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

6절 공인 인증서를 대체하는 기술

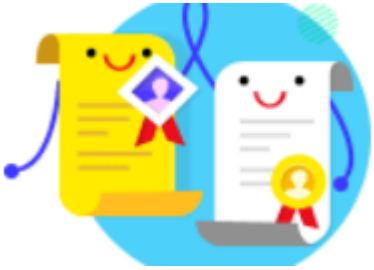
제1절 인증서

1.1 인증서란 무엇인가?

1.2 인증서를 사용하는 시나리오

1.1 인증서란 무엇인가?

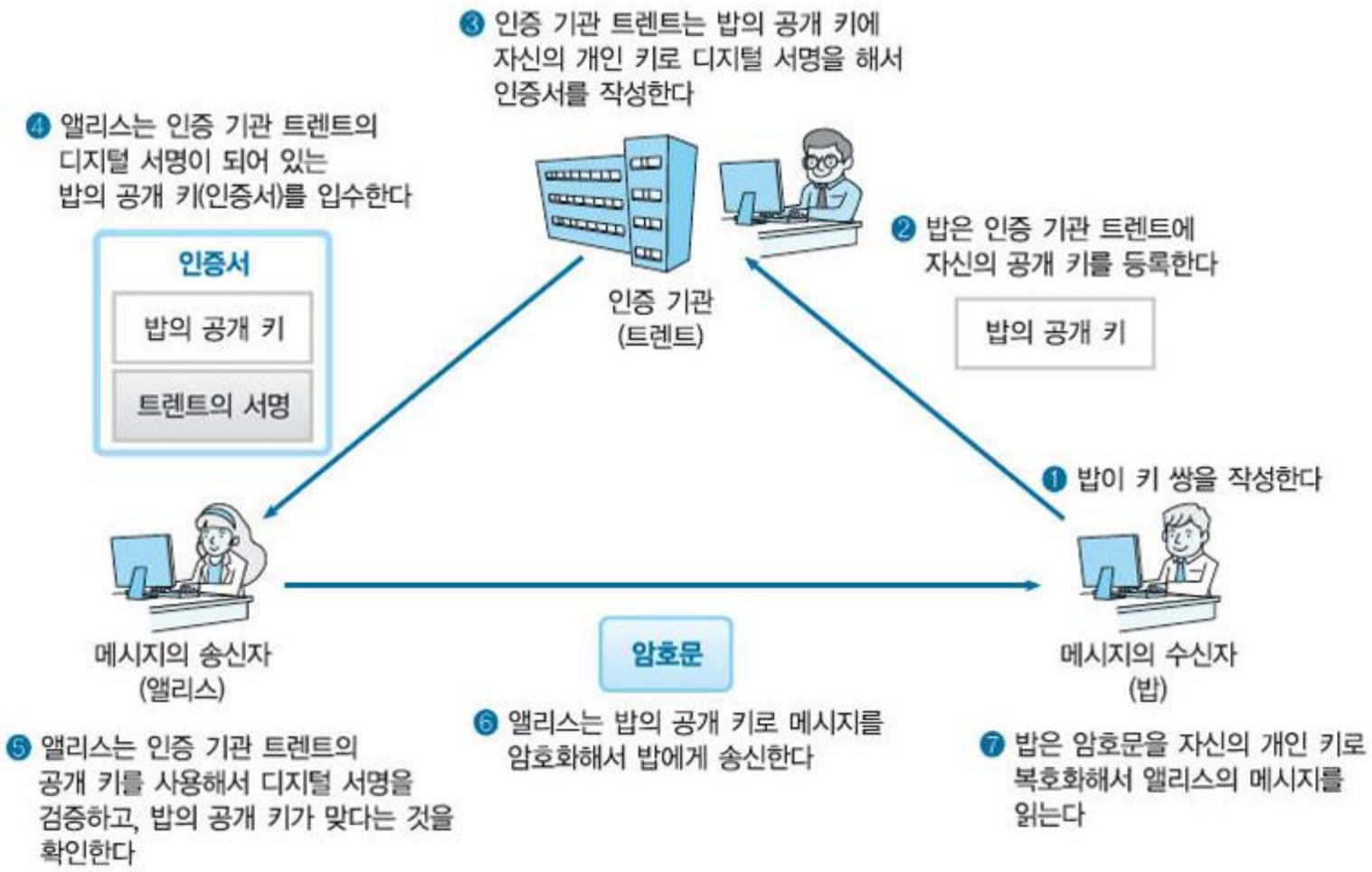
- 공개 키 인증서(public-key certificate; PKC)
  - 이름이나 소속, 메일 주소 등의 개인 정보
  - 당사자의 공개 키가 기재
  - **인증기관**(CA; Certificate Authority, certifying authority)의 개인 키로 디지털 서명



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 공인 인증서

2.1 공인 인증서 종류

2.2 인증서의 표준 규격 X.509

2.3 개인 공인 인증서

2.4 인증기관 인증서

2.5 인증서의 작성

2.6 인증서의 내용

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

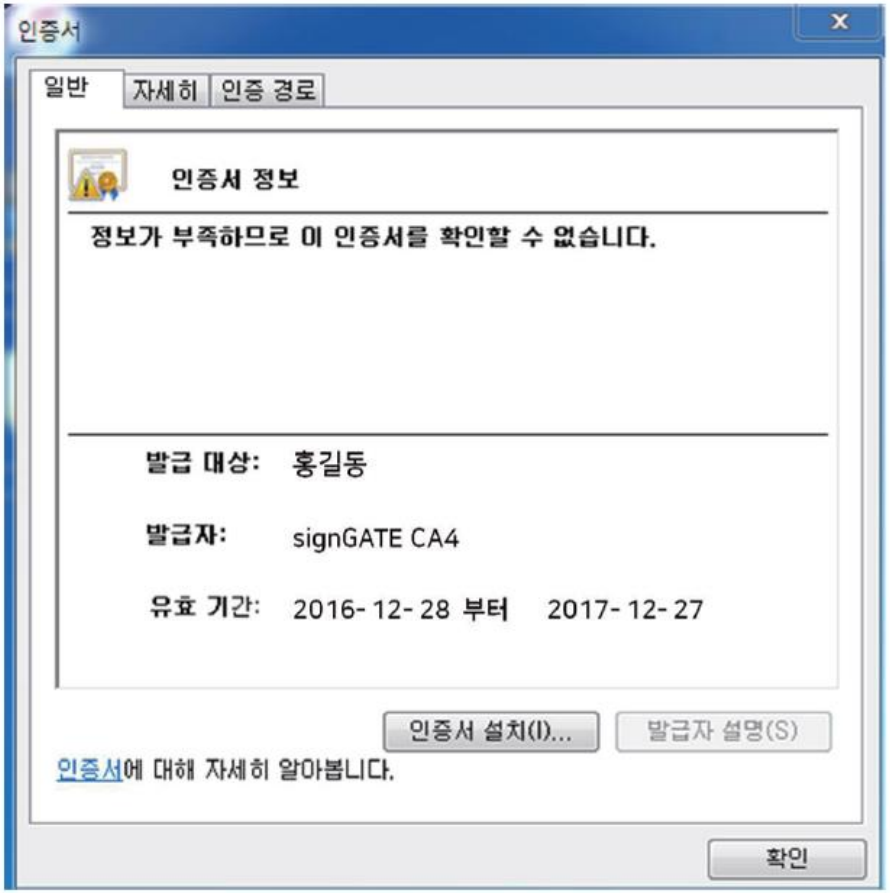
2.2 인증서의 표준 규격 X.509

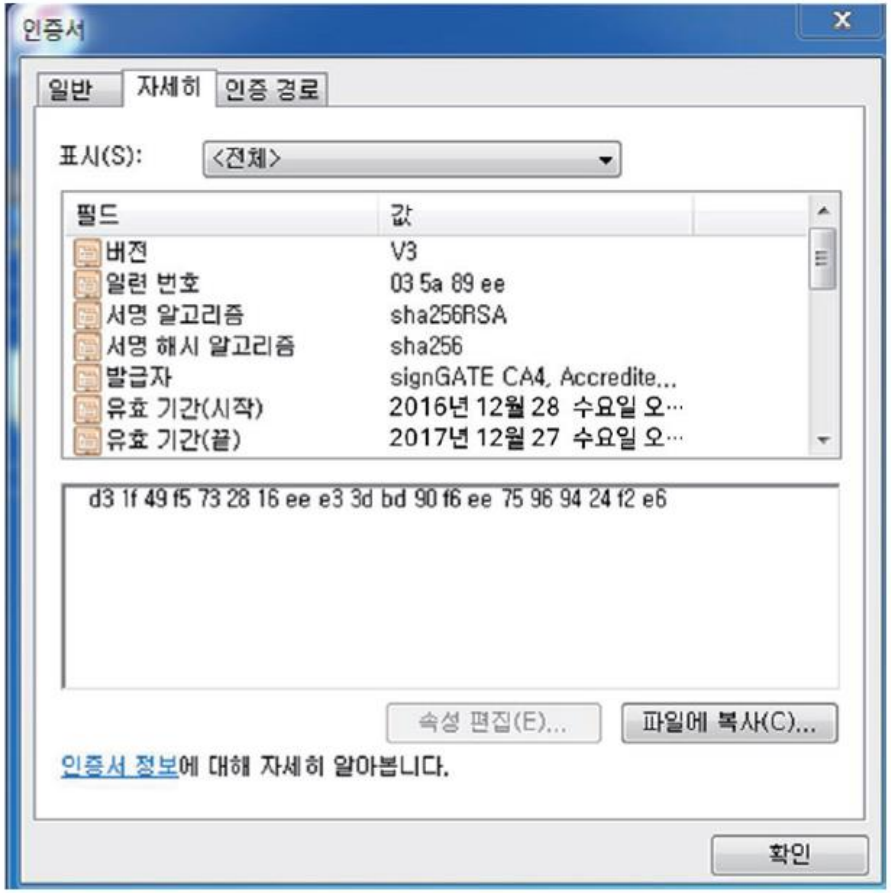
- X.509
  - 가장 널리 사용
  - ITU(International Telecommunication Union)나 ISO(International Organization for Standardization)에서 규정한 규격
  - 인증서의 생성・교환을 수행할 때 사용
  - 많은 애플리케이션에서 지원

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:

2.3 개인 공인 인증서





개인 공인 인증서

개인용 인증서 세부 필드

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 b4 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 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 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

2.4 인증기관 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
```

최상위 인증기관 인터넷진흥원의 인증서

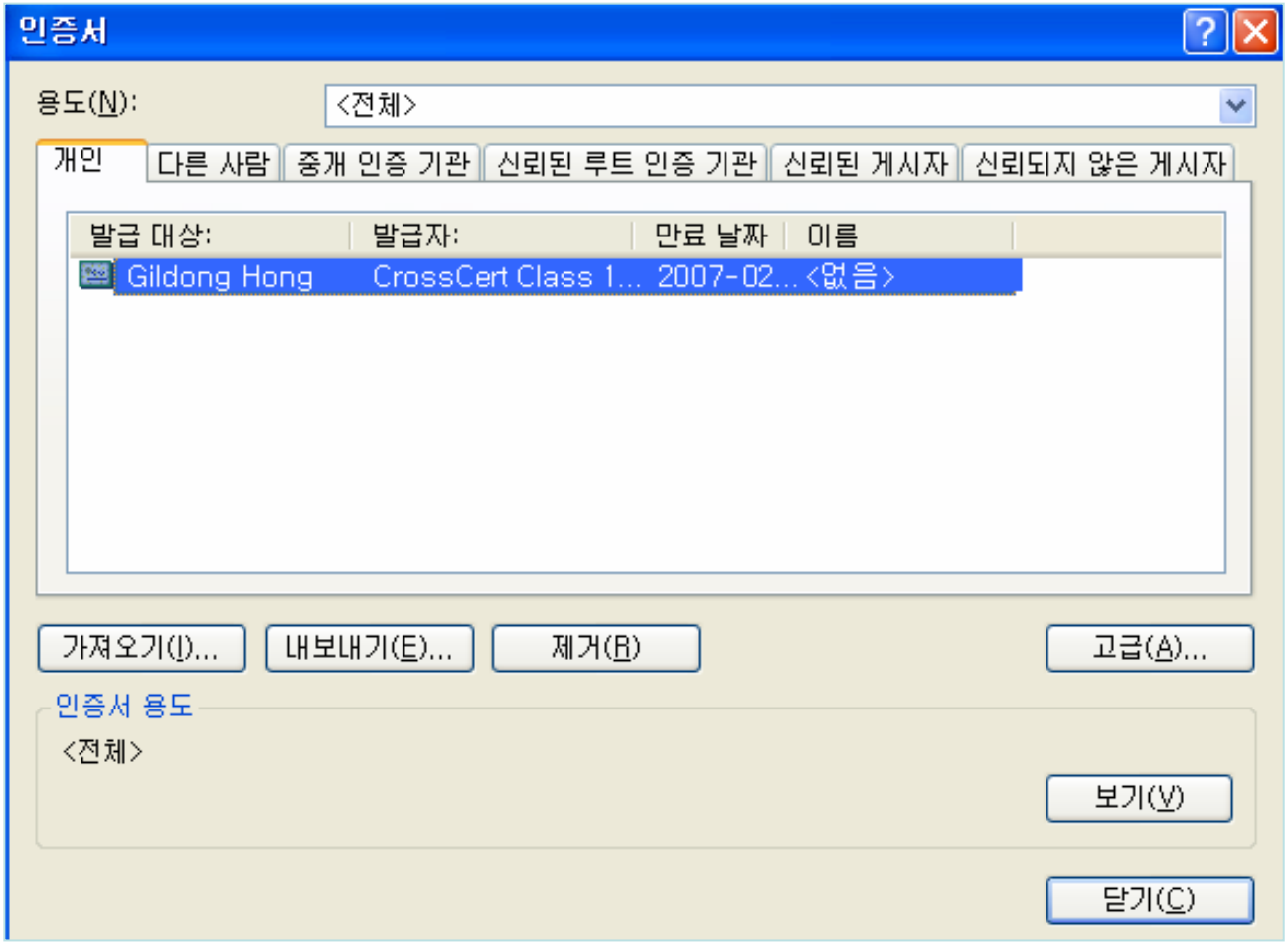
2.5 인증서의 작성

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

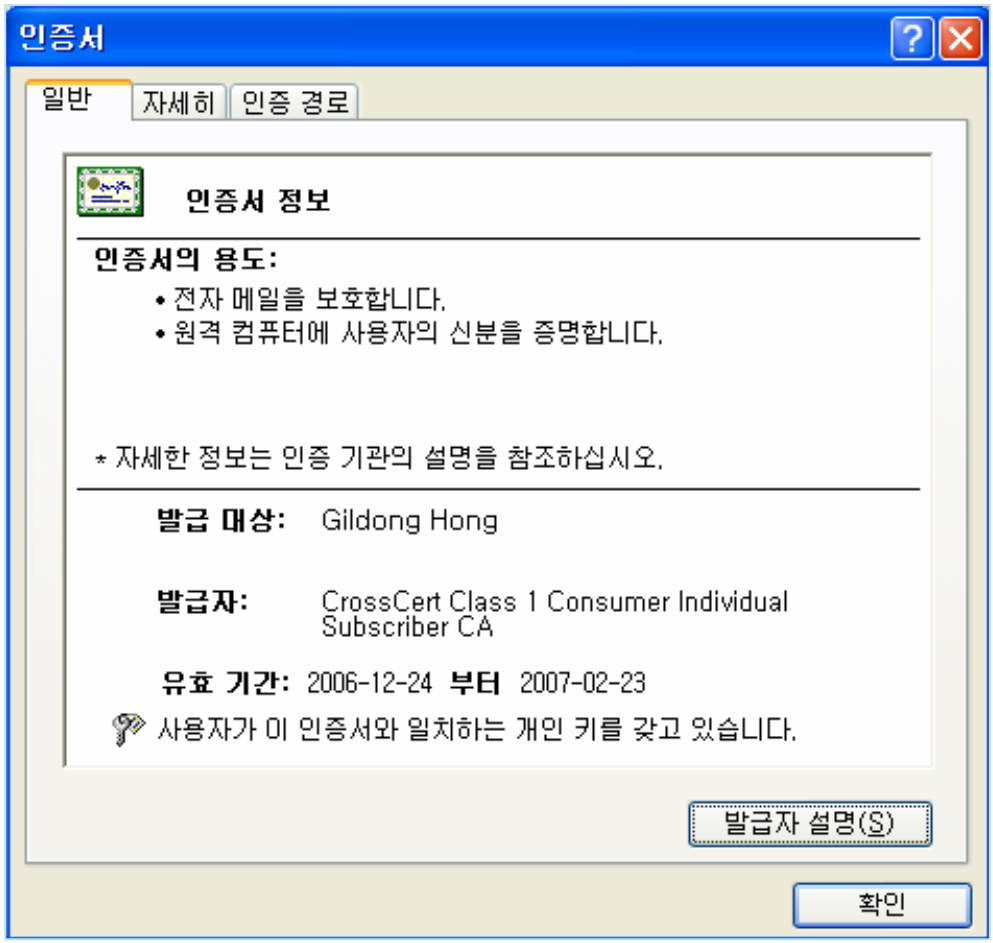
웹 브라우저에 표시되는 내용

- 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

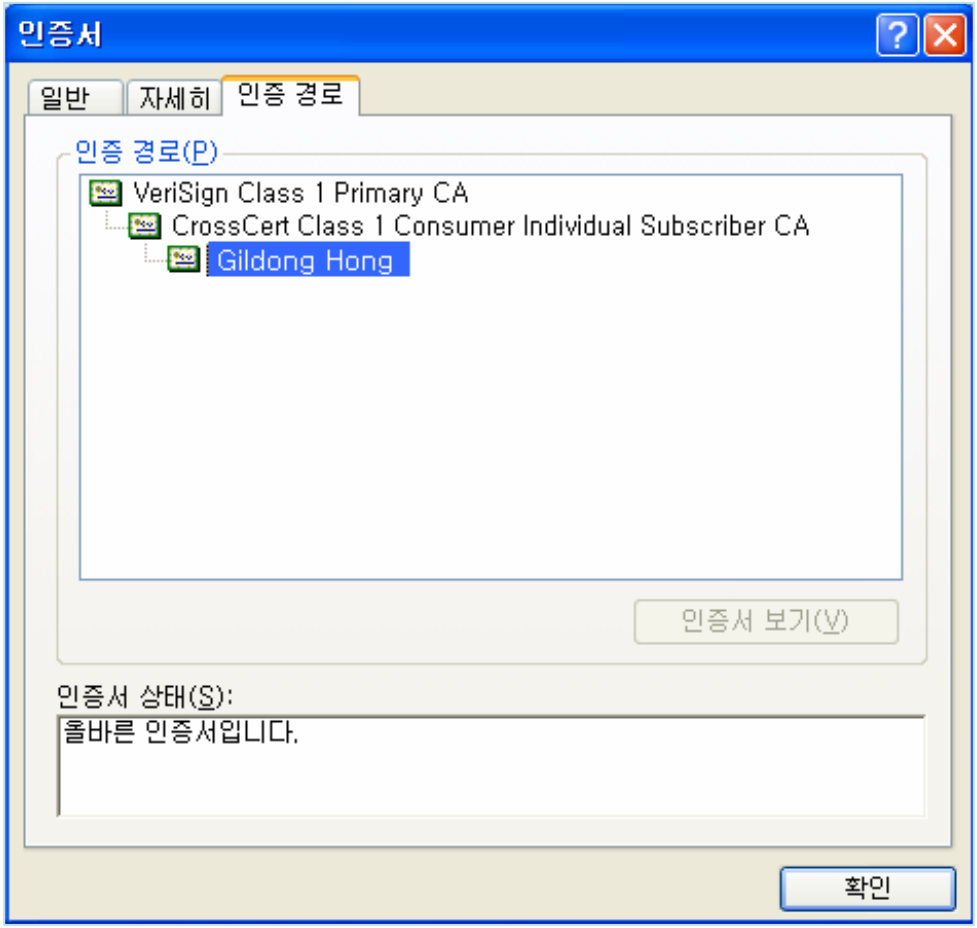
개인용 인증서


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

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

2.6 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

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
Y3JpYmVyQ0EvTGF0ZXN0Q1JMMlGsBgNVHSAEgaQwgaEwgZ4GC2CGSAGG+EUBBwEBMlGOMCgGCCsGAQUFBwlBFhxodHRwczovL3d3
dy52ZXJpc2lnbi5jb20vQ1BTMGlGCCsGAQUFBwICMFYwFRYOVmVyaVNpZ24sIEluYy4wAwlBARo9VmVyaVNpZ24ncyBDUFMgaW5jb3JwLiBi
eSByZWZlcmVuY2UgbGlhYi4gbHRkLiAoYyk5NyBWZXJpU2lnbjARBglghkgBhvhCAQEEBAMCB4AwEQYKYIZIAYb4RQEGCQQDAQH/MA0GC
SqGSIb3DQEBBAUAA4GBAGiQNr7YFsV0/FLHXrBDbgMlmuZebMvcwRHAKnDeuhlogPqb+iB/50f2ESGh5tkqPsSLg87Z5Hc5wWEP5U8nlsHK
9SlzjfBYSA51KA/2nhB2yo2NCQSE/aY4Xqn3Vi37qCPcpEVYvFQbF2fG2oprrg5x234gRVgMZ5feAlz7UeAE
-----END CERTIFICATE-----

인증서의 상세한 내용 (1/3)

Certificate :
DATA :
Version : 4
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:

제3절 공개 키 기반 구조 (PKI)

3.1 공개 키 기반 구조(PKI)

3.2 PKI 구성 요소

3.3 공인 인증기관

3.4 인증 기관의 역할

3.5 계층 구조를 갖는 인증서

3.1 공개 키 기반 구조(PKI)

- 공개 키 기반구조(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

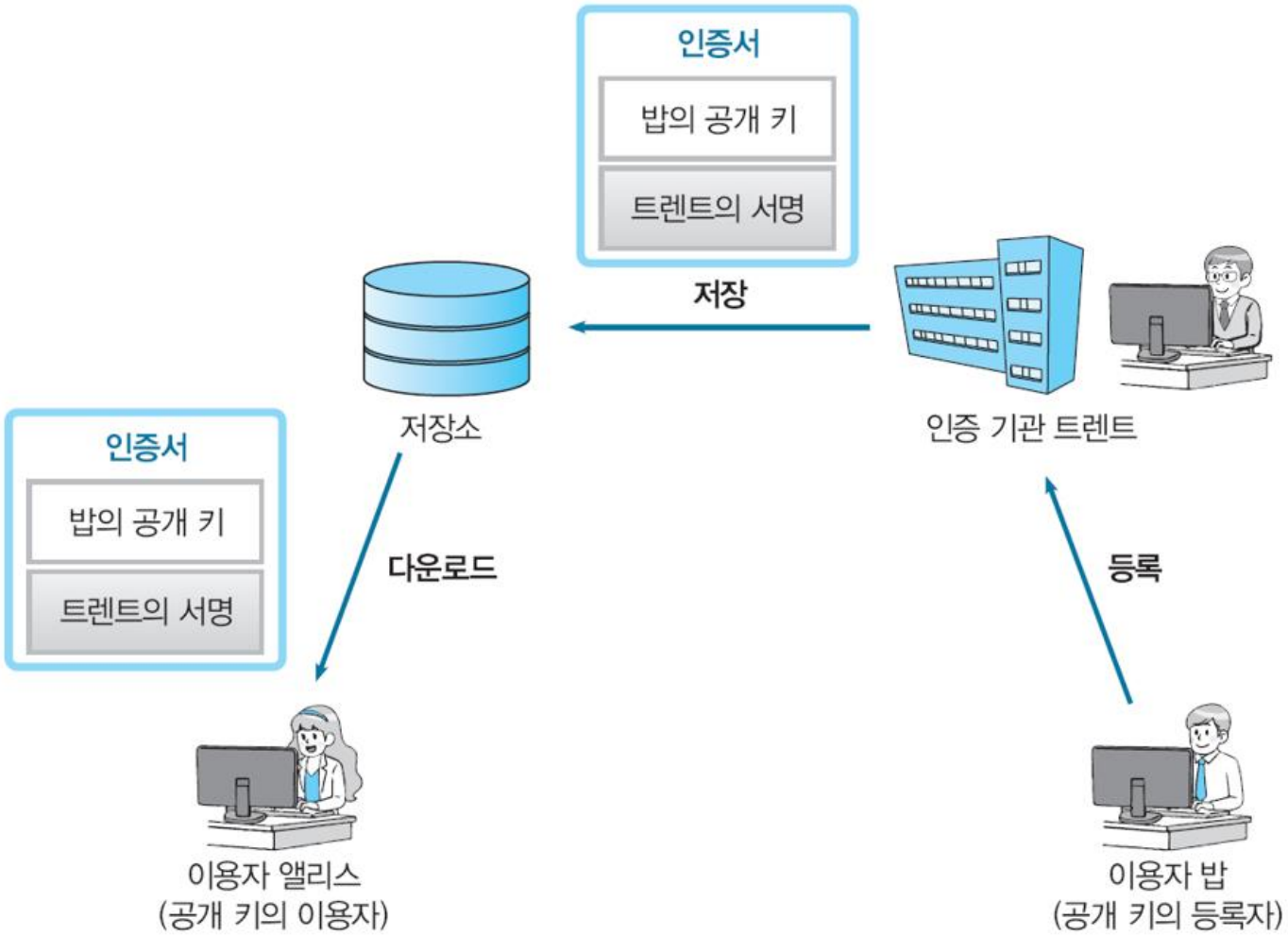
3.2 PKI 구성 요소

- **이용자:**
  PKI를 이용하는 사람

- **인증 기관:**
  인증서를 발행하는 사람

- **저장소:**
  인증서를 보관하고 있는 데이터베이스

PKI 구성 요소


인증서
밥의 공개 키
트렌트의 서명
저장
저장소
인증 기관 트렌트
인증서
밥의 공개 키
트렌트의 서명
다운로드
등록
이용자 앨리스
(공개 키의 이용자)
이용자 밥
(공개 키의 등록자)

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(CA; certification authority)
  - 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

3.3 공인 인증기관

- 미래창조과학부 산하에 민간 최상위 인증기관인 한국인터넷진흥원(KISA)이 있음
- 전자서명법 제 4조의 규정에 의해 지정된 공인인증기관은 6개가 있음
  - 개인 또는 기업 등의 요청에 따라 공인인증서를 발급
  - 철저한 심사 절차를 통해 발급
  - 법적 효력과 안전성 보장
- 2022.12.10 공인인증서 폐지 --> 대체안 발표

3.3 공인 인증기관

- 공동인증을 주관하고 있는 기관들
  - 구)공인인증기관 6곳

한국증권전산	www.signkorea.com	한국정보사회진흥원	sign.nia.or.kr
한국정보인증	www.signgate.com	한국전자인증	www.crosscert.com
금융결제원	www.yessign.com	한국무역정보통신	www.tradesign.net

한국의 전자 서명 인증 관리 체계도

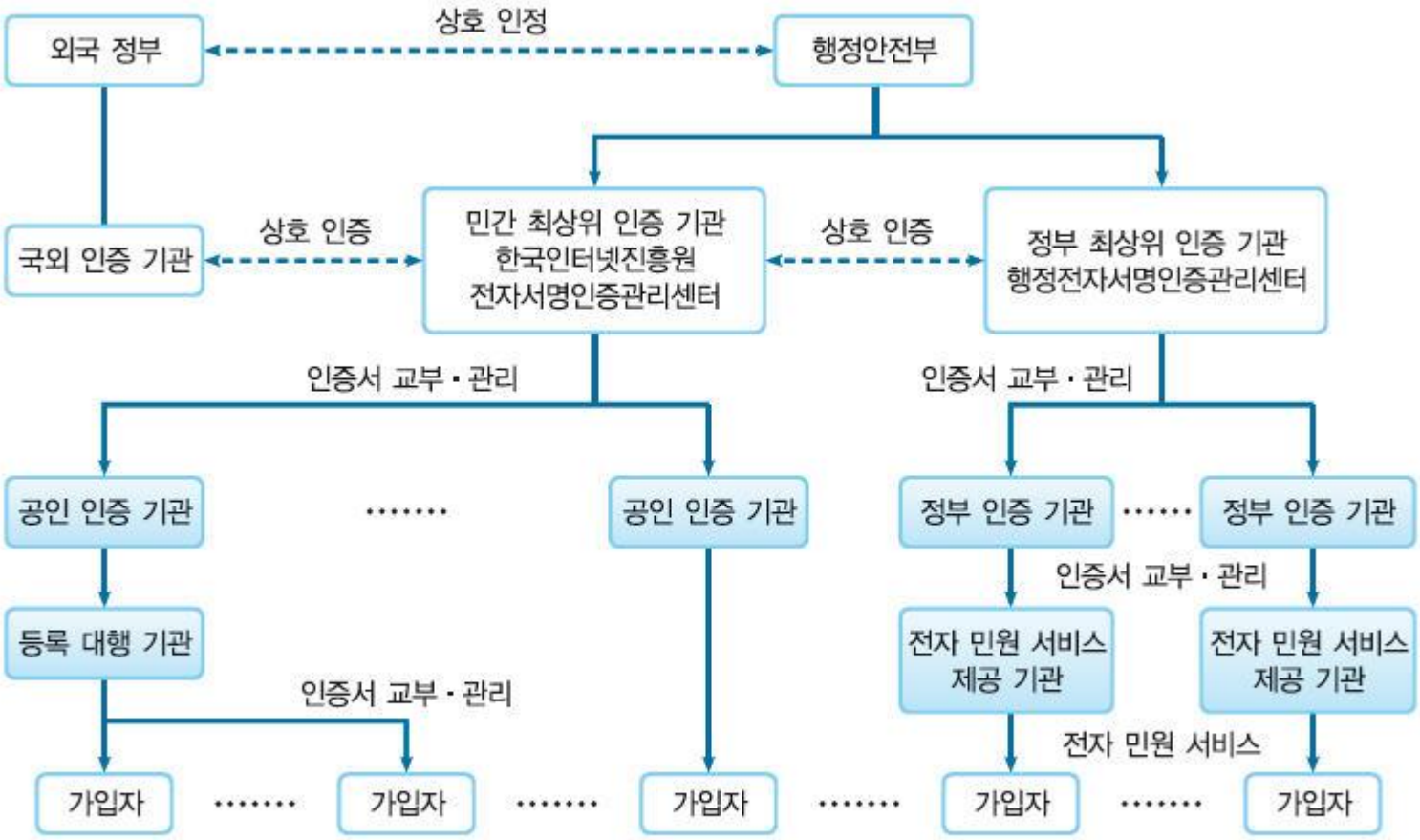


그림 11-9 · 한국의 전자 서명 인증 관리 체계도

저장소

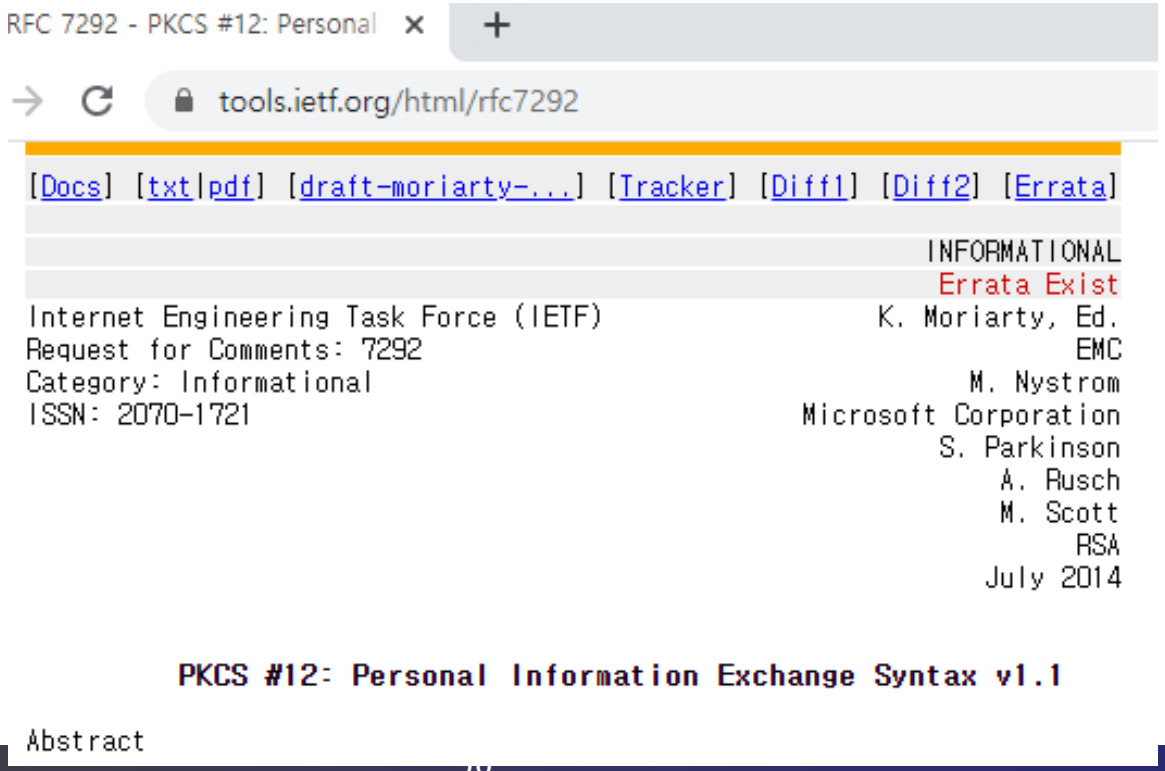
- 저장소(repository)
  - 인증서를 보존해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 한 데이터베이스
  - 인증서 디렉토리
  - 전화에 있어서 전화번호부와 같은 역할
  - 앨리스가 밥의 인증서를 입수할 때 저장소를 이용할 수 있음

3.4 인증 기관의 역할

- 키 쌍의 작성
- 인증서 등록
- 인증서 폐지와 CRL

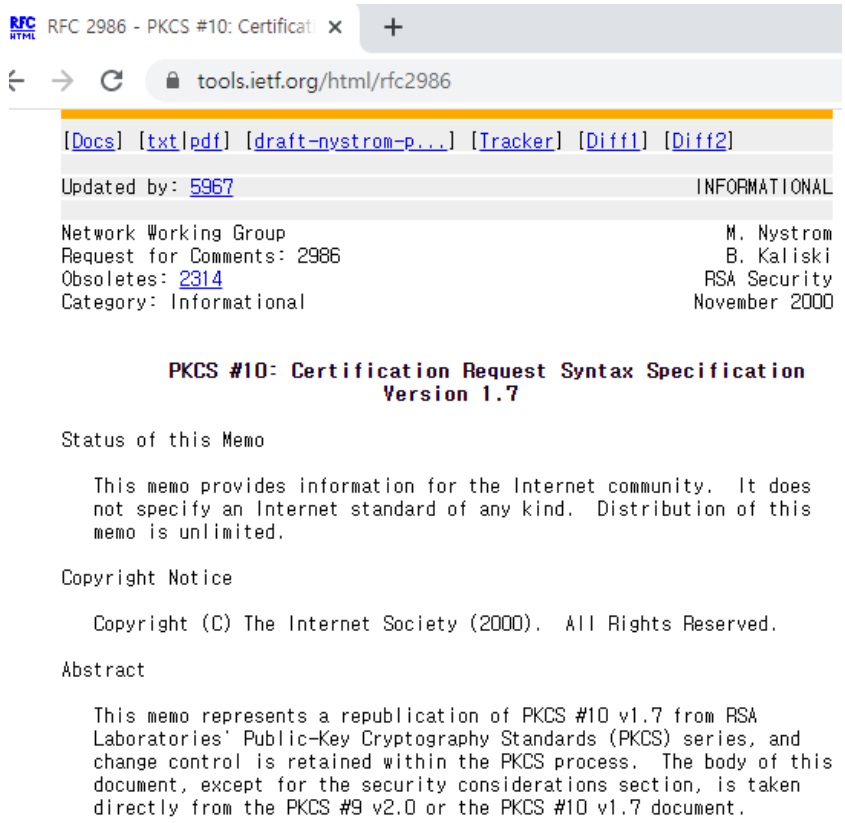
키 쌍의 작성

- 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



RFC 2986 - PKCS #10: Certificat

tools.ietf.org/html/rfc2986

[Docs] [txt|pdf] [draft-nystrom-p...] [Tracker] [Diff1] [Diff2]

Updated by: 5967 INFORMATIONAL

Network Working Group M. Nystrom
Request for Comments: 2986 B. Kaliski
Obsoletes: 2314 RSA Security
Category: Informational November 2000

PKCS #10: Certification Request Syntax Specification Version 1.7

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2000). All Rights Reserved.

Abstract

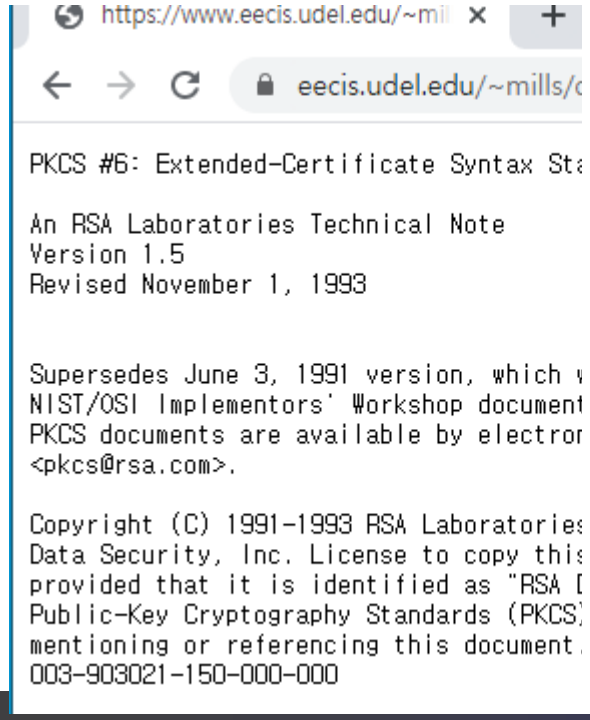
This memo represents a republication of PKCS #10 v1.7 from RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, and change control is retained within the PKCS process. The body of this document, except for the security considerations section, is taken directly from the PKCS #9 v2.0 or the PKCS #10 v1.7 document.

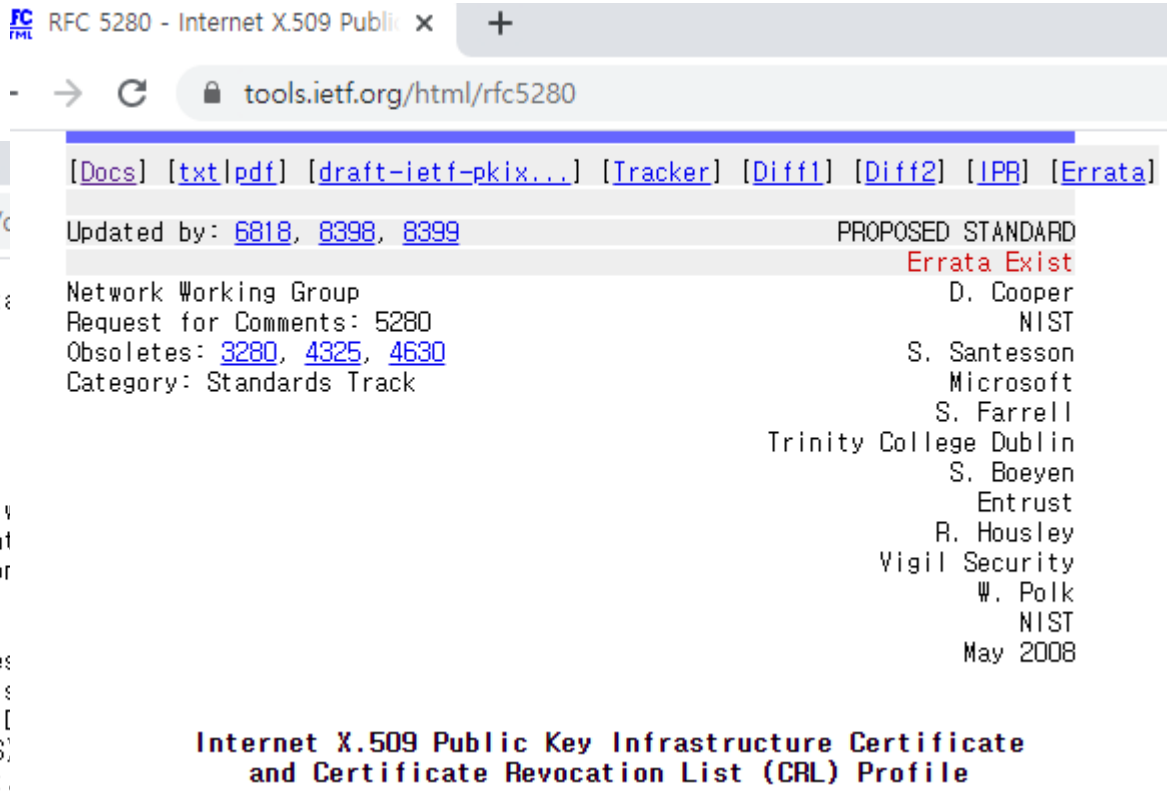
This memo describes a syntax for certification requests.

Table of Contents

인증서 등록

- 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

3.5 계층 구조를 갖는 인증서

회사 내의 사내 PKI

서울 본사(서울 본사 인증기관)

↓

충남 지사(충남 지사 인증기관)

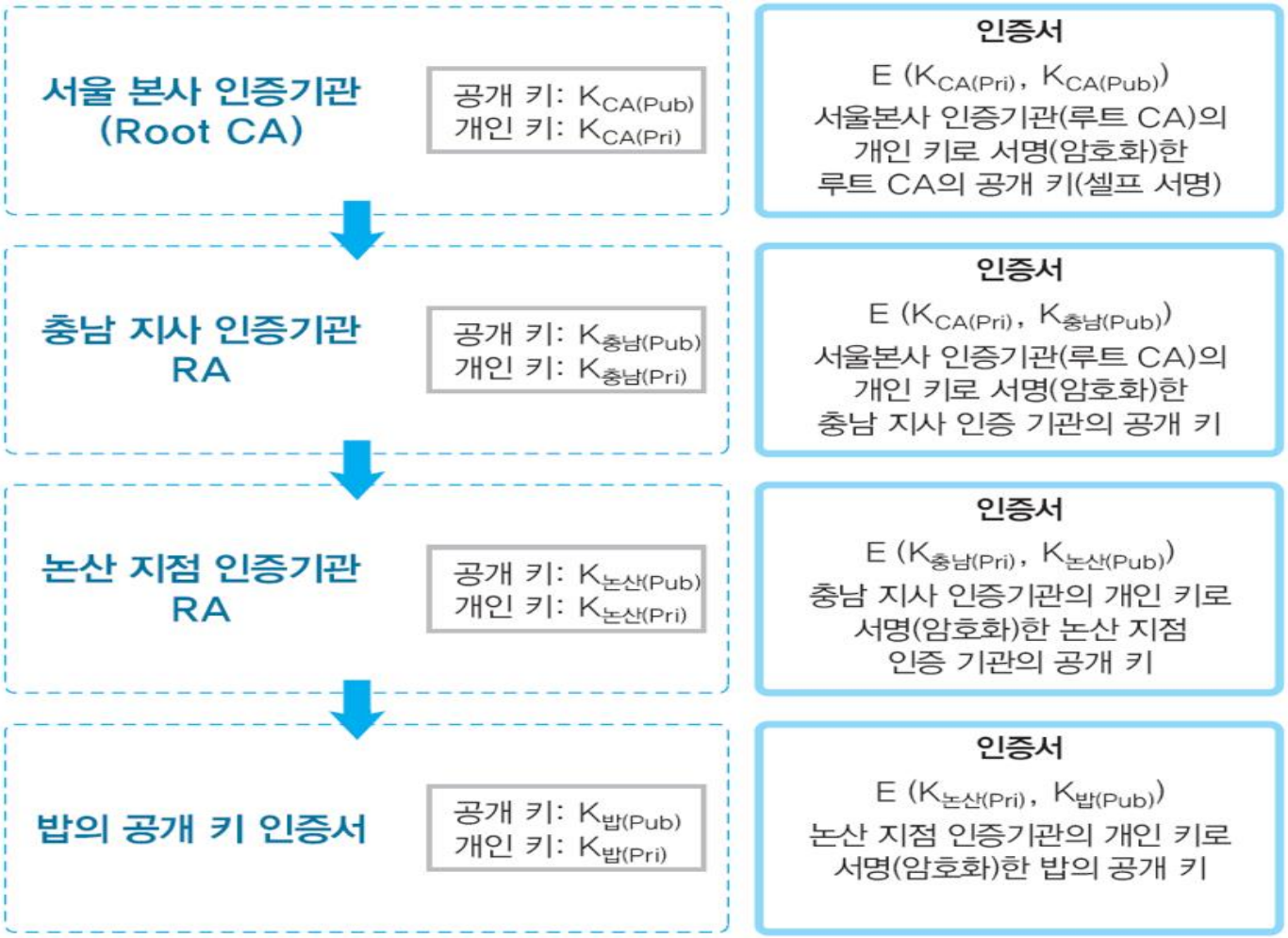
↓

논산 지점(논산 지점 인증기관)

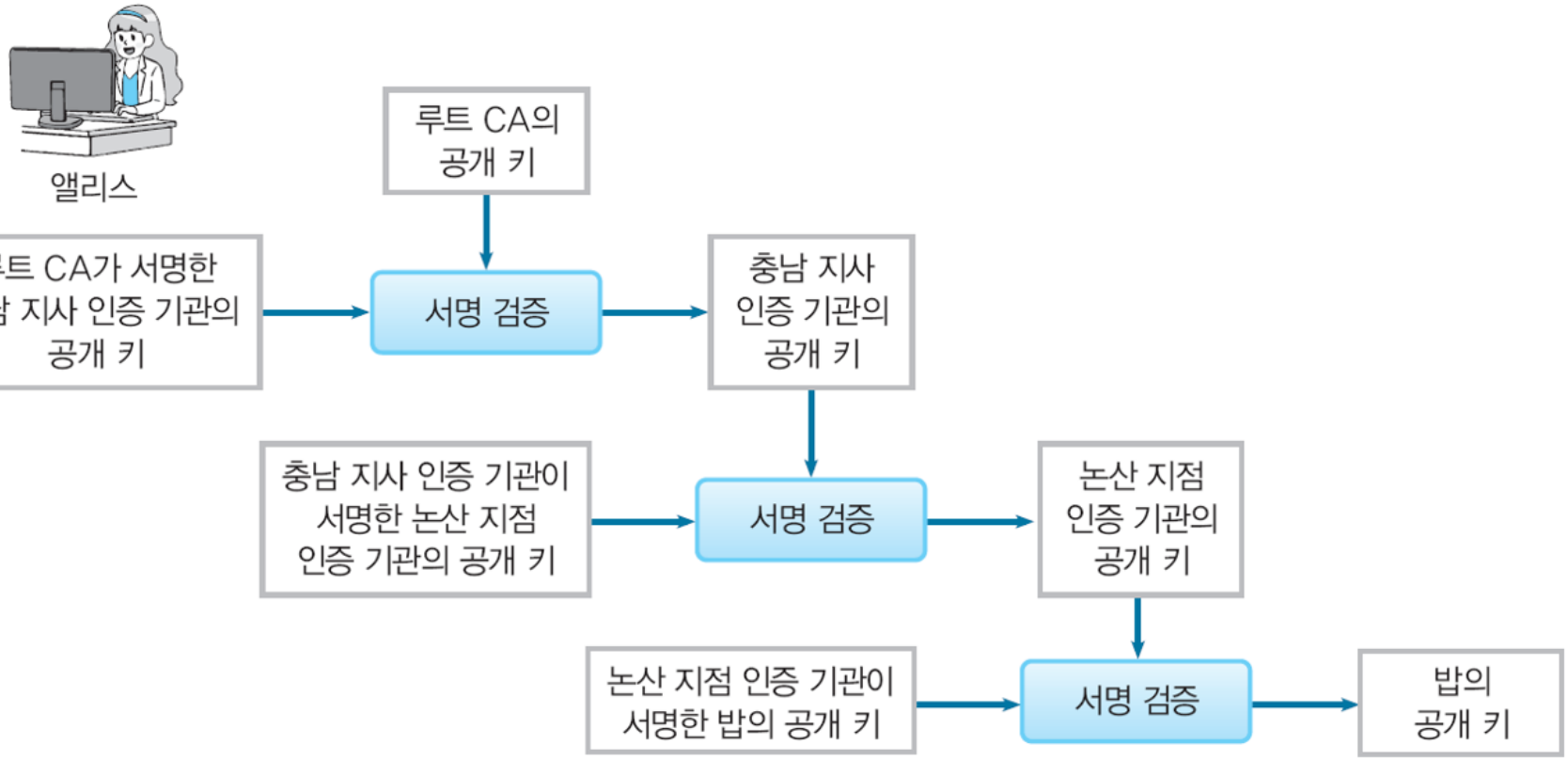
- 루트 CA
  - 최상위 인증 기관

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

계층 구조를 갖는 인증기관



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 전자서명인증관리센터**에서 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 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

4.7 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 닮은 사람을 등록하는 공격

- 오인하기 쉬운 사용자 정보를 사용
  - Name = Bob 을 Name = BOB 로
- 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 통지해야 함

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 도착하기 전 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

CRL

1.밥이 앨리스로부터 돈을 뜯어낼 계획수립
2.밥은 가명을 써서 계좌 X-5897을 개설
3.앨리스에게 송금 요청을 하고 자신의 서명을 붙인다
4.트렌트에게 개인키가 도난 당했다고 보고한다

5.앨리스에게 CRL이 도착하기 전에 앨리스가 해당 금액을 계좌 X-5897로 송금을 했다면

6.밥은 예금을 인출한다

7.앨리스가 나중에 CRL을 받고 밥에게 항의한다

8.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 보안 문제 일으킴
  - 통신을 가로채 개인 정보를 수집하여
    사용자의 인터넷 이용 맞춤 광고를 내보내는 소프트웨어
  - 루트 인증서를 인스톨하여 Web사이트와 Web브라우저 사이에 들어간 후, 방문한 Web사이트 인증서를 바꿔치기하여 Web브라우저에 제시
  - 전형적인 중간자 공격으로 통신 갈취

레노버 '해킹 노트북' 2년간 1,000만대 이상 판매, 사건 A to Z

MACGUYVER | 오후 5:35 | No comments

레노버가 결국 자신들의 PC에 슈퍼피쉬로 불리는 애드웨어를 설치했었음을 인정했습니다. 지난 20일, 미국의 IT 전문 보도매체인 리코드에서는 레노버가 한참이나 부인한 다음, 결국 자신들이 한 일임을 시인했다고 밝혀왔는데요.

이러한 슈퍼피쉬의 경우는 사용자의 인터넷 사용 패턴을 분석해서 그에 맞는 광고를 띄우는 방식의 애드웨어입니다. 더구나 슈퍼피쉬로 인해서 해커들에게 침입 경로가 생기는 만큼 컴퓨터 전체에 대한 보안이 취약해진다는 점에서 큰 논란이 되고 있습니다.

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.
    - 정부관련 기관 ?

제6절 공인 인증서를 대체하는 기술

공인 인증서 폐지 배경

- **‘전자 서명법’ 개정에 따라 2020년 12월 10일부로 공인인증서 폐지**
- 기존 공인인증서와 민간인증서 모두 ‘공동 인증서’로 사용됨
- 공인인증서의 독점 지위를 폐지하고, 사설인증서와의 경쟁을 촉발

HOME > 뉴스 > 보안

“공인인증서 폐지됐는데 여전히 사용되는 이유는”

김선애 기자 | 승인 2021.04.26 14:27 | 댓글 0

☰ 서울경제

“공인인증서 우월적 지위 폐지…여러 사설인증과 동등한 지위서 경쟁”
KISA “안전하고 편리한 인증 서비스 위해 전자서명 인증 사업자 선정 신속 진행”

공인인증서가 폐지된 이유는 크게 세 가지를 꼽을 수 있다. 첫째, 공인인증서를 사용하기 위해 Active X나 여러 보안 프로그램들을 필수 설치해야 한다는 점이다. 둘째, 공인인증서의 유효기간 1년이라 매해 갱신을 해야 하는 번거로움이 있다. 또 갱신을 하면 기존에 등록된 타행인증서 등록도 전부 초기화되어 각 은행 인터넷 뱅킹에 접속해 다시 타행등록을 해줘야 한다. 셋째, 공인인증서의 우월적 지위 때문에 새로운 전자서명 서비스의 시장진입이 어려웠고, 기술과 서비스의 혁신이 잘 이루어지지 않았다.

공인 인증서 폐지 이유

갱신과 보관의 불편

- 매년 갱신의 필요와 보관의 불편함

사이트 사용의 복잡

- 사용을 위한 엑티브X 프로그램 설치, 복잡한 과정 진행 등

민간 전자 인증 시장의 발전

- 6개의 공인인증기관만 공인인증서를 발급할 수 있었기 때문에 민간 전자인증 시장 발전 저해 영향

공인 인증서를 대체하는 기술

- **공동인증서**
  - 기존의 공인인증서가 공동인증서로 변경
  - 기존 6개 공인인증서 발급 기관 발급:금융결제원, 코스콤(구, 한국증권전산), 한국정보인증, 한국전자인증, 한국전산원, 한국무역정보통신
  - 유효기간: 1~3년
  - 주요 사용처: 금융, 공공기관, 전자거래, 사업자범용(일부)
  - 예)

인증서 종류	발급기관	인증서 유효기간	주요 사용처
금융인증서	금융결제원	3년	금융, 공공기관, 전자거래
한국전자인증서	한국전자인증	2년	금융, 공공기관, 전자거래 사업자범용 인증서

금융 인증서

- 기존 공인인증기관인 금융결제원 (금융인증센터)에서 제공하는 인증서

  https://www.yessign.or.kr

- 기존 공인인증서에 비해 빠르고 편하게 본인 인증이 가능함
- 6자리의 비밀번호 또는 패턴, 지문, 홍채 등의 생체정보를 통해 본인 인증이 가능하며 유효기간은 3년
- 금융, 공공기관, 전자거래 등 대부분의 **개인인증서를 필요로 하는 모든 서비스**를 지원

공인 인증서와 금융 인증서 비교

공동인증서	구분	금융인증서
6개 공인인증기관	발급기관	금융결제원
사용자 기기	보관방식	클라우드 서버
1년 (수동 갱신)	유효기간	3년 (자동 갱신)
영문+숫자+ 특수문자 혼합	비밀번호	6자리 숫자

한국전자인증서

- 기존 공인인증기관인 **한국전자인증**에서 제공하는 인증서

  https://www.crosscert.com/

- 기존 공인인증서에 비해 빠르고 편하게 본인 인증이 가능함
- 금융, 공공기관, 전자거래 등 대부분의 **개인인증서를 필요로 하는 모든 서비스**를 지원함
- 사업자 범용 공동인증서 지원

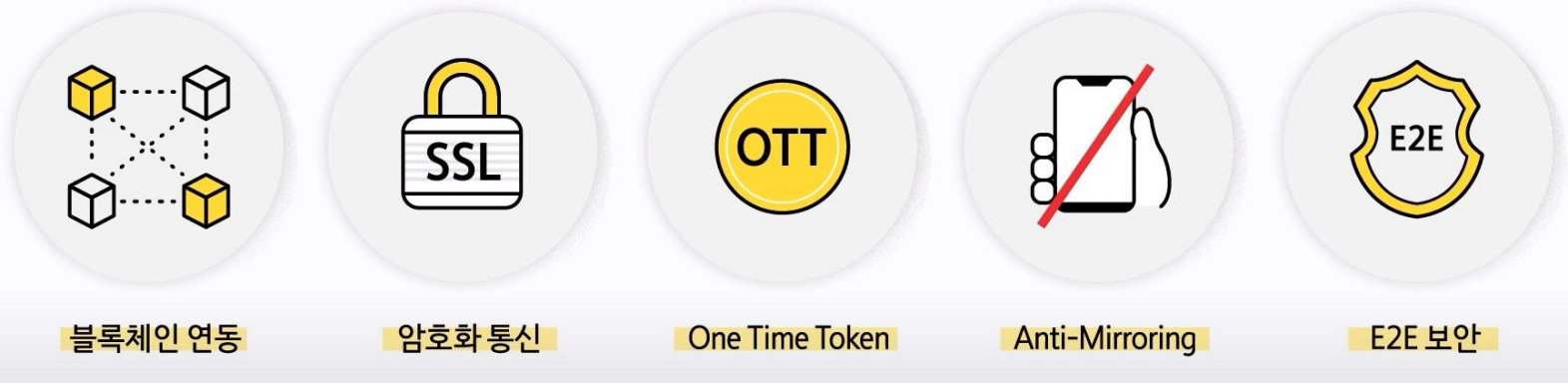
• 민간 인증서

– 예)

인증서 종류	발급기관	인증서 유효기간	주요 사용처
카카오인증서	카카오	2년	일부 금융, 공공기관, 전자거래
네이버인증서	네이버	3년	세금 납부, 일부 전자거래
PASS 인증서	통신 3사	3년	일부 금융, 공공기관, 전자거래
KB 모바일 인증서	KB국민은행	기간 없음	KB금융 비대면 서비스
토스 인증서	비바리퍼블라카	2년	일부 금융, 보험 서비스
페이코인증서	NHN PAYCO	2년	NHN 계열사 서비스, 일부 공공기관

카카오 인증서

- 카카오페이 기반의 인증서로 카카오톡을 통한 금융, 공공 인증 서비스 제공
- 카카오톡에 공개키(PKI) 인증 기술 결합, 전자문서 블록체인 연동
- One Time Token, SSL 암호화 통신, Anti-mirroring 등 지원
- 인증서의 유통기한은 2년



네이버 인증서

- 네이버앱을 통해 발급받을 수 있는 인증서로, 네이버 회원일 경우 손쉽게 발급 가능
- FIDO (Fast IDentity Online), PKI, 블록체인 등 여러 보안 기술을 적용, 일부 사이트의 경우 네이버 로그인을 통해 인증과정 간소화
- 유효기간은 3년

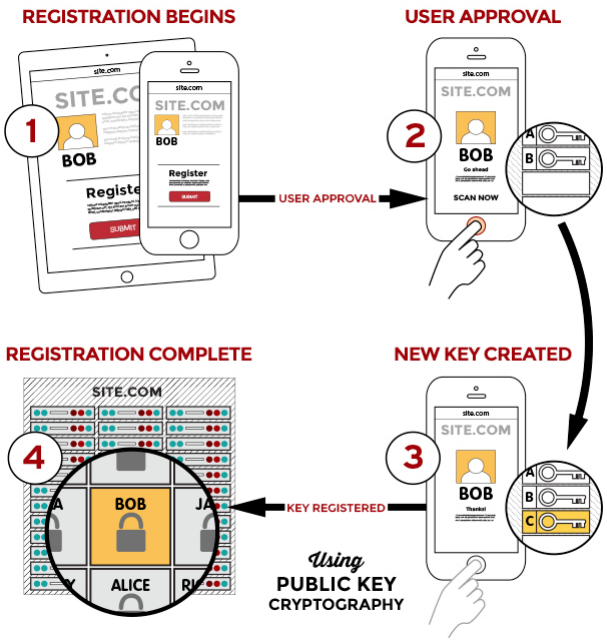
FIDO(Fast IDentity Online)

- FIDO Alliance: 온라인 환경에서 바이오인식기술을 활용한 인증방식에 대한 기술표준(De Facto)을 정하기 위해 2012년 7월 설립됨
- 이용자 단말에서의 사용자 로컬 인증과 서비스 제공 기관의 서버에서 수행하는 원격인증을 분리
- 구글, MS, 페이팔, 마스터카드, 레노버, LG전자 등 90개 업체가 참여 하여 활발하게 활동
- FIDO 기술 개념도

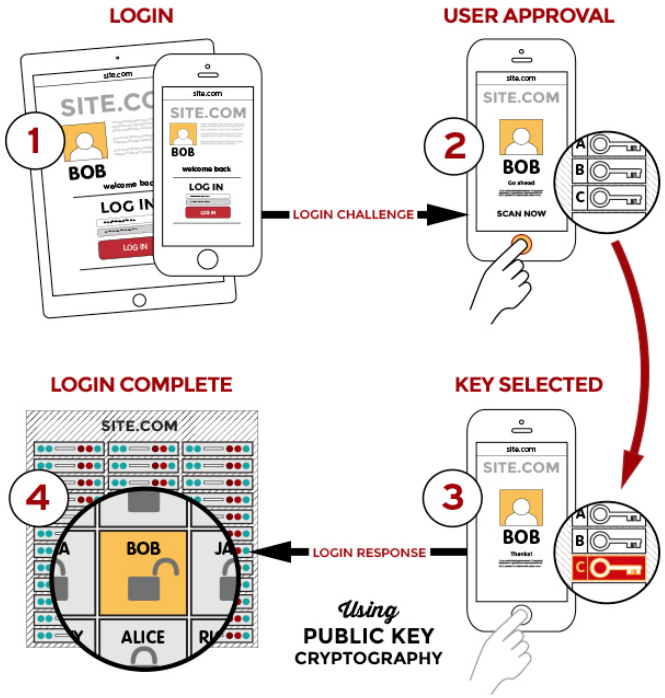
(출처: ETRI 기술동향 문서)

- FIDO 동작 과정
  https://fidoalliance.org/how-fido-works

  - FIDO 등록



  - FIDO 로그인



PASS 인증

화이트박스 암호: 알고리즘을 큰 룩업테이블로 만들고 그 안에 암호키를 소프트웨어로 구현된 암호 알고리즘과 뒤섞인 상태로 숨겨둠으로써 내부의 동작을 분석하더라도 암호키를 쉽게 유추하지 못 하도록 하는 기법

- PASS 앱 기반 인증서로 SK텔레콤, KT, LG유플러스가 공동 출시
- FIDO, 생체인증, WBC (White-Box Cryptography, 화이트박스 암호) 기반 보안 솔루션 지원
- 본인 인증만 제공하던 PASS 앱에 전자서명 기능을 추가
- 백신, 위변조 방지 등의 보안 기술을 적용
- 빠르게 발급받을 수 있으며, 유효기간은 3년

KB 모바일 인증

TAP: 하드웨어 기반의 **TEE**와 **WBC** 기반의 소프트웨어 보호기술을 사용하여 모든 기기**(Android** 및 **iOS)** 환경에 적용 가능한 보안 솔루션 - **K-SXXX** 회사 개발

- KB 국민은행에서 발급하는 모바일 인증으로 국민은행 모바일 서비스에서 활용 가능
- 패턴, 생체인식 기술 및 트러스토닉 애플리케이션 프로텍션 (Trustonic Application Protection: TAP)'을 적용 기술 적용
- 유효기간이 존재하지 않음

Toss 인증

- Toss와 한국전자인증 공동으로 운용하는 인증서
- 토스 어플리케이션, 또는 토스 웹사이트에서 핸드폰번호와 생년월일을 사용하여 간편하게 접속 가능
- PIN, 생체인증 기술 및 PKI, FIDO 기술 사용
- 유효기간은 2년

페이코 인증

- NHN 페이코에서 제공하는 인증서
- 패턴, 생체인식, 클라우드 블록체인 기술 적용
- 유효기간은 2년

- 금융권별 이용가능 인증서 현황

		12.10일 이전	12.10일 이후		
		공인인증서	공동인증서	금융기관 자체 인증서	금융인증서
		금융결제원, 코스콤 등 발급	금융결제원, 코스콤 등 발급	개별 금융기관 발급	금융결제원 발급
은행		○	○	국민, 농협 하나, 기업 등	22개 금융기관 등*
보험	생명	○	○	KB생보 등	메트라이프생명, 교보생명 등
	손해	○	○	KB손보 등	DB손보 등
증권사		○	○	KB증권 등	×
기타 (카드사 등)		○	○	KB국민카드 KB저축은행 등	우리카드, 롯데카드 등

(2020. 12. 10이용 가능) 산업, 국민, 수협, 우리, SC제일, 대구, 부산, 광주, 제주, 전북, 경남, 새마을금고, 하나, 신한 (14개 기관)

(2020. 12. 10 이후 이용 가능) 기업, 농협, 산림조합중앙회, 중국공상, 케이뱅크, 씨티, 카카오뱅크, 신협 등

11장 인증서

연습문제 풀이

연습문제

1. 공개 키 인증서에 들어가는 내용이 아닌 것은?

① 이름

② 공개 키

③ 개인 키

④ 메일 주소

⑤ 유효 기간

연습문제

2. 인증기관은 공개 키 등록자에 대한 인증을 하기 위해 사용자의 인증서에 자신의 _____로 서명을 한다.

① 공개 키

② 개인 키

③ 대칭 키

④ 세션 키

⑤ 라운드 키

연습문제

3. ITU-T 권고안에서 말하는 인증서 표준규격은 다음 중 어느 것인가?

① RFC 822

② X.25

③ PKI

④ X.509

⑤ X.800

연습문제

4. 인증서의 구체적인 내용에 속하는 것들을 묶은 것이다. 속하지 않는 항목을 포함하고 있는 것은?

① 버전 번호, 일련번호, 서명 알고리즘 식별자

② 발행자 이름, 유효기간, 소유자 이름

③ 소유자의 공개 키 정보, 발행자 유일 식별자

④ 버전 번호, 유효기간, 소유자 유일 식별자

⑤ 발행자 이름, 소유자 개인 키 정보, 발행자 유일 식별자

연습문제

5. 공개 키 인증서는 크게 나누어 세 부분으로 이루어져 있는데 여기에 속하지 않는 것은?

① 서명 전 인증서

② 디지털 서명 알고리즘

③ 디지털 서명 본체

④ 디지털 서명 발행주체

⑤ 답 없음

연습문제

6. 공개 키 기반(PKI)에 대한 설명으로 적합한 것은?

① 공개 키를 효과적으로 운용하기 위해 정해진 많은 규격이나 선택사양의 총칭이다.

② 공개 키를 도난당하지 않도록 한 장소에 모아 관리하는 관리소이다.

③ 공개 키를 발급하는 기관들의 전체 모임을 말한다.

④ 공개 키의 활용방안 및 새로운 공개 키를 개발하기위한 연구기관이다.

⑤ 공개 키에 대한 공격유형의 연구나 취약점을 보완하기 위한 연구기관이다.

연습문제

7. 공개 키 기반(PKI)을 개발하게 된 주요한 목적에 대한 설명으로 적합한 것은?

① 공개 키의 안전성에 대한 검증을 하기위한 것이 목적이다.

② 공개 키를 안전하고, 편리하고, 효율적으로 획득하는 것이 목적이다.

③ 공개 키에 대한 공격을 사전에 방지하기 위한 것이 목적이다.

④ 공개 키의 활용방안 및 새로운 공개 키를 개발하기 위한 것이 목적이다.

⑤ 공개 를 통일하기 위해 국가 간의 협조체제를 구축하기 위한 것이 목적이다.

연습문제

8. 공개 키 기반(PKI)의 구성요소로만 묶인 것은?

① 검증기관, 인증기관, 저장기관

② 인증기관, 발급기관, 관리기관

③ 이용자, 인증기관, 저장소

④ 이용자, 폐지기관, 관리기관

⑤ 이용자, 발급기관, 폐지기관

연습문제

9. 공개 키를 인증기관에 등록할 때 이용자가 하는 일이 아닌 것은?

① 키 쌍을 작성한다.

② 인증기관에 공개 키를 등록한다.

③ 인증기관으로부터 인증서를 발행 받는다.

④ 등록한 공개 키를 무효로 한다.

⑤ 자신의 공개 키를 암호화 한다.

연습문제

10. 인증기관에서 하는 일이 아닌 것은?

① 키 쌍을 작성한다.

② 공개 키 등록 때 본인을 인증한다.

③ 인증서를 작성해서 발행한다.

④ 사용자의 개인 키를 보관한다.

⑤ 인증서를 폐지한다.

연습문제

11. 인증기관에서 하는 일 중에 공개 키 등록과 본인 인증을 일일이 할 수 없을 경우에 일을 분담하기 위한 기관을 설정하는데 이런 기관을 뭐라고 부르는가?

① 등록기관

② 저장기관

③ 지역기관

④ 대행기관

⑤ 폐지기관

연습문제

12. 인증서를 보존해 두고, PKI의 이용자가 인증서를 입수할 수 있도록 한 데이터베이스를 무엇이라고 하는가?

① 인증서 은행
② 인증서 폴더
③ 인증서 디렉토리
④ 인증서 웨어하우스
⑤ 인증서 하드

연습문제

13. PKI를 이용할 경우에 복호화 키에 대한 접근을 할 수 없는 경우가 생기는데 이 경우에 자신이 사용하는 키 쌍을 복구해야 할 경우가 생긴다. 그 경우에 해당되지 않는 것은?

① 패스워드를 잊어버렸을 경우

② PIN(Personal Identification Number)을 잊어버렸을 경우

③ 디스크 드라이버에 결함이 생겼을 경우

④ 하드웨어 토큰이 망가졌을 경우

⑤ 다른 시스템으로부터 PKI에 접근을 해야 할 경우

연습문제

14. 인증서 폐지요청의 사유로 해당되지 않는 것은?

① 공개 키 인증서의 사용자 수가 일정 수 이상을 초과하였을 경우

② 개인 키가 노출되었을 경우

③ 가입 상태가 변경되었을 경우

④ 이름이 변경되었을 경우

⑤ 본인이 해당 개인 키를 사용할 권한을 잃은 경우

연습문제

15. 인증서를 폐지하는 경우 인증기관은 인증서 폐지 목록을 작성하는 데 이것을 영어로 _____이라고 한다.

① URL(User Revocation List)

② CRL(Certificate Revocation List)

③ UEL(User Expiration List)

④ REL(Registration Expiration List)

⑤ CEL(Certificate Expiration List)

연습문제

16. 한 사용자가 다른 사용자의 인증서를 얻기 위해서 연속된 인증절차를 거치게 되는데 이것을 무엇이라고 하는가?

① Continuous Certificate

② Serial Certificate

③ Chain of Certificate

④ Trail of Certificate

⑤ Line of Certificate

참고문헌

- “네트워크 보안 에센셜 3판”, 윌리엄 스톨링스 저(전태일 등역) , 교보문고
- '공인' 사라지자 은행들, 속속 인증서비스…"신사업 포석", 메일경제, https://www.mk.co.kr/news/economy/view/2020/12/1277926/
- 공인인증서 폐지, 대체인증 기술은?, 투이컨설팅, http://www.2e.co.kr/news/articleView.html?idxno=301030
- [커버스토리] 전자서명법 개정, 인증 시장 불붙는다, 컴퓨터월드, https://www.comworld.co.kr/news/articleView.html?idxno=49880
- 공인 인증서 '퇴장'... 카카오, 네이버 인증서 직접 써보니, 한국경제 IT과학, https://www.hankyung.com/it/article/202012117435g
- '공인 인증서 폐지' 대안과 이유, 민간인증서의 특징, 정보메거진, https://daniel615.tistory.com/368
- PASS 인증서 서비스소개서, PASS, https://www.passauth.co.kr/main
- 페이코 인증서 소개서, NHN PAYCO 인증센터, https://cert.payco.com/
- 카카오페이 인증 소개, 카카오페이, https://www.kakaosign.com/ct/features
- 한국전자인증 보안솔루션 Toss 인증 서비스, https://solution.crosscert.com/toss/
- FIDO(Fast IDentity Online) 규격, 금융보안원 보안연구부 보안기술팀
- FIDO Alliance, https://fidoalliance.org/

Q & A

Thank You!