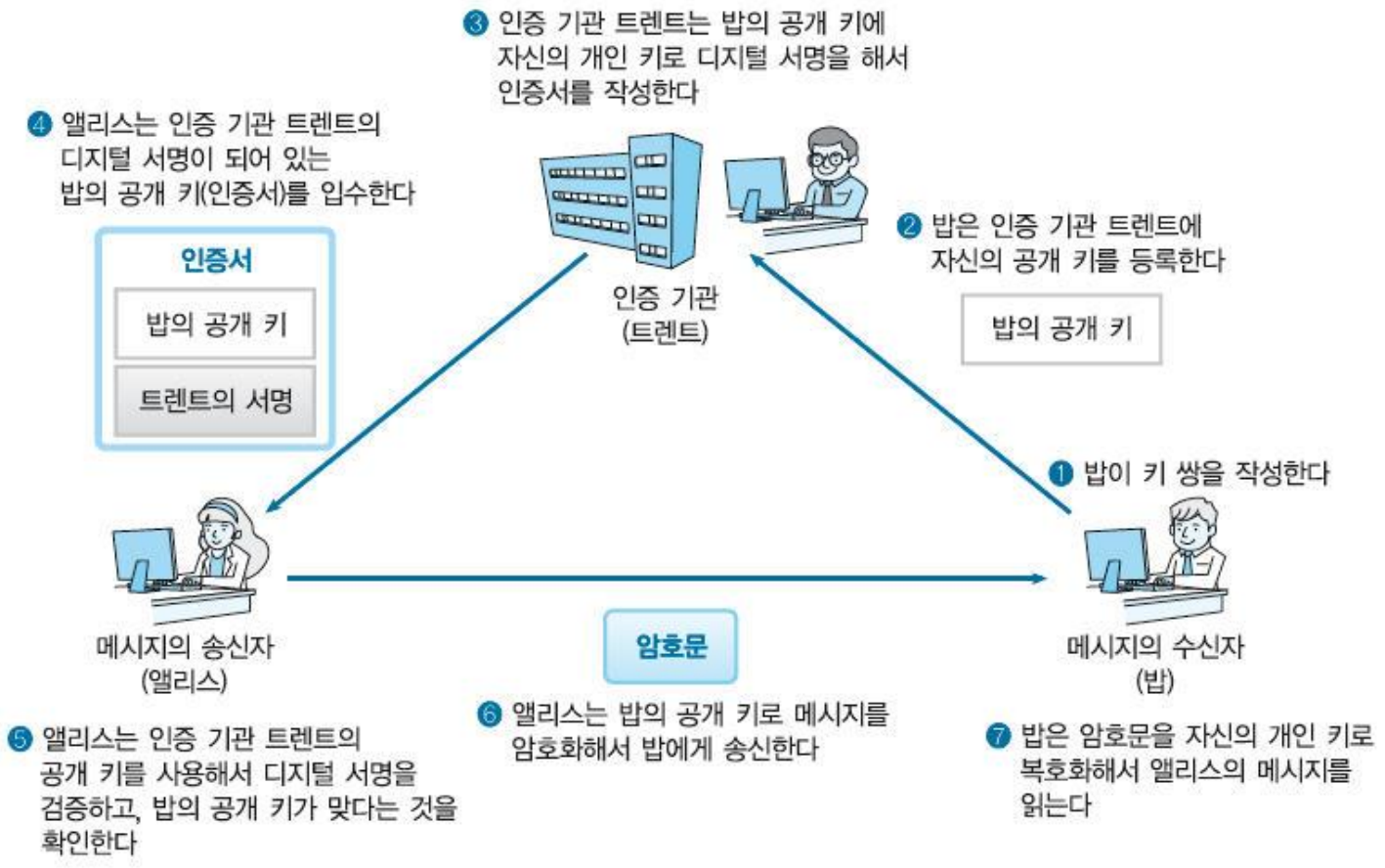


그림 11-1 • 인증 기관 트렌트를 이용해서 앨리스가 밥에게 암호문을 보내는 예

제2절 인증서 만들기

2.1 베리사인의 무료 시험 서비스

2.2 인증서의 작성

2.3 인증서를 웹 브라우저로부터 내보내기

2.4 인증서의 내용

2.5 인증서의 표준 규격 X.509

2.1 베리사인의 무료 시험 서비스

- 개인을 위한 인증서(디지털 ID라 부르고 있다)를 60일간의 무료 시험판으로 만들어서 제공하는 서비스
- 웹 브라우저만 있으면 온라인에서 바로 발행할 수 있는 서비스
- 본인 인증은 메일이 도착하는지의 여부만으로 확인

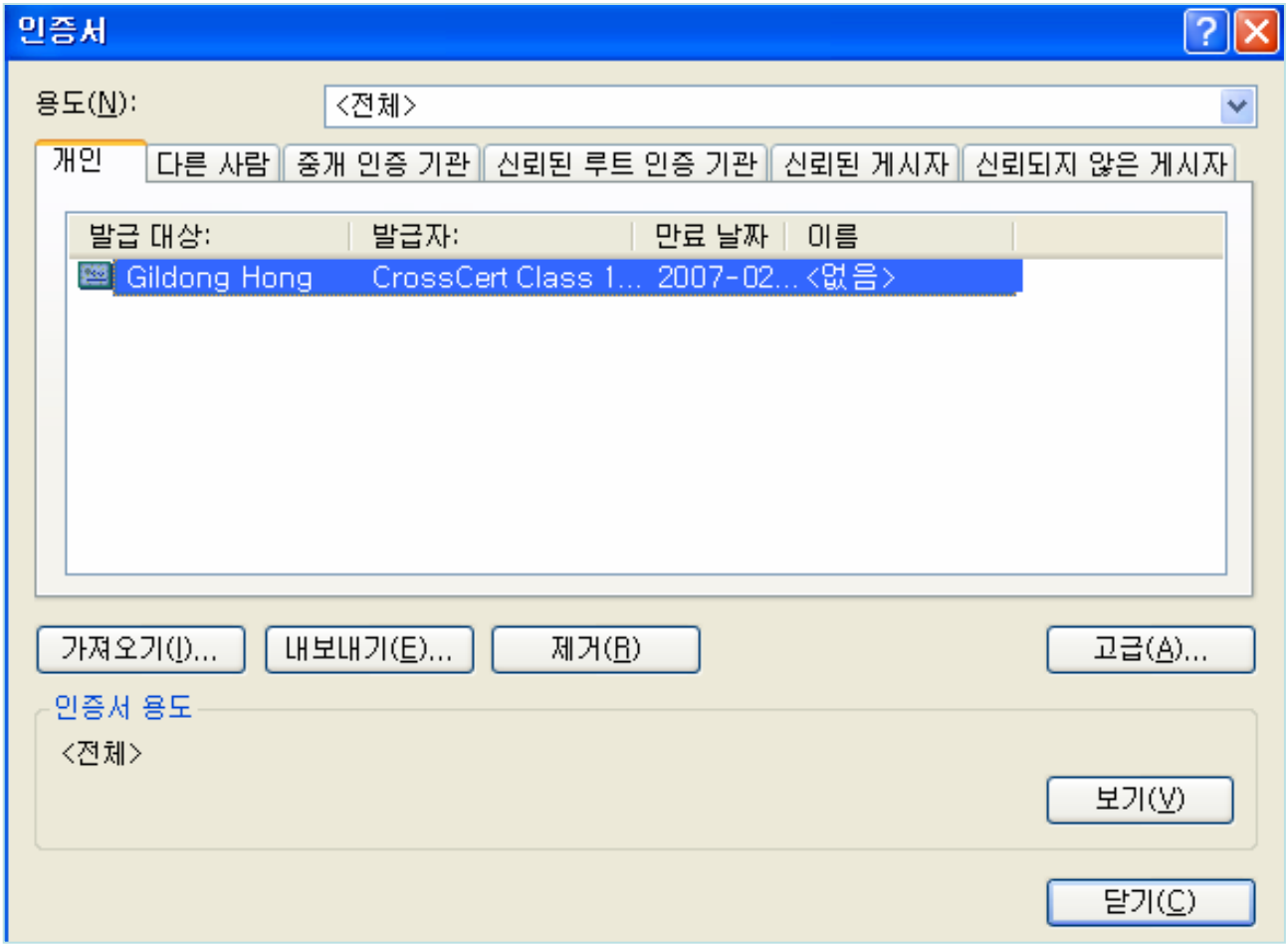
2.2 인증서의 작성

- SSL로 보호된 웹 사이트에서 다음의 정보를 입력하고 인증서를 작성
  - 이름: Gil Dong Hong
  - 메일 주소: gildong@novel.ac.kr
  - 패스워드: xxxxxxxx

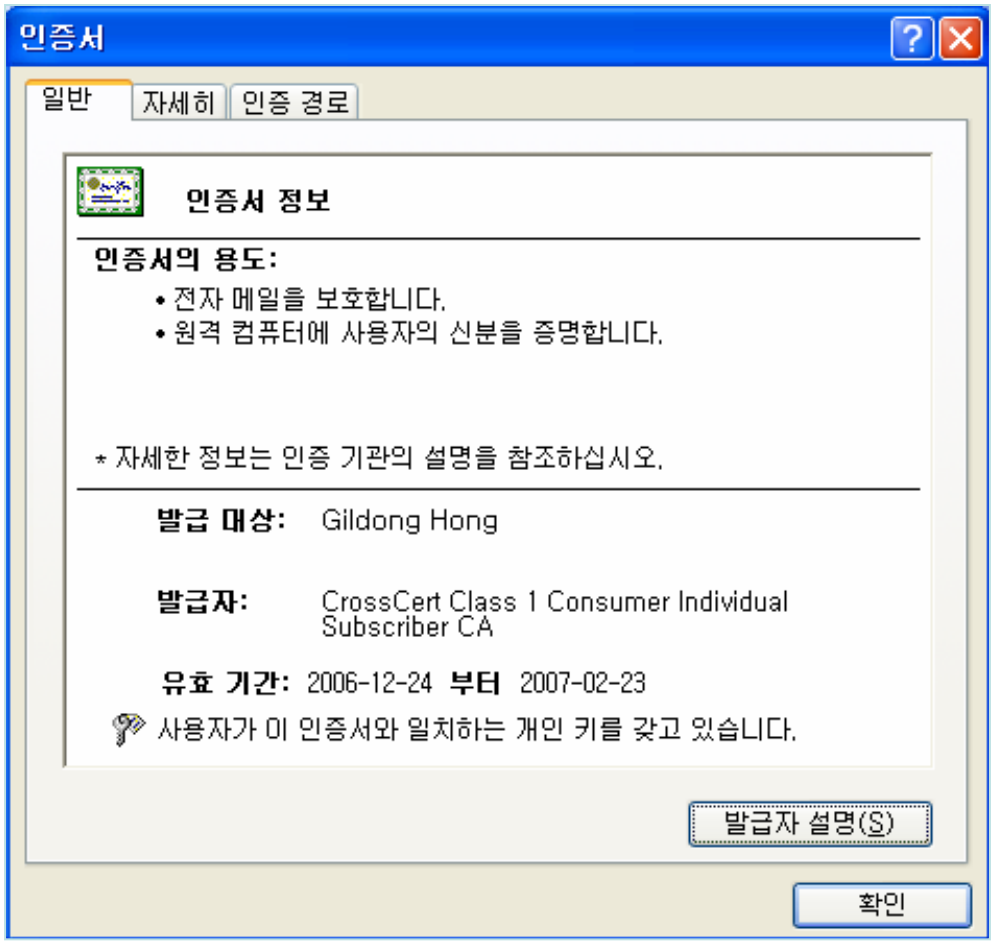
웹 브라우저에 표시되는 내용

- 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 = Gil Dong Hong
- Email Address = gildong@novel.ac.kr

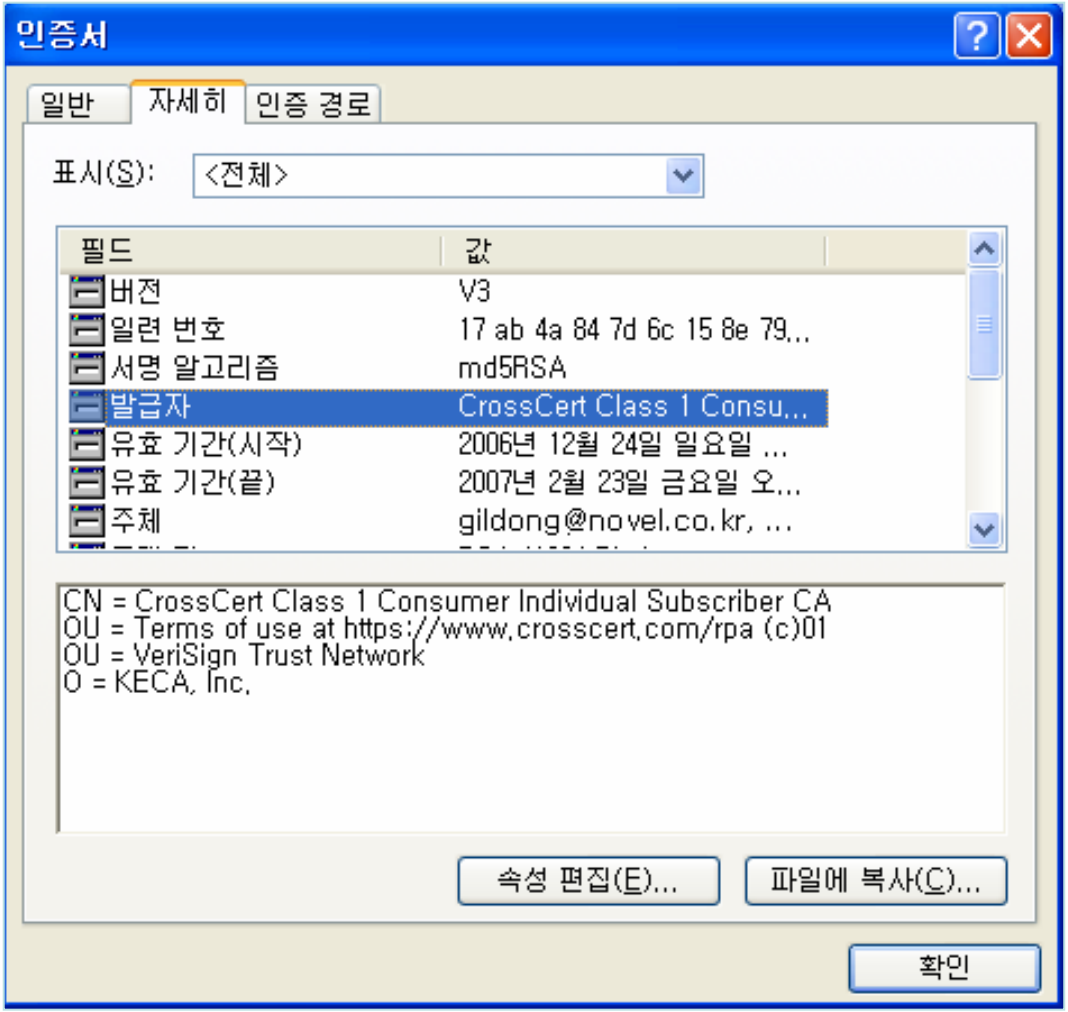
개인용 인증서


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)

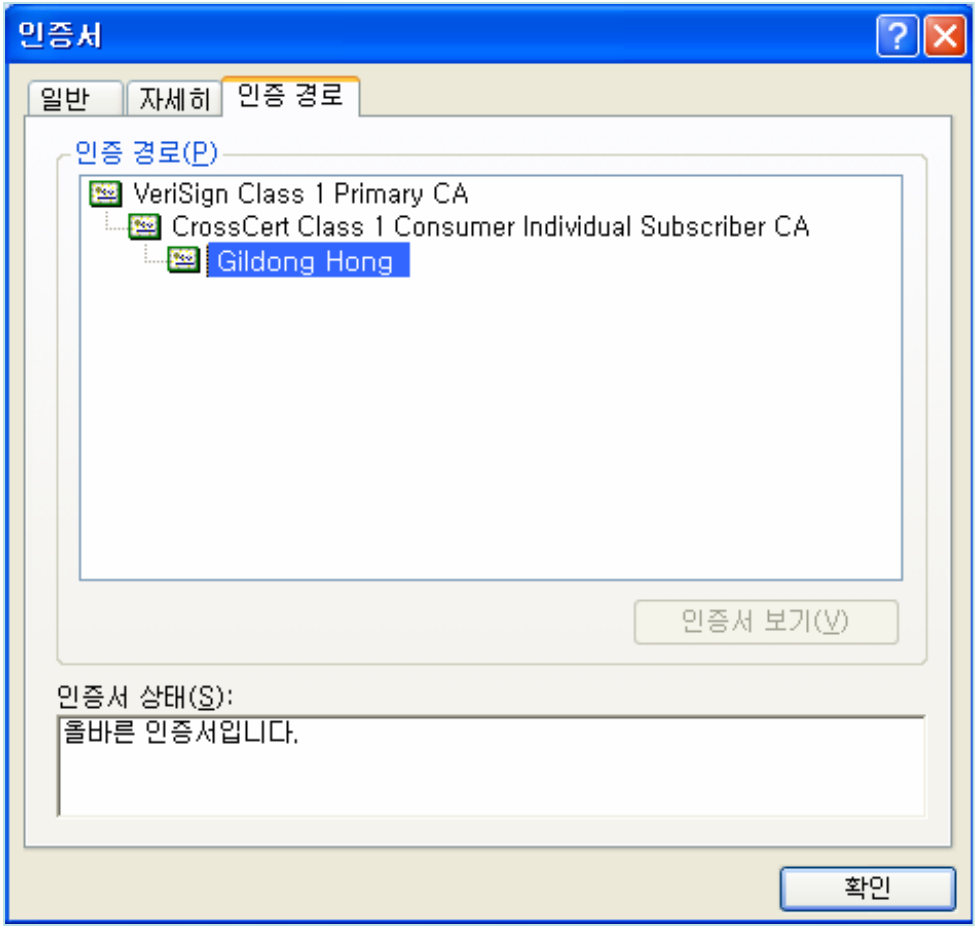
자세하게 내용을 표시


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

2.3 인증서를 웹 브라우저로부터 내보내기

- 홍길동의 인증서를 웹 브라우저로부터 내보내기를 하면 단독 파일로서 인증서를 꺼낼 수 있다

한국전자인증이 작성한 밥의 인증서

-----BEGIN CERTIFICATE-----
MIIE5TCCBE6gAwIBAgIQF6tKhH1sFY55TC7o6CZ9lzANBgkqhkiG9w0BAQQFADCBsjETMBEGA1UEChMKS0VDQSwgSW5jLjEfMB0GA1UECx
MWVmVyaVNpZ24gVHJ1c3QgTmV0d29yazE8MDoGA1UECxMzVGVybXMgb2YgdXNlIGF0IGh0dHBzOi8vd3d3LmNyb3NzY2VydC5jb20vcnBhl
ChjKTAxMTwwOgYDVQQDEzNDcm9zc0NlcnQgQ2xhc3MgMSBDb25zdW1lciBJbmRpdmlkdWFsIFN1YnNjcmliZXIgQ0EwHhcNMDYxMjI0MDA
wMDAwWhcNMDcwMjIyMjM1OTU5WjCCAVUxEzARBgNVBAoUCktFQ0EsIEluYy4xPDA6BgNVBAsUM0Nyb3NzQ2VydCBDbGFzcyAxIENvbnN1
bWVyIEluZGl2aWR1YWwgU3Vic2NyaWJlciBDQTE0MDIGA1UECxMrVGVybXMgb2YgdXNlIGF0IHd3dy5jcm9zc2NlcnQuY29tL3JwYSAoYykwM
TEjMCEGA1UECxMaQXV0aGVudGljYXRlZCBieSBDcm9zc0NlcnQxJzAlBgNVBAsTHk1lbWJlciwgVmVyaVNpZ24gVHJ1c3QgTmV0d29yazEeM
BwGA1UECxMVUGVyc29uYSBOb3QgVmFsaWRhdGVkMSYwJAYDVQQLEx1EaWdpdGFsIElEIENsYXNzIDEgLSBOZXRzY2FwZTETMBEGA1U
EAxMKVGFlSWwgSmVvbjEfMB0GCSqGSIb3DQEJARYQdGlqZW9uQGRqdS5hYy5rcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA4wh
HBeppbO/ZjFmgefxKhKVEkTuSTBwJTubG+4hnQj67/nV1uTiXNdxrIMoHLXH6+tUYUfT3taCHFx4lOsu+l/gWPakzGVM4RbfkijFlWyas0GpGw1A
ttLK84Bb8lx05i72TDsGsQBA/4uhObiClbKskucVbsfs/mhBGD6FXmyMCAwEAAaOCAVQwggFQMAkGA1UdEwQCMAAwbgYDVR0fBGcwZTBj
oGGgX4ZdaHR0cDovL29uc2l0ZWNybC5jcm9zc2NlcnQuY29tL0tFQ0FJbmNDcm9zc0NlcnRDbGFzczFDb25zdW1lckluZGl2aWR1YWxTdWJz
Y3JpYmVyQ0EvTGF0ZXN0Q1JMMIGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsGAQUFBwIBFhxodHRwczovL3d3
dy52ZXJpc2lnbi5jb20vQ1BTMGIGCCsGAQUFBwICMFYwFRYOVmVyaVNpZ24sIEluYy4wAwIBARo9VmVyaVNpZ24ncyBDUFMgaW5jb3JwLiBi
eSByZWZlcmVuY2UgbGlhYi4gbHRkLiAoYyk5NyBWZXJpU2lnbjARBglghkgBhvhCAQEEBAMCB4AwEQYKYIZIAYb4RQEGCQQDAQH/MA0GC
SqGSIb3DQEBBAUAA4GBAGiQNr7YFsV0/FLHXrBDbgMlmuZebMvcwRHAKnDeuhlogPqb+iB/50f2ESGh5tkqPsSLg87Z5Hc5wWEP5U8nlsHK
9SlzjfBYSA51KA/2nhB2yo2NCQSE/aY4Xqn3Vi37qCPcpEVYvFQbF2fG2oprrg5x234gRVgMZ5feAlz7UeAE
-----END CERTIFICATE-----

2.4 인증서의 내용

- 특정 소프트웨어를 사용하면 인증서의 내용을 자세히 표시할 수도 있다
  - X.509인증서 구조
    - 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

인증서의 상세한 내용 (1/3)

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):

인증서의 상세한 내용 (2/3)

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/KECAIncCrossCertClass1ConsumerIndividualSubscriberCA/LatestCRL
x509 Certificate Policies:
policyID = 2.16.840.1.113733.1.7.1.1

인증서의 상세한 내용 (3/3)

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:

2.5 인증서의 표준 규격 X.509

- X.509
  - ITU(International Telecommunication Union)나 ISO(International Organization for Standardization)에서 정하고 있는 규격

인증서의 규격 X.509 개요

서명 전 인증서	
규격의 버전	3
인증서 일련 번호	17:ab:4a:84:7d:6c:15:8e:79:4c:2e:e8:e8:26:7d:23:
디지털 서명 알고리즘	md5WithRSAEncryption
인증서의 발행자	CrossCert Class 1 Consumer Individual Subscriber CA
유효 기한 개시	Dec 24 00:00:00 2006 UTC
유효 기한 종료	Feb 22 23:59:59 2008 UTC
공개 키의 소유자	GilDong Hong, /Email=gildong@novel.ac.kr
공개 키 알고리즘	rsaEncryption
공개 키	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	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:

제3절 공개 키 기반 구조 (PKI)

3.1 공개 키 기반 구조(PKI)

3.2 PKI 구성 요소

3.3 인증 기관의 역할

3.4 계층 구조를 갖는 인증서

3.1 공개 키 기반 구조(PKI)

- 공개 키 기반(public-key infrastructure)
  - 공개 키를 효과적으로 운용하기 위해 정한 많은 규격이나 선택사양의 총칭
    - PKCS(Public-Key Cryptography Standards)
      - RSA사가 정하고 있는 규격의 집합
    - RFC(Requests for Comments) 중에도 PKI에 관련된 문서
      - 인터넷의 선택사양을 정한다
    - X.509
    - API(Application Programming Interface) 사양서

3.2 PKI 구성 요소

- 이용자:
  PKI를 이용하는 사람

- 인증 기관:
  인증서를 발행하는 사람

- 저장소:
  인증서를 보관하고 있는 데이터베이스

PKI 구성 요소

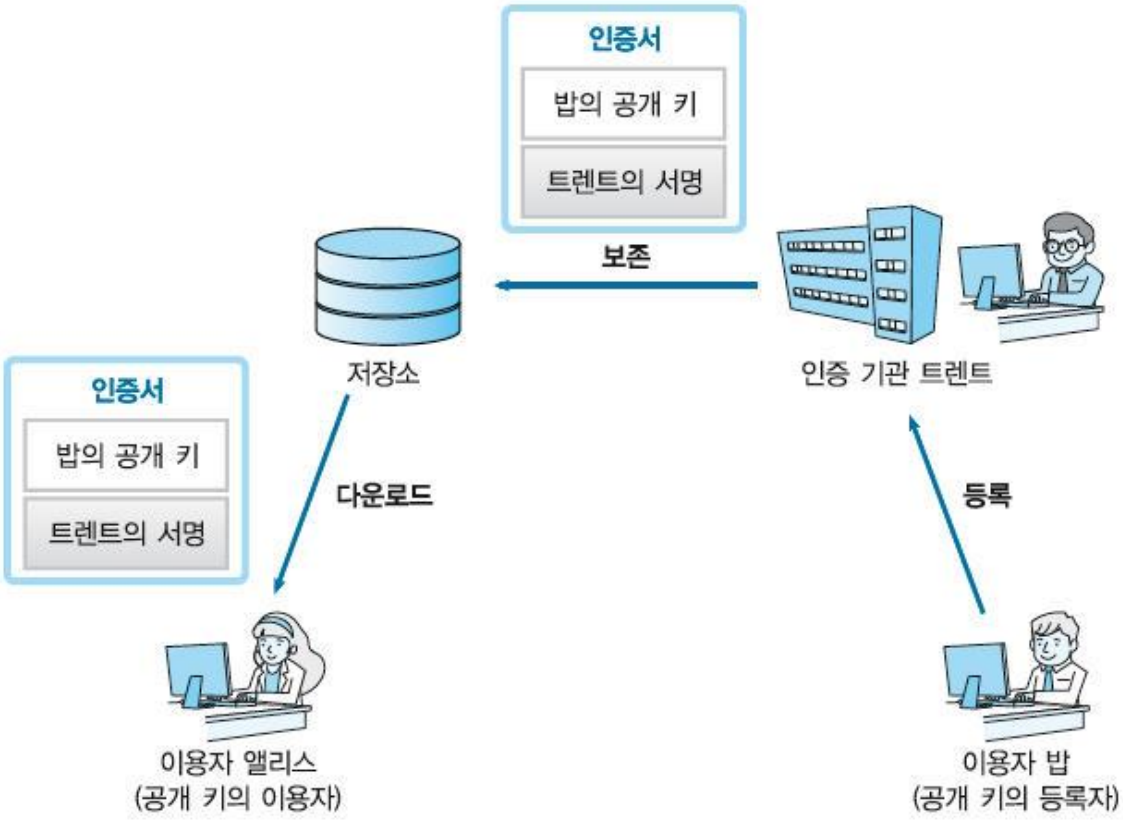


그림 11-8 • PKI 구성 요소

이용자

- PKI를 사용해서 자신의 공개 키를 등록하고 싶어 하는 사람과
- 등록되어 있는 공개 키를 사용하고 싶어 하는 사람

이용자가 하는 일

- 키 쌍을 작성한다(인증 기관이 작성하는 경우도 있다)
- 인증 기관에 공개 키를 등록한다
- 인증 기관으로부터 인증서를 발행 받는다
- 필요할 경우 인증 기관에 신청해서 등록한 공개 키를 무효로 한다
- 수신한 암호문을 복호화한다
- 메시지에 디지털 서명을 한다

공개키 사용자가 하는 일

- 메시지를 암호화해서 수신자에게 송신한다
- 디지털 서명을 검증한다

인증 기관

- 인증 기관(certification authority; CA)
  - 인증서의 관리를 행하는 기관
  - 키 쌍을 작성한다(이용자가 작성하는 경우도 있다)
  - 공개 키 등록 때 본인을 인증한다
  - 인증서를 작성해서 발행한다
  - 인증서를 폐지한다

등록 기관

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

한국의 전자 서명 인증 관리 체계도

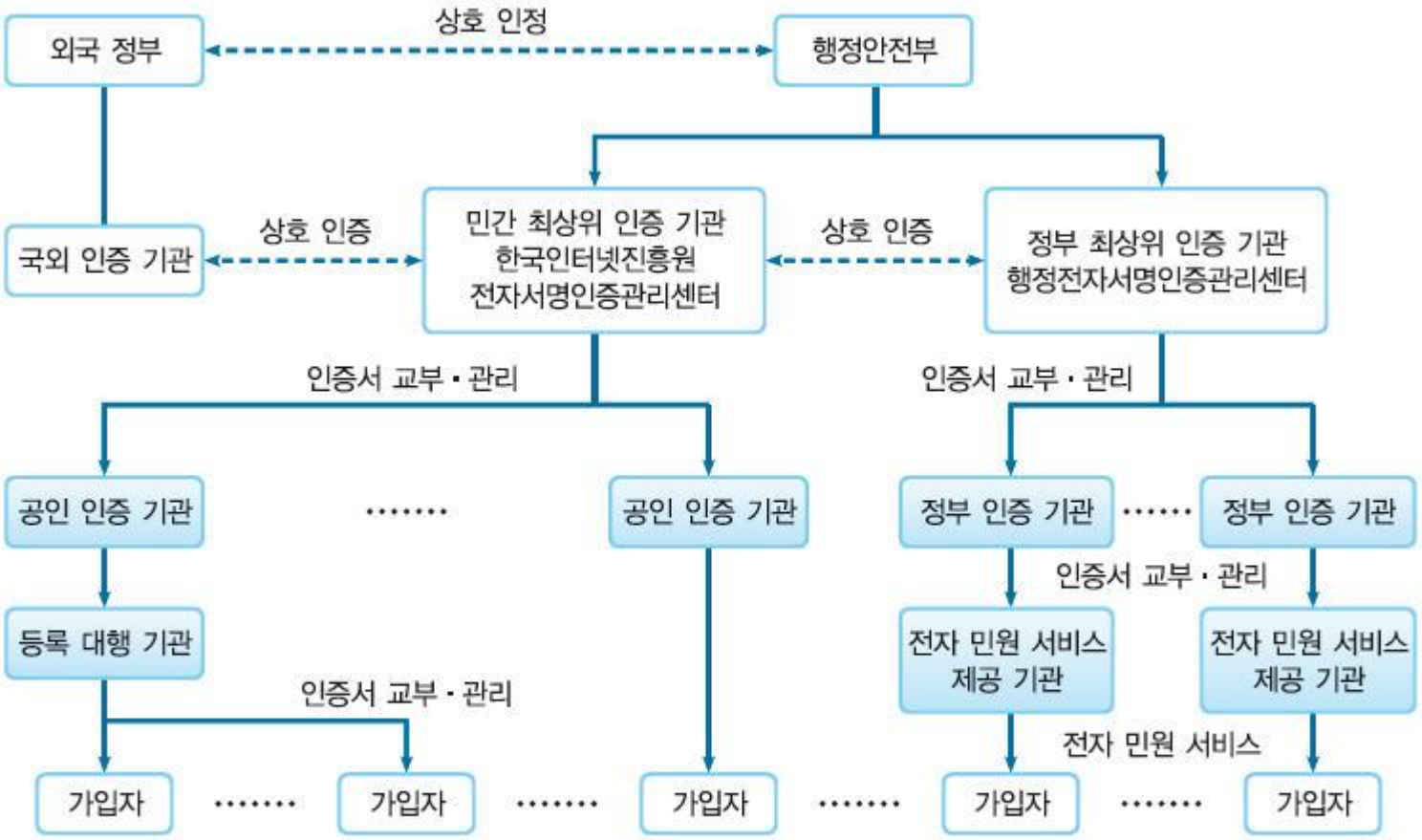


그림 11-9 · 한국의 전자 서명 인증 관리 체계도

저장소

- 저장소(repository)
  - 인증서를 보존해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 한 데이터베이스
  - 인증서 디렉토리
  - 전화에 있어서 전화번호부와 같은 역할
  - 앨리스가 밥의 인증서를 입수할 때 저장소를 이용할 수 있다

3.3 인증 기관의 역할

- 키 쌍의 작성
- 인증서 등록
- 인증서 폐지와 CRL

키 쌍의 작성

- PKI의 이용자가 작성하기
- 인증 기관이 작성하기
  - 「개인 키를 이용자에게 보내는」 추가 업무
    - 방법은 PKCS #12(Personal Information Exchange Syntax Standard)로 정의

인증서 등록

- 이용자는 인증 기관에 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
- 인증 기관의 최신 CRL을 조사해서 그 인증서 유효성 확인 필요

3.4 계층 구조를 갖는 인증서

회사 내의 사내 PKI

서울 본사(서울 본사 인증기관)

↓

충남 지사(충남 지사 인증기관)

↓

논산 지점(논산 지점 인증기관)

- 루트 CA
  - 최상위 인증 기관

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

계층 구조를 갖는 인증기관

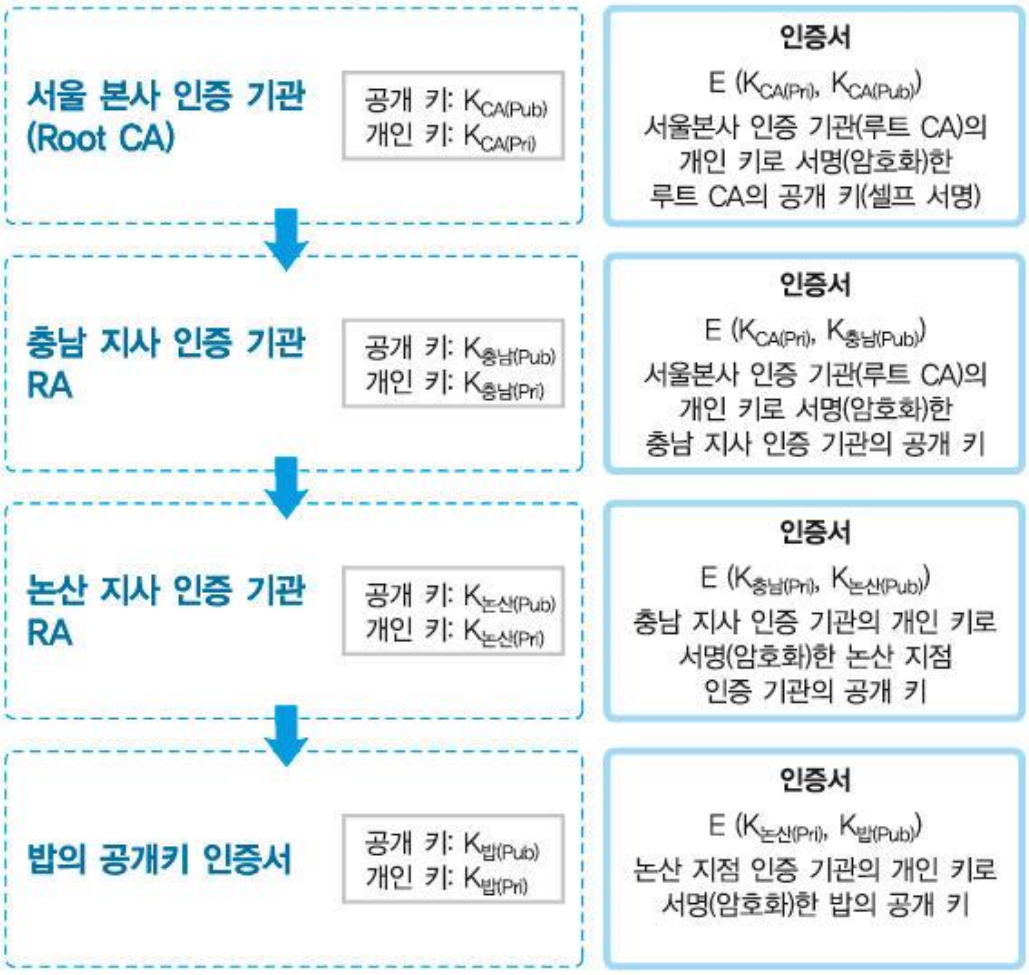


그림 11-10 • 계층 구조를 갖는 인증 기관

앨리스가 밥의 바른 공개 키를 얻는 과정

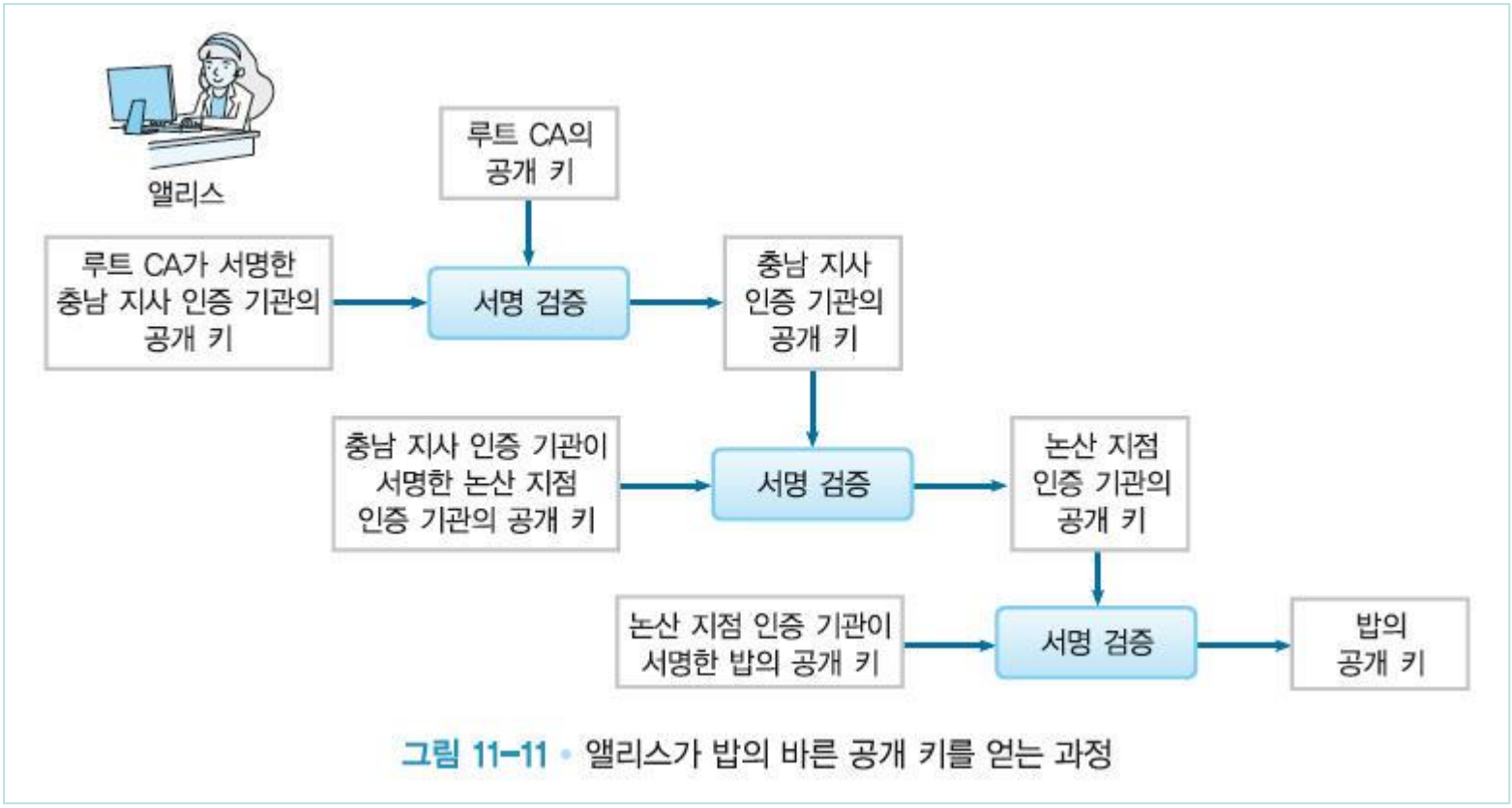


그림 11-11 • 앨리스가 밥의 바른 공개 키를 얻는 과정

제4절 인증서에 대한 공격

4.1 공개 키 등록 이전 공격

4.2 닮은 사람을 등록하는 공격

4.3 인증 기관의 개인 키를 훔쳐내는 방법

4.4 공격자 자신이 인증 기관이 되는 공격

4.5 CRL의 허점을 찌르는 공격 1

4.6 CRL의 허점을 지르는 공격 2

4.1 공개 키 등록 이전 공격

- 인증 기관이 디지털 서명을 수행하기 이전에 적극적 공격자 맬로리가 공개 키를 자신의 것과 살짝 바꿔치기 한다
- 인증 기관은「밥의 정보」와「맬로리의 공개 키」의 조합에 대해 디지털 서명을 하게 된다.

4.2 닮은 사람을 등록하는 공격

- 오인하기 쉬운 사용자 정보를 사용
  - Name = Bob
    - Name = BOB

- 이 공개 키는 이름은 BOB으로 되어 있지만, 맬로리의 공개 키

- 맬로리는 밥의 행세를 하며 Name = BOB으로 되어 있는 인증서를 앨리스에게 보낸다

4.3 인증 기관의 개인 키를 훔쳐내는 방법

- 인증 기관의 개인 키를 훔쳐낸다
- 인증 기관의 개인 키가 도난 당했다면(누설되었다면), 인증 기관은 자신의 키가 누설되었다는 것을 CRL을 사용해서 이용자에게 통지

4.4 공격자 자신이 인증 기관이 되는 공격

- 맬로리 자신이 인증 기관이 된다
- 인증 기관이 된 맬로리는 자신의 공개 키라도 「이것은 밥의 공개 키이다」라고 주장하는 인증서를 자유롭게 발행
- 인증 기관을 신뢰할 수 없으면 인증서가 아무리 바르더라도 그 공개 키를 사용해서는 안 된다

4.5 CRL의 허점을 찌르는 공격 1

- 공격자 맬로리는 CRL이 도착할 전에 빠른 공격을 시도

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

4.6 CRL의 허점을 지르는 공격 2

- 밥이 앨리스로부터 돈을 뜯어낼 계획수립
- 밥은 가명을 써서 계좌 X-5897을 개설
- 앨리스에게 송금 요청을 하고 자신의 서명을 붙인다
- 트렌트에게 개인키가 도난 당했다고 보고한다
- 앨리스에게 CRL이 도착하기 전에 앨리스가 해당 금액을 계좌 X-5897로 송금을 했다면
- 밥은 예금을 인출한다
- 앨리스가 나중에 CRL을 받고 밥에게 항의한다
- 밥은 자신의 개인키가 도난 당했다고 주장하고 돈을 착복한다

제5절 인증서에 대한 Q&A

5.1 인증서의 필요성

5.2 독자적인 인증 방법을 사용하는 것이 안전한 것이 아닌가?

5.3 인증 기관을 어떻게 신뢰할 것인가?

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 경우, 중간자(man-in-the-middle)공격이 가능해진다.
  - 인증기관으로부터 인증서를 입수하면 중간자 공격(man-in-the-middle attack)의 가능성을 줄일 수 있다.

인증 기관의 필요성

- 신뢰할 수 있는 공개 키를 입수할 수 있다면 인증 기관은 불필요하다.

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

5.2 독자적인 인증 방법을 사용하는 것이 안전한 것이 아닌가?

- 의문: 인증서 형식이든 PKI든 공개되어 있는 기술을 사용하는 것에 불안을 느낀다. 공개되어 있는 기술을 사용한다는 것은 공격자에게 공격을 위한 정보를 제공하는 것이 된다고 생각한다. 그것보다는 사내에서 독자적으로 개발한 비밀 인증 방법을 사용하는 편이 안전하지 않을까?
- 답:
  - 그렇지 않다.
  - 비밀 인증 방법을 독자 개발하는 것은「감추는 것에 의한 보안」(security by obscurity)라는 전형적인 잘못이다.

5.3 인증 기관을 어떻게 신뢰할 것인가?

- 의문: 인증 기관의 기능은 대강 이해를 했지만, 결국 맴도는 것 같은 느낌이 든다. 공개 키를 신뢰하기 위해서는 인증서를 발행한 인증 기관을 신뢰해야 하는데, 그렇다면 인증 기관은 어떻게 신뢰하는 것일까?

- 답:
  - 이 의문은 정당하다.
  - 이 의문은「신뢰」가 어떻게 형성되는가 하는 본질적인 문제와 관계되어 있기 때문이다.

Q & A

Thank You!