인증과 공개키기반구조

이 병 천

2011. 11. 22

중부대학교 정보보호학과

목차

1. 인증

- 인증이란?
  - 인증을 하고자 하는 주체(Subject)에 대해 식별(Identification)을 수행하고, 이에 대한 인증(Authentication & Authorization) 서비스를 제공하는 시스템
- **AAA** 서비스
  - Authentication - 인증
  - Authorization - 인가
  - Accounting - 기록

인증시스템 사례

- 컴퓨터 로그인
  - 부팅시 로그인 - 관리자, 사용자
  - 화면보호기
  - 원격 로그인
- 서비스 로그인
  - 포털사이트 로그인
  - 업무 서비스 로그인
- 어플리케이션 로그인
  - 공인인증서 활용

1.1 인증의 종류

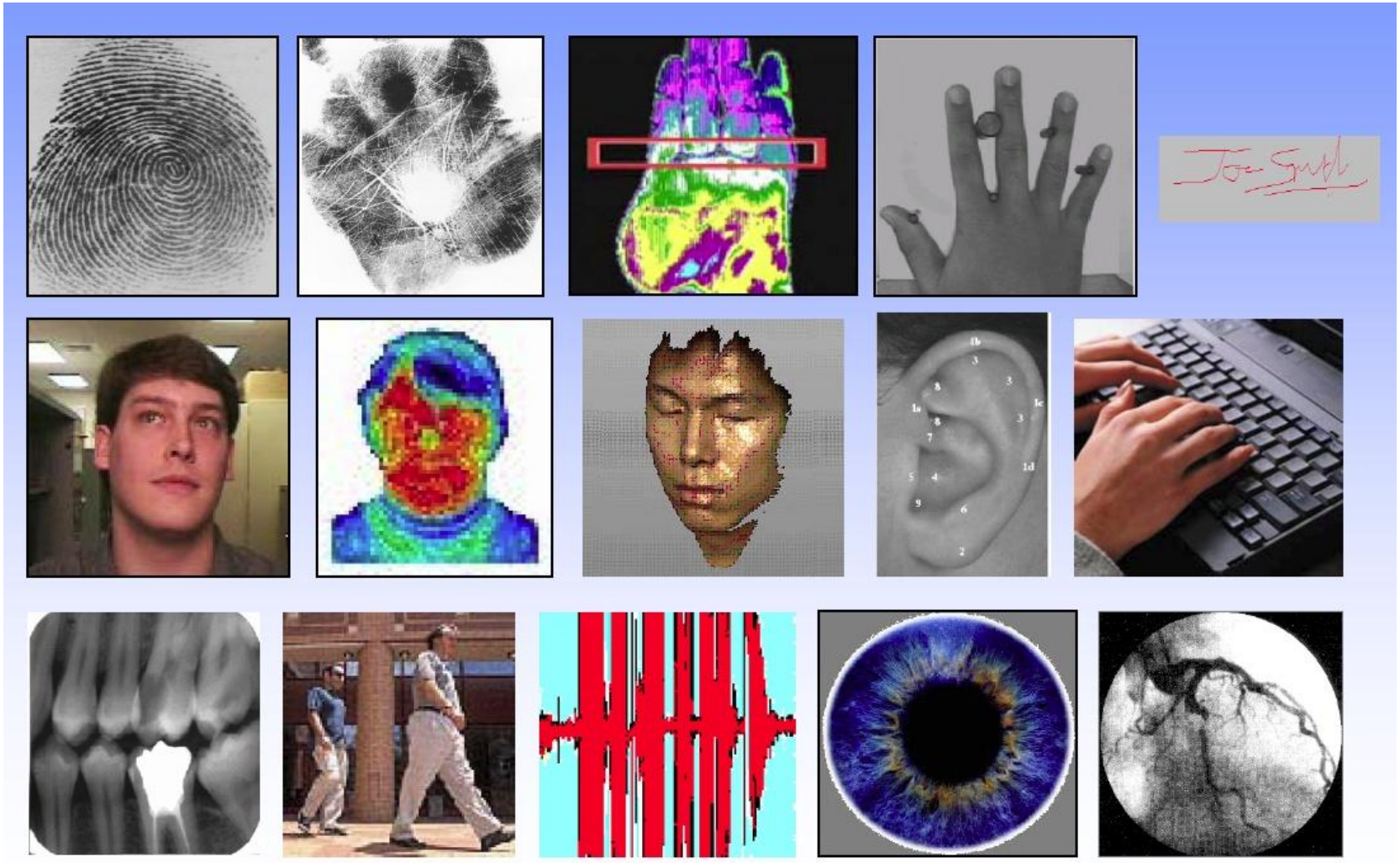
- 사용자 인증 **(Identification)**
  - 사용자의 신원을 확인하고 인증
- 메시지 인증 **(Message Authentication)**
  - 메시지가 특정 사용자에 의해 만들어졌음을 인증
  - Message Authentication Code, 전자서명

인증의 세가지 접근방법

- **Something You Know**
  - 사용자가 기억하는 지식을 이용
  - 사례: 패스워드, PIN 등
- **Something You Are**
  - 생체조직(Biometrics)을 통한 인증
  - 사례: 지문, 손모양, 망막, 홍채, 서명, 키보드, 목소리, 얼굴
- **Something You Have**
  - 사용자가 인증 수단을 소유해 인증을 수행
  - 사례: 스마트키, 스마트카드, 신분증, 인터넷뱅킹 카드와 OTP, 공인인증서 등
  - Something You Have는 다른 사람이 쉽게 도용할 수 있기 때문에 단독으로 쓰이지 않고, 일반적으로 Something You Know나 Something You Are와 함께 쓰임.

Biometric을 이용한 인증

❖



멀티팩터 인증

- 하나의 인증수단 만으로는 취약성이 있는 경우 두 가지 이상의 서로 다른 인증 수단을 함께 사용하는 방법

- 신분증
  - 학생증, 주민등록증, 운전면허증 등
  - 본인임을 확인하기 위해 얼굴을 대조하므로 신분증은 Something You Have와 Something You Are 둘 다를 인증 수단으로 이용.

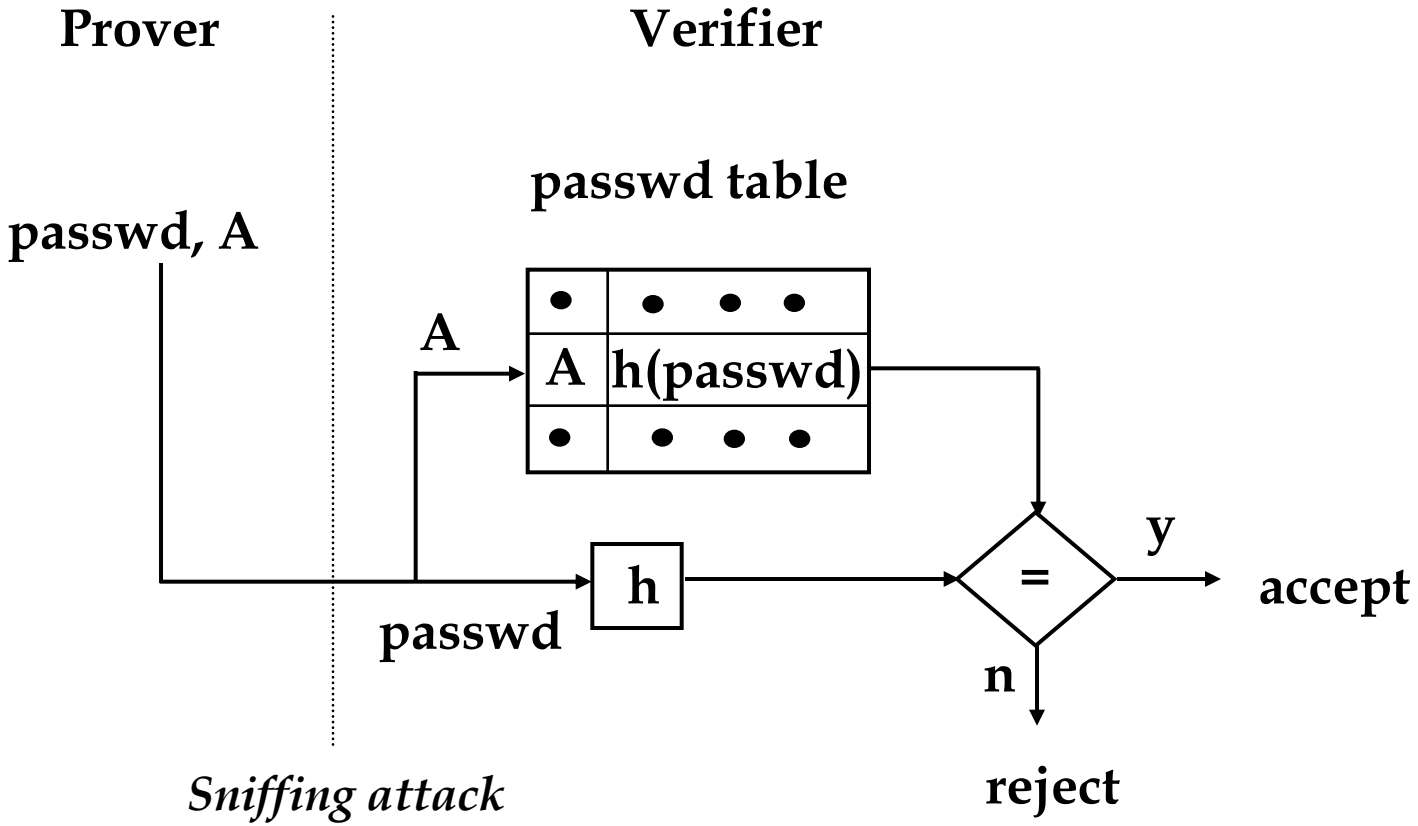
- 인터넷 뱅킹
  - 인터넷뱅킹시 인증서와 함께 보안카드나 OTP를 병행 사용
  - 서명시 비밀키 접근암호 이용

인터넷뱅킹에 사용되는 OTP

1.2 암호학적 인증 기법

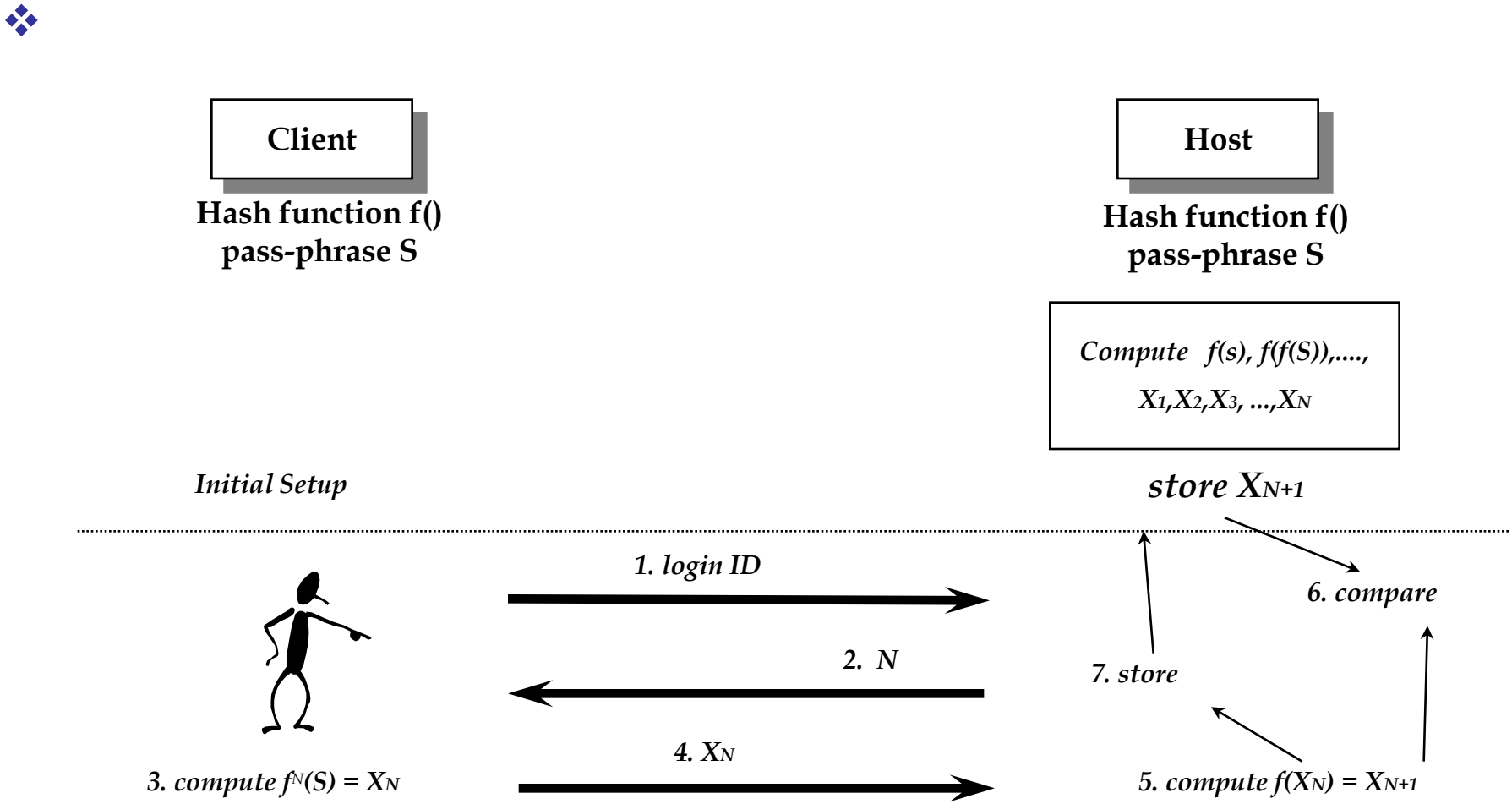
- 패스워드 기반 **(Weak Authentication)**
  - crypt *passwd* under UNIX
  - one-time password
- 도전-응답 기법 **(Strong Authentication)**
  - 질문에 대해 정확한 대답을 할 수 있어야 인증
  - 대칭키암호, 해쉬함수, 비대칭키암호 이용
- 암호 프로토콜 이용
  - Fiat-Shamir identification protocol
  - Schnorr identification protocol

패스워드를 이용한 인증



Replay attack - Static password

S/Key (One-time Password)



Schnorr Identification

$$x = \log_g Y \bmod p, \qquad (Y = g^x \bmod p)$$

Prover | **Verifier**

$t \in_R Z_q^*$

$R = g^t \bmod p$

R *Commitment* →

$u \in_R Z_q^*$

← u *Challenge*

$w = t - ux \bmod q$

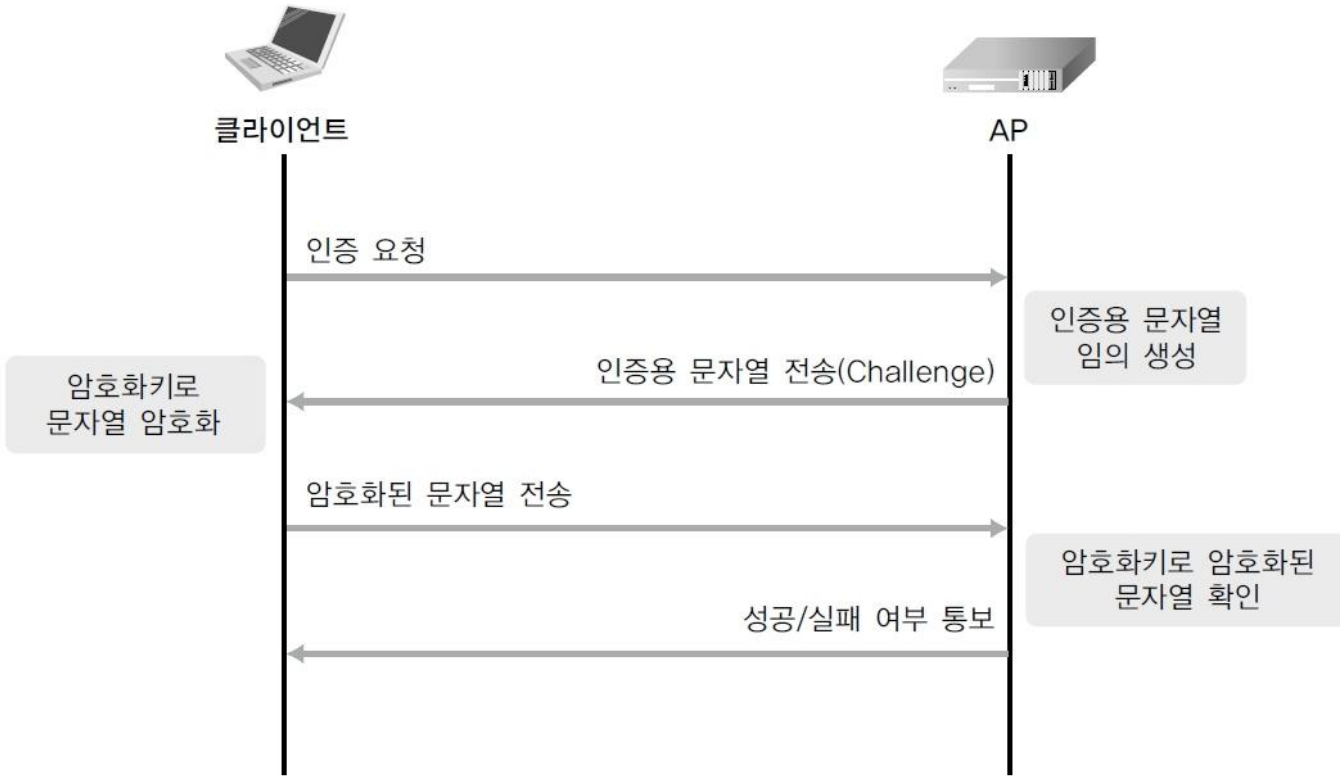
w *Response* →

$R \overset{?}{=} g^w Y^u \bmod p$

1.3 인증 시스템

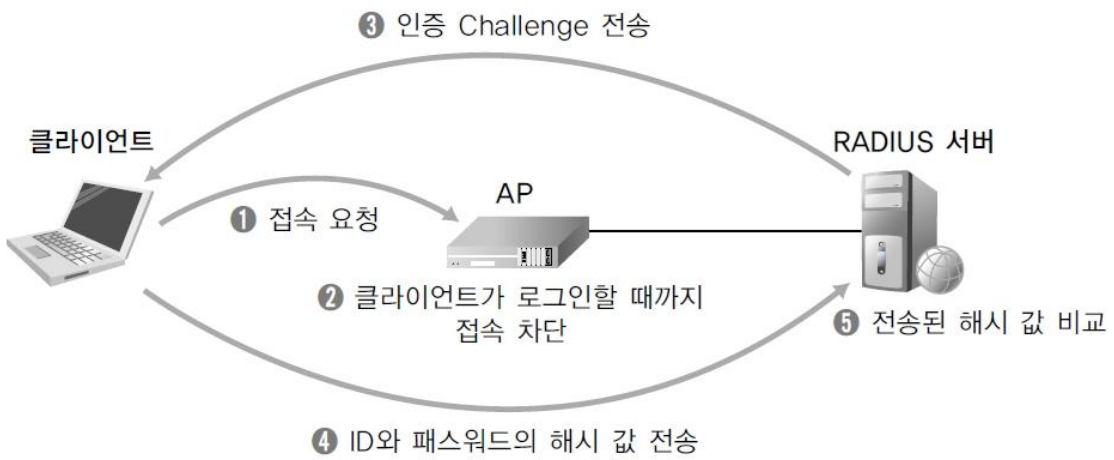
❖ WEP(Wired Equivalent Privacy)

- 무선 랜 통신을 암호화하기 위해 802.11b 프로토콜부터 적용
- 1987년에 만들어진 RC 4 암호화 알고리즘을 기본으로 사용
  - 64/128비트 사용 가능. 64비트는 40비트, 128비트는 104비트 RC 4 키 사용
- WEP을 이용한 암호화 세션

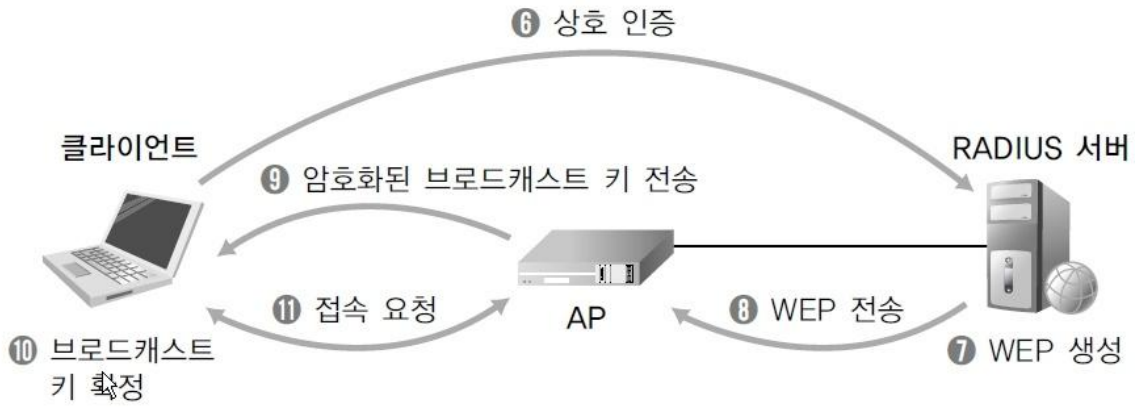


- ***암호화 과정에서 암호화키와 함께 24비트의 IV(Initial Vector)를 사용. 통신 과정에서 IV는 랜덤으로 생성되어, 암호화키에 대한 복호화를 어렵지만 24비트의 IV는 통신 과정에서 24비트의 짧은 길이로 인해 반복 사용되며, 반복 사용이 WEP 키의 복호화를 쉽게 함***
- ***무선 통신에서 네트워크 패킷에 포함된 IV를 충분히 수집하여 WEP 키를 크랙할 경우1분 이내에도 복호화 가능***

RADIUS와 802.1X를 이용한 무선랜 인증



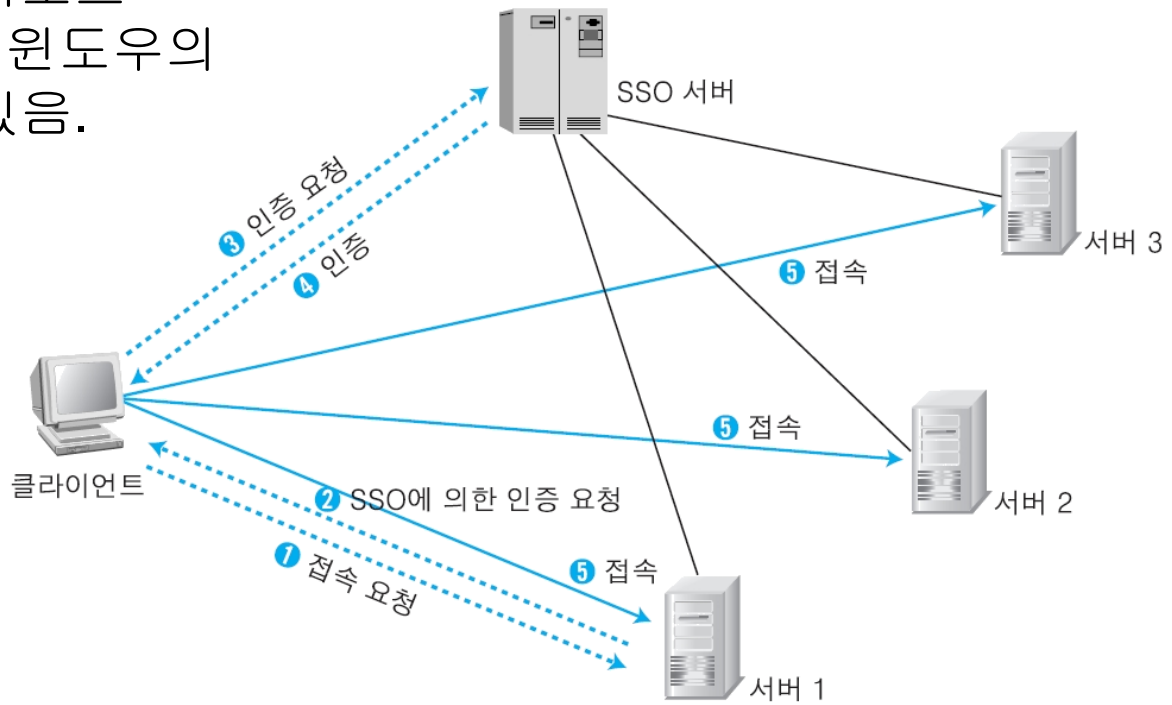
[그림 12-29] RADIUS와 802.1X를 이용한 무선 랜 인증 1



[그림 12-30] RADIUS와 802.1X를 이용한 무선 랜 인증 2

싱글사인온

- **Single Sign On(SSO)**
  - 모든 인증을 하나의 시스템에서. 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면 다른 시스템에 대한 접근 권한도 모두 얻음.
  - 이러한 접속 형태의 대표적인 인증 방법으로는 커버로스(Kerberos)를 이용한 윈도우의 액티브 디렉토리가 있음.



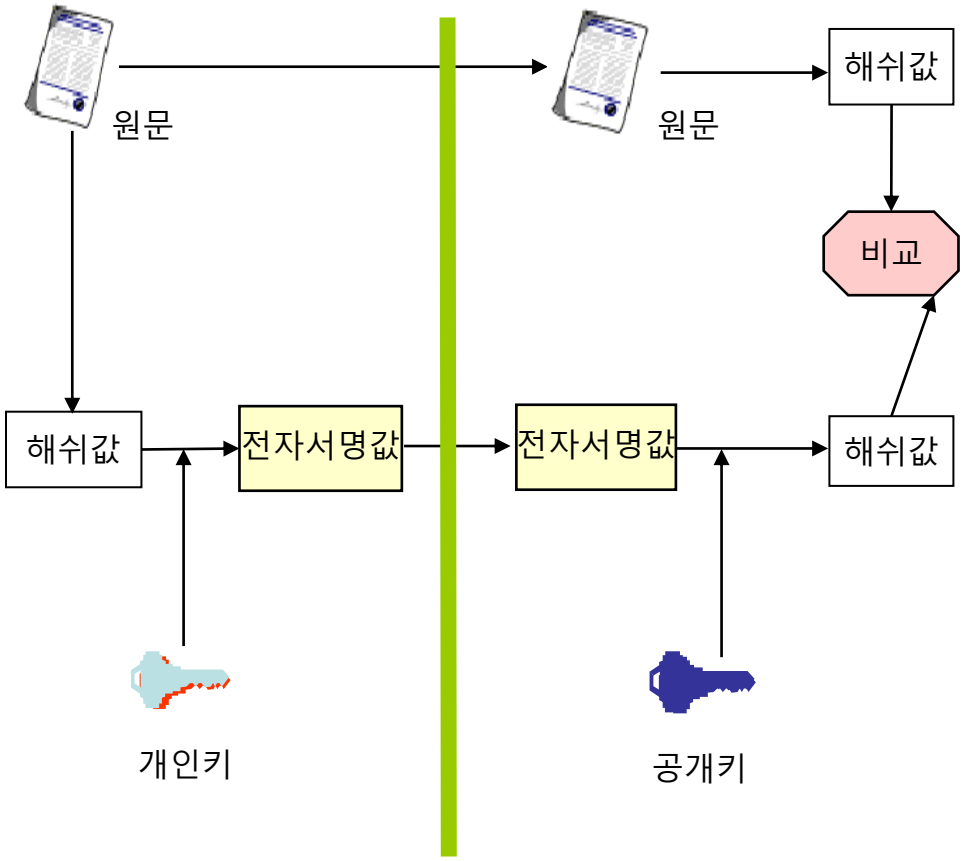
[그림 10-7] SSO에 의한 인증

인증의 범위 확장

- 서버별 인증
  - 서버별 사용자 등록
  - 사용자가 각기 다른 아이디, 패스워드 관리 필요
- 조직 내 인증
  - 싱글사인온. 한번의 사용자 등록으로 조직내 모든 서버에 인증 가능
- 공인인증
  - 제한 없는 인증 확장을 위해 공인인증이 필요
  - 공인인증서
  - 공개키기반구조

2. 공인인증서

❖ 공개키 암호를 이용하는 전자서명



전자서명의 기능

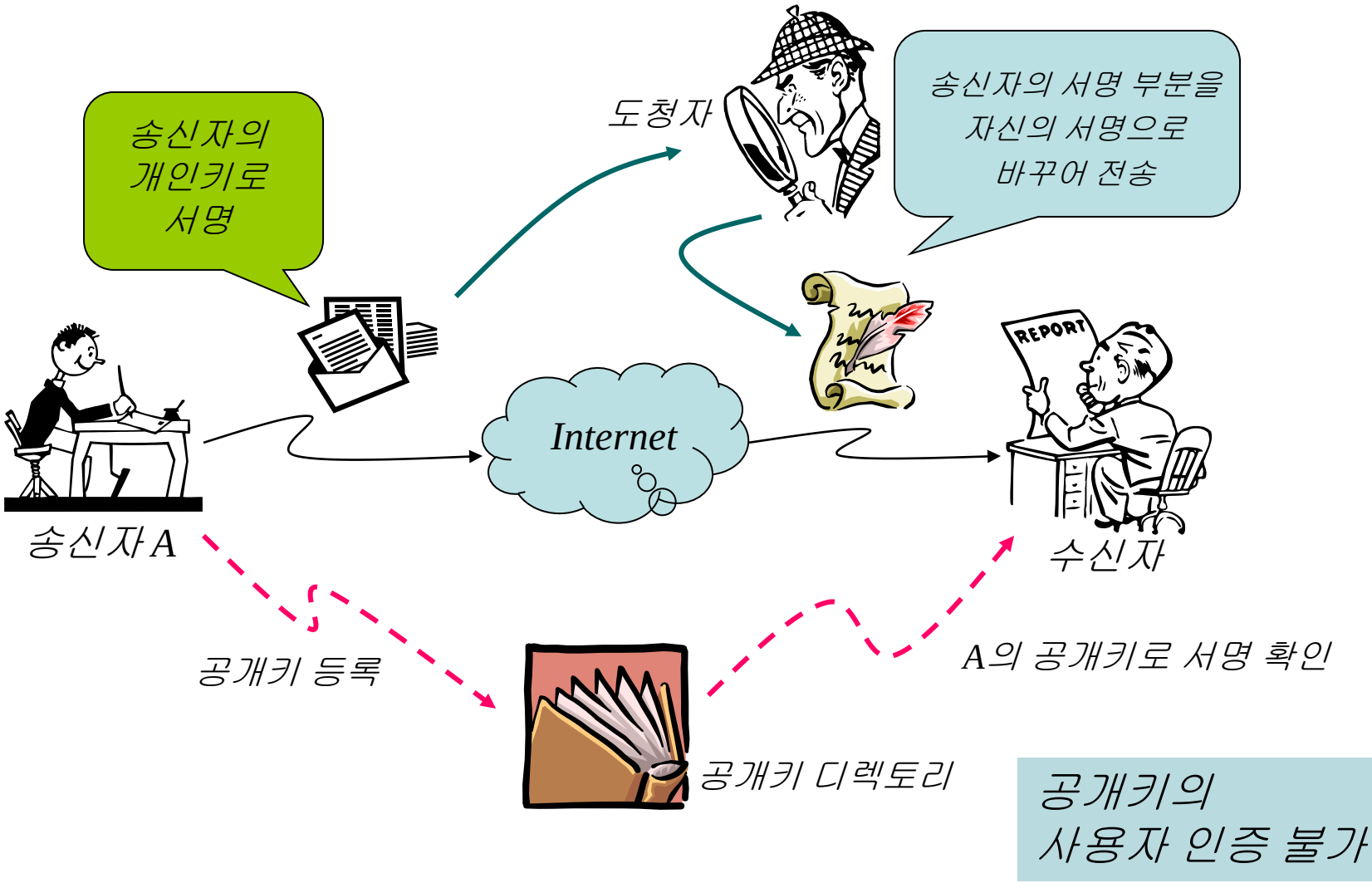
※ 본인 인증
송신자 본인이 서명했음을 인증

※ 무결성 보장
원문의 해쉬값과 전자서명값을 복호화한 해쉬값을 비교함으로서 위.변조 여부를 판단

※ 부인 봉쇄
송신자는 자신만이 가지고 있는 개인키를 이용하여 전자서명을 하였으므로 문서를 전송하지 않았다고 부인 불가

공개키의 진위성 확인?

공개키 디렉토리 모델


송신자의
개인키로
서명
도청자
송신자의 서명 부분을
자신의 서명으로
바꾸어 전송
REPORT
Internet
송신자 A
수신자
공개키 등록
A의 공개키로 서명 확인
공개키 디렉토리
공개키의
사용자 인증 불가

2.1 공개키인증서

- **공개키인증서 (Certificate)**
  - 사용자의 공개키와 사용자의 ID정보를 결합하여 인증기관이 서명한 문서, 공개키의 인증성을 제공
  - 사용자 확인, 특정한 권한, 능력을 허가하는데 이용
  - 정보화 사회에서 개인의 신분증 역할
  - 인증기관(CA)은 자신의 개인키를 사용하여 전자서명을 생성하여 인증서에 첨부, CA의 공개키를 사용하여 인증서 유효성 확인

사용자 A의 공개키

+

사용자 A의 공개키에 대한 인증기관(CA)의 전자서명

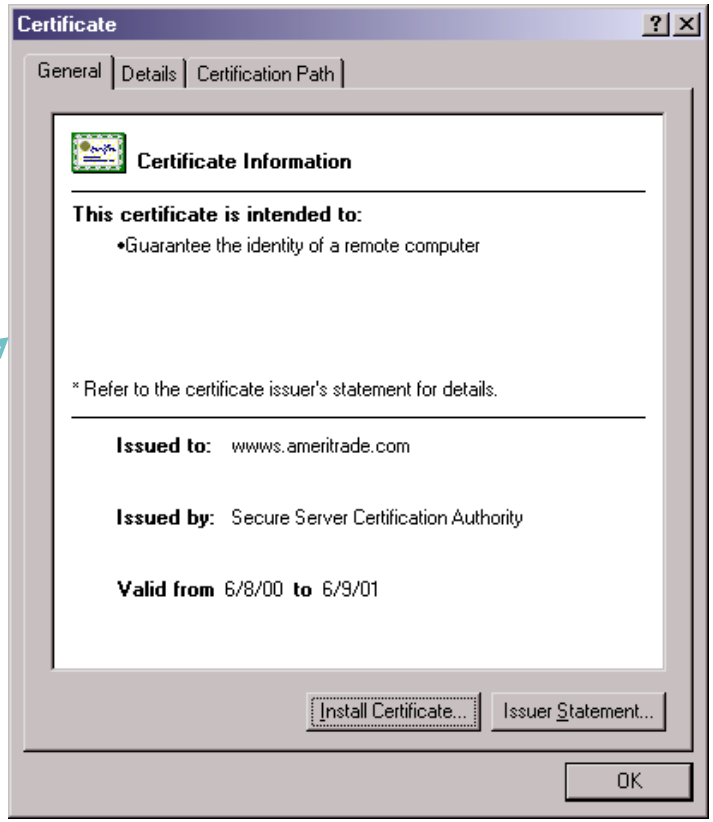
=

사용자 A의 인증서(사용자 A의 공개키와 이것을 증명코자 하는 신뢰(인증)기관의 전자서명 포함)

공개키인증서 확인

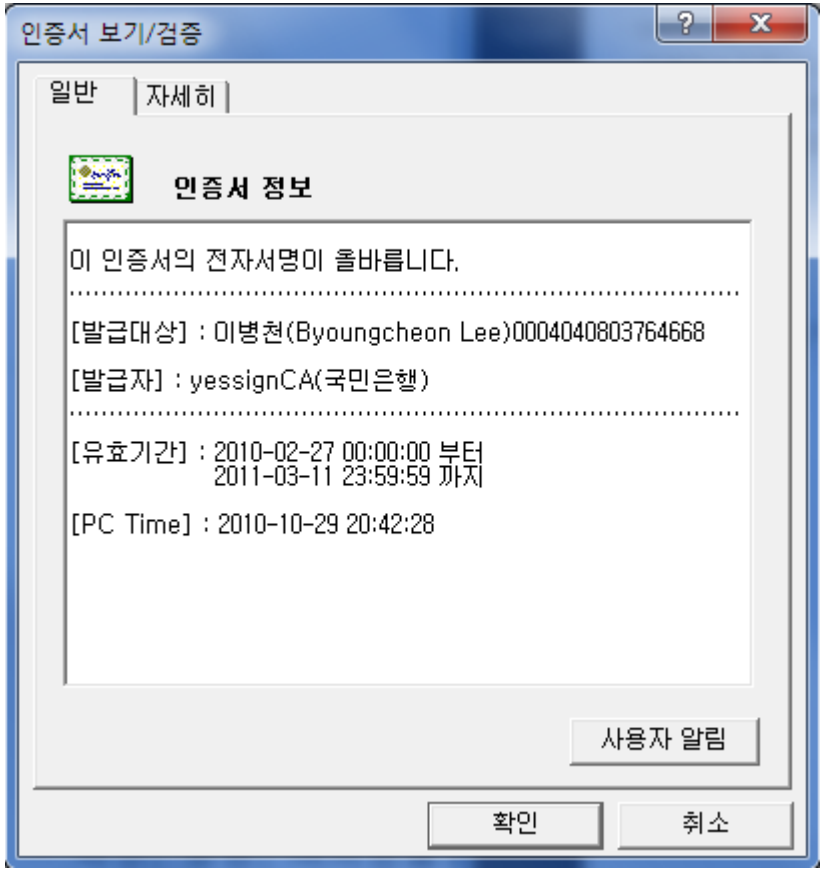
https 접속

클릭

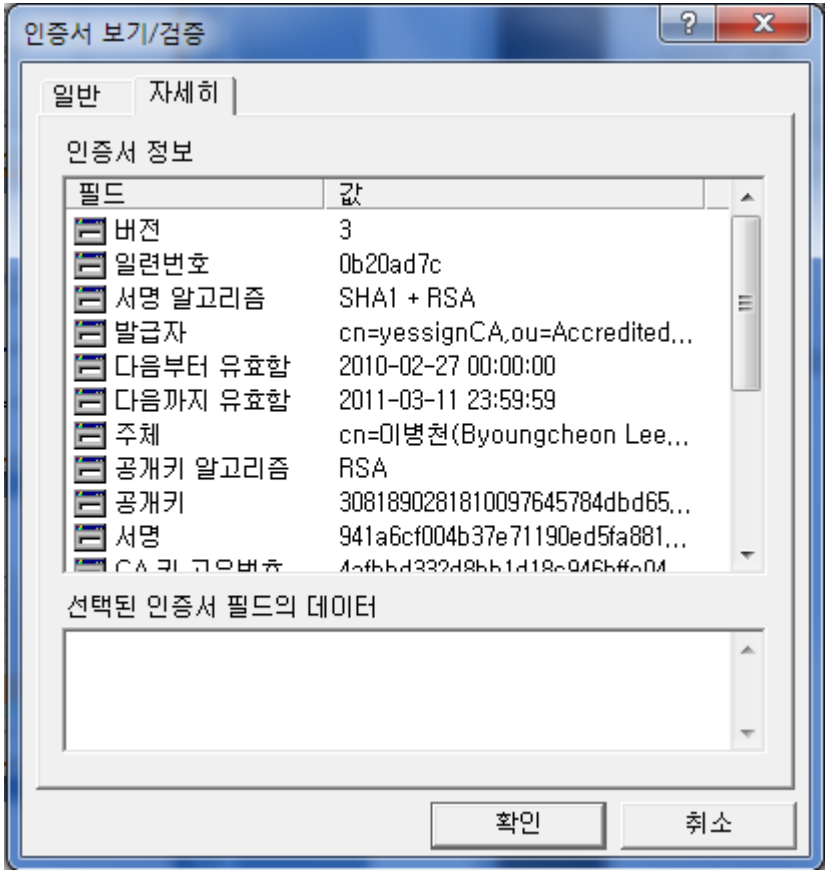


공개키인증서

일반정보



상세정보

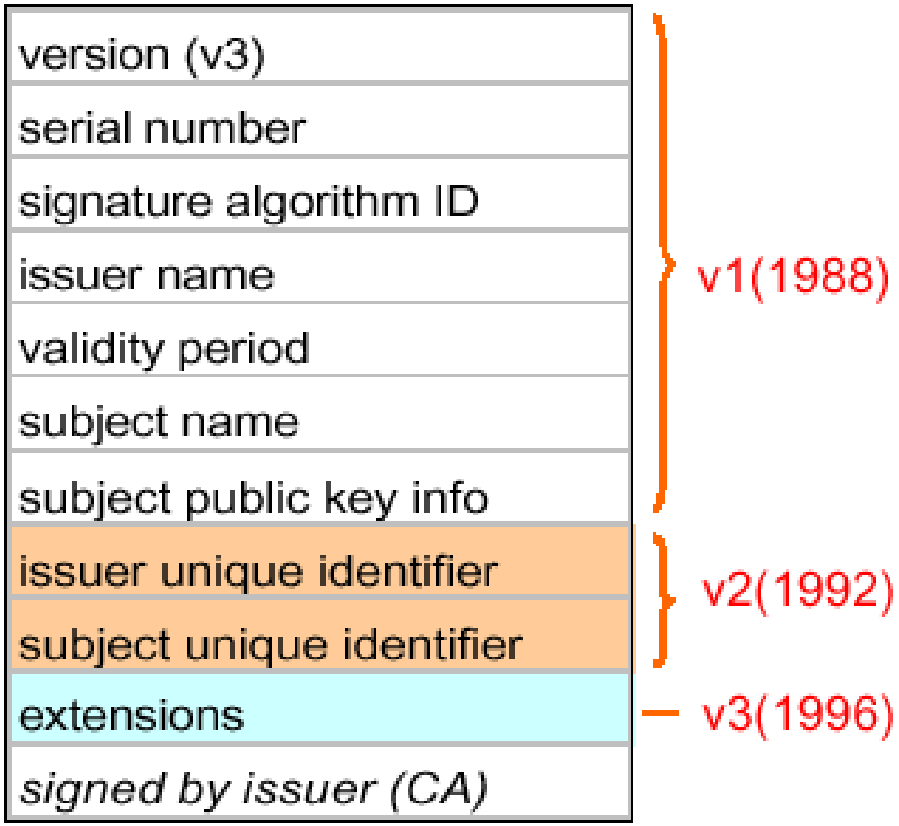


2.2 인증서의 구조

- **X.509 인증서 표준**
  - ITU에 의해 제안된 인증서에 대한 기본 형식을 정의한 규격
  - X.509 v1 (1988)
  - X.509 v2 (1992)
    - 인증서 취소 목록(CRL: Certificate Revocation List)을 도입
    - 고유 ID (Unique identifier) 도입
  - X.509 v3 (1996)
    - 인증서를 정의하는 다양한 환경에 맞는 조건과 서명 알고리즘들의 선택이 가능하도록 확장영역을 추가

인증서의 구조

❖ 공개키인증서의 구조

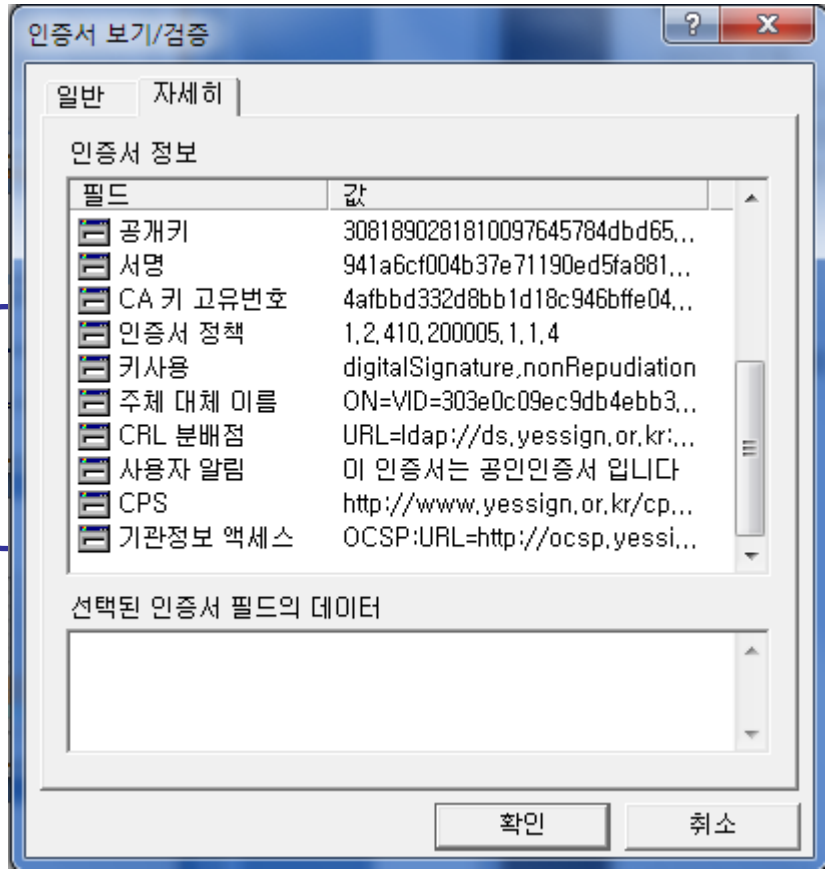


인증서의 구조

- **공개키인증서에 포함된 정보**
  - 버전(Version) : 인증서 형식의 연속된 버전의 구분
  - 일련번호(Serial Number) : 발행 CA내부에서는 유일한 정수값
  - 알고리즘 식별자(Algorithm Identifier) : 인증서를 생성하는데 이용되는 서명 알고리즘을 확인하기 위한 서명 알고리즘 OID
  - 발행자(Issuer) : 인증서를 발행하고 표시하는 CA
  - 유효기간(Period of validity) : 인증서가 유효한 첫번째와 마지막 날짜 두 개로 구성
  - 주체(Subject) : 인증서가 가리키는 사람
  - 공개키 정보(Public-key information) : 주체의 공개키와 이 키가 사용될 알고리즘의 식별자
  - 서명(Signature) : CA의 개인 서명키로 서명한 서명문

X.509 v3 확장자

- **X.509 v3에서 확장자의 개념이 도입됨**
  - 용도: X.509 실현자가 그들의 용도에 적합하게 인증서 내용을 추가적으로 정의할 수 있게 하기 위함
  - 확장 영역은 다음과 같은 부분으로 구분
    - 키 및 정책 확장자
    - 주체와 발급자에 대한 속성 정보
    - 인증서 경로 규제 정보
    - CRL을 위한 확장자



2.3 인증서의 종류

- 공인인증서
  - 공인인증기관이 발행하는 인증서
  - 전자서명법에 따라 유효성을 널리 인정받음

- 사설인증서
  - 개인, 회사, 조직 등이 발행하는 인증서
  - 특정 조직 내에서 활용

3. 공개키기반구조

❖ 사회적 기반구조

- 교통, 인터넷, 통신, 등

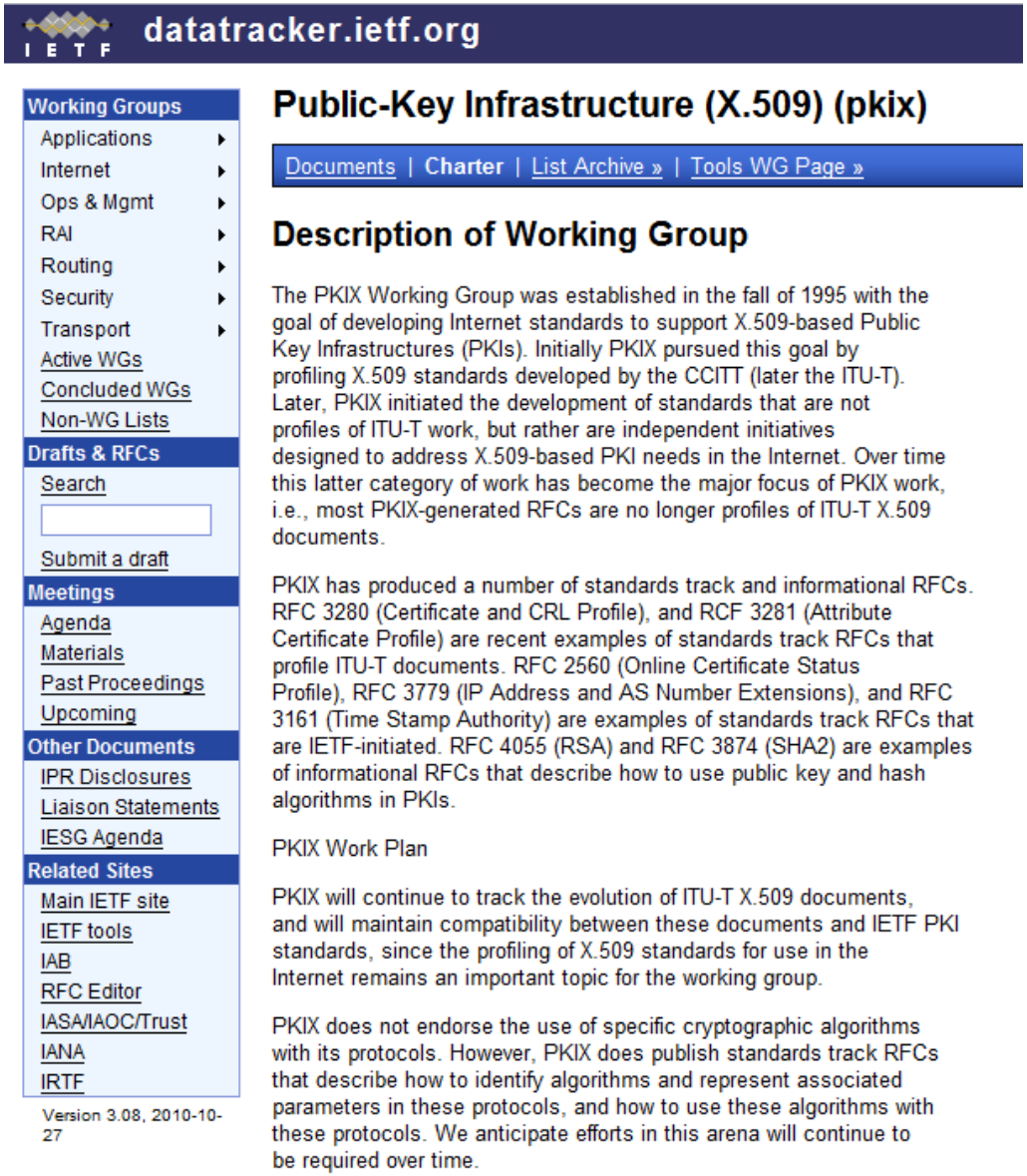
❖ 공개키기반구조(PKI, Public Key Infrastructure)

- 공개키 인증서의 인증성을 제공하는 신뢰구조
- 다수의 인증기관들을 포함하는 복잡한 구조에서의 상호 인증을 위한 계층적 인증 체계 - 인증서 발행, 배달, 관리, 인증네트워크

❖ PKI의 표준안

- X.509, The Directory: Authentication Framework, 1993.
- PKIX: Internet X.509 Public Key Certificate Infrastructure.

http://datatracker.ietf.org/wg/pkix/



datatracker.ietf.org

Working Groups
- Applications
- Internet
- Ops & Mgmt
- RAI
- Routing
- Security
- Transport
- Active WGs
- Concluded WGs
- Non-WG Lists

Drafts & RFCs
- Search
- Submit a draft

Meetings
- Agenda
- Materials
- Past Proceedings
- Upcoming

Other Documents
- IPR Disclosures
- Liaison Statements
- IESG Agenda

Related Sites
- Main IETF site
- IETF tools
- IAB
- RFC Editor
- IASA/IAOC/Trust
- IANA
- IRTF

Version 3.08, 2010-10-27

Public-Key Infrastructure (X.509) (pkix)

Documents | **Charter** | List Archive » | Tools WG Page »

Description of Working Group

The PKIX Working Group was established in the fall of 1995 with the goal of developing Internet standards to support X.509-based Public Key Infrastructures (PKIs). Initially PKIX pursued this goal by profiling X.509 standards developed by the CCITT (later the ITU-T). Later, PKIX initiated the development of standards that are not profiles of ITU-T work, but rather are independent initiatives designed to address X.509-based PKI needs in the Internet. Over time this latter category of work has become the major focus of PKIX work, i.e., most PKIX-generated RFCs are no longer profiles of ITU-T X.509 documents.

PKIX has produced a number of standards track and informational RFCs. RFC 3280 (Certificate and CRL Profile), and RCF 3281 (Attribute Certificate Profile) are recent examples of standards track RFCs that profile ITU-T documents. RFC 2560 (Online Certificate Status Profile), RFC 3779 (IP Address and AS Number Extensions), and RFC 3161 (Time Stamp Authority) are examples of standards track RFCs that are IETF-initiated. RFC 4055 (RSA) and RFC 3874 (SHA2) are examples of informational RFCs that describe how to use public key and hash algorithms in PKIs.

PKIX Work Plan

PKIX will continue to track the evolution of ITU-T X.509 documents, and will maintain compatibility between these documents and IETF PKI standards, since the profiling of X.509 standards for use in the Internet remains an important topic for the working group.

PKIX does not endorse the use of specific cryptographic algorithms with its protocols. However, PKIX does publish standards track RFCs that describe how to identify algorithms and represent associated parameters in these protocols, and how to use these algorithms with these protocols. We anticipate efforts in this arena will continue to be required over time.

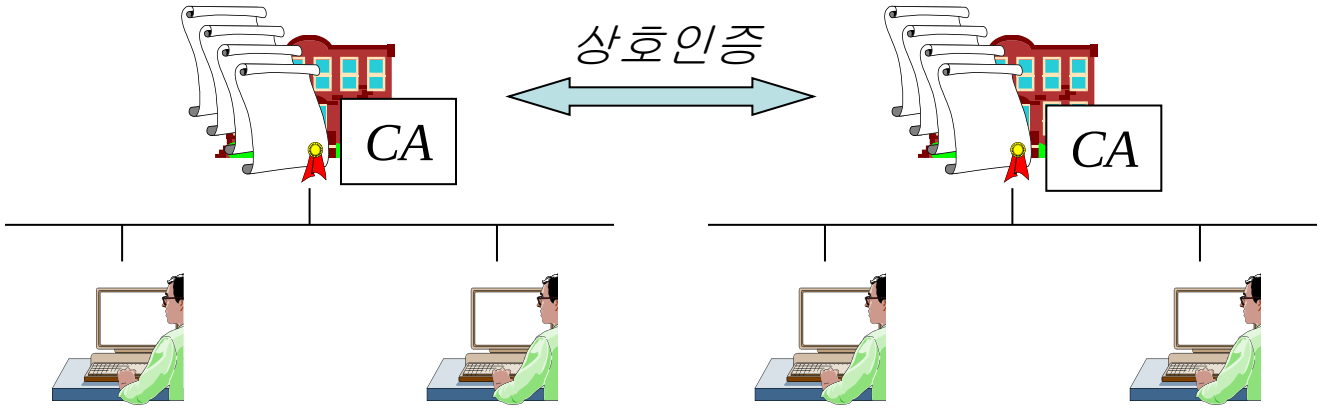
3.1 신뢰의 확장

- **PKI 인증 방식의 확장**
  - 단일 인증 기관을 이용한 인증 방식
  - 상호인증 기법을 이용한 인증 방식
  - 계층적 구조를 이용한 인증 방식

신뢰의 확장

❖ 상호인증을 이용한 인증

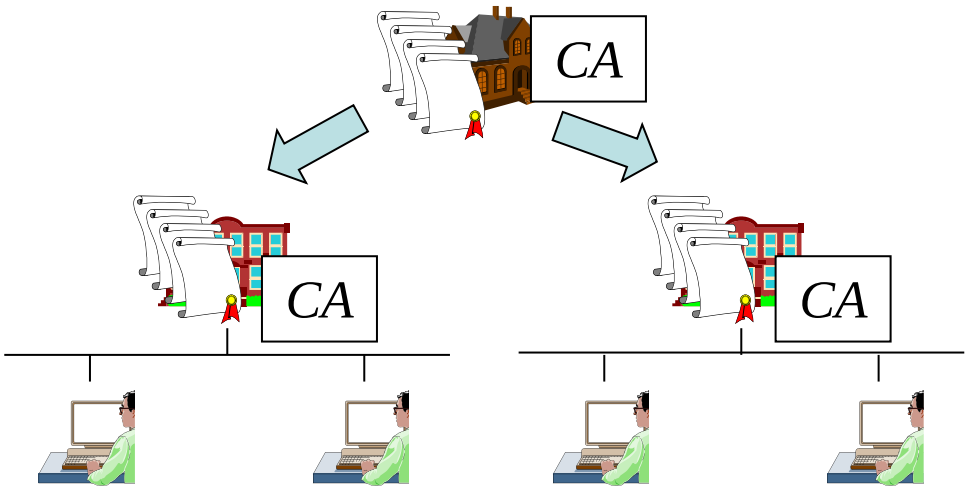
- ➢ 인증 기관이 각 사용자의 공개키에 대한 인증서 발급
- ➢ 인증기관 상호간에 인증기관의 공개키에 대한 인증서 발급
  - 네트워크형 구조 구성
  - 추가적인 확장이 용이하지 않다.

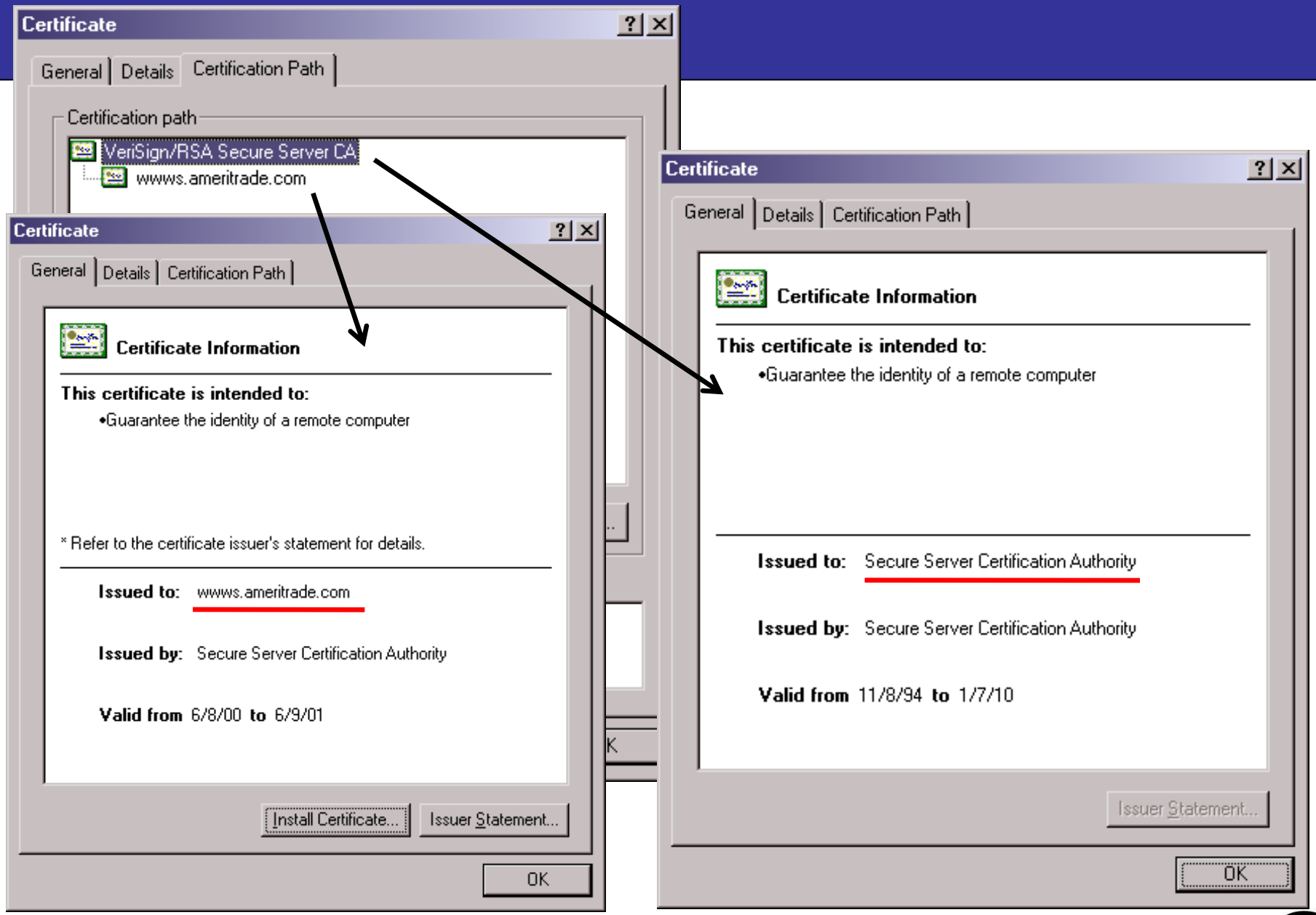


신뢰의 확장

❖ 계층적 구조를 이용한 인증

- ➢ 인증 기관들은 역할에 따라 계층적으로 구성됨.
- ➢ 상위 인증기관이 하위 인증기관의 공개키에 대해 인증
  - 계층형 인증구조 구성
  - 추가적인 인증 서비스 영역 확장이 용이




Certificate
General
Details
Certification Path
Certification path
VeriSign/RSA Secure Server CA
wwws.ameritrade.com
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
* Refer to the certificate issuer's statement for details.
Issued to: wwws.ameritrade.com
Issued by: Secure Server Certification Authority
Valid from 6/8/00 to 6/9/01
Install Certificate...
Issuer Statement...
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended to:
•Guarantee the identity of a remote computer
Issued to: Secure Server Certification Authority
Issued by: Secure Server Certification Authority
Valid from 11/8/94 to 1/7/10
Issuer Statement...
OK

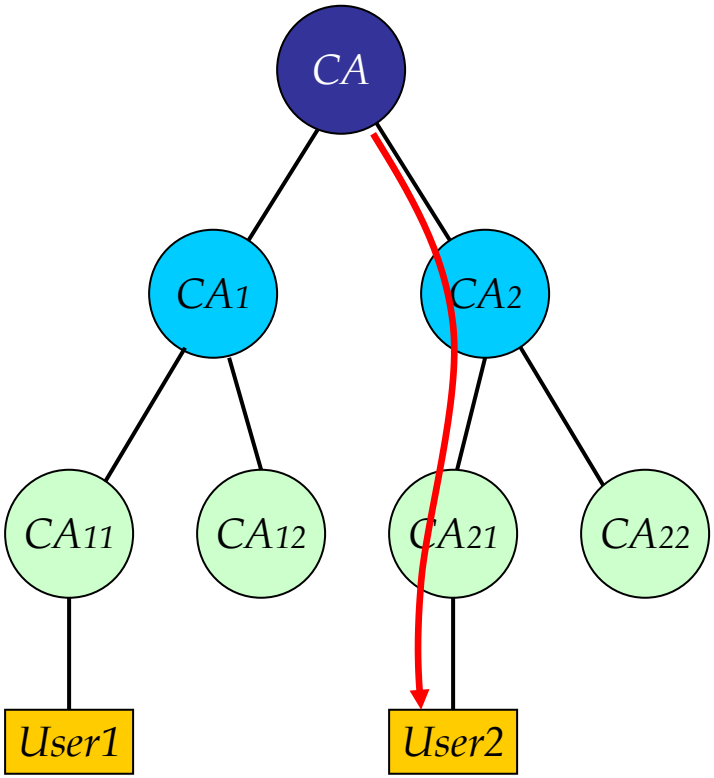
3.2 PKI 구성 방식

- **순수 계층 방식**
  - 최상위 인증 기관인 root CA에 대한 신뢰에 바탕을 둠
  - 하부의 CA간의 상호 인증은 원칙적으로 배제
  - 루트 CA간의 상호인증을 통한 국제간 상호 동작을 원활히 함

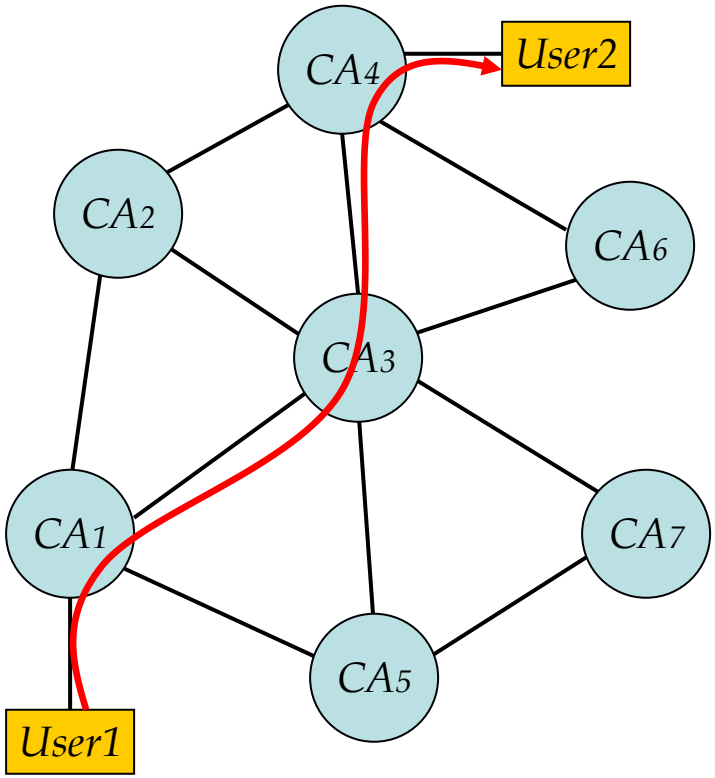
- **네트워크 구조 방식**
  - 모든 구조가 평면적으로 구성
  - 모든 CA간에 상호인증을 허용
  - 상호인증의 수가 대폭 증가하는 단점이 있다.

- **이 두 가지를 적절히 조합하여 사용하는 것이 일반적임**

PKI 구성 방식



순수 계층 방식

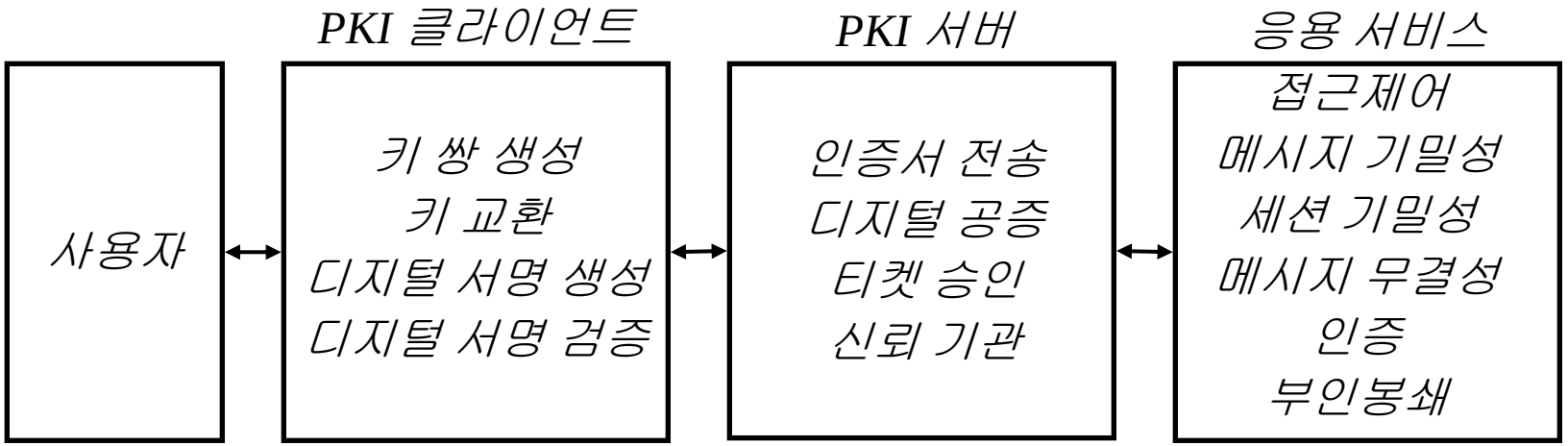


네트워크 구조 방식

3.3 PKI 구성요소

❖ **PKI 기본 기능**

PKI 기능	
인증서 관리 기능	보조 기능
인증서 생성 인증서 보관 인증서 취소, 폐기 인증 정책 수립	데이터 보관 디렉토리 명명 및 등록

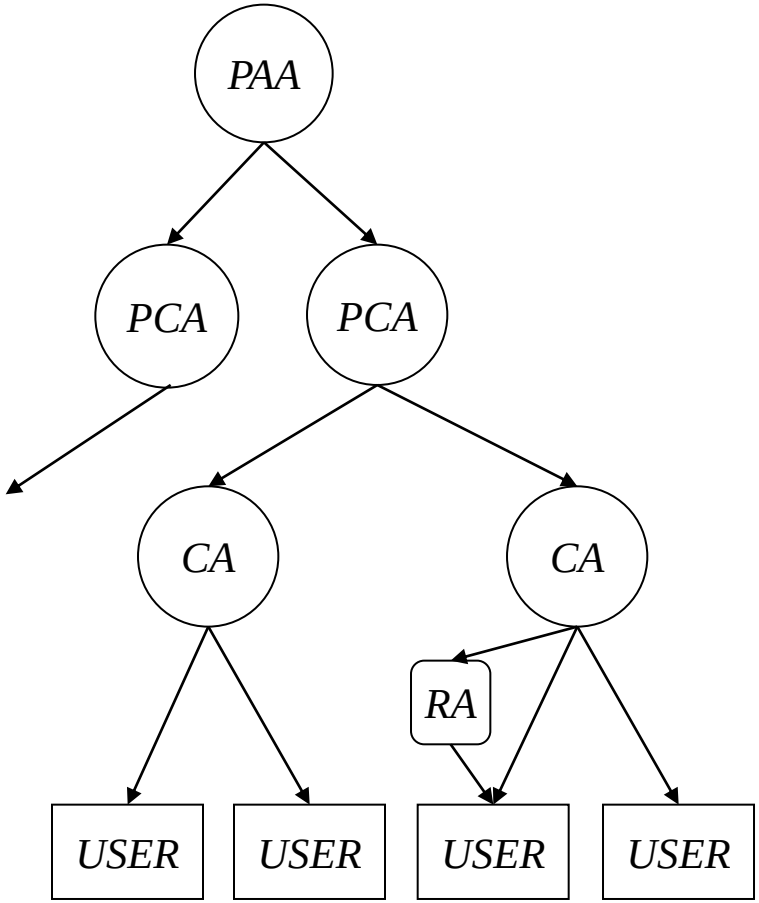


PKI 구성요소

❖ 참여자

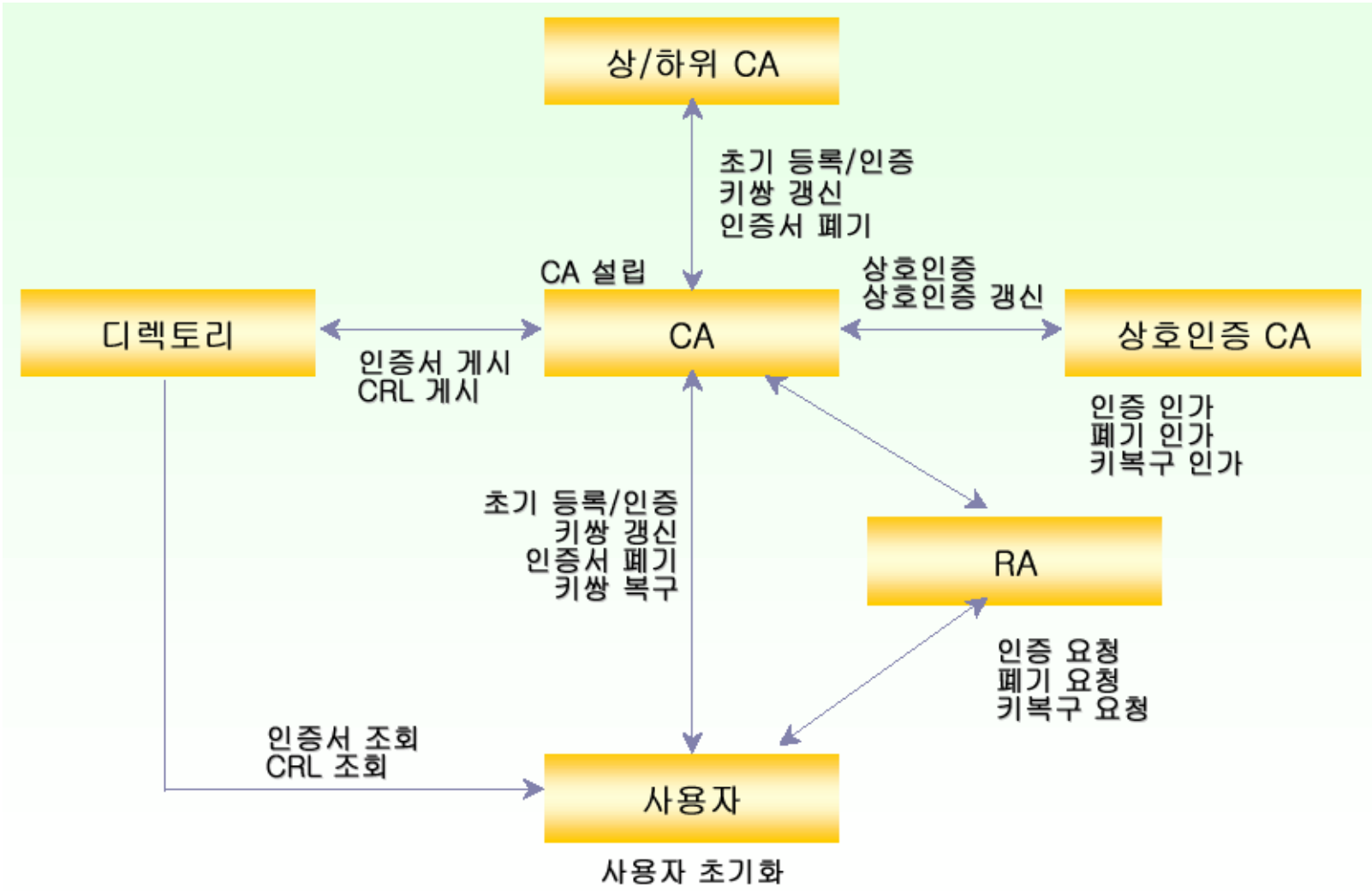
인증 기관	역할과 기능에 따라 계층적으로 구성 인증 정책 수립 및 인증서 발행 및 관리
등록 기관	인증 기관과 사용자 사이에 등록 기관을 두어 인증 기관 대신 사용자들의 신분확인 등을 대행
디렉토리	인증서와 사용자 관련 정보들을 저장, 검색을 위한 장소
사용자	일반적인 사람뿐 아니라 이용하는 시스템 포함

계층별 인증기관의 역할



정책 승인 기관 (PAA : Policy Approval Authorities)	● PCA 를 위한 정책 수립 및 PCA 의 정책 승인 ● PCA 의 인증서 발행
정책 인증 기관 (PCA : Policy Certification Authorities)	● CA 의 정책 수립 ● 수립된 정책의 적절한 운용 검사 ● CA 의 인증서 발행
인증 기관 (CA : Certification Authority)	● PCA 의 정책에 의해 하위 CA, 사용자, RA 의 인증서 발행
등록기관 (RA : Registration Authority)	● 사용자와 CA 간에서 사용자 등록 수행 ● 사용자 신원 확인 ● 인증서 발급 없슴

PKI 서비스 흐름도


상/하위 CA
초기 등록/인증
키쌍 갱신
인증서 폐기
CA 설립
상호인증
상호인증 갱신
디렉토리
CA
상호인증 CA
인증서 게시
CRL 게시
인증 인가
폐기 인가
키복구 인가
초기 등록/인증
키쌍 갱신
인증서 폐기
키쌍 복구
RA
인증 요청
폐기 요청
키복구 요청
인증서 조회
CRL 조회
사용자
사용자 초기화

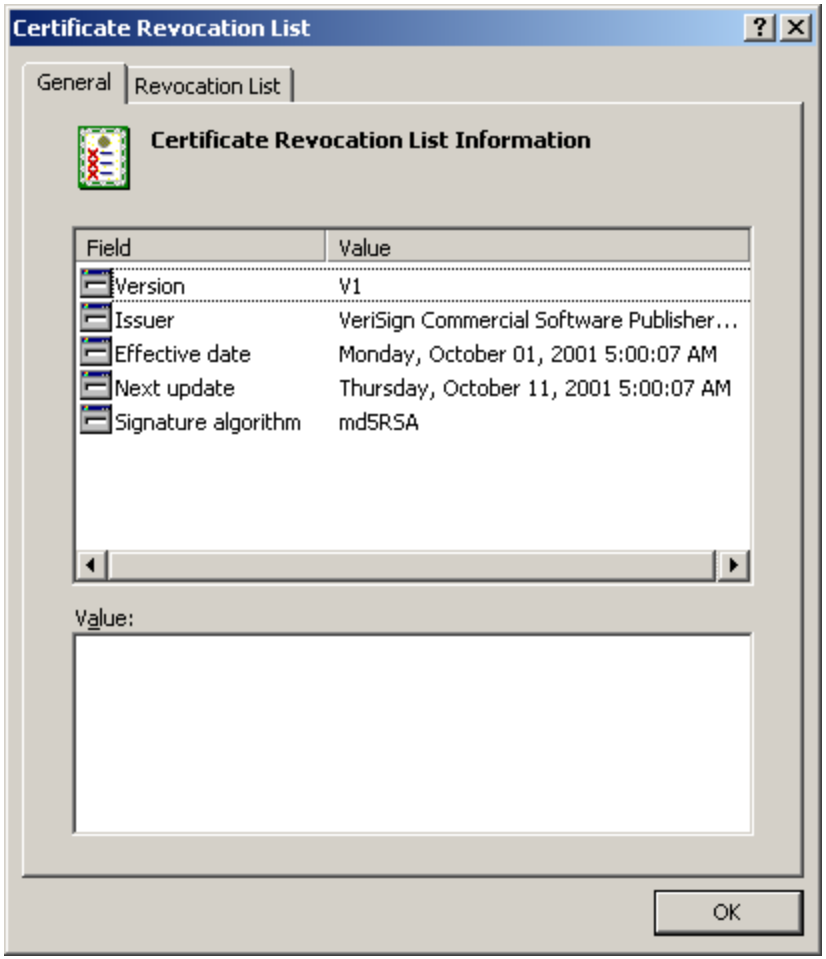
3.4 인증서의 취소

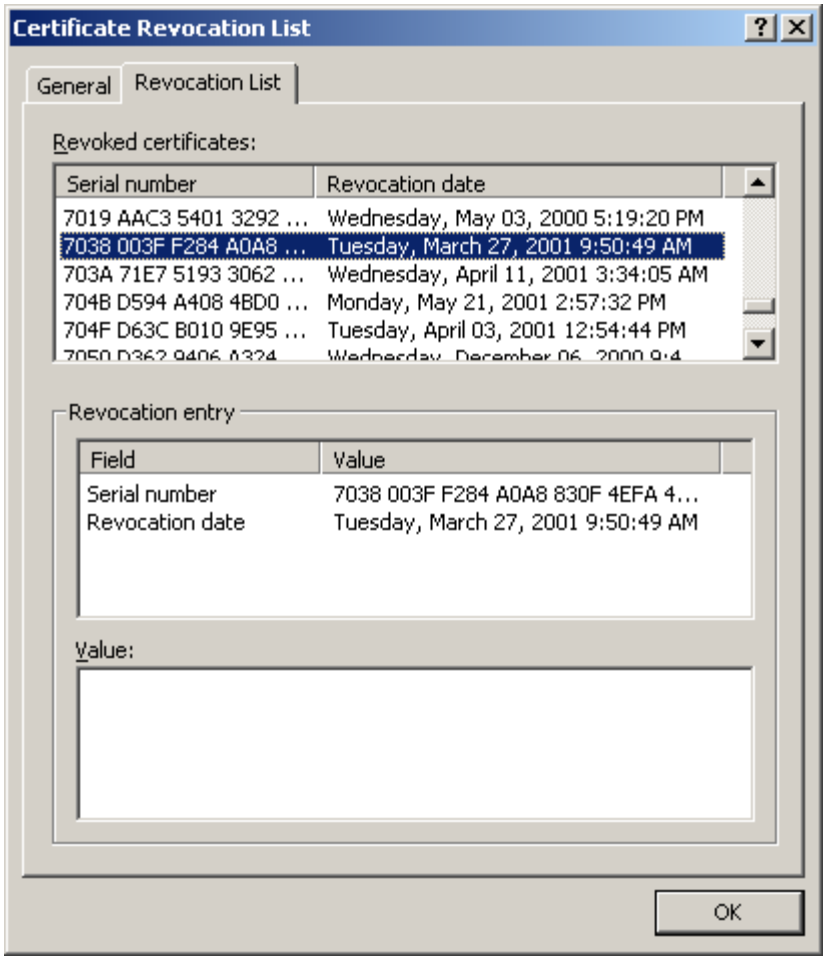
- 인증서 취소 사유
  - 인증서 발행 조직에서의 탈퇴
  - 비밀키의 손상
  - 비밀키 유출의 의심
- 인증서 취소 메커니즘
  - X.509에 정의된 인증서취소목록(CRL)을 이용

인증서의 취소

- **인증서취소목록(CRL)의 기본 영역**
  - 서명 알고리즘 : CRL에 서명한 서명 알고리즘 ID 및 관련 데이터
  - 발급자 : 발급자 CA의 X.509 이름
  - 최근 수정 일자 : 최근 수정 일자(UTC Time)
  - 차후 수정 일자 : 다음 수정 일자(UTC Time)
  - 취소 인증서 목록 : 취소된 인증서 목록들
  - CRL확장자 : CRL 확장자 유무 및 내용
  - 발급자 서명문 : 발급자의 서명문

인증서 취소 목록


Certificate Revocation List
General
Revocation List
Certificate Revocation List Information
Field
Value
Version
V1
Issuer
VeriSign Commercial Software Publisher...
Effective date
Monday, October 01, 2001 5:00:07 AM
Next update
Thursday, October 11, 2001 5:00:07 AM
Signature algorithm
md5RSA
Value:
OK


Certificate Revocation List
General
Revocation List
Revoked certificates:
Serial number
Revocation date
7019 AAC3 5401 3292 ...
Wednesday, May 03, 2000 5:19:20 PM
7038 003F F284 A0A8 ...
Tuesday, March 27, 2001 9:50:49 AM
703A 71E7 5193 3062 ...
Wednesday, April 11, 2001 3:34:05 AM
704B D594 A408 4BD0 ...
Monday, May 21, 2001 2:57:32 PM
704F D63C B010 9E95 ...
Tuesday, April 03, 2001 12:54:44 PM
Revocation entry
Field
Value
Serial number
7038 003F F284 A0A8 830F 4EFA 4...
Revocation date
Tuesday, March 27, 2001 9:50:49 AM
Value:
OK

인증서 취소 목록

- **CRL 공개**
  - 취소된 인증서에 대한 목록을 공개 디렉토리에 보관
  - 네트워크를 통해 접속할 수 있도록 함
- **CRL 생성 방법**
  - 주기적인 CRL 생성 방식
  - 즉각적인 CRL 생성 방식
    - 신속성, 안전성 면에서 우수
    - 해당 CA에 상당한 부하가 예상
  - 두 방식의 절충 방식이 바람직

3.5 PKI 관리

❖ PKI 관리 프로토콜을 위한 요구사항 -IETF

- 정기적으로 키 갱신 가능
- 기밀성의 사용은 최소화
- 다양한 상용 보안 알고리즘의 사용 가능
- 최종 개체, RA, CA에 의한 키 쌍의 생성을 배제해서는 안됨
- 최종 개체, RA, CA를 위한 인증서의 공표를 지원해야 됨
- E-mail, HTTP, TCP/IP, FTP와 같은 다양한 전송 메커니즘을 이용할 수 있어야 함
- 인증서 생성에 대한 최종 책임은 CA에게 있음
- CA 키 쌍의 갱신은 자연스럽고 계획적으로 이루어져야 함
- CA는 RA의 기능들을 수행할 수 있어야 함
- 최종 개체가 인증서를 요구할 경우, 최종 개체는 공개키에 대응하는 개인키를 증명할 수 있어야 한다.

인증실무준칙 (CPS)

❖ 정의

- 인증실무준칙 (CPS :Certification Practice Statements)
- 인증기관이 인증서를 발급하기 위해 사용하는 실무 절차에 관한 세부 규정
- 인증서 신뢰, 인증 업무에 대한 이해를 위해 CA에 의해 발행되는 인증업무에 대한 세부적인 기술 문서
- 인증 정책에 비해 좀 더 구체적
- 인증 정책, 사용자 인증 절차, 비밀 키 관리 절차 등이 포함
- CA는 이 규정에 의해 모든 업무 수행
  - 반드시 CPS를 작성하여 공개
  - 사용자들은 이를 이용 CA의 신뢰도를 측정

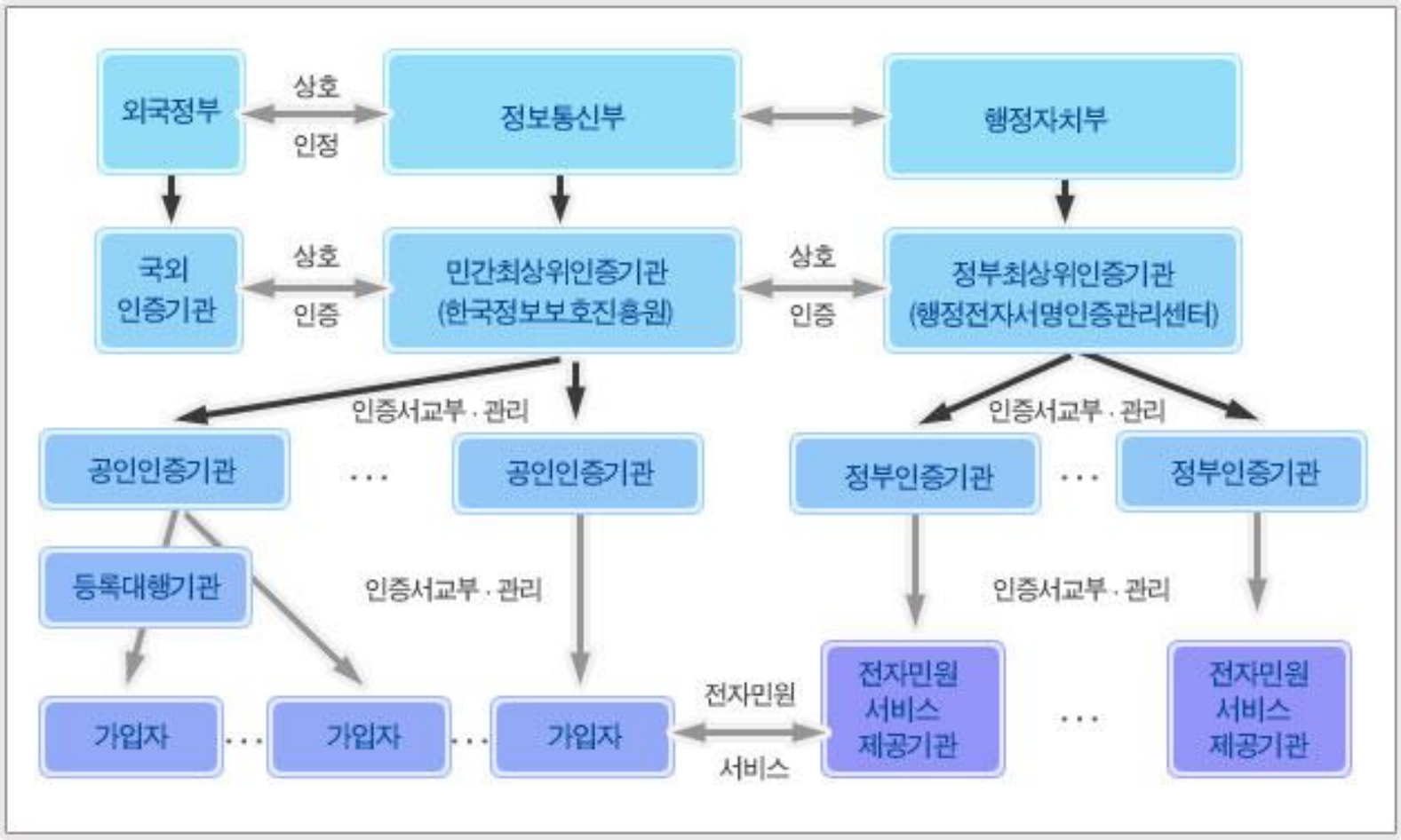
인증실무준칙 (CPS)

인증업무준칙

홈 > 고객지원 > 인증업무준칙

본 인증업무준칙은 금융결제원 전자인증센터가 발급하는 yessign 인증서의 발급 · 이용 등에 관한 전반적인 사항 및 금융결제원 yessign 인증서비스 관련 당사자의 의무와 책임을 규정한 것으로 전자서명 관련 법률을 준수합니다.

3.6 공개키 기반구조 현황



국내외 전자인증체계

구 분	국 내	해 외	구축용도
정부인증체계	정부전자인증체계(GPKI)	미국 FPKI 캐나다 GOC-PKI 호주 PKI 유럽 PKI 아시아 국가별 PKI	정부 행정업무 인증 인프라
공인인증체계	•한국정보인증(주) http://www.signgate.com •(주)코스콤 http://www.signkorea.com •금융결제원 http://www.yessign.or.kr •한국전자인증(주) http://www.crosscert.com •한국무역정보통신 http://www.tradesign.net	추진사례 없음	민간 전자거래 등에서 법적인 효력을 인정하기 위해 국가기관에서 지정
민간전자인증체계	기업체 사설인증체계 금융기관 사설인증체계	VeriSign Baltimore Certicom British Telecom	전자상거래 전자우편 웹서버인증서

정부기관 전자인증 도입사례

행정자치부	교육부	조달청	특허청
			
전자민원 (G4C)	교육행정정보서비스 (NEIS)	전자조달시스템 (G2B)	특허넷시스템

인증 시스템		인증센터 구축	RA	X	CA
인증서 사용	행정	전자관인	공인인증(교육부용)	전자관인 , 공인인증	사설인증, 전자관인
	대민	공인인증	공인인증	공인인증서	사설인증서, 공인인증서
인증·보안 적용		전자결재 민원신청서 적용	행정업무 중요 정보의 암호화, 전자서명	입찰업무 전자입찰서 (XML 기반)	행정업무 전자출원 적용
운영		센터 운영	RA 이중화	X	사설 CA시스템
인원		운용관리(10~20명)	지역교육청 전산실 담당자	RA 운영인원(X)	운영인원 필요