Crypto'2001

No More Panic in Florida: Is it Reality or Dream?

Aug. 21, 2001

IRIS(International Research center for Information Security)

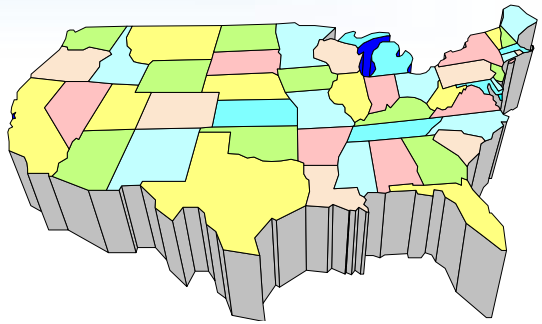
ICU(Information and Communications Univ.), **Korea**

Kwangjo Kim, Jinho Kim, Byoungcheon Lee

Contents

1. Introduction

- **Panic in Florida, 2000**
  - Manual counting vs. Electronic counting
  - Booth voting vs. Network voting
  - Local verifiability vs. Universal verifiability



- **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.
- **Caltech-MIT**
  - Joint project started in 2000 to develop reliable and uniform US voting machine
  - To solve the problems that threatened the 2000 American presidential election in Florida
- **Cybervote**
  - Remote Internet voting with mobile handset
  - European Communities
- **Our contribution**
  - Internet voting system using PKI
  - The system satisfies most of important security requirements

2. 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)

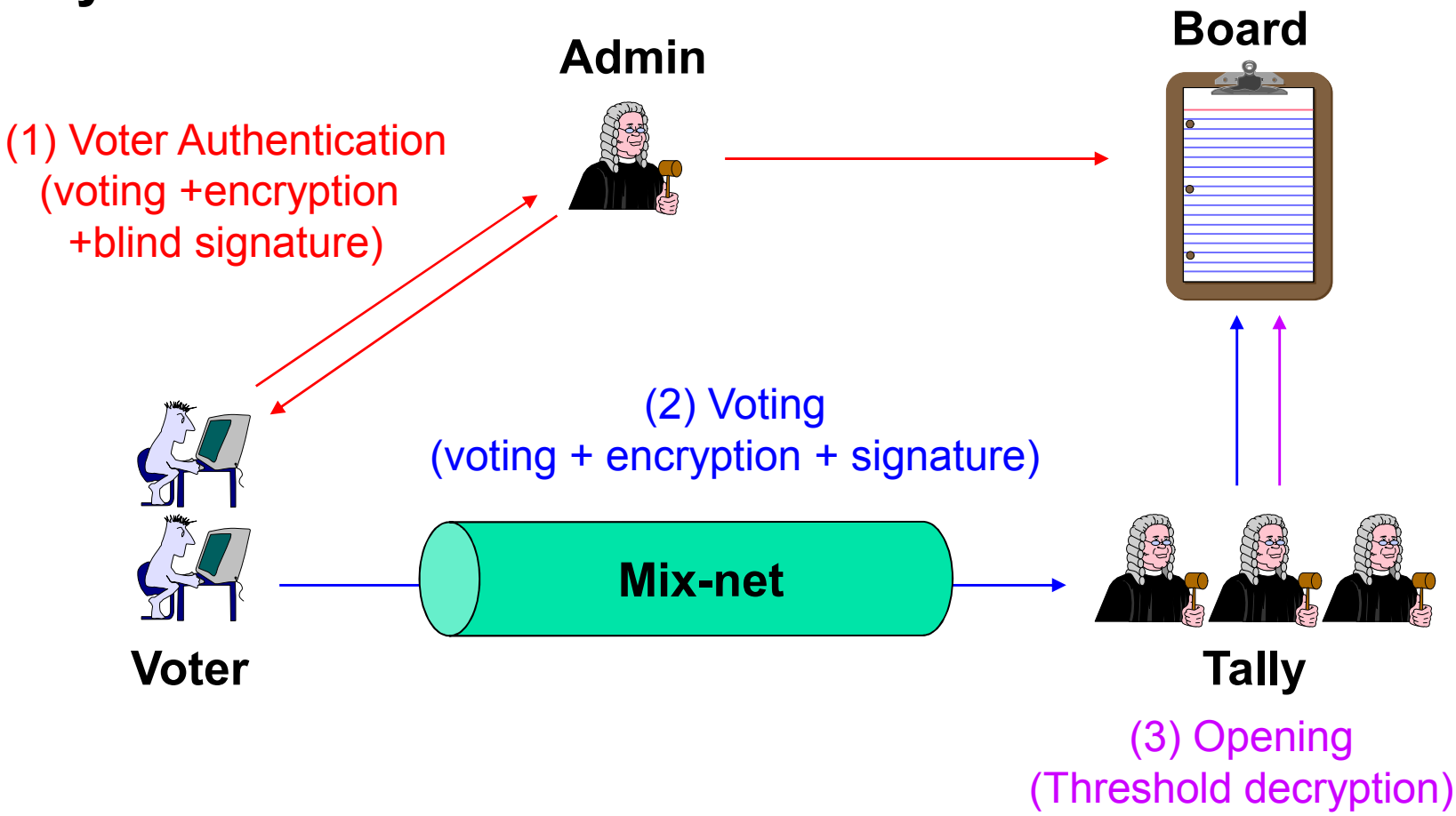
3. Voting Scheme

- **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

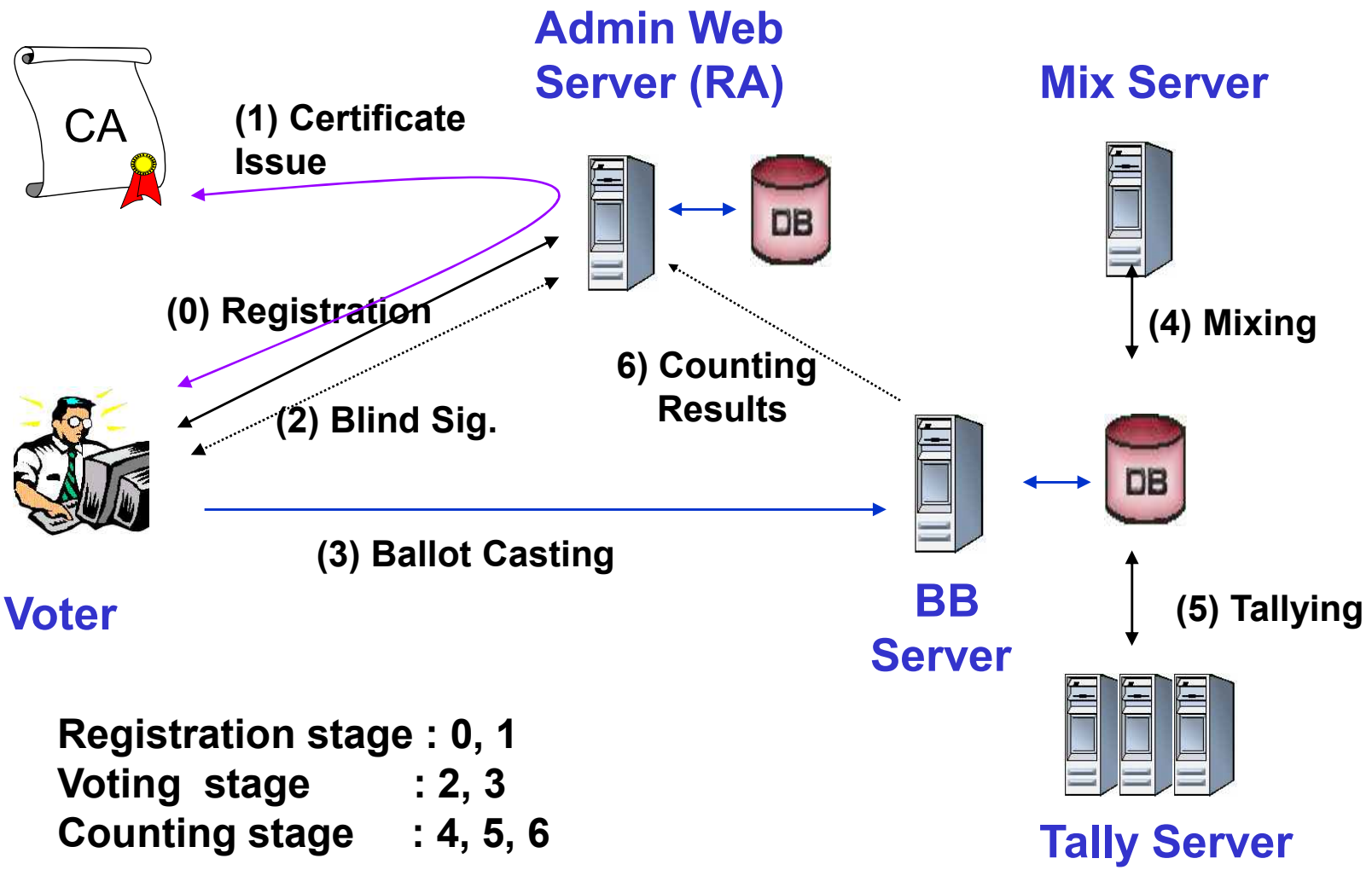
    http://theory.lcs.mit.edu/~cis/voting/voting.html
- **OMAFO99 Scheme**
  - Improved version of FOO92
  - Features : Blind signature + Mix-net + threshold encryption

OMAFO99 scheme

- **System overview**

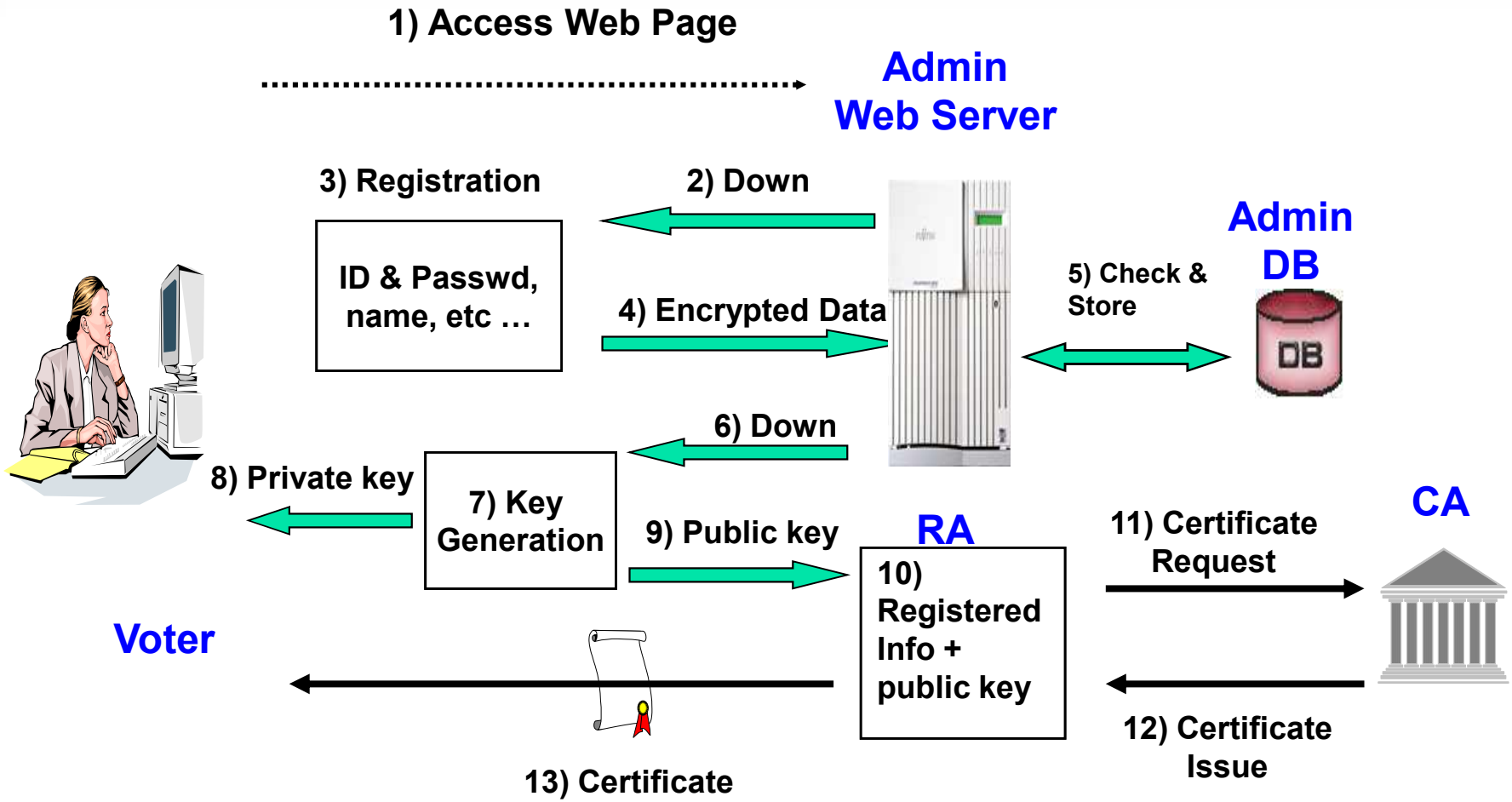


4. System Configuration

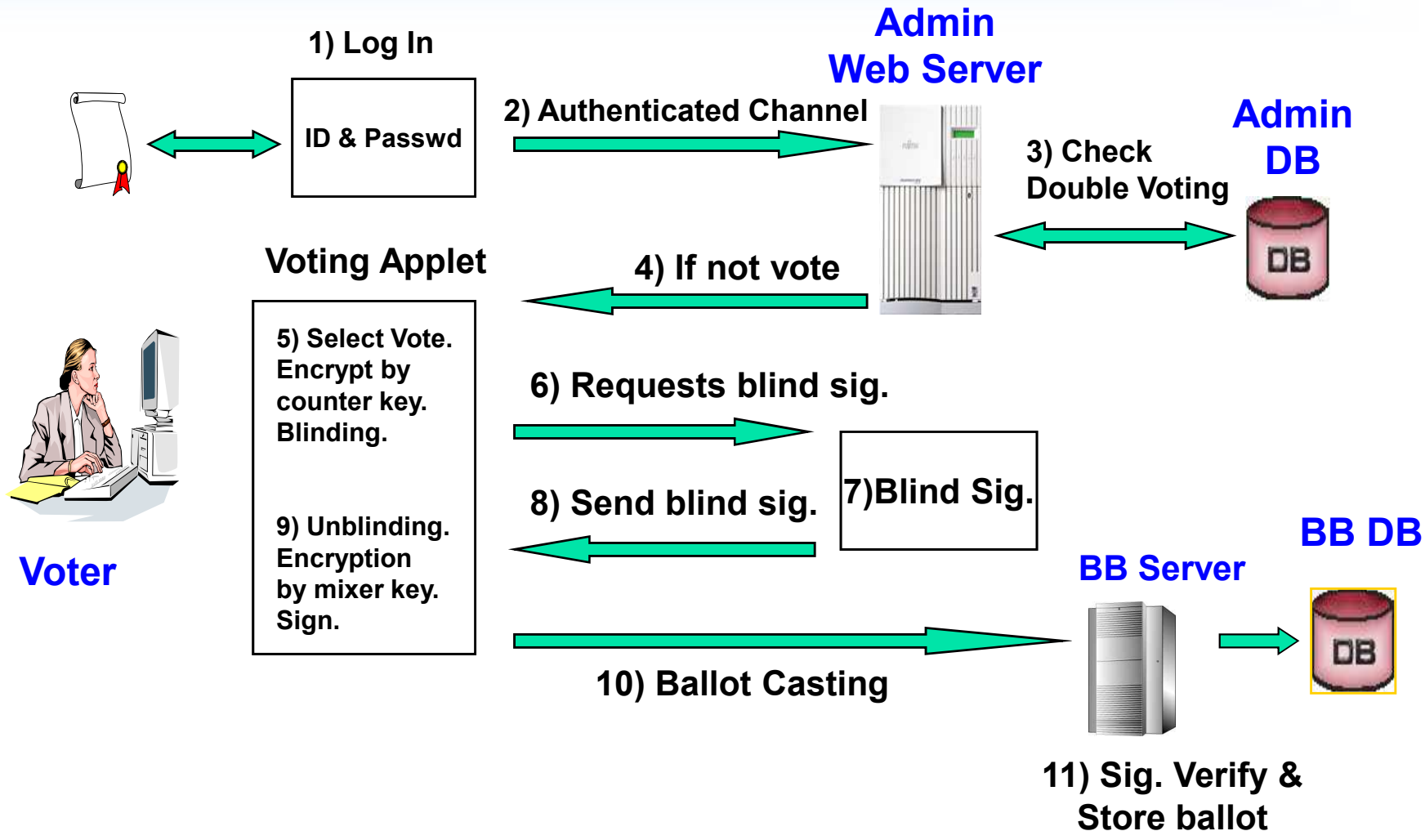


Registration stage : 0, 1
Voting stage : 2, 3
Counting stage : 4, 5, 6

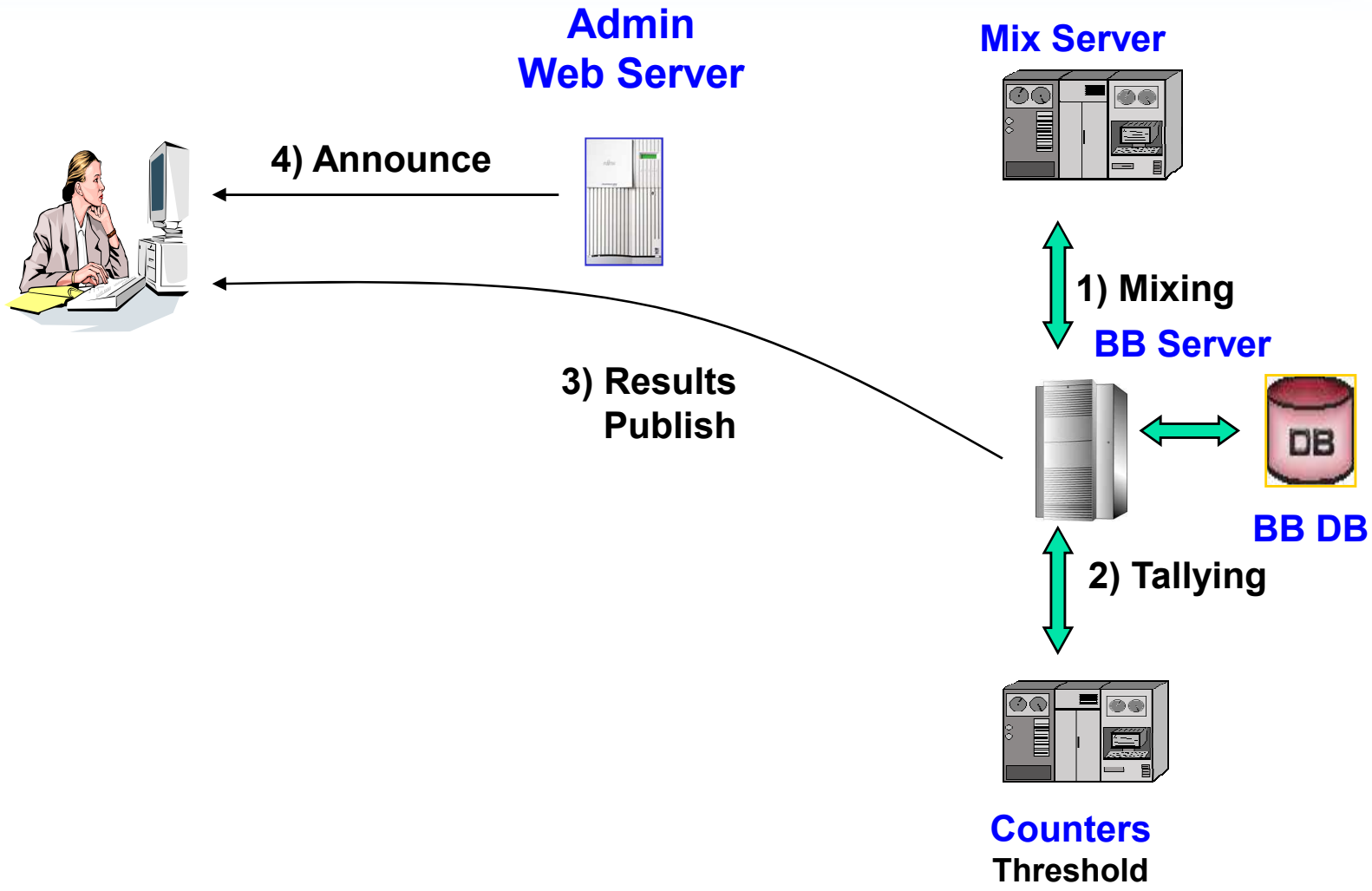
Registration stage



Voting Stage



Counting Stage



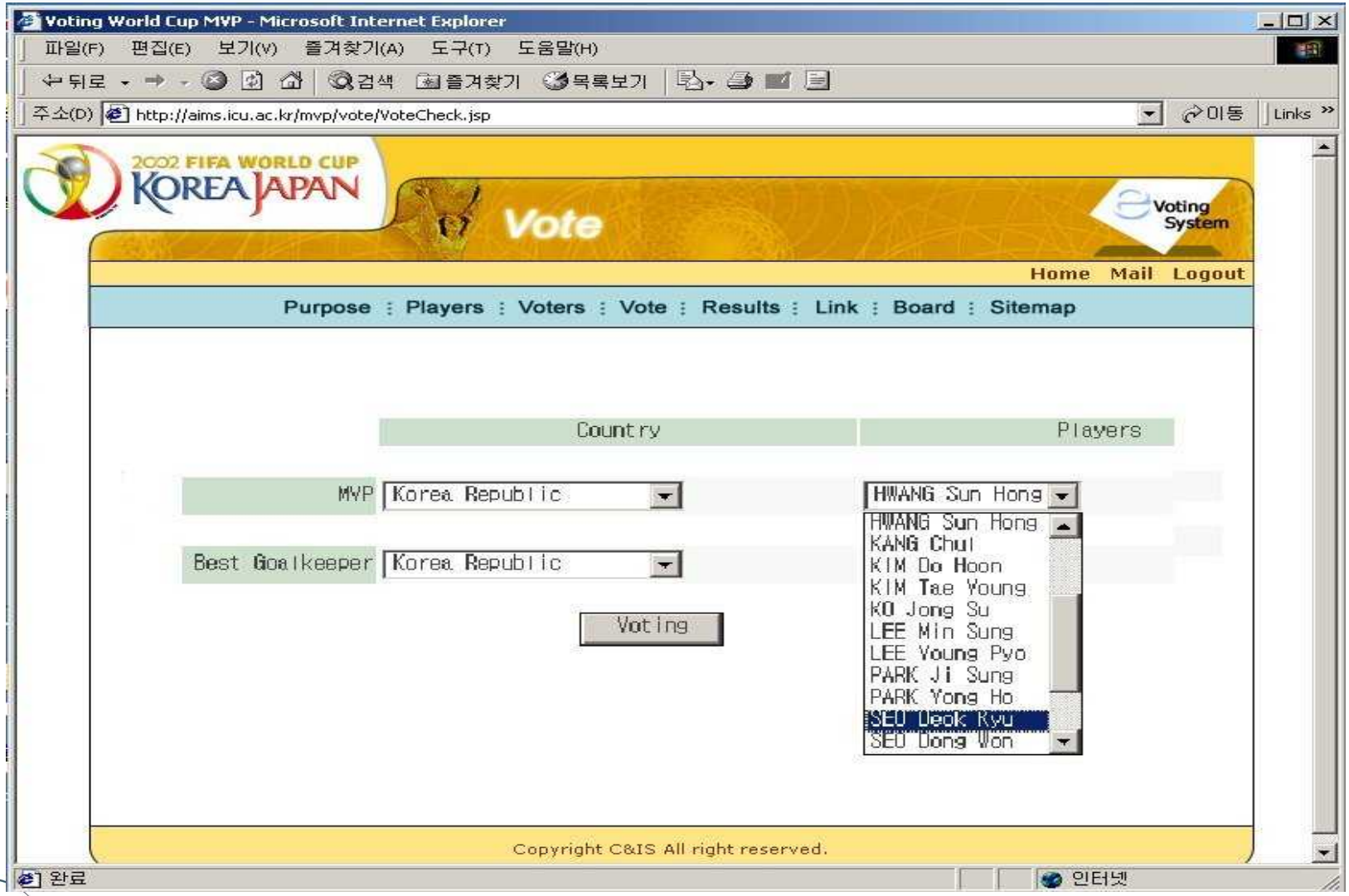
5. Typical Implementation

- **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

6. Target

- **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

Example


Voting World Cup MVP - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로 검색 즐겨찾기 목록보기
주소(D) http://aims.icu.ac.kr/mvp/vote/VoteCheck.jsp
이동 Links
2002 FIFA WORLD CUP KOREA JAPAN
Vote
Voting System
Home Mail Logout
Purpose : Players : Voters : Vote : Results : Link : Board : Sitemap
Country
Players
MVP
Korea Republic
HWANG Sun Hong
Best Goalkeeper
Korea Republic
Voting
HWANG Sun Hong
KANG Chul
KIM Do Hoon
KIM Tae Young
KO Jong Su
LEE Min Sung
LEE Young Pyo
PARK Ji Sung
PARK Yong Ho
SEO Deok Kyu
SEO Dong Won
Copyright C&IS All right reserved.
완료
인터넷

7. Summary

- **Experimental Design of Internet voting system**
  - User friendly and secure Internet voting system
  - Applying PKI to the voting system
- **Expected Results**
  - cyber MVPs of 2002 FIFA World Cup Korea-Japan™
  - Contribution to the development of information security related-industry such as PKI.
  - Valuable lessons to the planned Internet voting systems such as Cybervote in EC.
- **Help**
  - No hacking from crypto society.
  - Any comments are welcome.
  - Social engineering, political problem, etc