

제 11 장 인증서



박종혁 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 인증서

1.1 인증서란 무엇인가?

1.2 인증서를 사용하는 시나리오

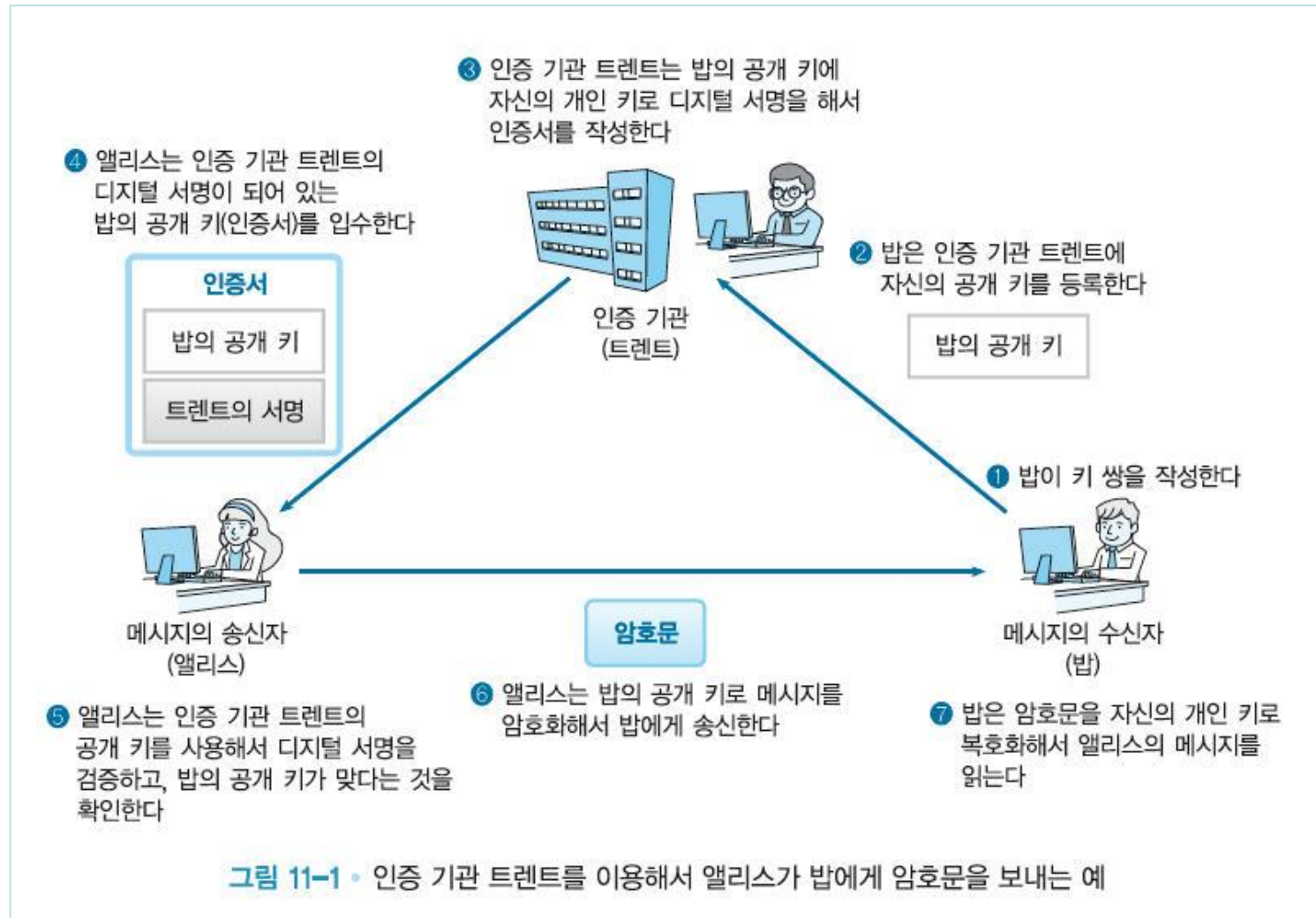
1.1 인증서란 무엇인가?

- 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



제2절 인증서 만들기

2.1 공인 인증서 종류

2.2 베리사인의 무료 시험 서비스

2.3 인증서의 작성

2.4 인증서를 웹 브라우저로부터 내보내기

2.5 인증서의 내용

2.6 인증서의 표준 규격 X.509

2.7 개인 공인 인증서

2.8 인증기관 인증서

2.1 공인 인증서 종류

- 범용 공인인증서

- 모든 분야에서 이용
- 인터넷뱅킹, 온라인증권, 전자상거래, 전자정부 민원서비스, 4대 사회보험, 국세청 홈텍스, 전자세금계산서, 전자입찰/조달, 온라인 교육, 예비군 등 다양한 분야에서 활용
- 소정의 수수료

- 용도제한 공인인증서

- 은행 및 보험, 신용카드 업무, 정부 민원업무 등 특정분야에서만 이용
- 해당 기관이 고객에게만 발급
- 무료

2.2 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

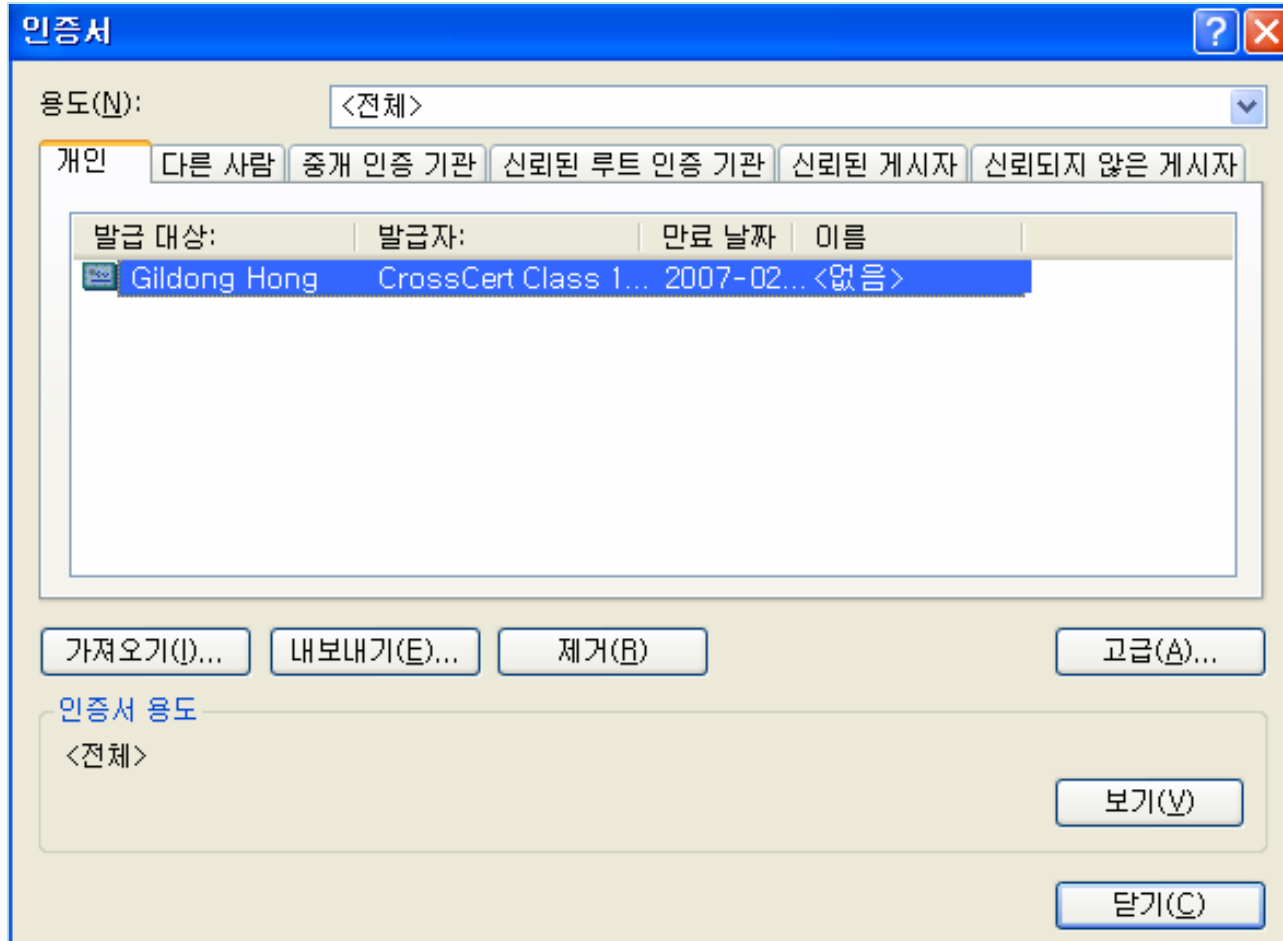
2.3 인증서의 작성

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

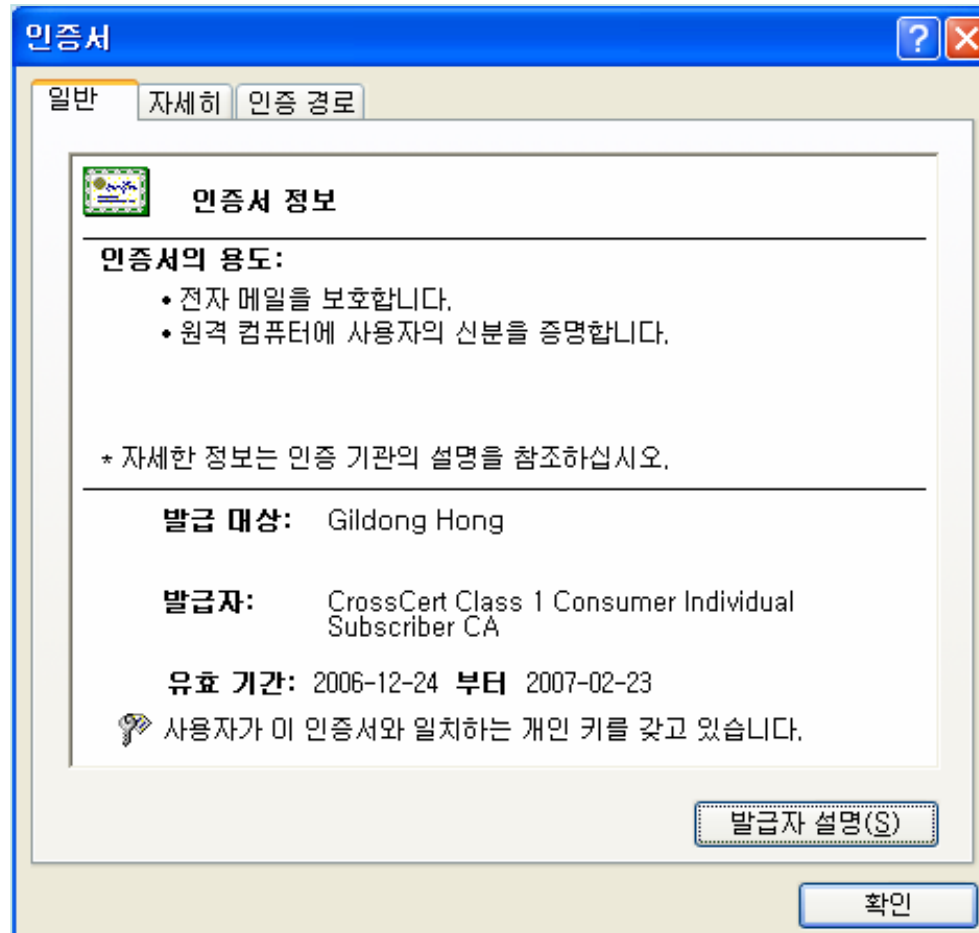
웹 브라우저에 표시되는 내용

- 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

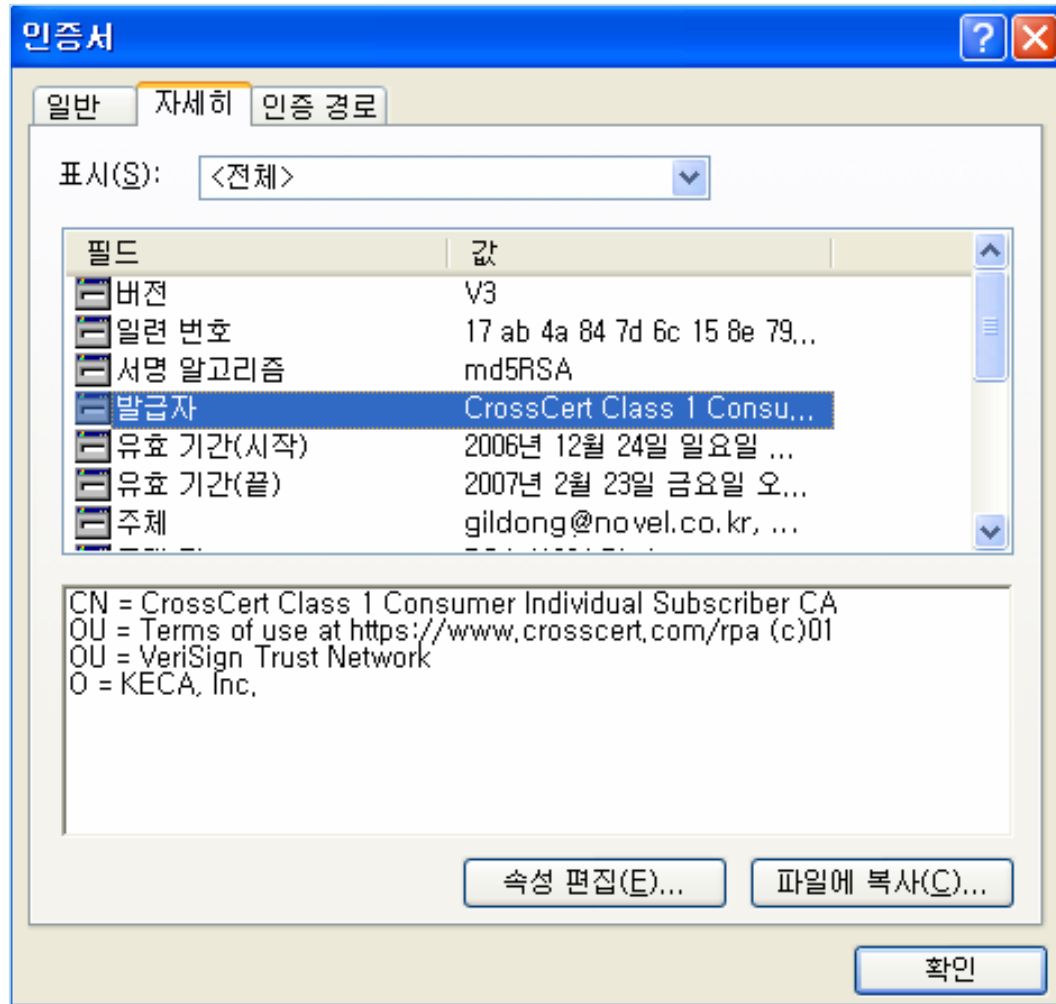
개인용 인증서



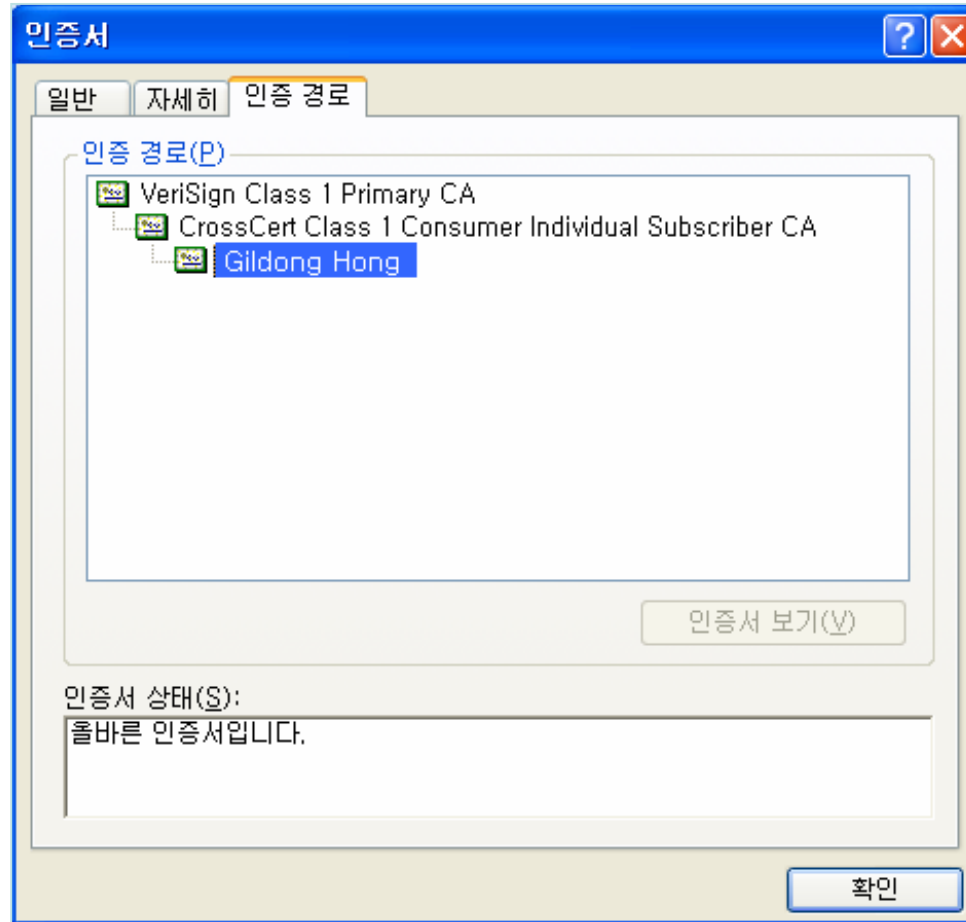
자세하게 내용을 표시



보다 자세하게 내용을 표시



인증서의 계층 표시



2.4 인증서를 웹 브라우저로부터 내보내기

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

한국전자인증이 작성한 밥의 인증서

-----BEGIN CERTIFICATE-----

MIIE5TCCBE6gAwIBAQIQF6tKhH1sFY55TC7o6CZ9IzANBgkqhkiG9w0BAQQUFADCBsjETMBEGA1UEChMKSOVDQSwgSW5JLjEjMB0GA1UECwMWMWVmbVyaVnNpZ24gVHJ1c3QgTmV0d29yazE8MDoGA1UECwMzVGvYbXMgb2YgdXNlIGF0IHR5dHh5d3d3LmNyb3NzY2VydC5jb20vcnBhIChjKTAxMTwwOgYDVQQDEzNDcm9zc0NlcnQgQ2xhc3MgMSBDb25zdW1lciBJbWRpdmlkdWVzIFN1YnNjcmlhZlZlZlQ0EwHhcNMDYxMjI0MDAwMDAwWhcNMDcwMjlyMjM1OTU5WjCCAVUxZzARBGNVBAoUcktFQ0EsiEluYy4xPDA6BgNVBAsUM0Nyb3NzQ2VydCBDYGFzcyAxIENvbnN1bWVylEluZGI2aWR1YWwgU3Vic2NyaWJlciBDQTE0MDIGA1UECwMrVGvYbXMgb2YgdXNlIGF0IHd3dy5jcm9zc2NlcnQuY29tL3JwYSAoYykwMTEjMCEGA1UECwMaQXV0aGVudGljYXRlZCBieSBDb25zdW1lcnQxZjAlBgNVBAsTHk1IbWJlciwvVmVyaVnNpZ24gVHJ1c3QgTmV0d29yazEeMBwGA1UECwMVUGVyc29uYSBOb3QgVmFsaWRhdGVkMSYwJAYDVQQLEw1EaWdpdGFsIEEiENsYXNzIDEGLSBOZXRzY2FwZTETMBEGA1UEAxMKVGFISWwgSmVvbGJfEjMB0GCSqGSIb3DQEJARYQdGlqZW9uQGRqdS5hYy5rcjCBnzANBgkqhkiG9w0BAQEFAAOBJQAawgYkCgYEA4whHBepbO/ZjFmgfXKhKVEkTuSTBwJTubG+4hnQj67/nV1uTiXNdxrIMoHLXH6+tUYUfT3taCHFx4IOsu+I/gWPakzGVM4RbfkijFIWYas0GpGw1AttLK84Bb8lx05i72TDsGsQBA/4uhObiClbKskucVbsfs/mhBGD6FXmyMCAwEAAAOCAVQwggFQMAKGA1UdEwQCAAwbgYDV0fBGcwZTBj oGGgX4ZdaHR0cDovL29uc2I0ZWNYbC5jcm9zc2NlcnQuY29tL0tFQ0FJbMNDcm9zc0NlcnRDbGFzc2FDb25zdW1lckluZGI2aWR1YWwtdWJz Y3JpYmVvQ0EvTGFOZXRhZG91JmMIGsBGNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMIGOMCgGCCsGAQUFBwIBFhxodHRwczovL3d3 dy52ZXJpc2lnbi5jb20vQ1BTMGIgCCsGAQUFBwICMFYwFRYOVmVyaVnNpZ24sIEluYy4wAwIBARo9VmVyaVnNpZ24ncyBDUFMgaW5jb3JwLiBi eSBYdZlZlcmVhY2UgYbGhYi4gbHRkLiAoYyk5NyBWZXJpU2lnbjARBglghkgBhvhCAQEEBAMCB4AwEQYKYIZIAYb4RQEGCQQDAQH/MA0GC SgGSIB3DQEBAUAA4GBAGiQN7YFsv0/FLHXrBDbgMImuZebMvcwRHAKnDeuhlogPqb+iB/50f2ESGh5tkqPsSLg87Z5Hc5wWEP5U8nlSHK 9SIzjBfYSA51KA/2nhB2yo2NQCSE/aY4Xqn3Vi37qCpCpEVYvFqBf2fG2oprrrg5x234gRVgMZ5feAlz7UeAE

-----END CERTIFICATE-----

2.5 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](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](https://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:

2.6 인증서의 표준 규격 X.509

- X.509
 - 가장 널리 사용
 - ITU(International Telecommunication Union)나 ISO(International Organization for Standardization)에서 규정한 규격
 - 인증서의 생성 · 교환을 수행할 때 사용
 - 많은 애플리케이션에서 지원

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:

2.7 개인 공인 인증서

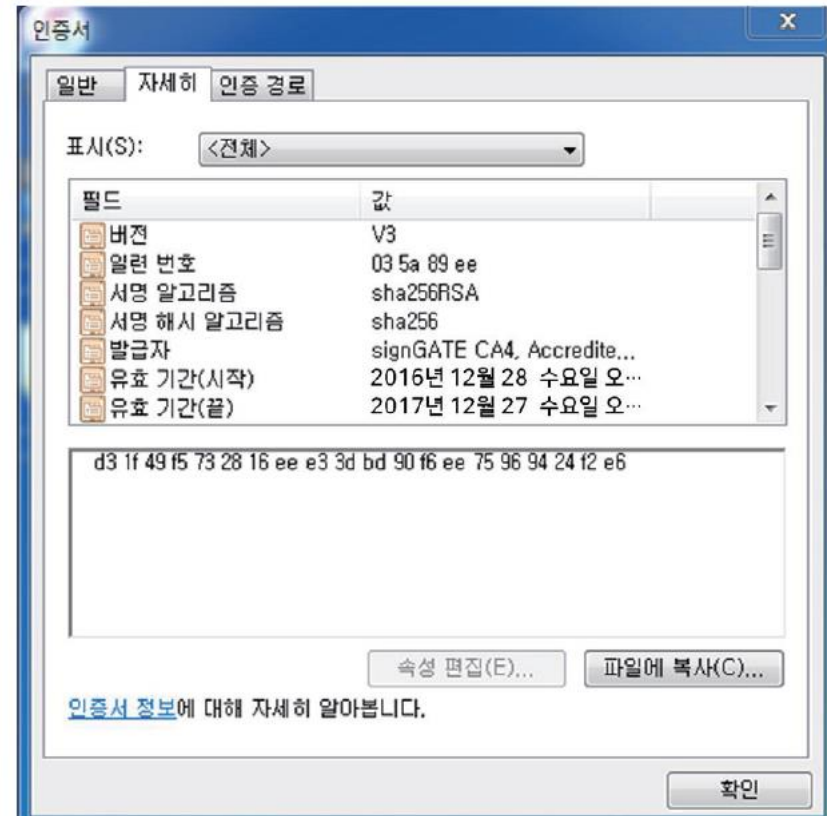
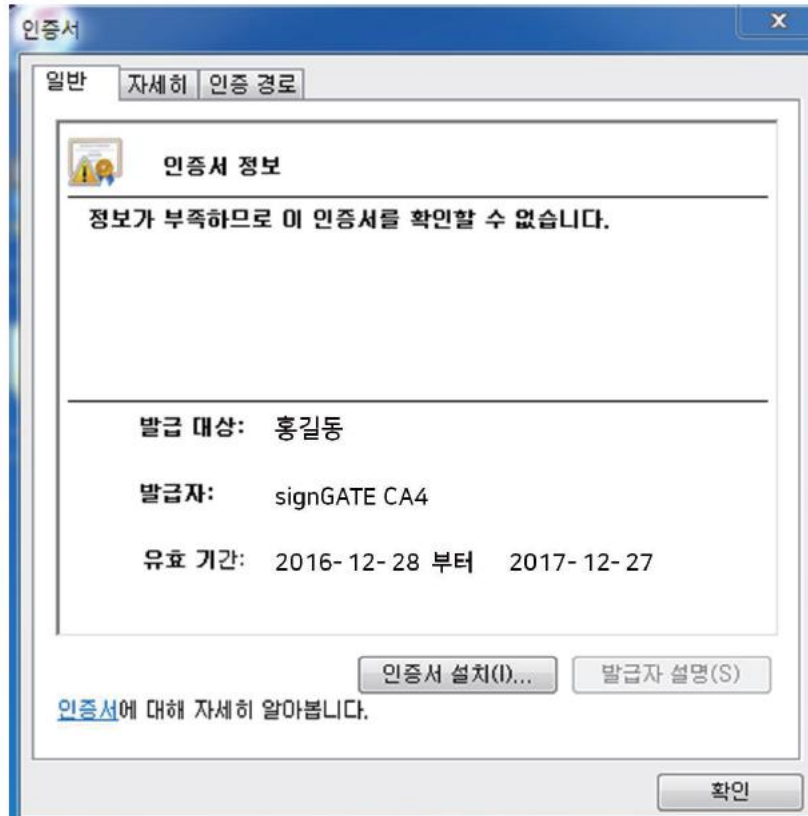


그림 11-2 • 개인 공인 인증서

개인용 인증서 세부 필드

필드	값
버전	V3
일련 번호	03 5a 89 ef
서명 알고리즘	sha256RSA
서명 해시 알고리즘	sha256
발급자	CN = signGATE CA4 OU = AccreditedCA O = KICA C = KR
유효 기간(시작)	2016년 12월 28일 수요일 오후 8:26:15
유효 기간(끝)	2017년 12월 27일 수요일 오후 11:59:59
주체	CN = 홍길동 OU = 중앙우체국 OU = 우체국 OU = 등록기관 OU = licensedCA O = KICA C = KR
공개 키	30 82 01 0a 02 82 01 01 00 c2 2d 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 ae 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 ae 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 b 4 3e 16 7c d4 15 a7 01 e0 59 6f ca e3 a5 52 0f 2f 92 db ca 3d a9 9e 3e 96 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 28 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 9 a 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 e6 84 f2 76 23 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.signgate.com:389/ou=dp6p26866,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.signgate.com:9020/OCSPServer
키 사용	Key Encipherment (20)
지문 알고리즘	sha1
지문	d3 1f 49 f5 73 28 16 ee e3 3d bd 90 f6 ee 75 96 94 24 f2 e6

2.8 인증기관 인증서

표 11-2 • 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
```

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

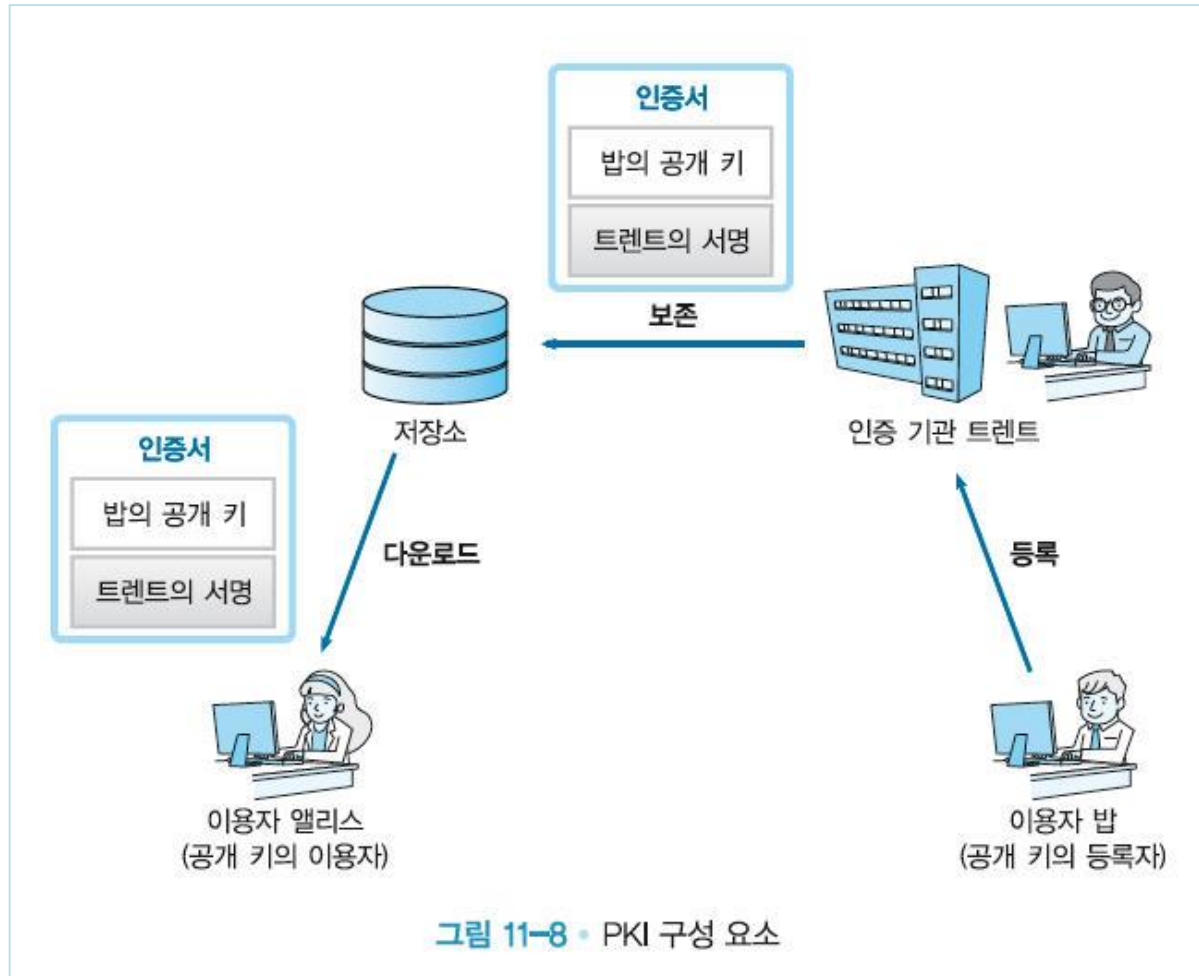
3.1 공개 키 기반 구조(PKI)

- 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



- 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 등록된 공개 키를 무효로 한다
- 수신한 암호문을 복호화한다
- 메시지에 디지털 서명을 한다

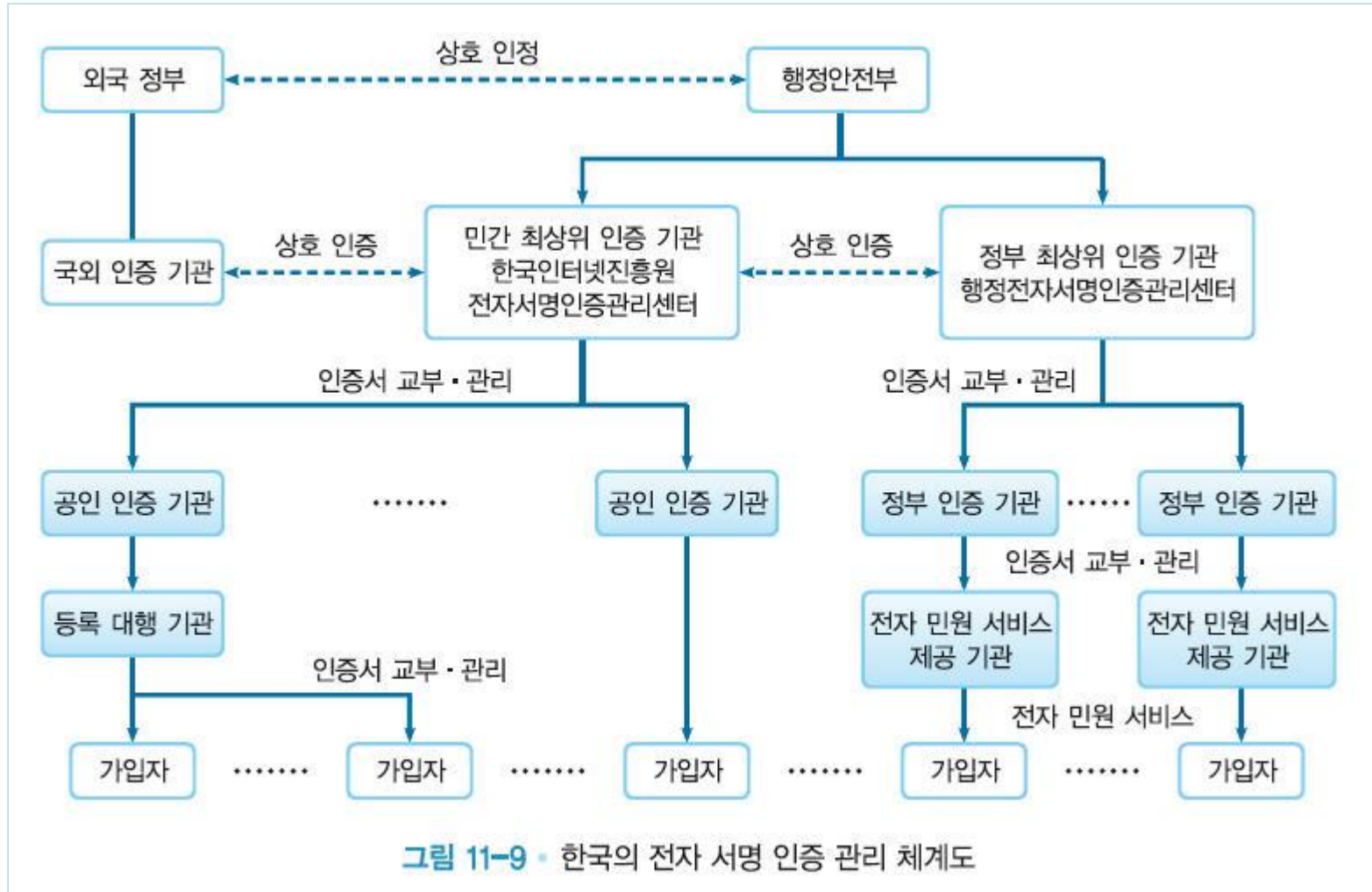
공개키 사용자가 하는 일

- 메시지를 암호화해서 수신자에게 송신한다
- 디지털 서명을 검증한다

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

한국의 전자 서명 인증 관리 체계도



- 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

- 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)



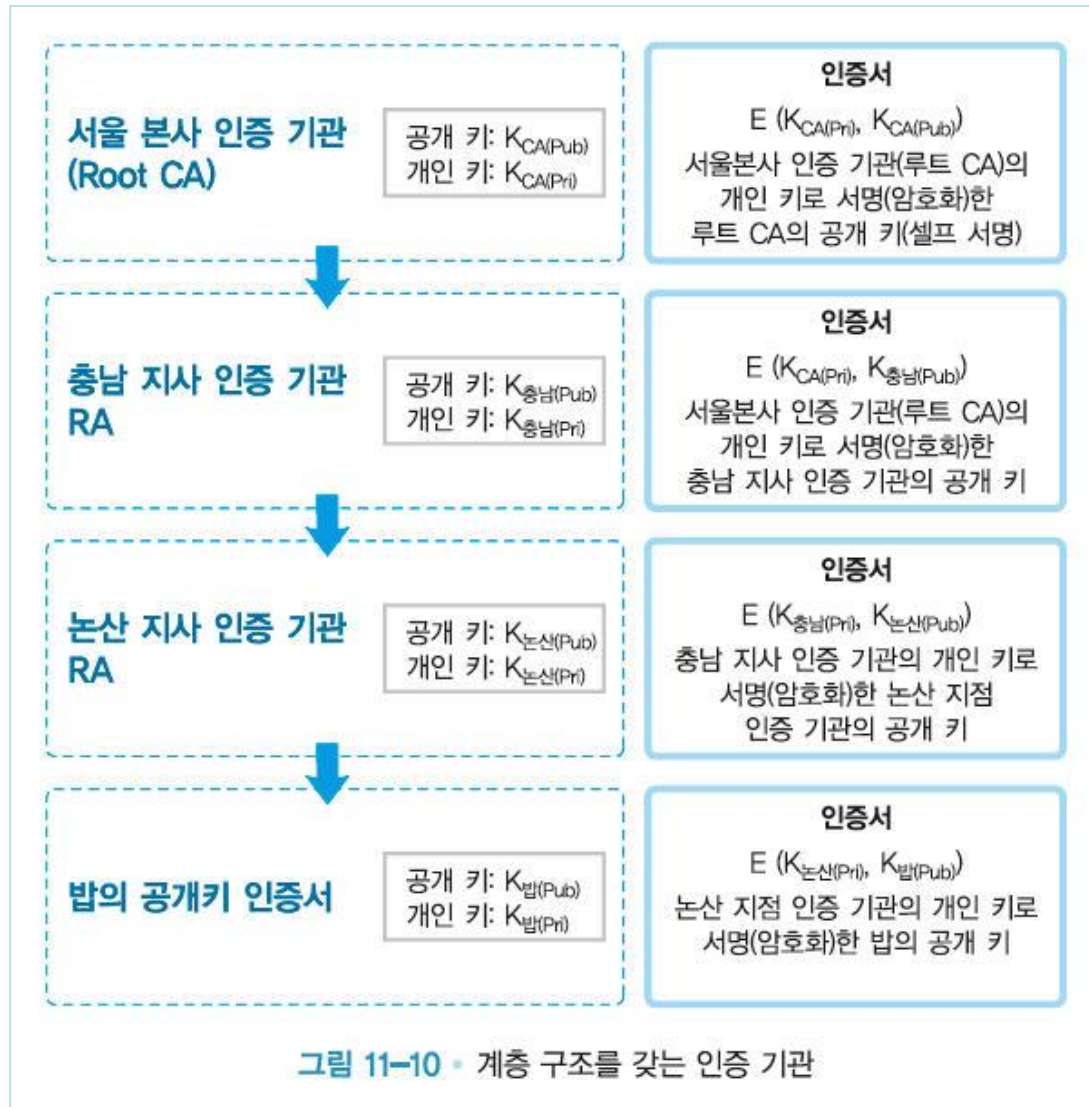
충남지사(충남지사 인증기관)



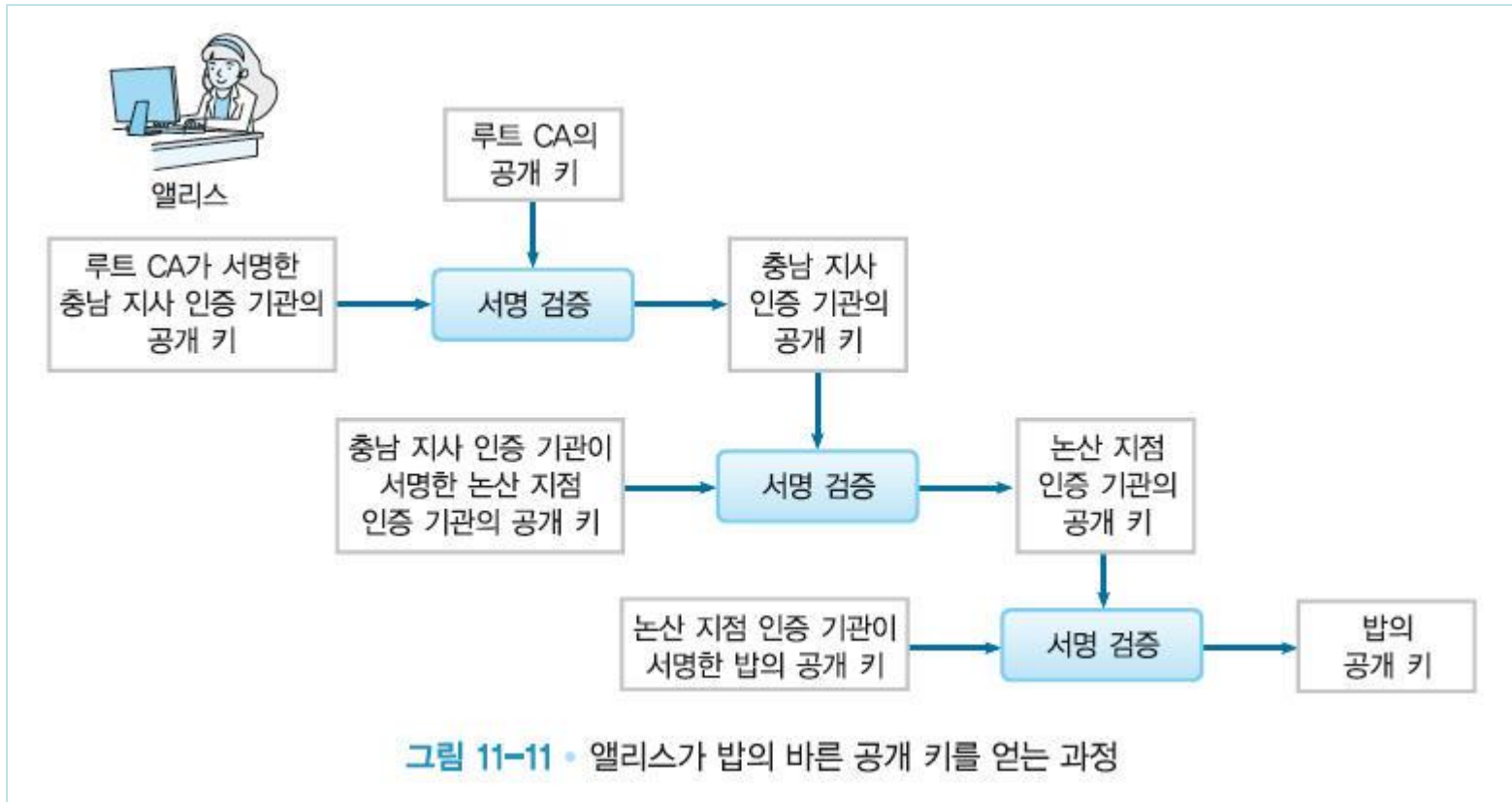
논산지점(논산지점 인증기관)

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

계층 구조를 갖는 인증기관



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

제4절 인증서에 대한 공격

4.1 공개 키 등록 이전 공격

4.2 닳은 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

4.7 Superfish

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 다투는 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

4.7 Superfish

- 2015년에 PC 벤더 Lenovo사의 컴퓨터에서 중대한 사건이 발생
 - 컴퓨터에 프리인스톨 되어 있던 Superfish라는 애드웨어가 보안상의 문제 일으킴
 - 통신을 가로채 개인 정보를 수집하여 사용자의 인터넷 이용 맞춤형 광고를 내보내는 소프트웨어
 - 루트 인증서를 인스톨하여 Web사이트와 Web브라우저 사이에 들어간 후, 방문한 Web사이트 인증서를 바꿔치기하여 Web브라우저에 제시
 - 전형적인 중간자 공격으로 통신 갈취

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 맘도는 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!