정보사회와 PKI

국제정보보호기술연구소(IRIS)
한국정보통신대학원대학교(ICU)

2001. 9. 14.

김 광 조, 이 병천

Content

1. 서론

- 정보사회의 발전
  - 정보통신 기술의 발전
  - 인터넷의 급격한 확대
  - 지식정보사회로 진보
- 비대면 전자상거래의 위험성
  - 기밀성, 신원확인, 무결성 보장 등
- 대응책
  - 전자서명의 이용
  - 1999년 2월 전자서명법 제정, 1999년 7월 시행
  - PKI의 필요성 인식 확대
  - 2002년까지 전자서명 이용자 1,000만 명 확보, 편의성 제고

인증서 발급 현황

- 전자서명 인증서 이용자수 100만명 돌파 (2001.8.8)
  - 총 104만2천697명 인증서 발급
    - 한국정보인증 15만6천90명
    - 한국증권전산 20만3천633명
    - 금융결제원 68만2천596명
    - 한국전산원 378명
  - 이용 형태별 분류
    - 인터넷뱅킹 64만명(61.5%)
    - 전자조달 및 입찰 34만명(32.6%)
    - 기타분야 6만명(5.9%) - 사이버트레이딩.쇼핑몰.보험.보안 전자우편
- 현재의 주요 인터넷 서비스 이용 인구 (향후 전자서명 인증서 활용 예상)
  - 인터넷 뱅킹 750만명
  - 사이버 증권거래 420만명

2. 전자서명

- 전자서명 이란
  - 공개키 알고리즘 방식을 이용하여 전자서명 생성키로 생성하는 디지털 정보에 대한 고유 정보
- 전자서명 요구사항
  - 서명자 인식
  - 문서내용 변경 여부 확인
  - 동일한 전자서명 재사용 불가
  - 문서작성 사실 부인 방지
- 전자서명을 통해 제공되는 주요 서비스
  - 사용자 인증 (User Authentication)
  - 데이터 무결성 (Data Integrity)
  - 부인 방지 (Non repudiation)

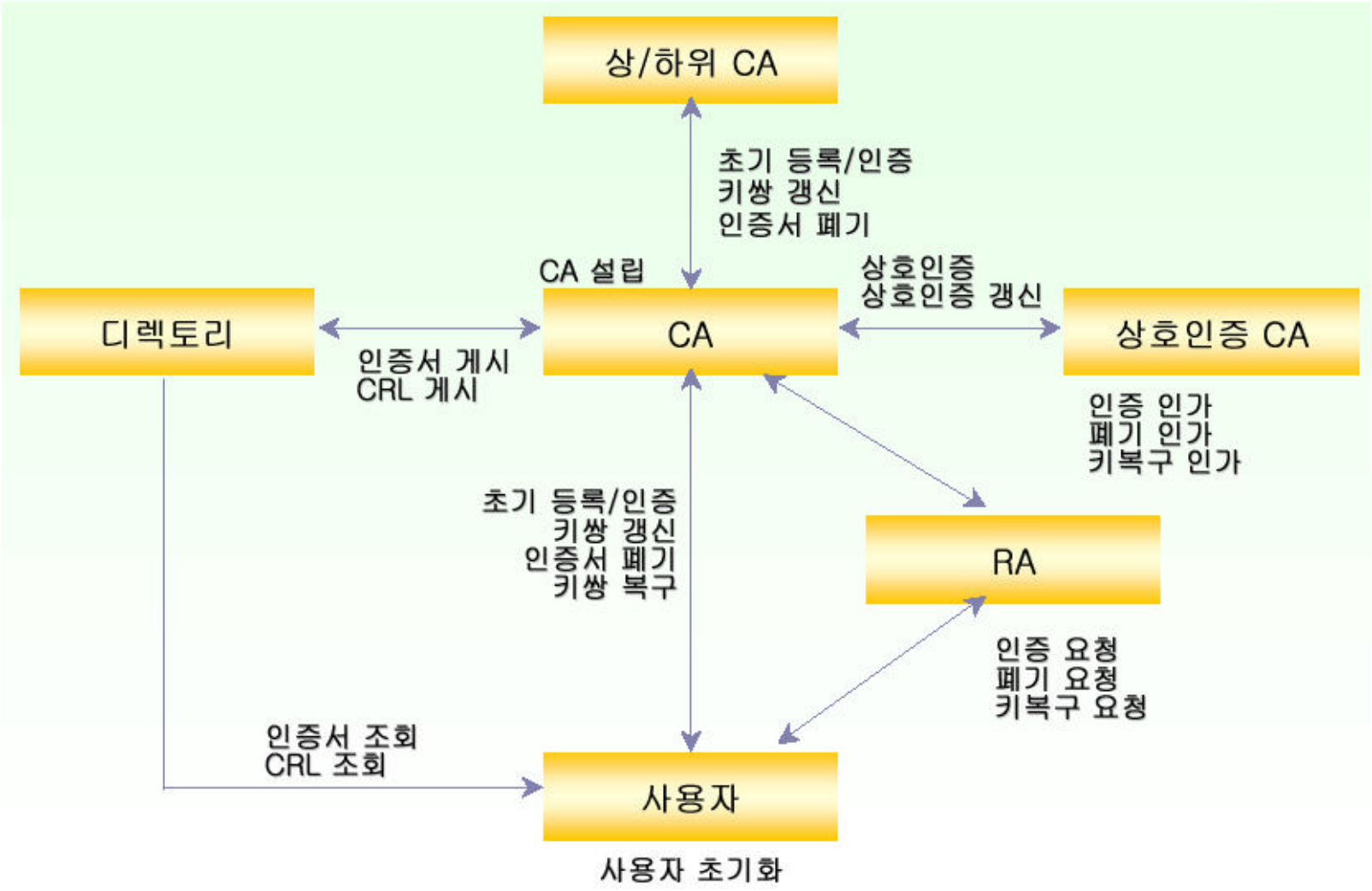
전자서명의 응용분야

- 공공 분야
  - 민원사무, 인허가 신청, 조세행정, 정부조달 EDI, 수출입통관, 공문서 유통, 전자출원 등
- 금융분야
  - 전자공시, 사이버 증권, 보험계약, 증권예탁, 인터넷 뱅킹, 전자자금이체, 전자지불, 전자쿠폰 등
- 전자상거래
  - 기업간 정보유통, 인터넷쇼핑, 각종 예약, 우체국전자상거래, 화물 운송 등
- 기타
  - 의료차트, 법원경매, 성적조회, 의료보험금 청구, 단말기 사용 등

공개키 인증서와 PKI

- 공개키 인증서
  - 개인의 인적 정보와 공개키를 결합하여 인증기관이 서명한 문서
    - 공개키의 인증성을 제공
  - 정보화 사회에서 개인의 신분증 역할
  - 다양한 정보보안 서비스 제공 가능 : 전자우편, 전자상거래, 전자화폐, 전자투표, 이동통신서비스, 소프트웨어 보호, ...
- 공개키 기반구조(PKI)
  - 공개키 인증서의 인증성을 제공하는 기반구조
  - 다수의 인증기관들을 포함하는 복잡한 구조에서의 상호 인증을 위한 계층적 인증 체계
  - 표준안:
    - X.509, The Directory: Authentication Framework, 1993.
    - PKIX: Internet X.509 Public Key Certificate Infrastructure.

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. 무선 PKI

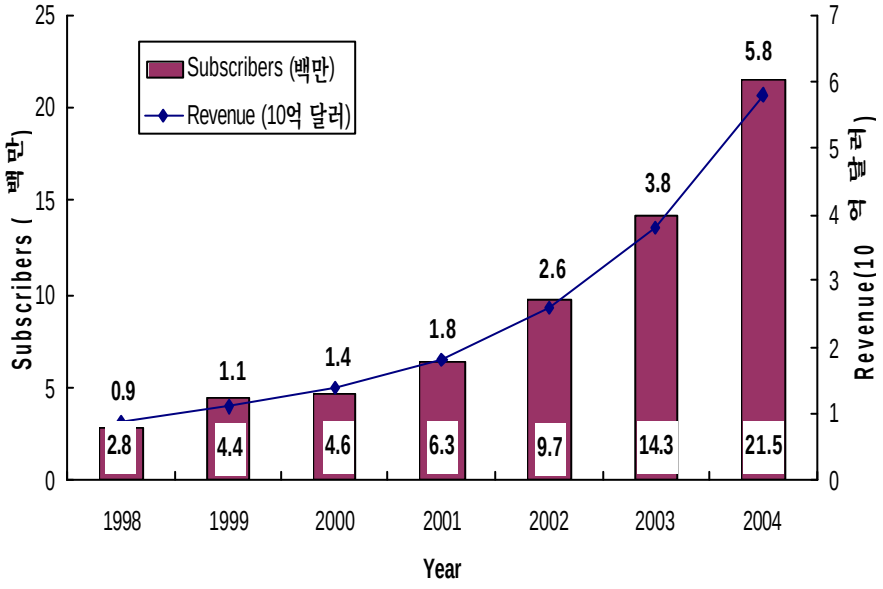
- 무선통신가입자수의 급격한 증가 (ARC group)
  - 1999년 428 만 명 → 2004년 123,500 만 명
- 무선통신가입자중 무선 데이터 통신 가입자 비중 (ARC group)
  - 1999년 7 % → 2004년 61 %
- 국내 무선데이터 시장 예측 (ETRI)
  - 1999년 12 조원 → 2004년 2,526 조원

무선 인터넷 시장 규모

향후 4년간 ('99 ~ 2002) 세계 무선 인터넷 서비스 시장규모는 150억 달러에 이를 것임

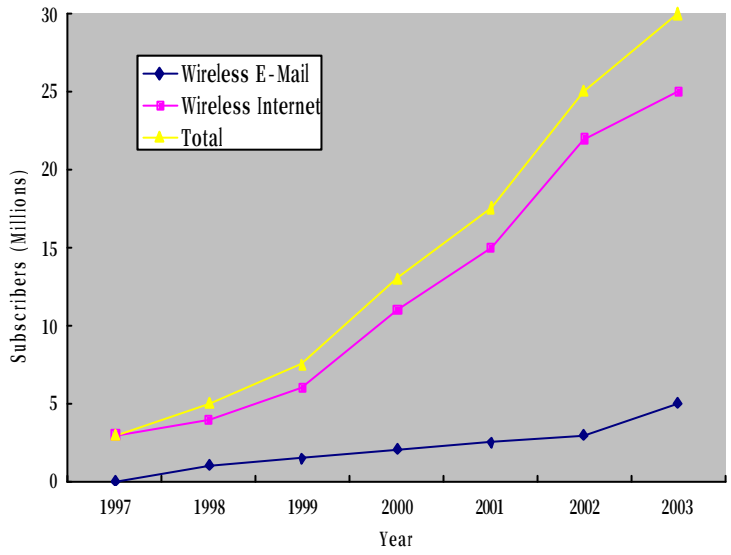
The U.S Mobile Data Market Place : 1999

(2001 ~ 2002 : PCS Network에 의한 Broadband Products 도입)



Wireless Internet and E-Mail Market : 1998

(2003년 29.6 Million Users)



예상 시장규모 (억 달러)	15	33	43	59	66

150억 달러

무선 인터넷 환경의 제약 사항

- **하드웨어 (compared to desktop computer)**
  - Less powerful CPUs
  - Less memory (ROM and RAM)
  - Restricted power consumption
  - Smaller displays
  - Different input devices (ex, a phone keypad)

- **네트웍 환경 (compared to wire environment)**
  - Less bandwidth
  - More latency
  - Less connection stability
  - Less predictable availability

무선 인터넷 표준기술 그룹 현황

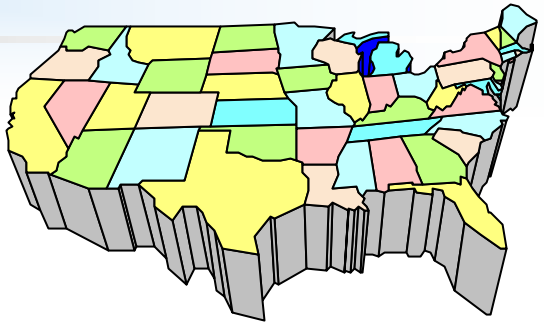
- **WAP**
  - 유럽을 중심으로 만들어짐
  - 1997년 결성
  - 에릭슨, 노키아, 모토로라, 폰닷컴(구 UP) 등이 중심
  - 현재 전세계 약 600여 업체가 참여
  - Gateway가 필요

- **Mobile Explorer(ME)**
  - Microsoft사와 퀄컴사가 합작으로 Wireless Knowledge를 세움
  - Window CE를 근간으로 한 이동 통신용 Web Brower를 개발

4. PKI 응용 – 인터넷 투표

- **2002 FIFA World Cup Korea-Japan™**
  - May. 31. 2002 ~ June. 30.2002
- **Objective**
  - Selection of MVP player in 2002 world-cup games
  - Demonstrating electronic voting system to the world in easy and friendly manner
  - Joint work of Korean and Japanese teams
- **Organization**
  - Korea : IRIS, Insol Soft, KISTI, Secui.com, STI
  - Japan : NTT, Univ. of Tokyo
- **Web-page**
  - http://mvp.worldcup2002.or.kr

Introduction



- **Lession in Florida, 2000**
  - Counting : Manual -> Automatic
  - Voting place : Fixed -> Any place
  - Verifiability : Local -> Universal
- **Why do we consider Internet voting?**
  - Anyone can vote using internet
  - Anywhere from home, office, overseas, etc.

  -> Solution for the problem of decreasing the participation rate in manual voting
- **What are the problems in Internet voting?**
  - Strong security requirements: anonymity, privacy, completeness, fairness, receipt-freeness, etc.
  - No perfect solution and system
  - PKI is not ready.

New Trial

- **California**
  - Shadow election test of Internet voting system for the public election in Conta Costa County in 2000.
- **CyberVote**
  - Remote Internet voting with fixed and mobile internet tech
  - 3-year R&D program funded by European Commission
- **Our contribution**
  - Using PKI, 1 vote – 1 certificate
  - System satisfies most of important security requirements
  - First trial to worldwide voting

Security Requirements

- **Basic requirements**
  - Privacy : All votes must be secret
  - Completeness : All valid votes are counted correctly
  - Soundness : The dishonest voter cannot disrupt the voting
  - Unreusability : No voter can vote twice
  - Eligibility : No one who isn't allowed to vote can vote
  - Fairness : Nothing can affect the voting
- **Advanced requirements**
  - Walk-away **:** The voter need not to make any action after voting
  - Robustness : The voting system should be successful regardless of partial failure of the system
  - Universal verifiability : Anyone can verify the validity of vote
  - Receipt-freeness : Voter should not be able to prove his or her vote to a buyer. (Voter does not have any receipt for the vote)

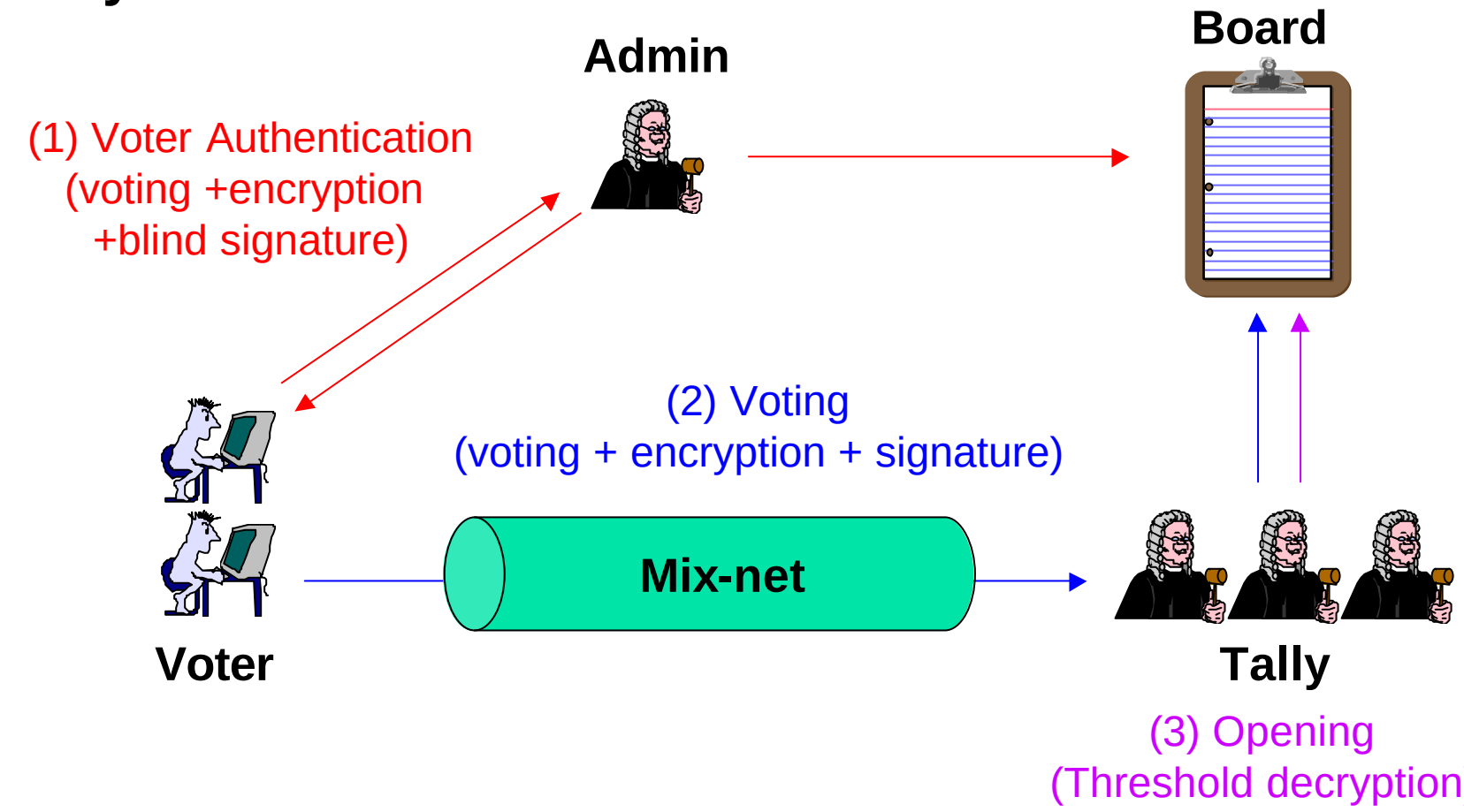
Voting Scheme

- **FOO92 Scheme**
  - Fujioka, Okamoto, Ohta, “A Practical Secret Voting Scheme for Large Scale Elections”, Auscrypt’92
  - Features: Blind signature + Mix-net + Bit commitment
- **Implementation examples**
  - Sensus : L.F. Cranor, Washington Univ. http://www.ccrc.wustl.edu/~lorracks/sensus
  - EVOX : M.A. Herschberg, R.L. Rivest, MIT

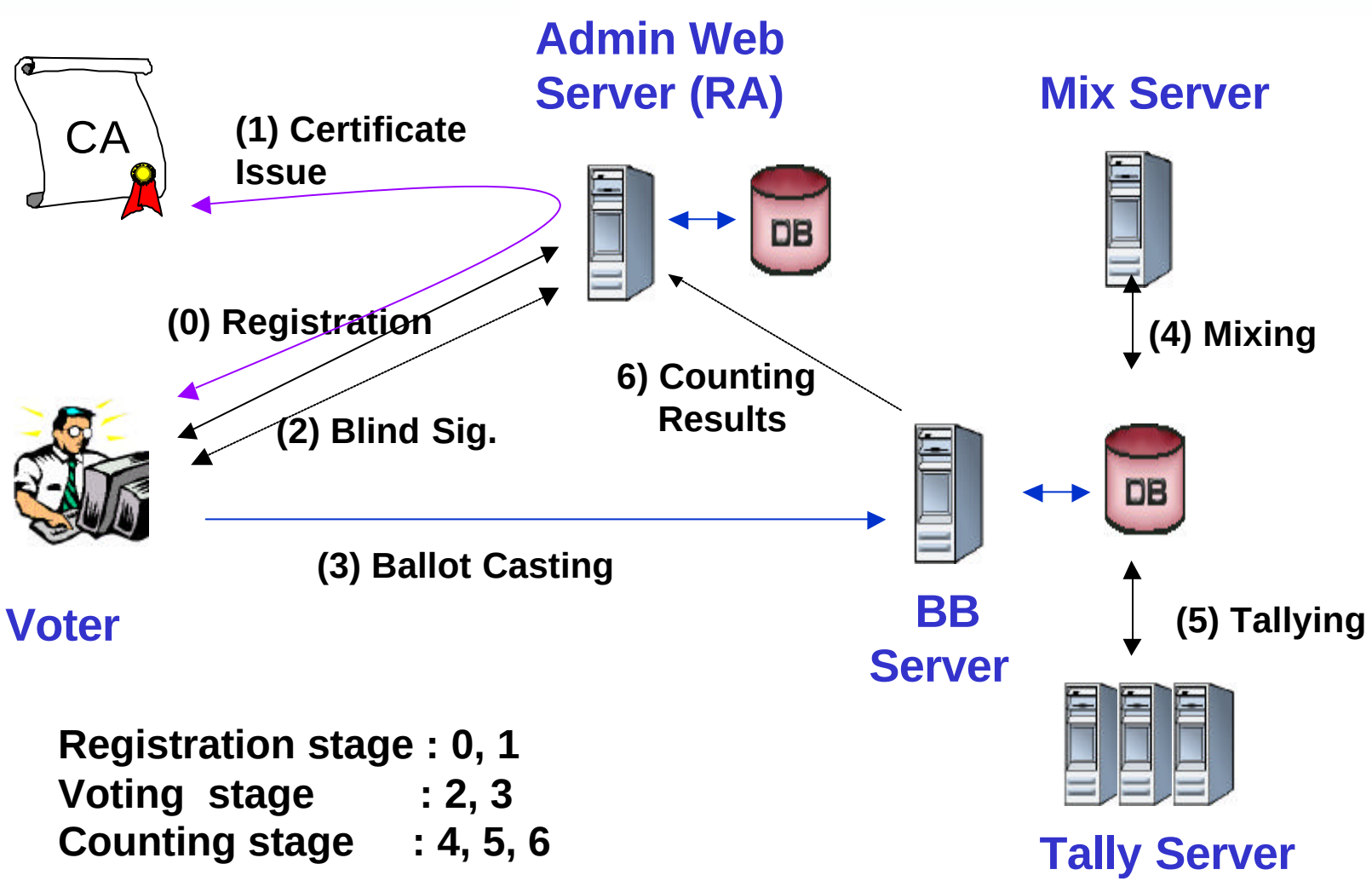
    http://theory.lcs.mit.edu/~cis/voting/voting.html
- **OMAFO99 Scheme**
  - Improved version of FOO92
  - Features : Blind signature + Mix-net + threshold encryption

OMAFO99 scheme

System overview

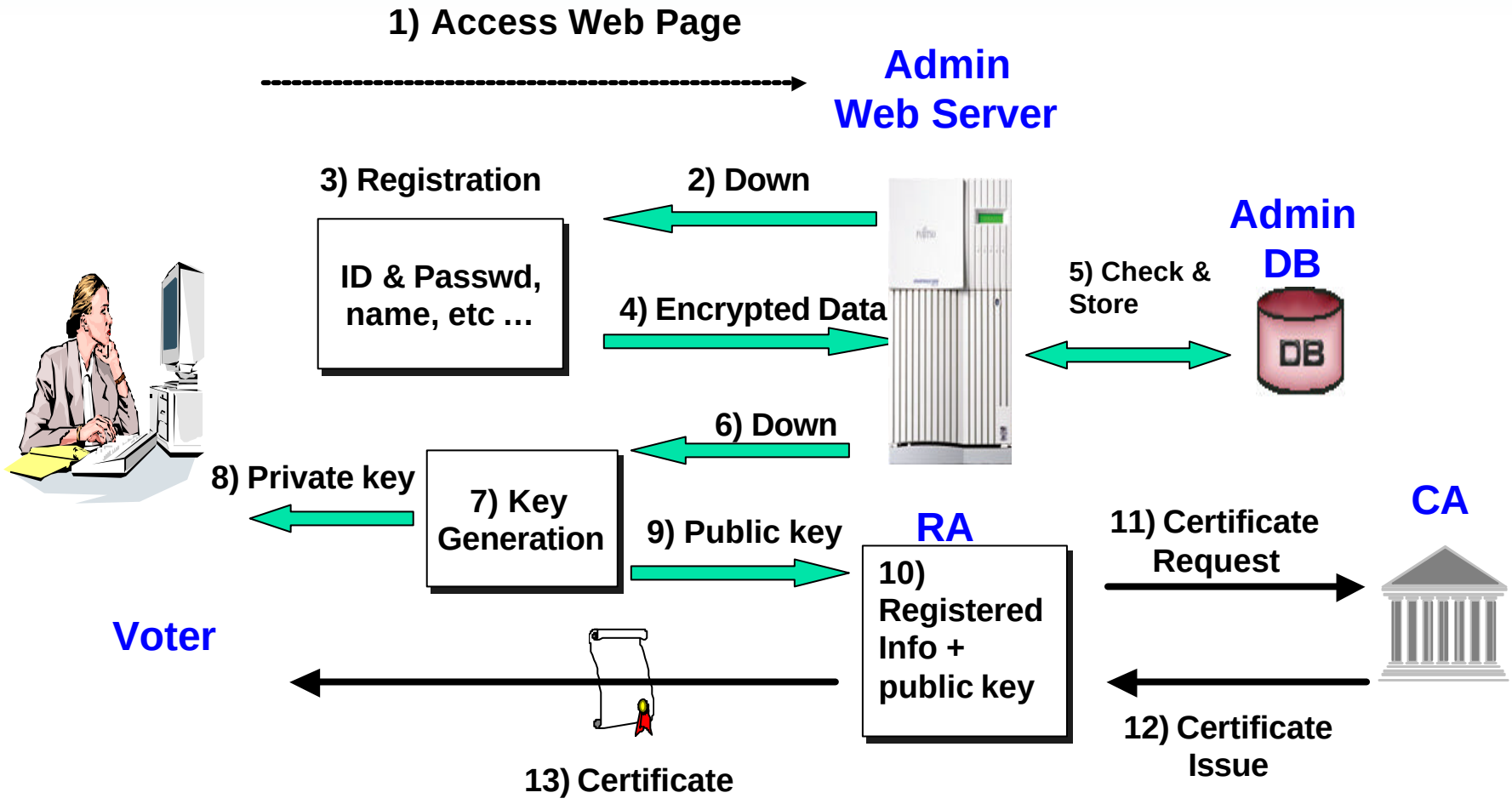


System Configuration

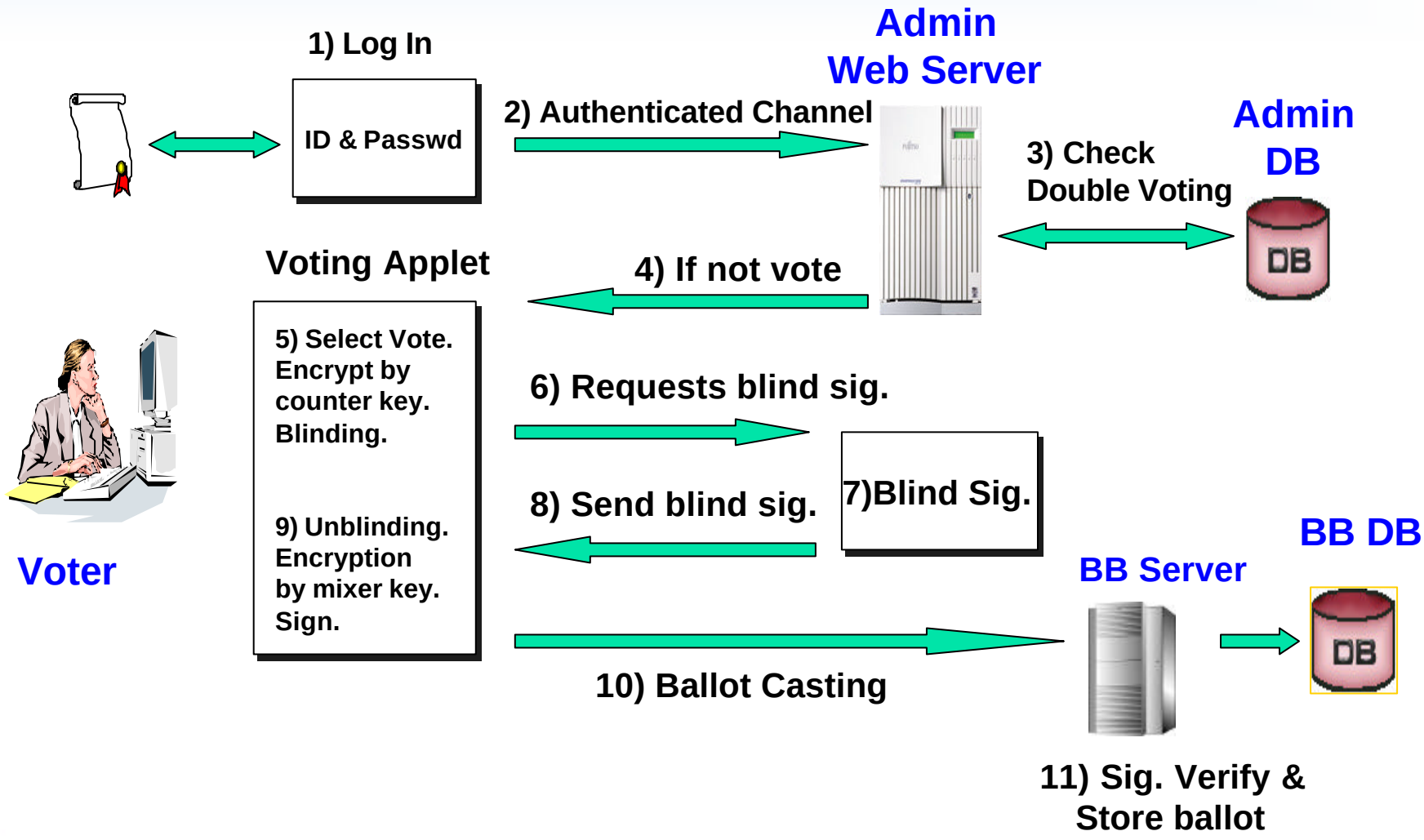


Registration stage : 0, 1
Voting stage : 2, 3
Counting stage : 4, 5, 6

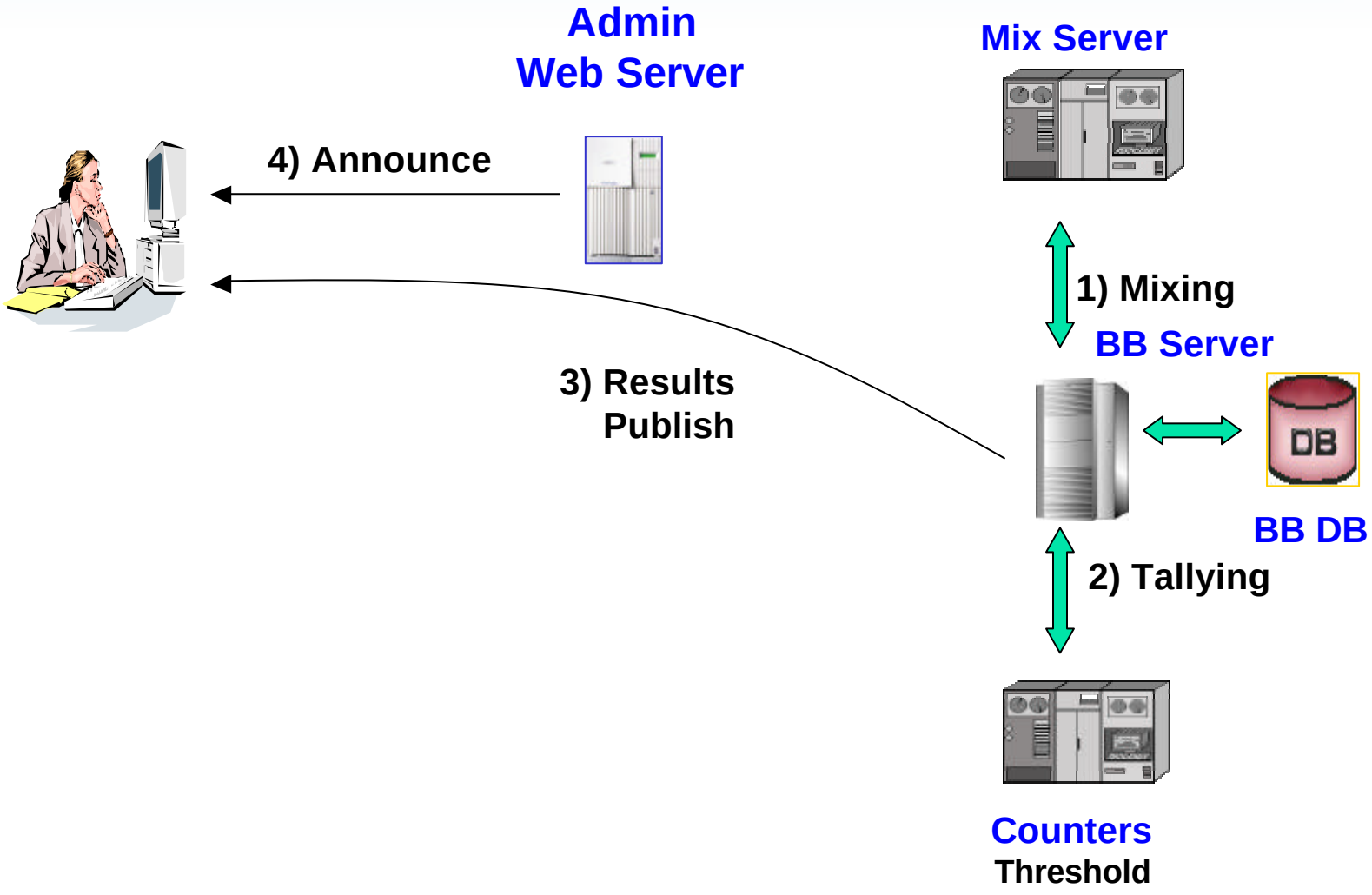
Registration stage



Voting Stage



Counting Stage



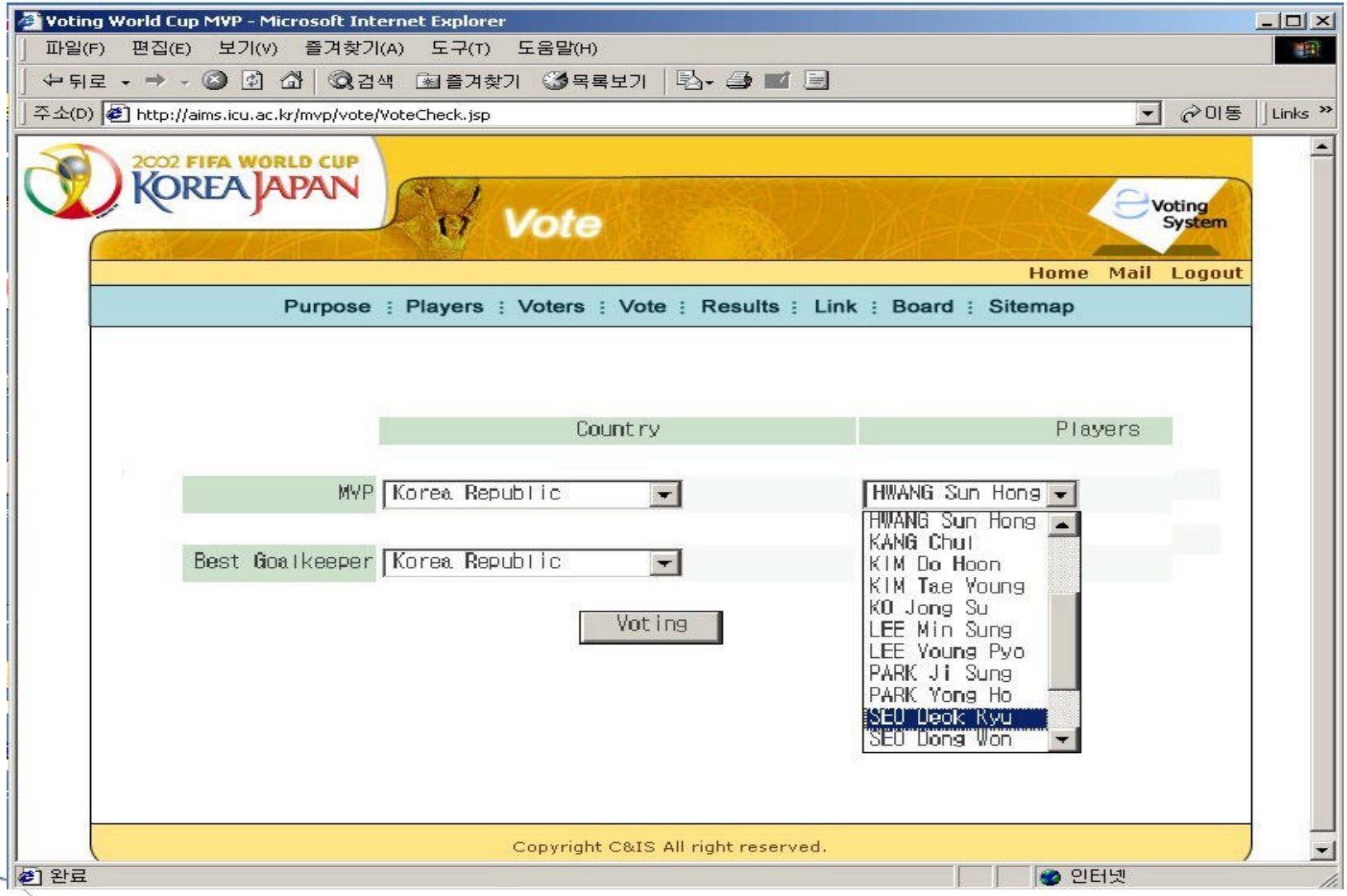
Typical Implementation

- **Built-in components**
  - Java crypto library J/LOCK by STI
  - CA server by KSIGN
  - Web interface by InsolSoft
  - Security management by SECUi.com
- **Severs**
  - AS,BB : Apache web server and Tomcat to support JSP
  - DB : Oracle DB + JDBC
  - M,T : Implemented in C language
- **Voting applet**
  - Signed java applet to access a secret key and to open connections to multiple addresses
  - Platform : WINDOW98 /+ on IBM PC

Application

- **2002 FIFA World Cup Korea-Japan™**
  - May. 31. ~ June. 30. 2002
- **Objective**
  - Selection of MVP player in 2002 world-cup games
  - Demonstrating electronic voting system to the world in easy and friendly manner
- **Participants**
  - Korea : IRIS, InsolSoft, KISTI, Samsung Secui.com, STI
  - Japan : NTT, Univ. of Tokyo
- **Web-page**
  - http://mvp.worldcup2002.or.kr

Web Interface



5. 결론

- 안전한 정보사회의 발전에 **PKI** 역할이 중요
- 무선인터넷의 발전에 따른 **WPKI** 구축 노력
- **PKI**의 응용분야 - 인터넷 전자투표 시스템
- 상호 연동 가능한 **PKI** 구축을 위한 국제 공동 노력
- 아사아 권에서 기술 주도력 확보
  - IWAP2001 (1st Int'l Workshop for Asian PKI)
  - http://www.iris.re.kr/iwap01