Design and Implementation of Internet Voting System to the Worldwide Level

August 28, 2001

IRIS(International Research center for Information Security)

ICU(Information and Communications Univ.), Korea

kkj@icu.ac.kr

Kwangjo Kim

Contents

1. Introduction

- **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 secure system
  - PKI is not ready.

Motivations

- **Our motivation and contribution - "Votopia"**
  - Prompt cryptographic voting techniques to the real life
  - Demonstrate public awareness of PKI
  - Satisfy most of security requirements
  - First trial of Internet voting to the worldwide scale such as 2002 FIFA World Cup Korea /Japan
  - Participation based on volunteership

- **Similar trial – "CyberVote"**
  - Remote Internet voting with fixed and mobile internet tech.
  - 3-year R&D program funded by European Commission

2. Requirements - cryptography

- **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)

Requirements – Security & Performance

- **Server side**
  - Network and computer security
    - Anti-hacking such as DOS attack
  - Large memory and communication bandwidth
  - Fault-tolerant and high reliable
  - Reasonable time of registration and voting

- **Client side**
  - Fast and Easy
  - Web Interface
  - No tamper-proof device provided
  - Various kinds of platform and browser

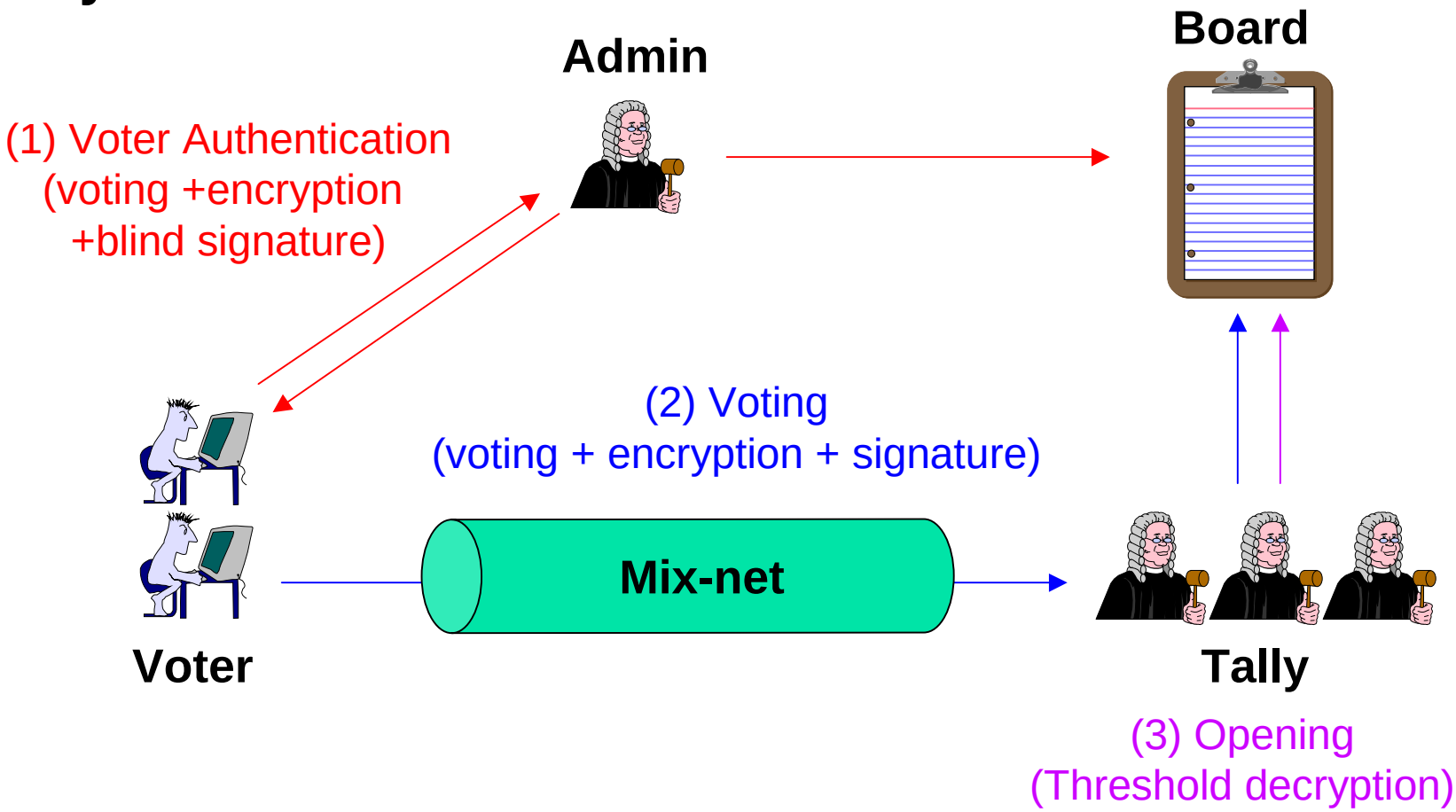
3. Voting Scheme

- **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

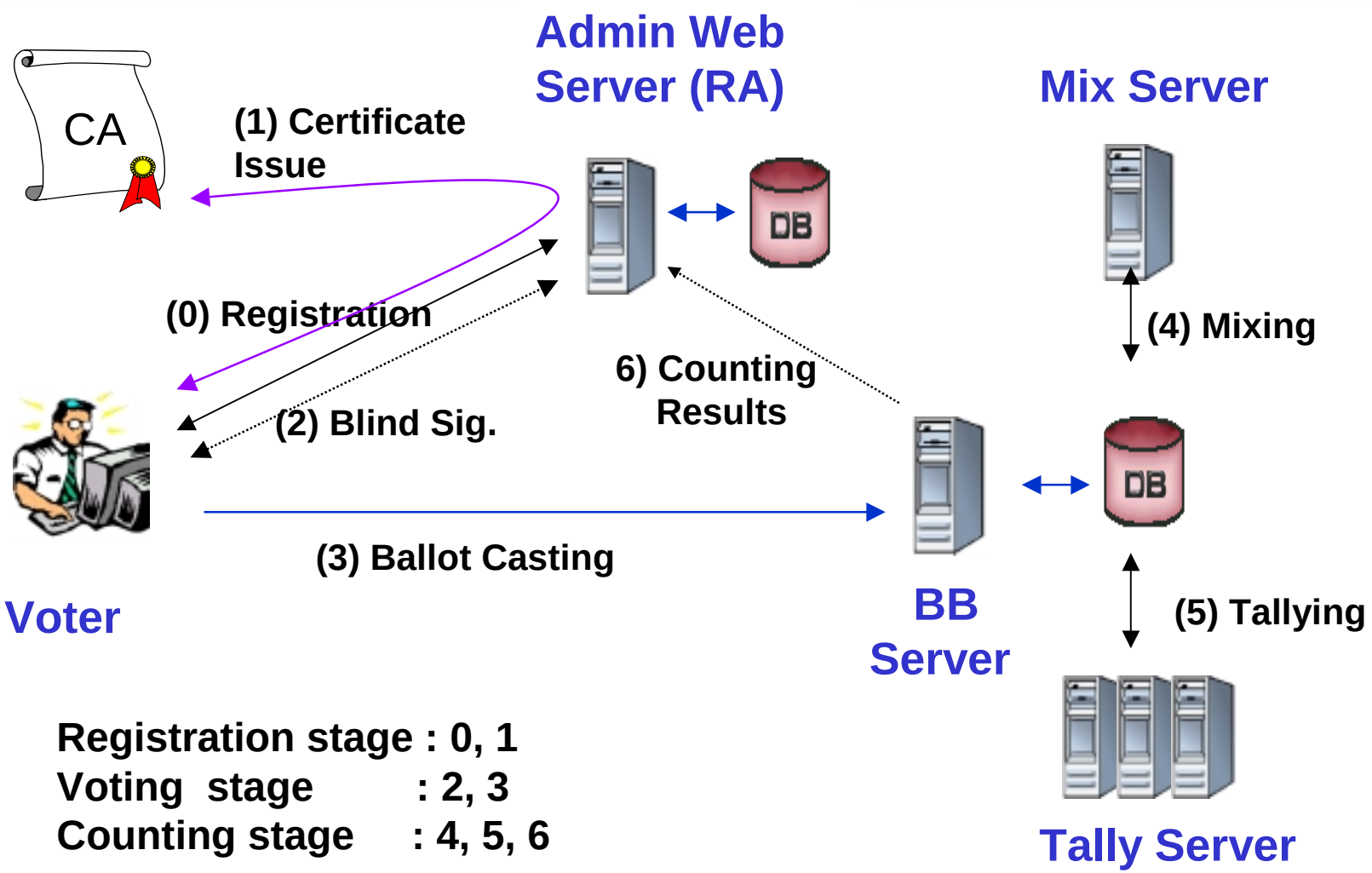
    http://theory.lcs.mit.edu/~cis/voting/voting.html
- **OMAFO99 Scheme**
  - Improved version of FOO92
  - Features : Blind signature + Mix-net (hybrid-mix) + threshold encryption

OMAFO99 scheme

- **System overview**

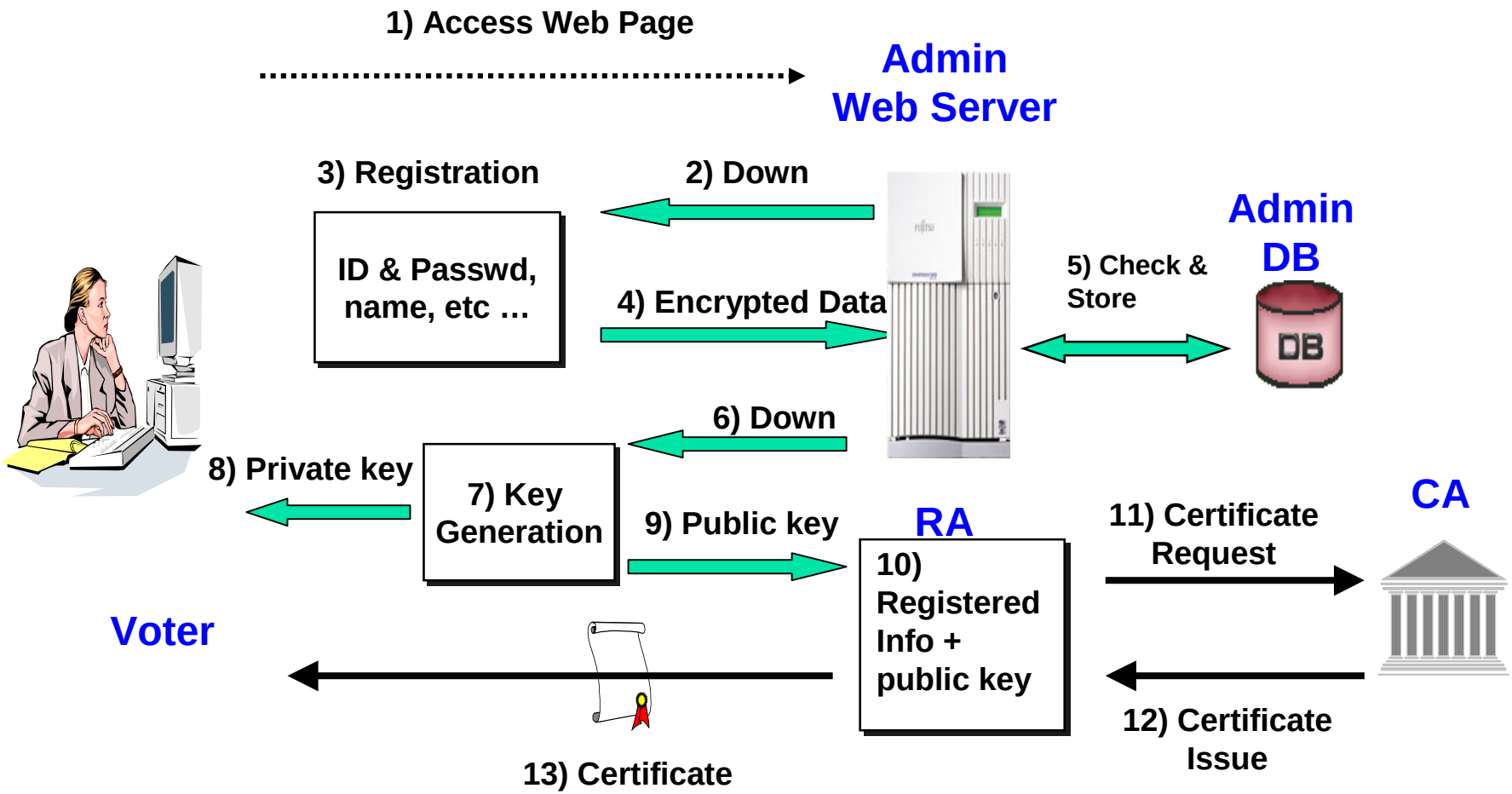


4. System Configuration

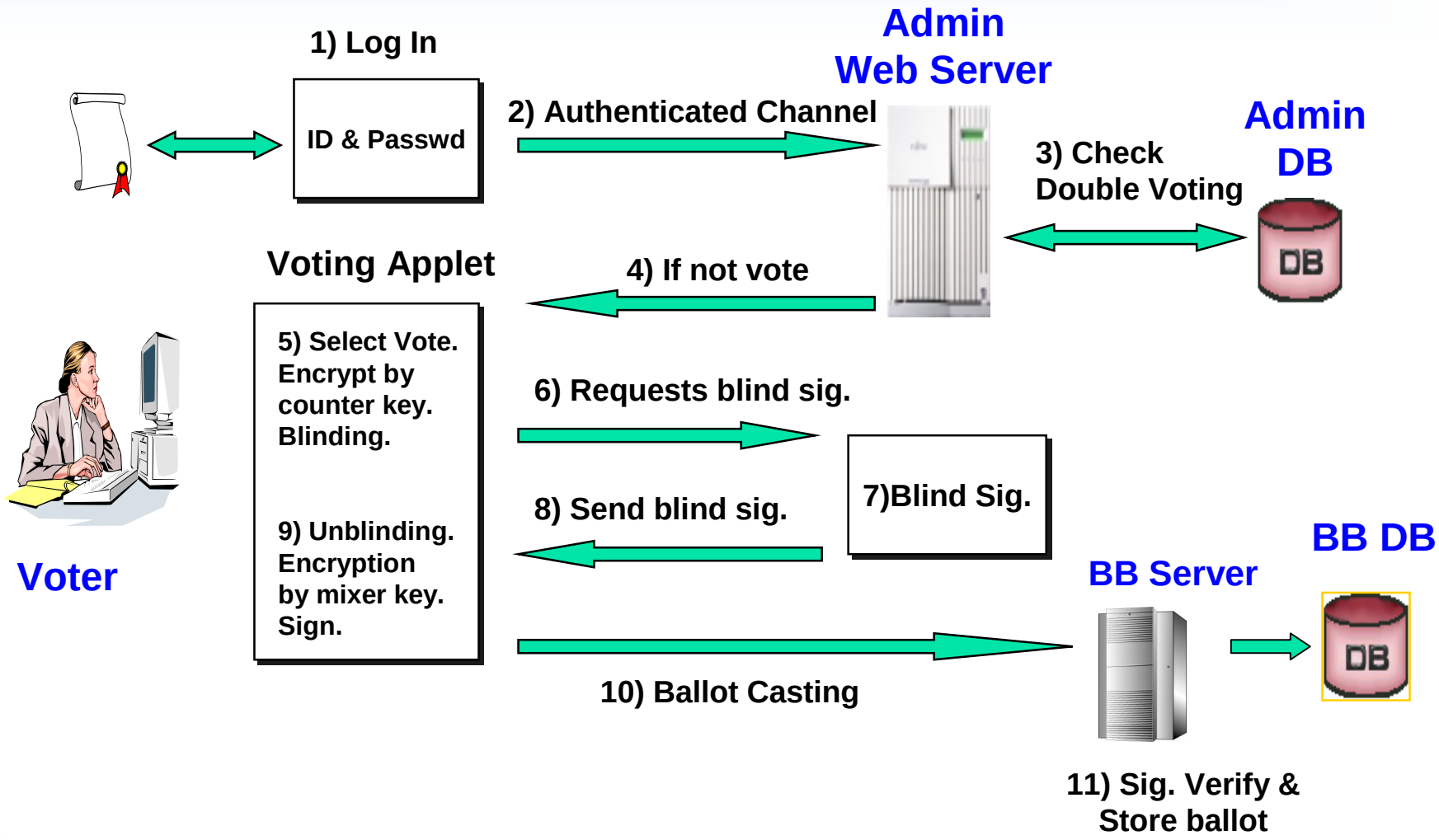


Registration stage : 0, 1
Voting stage : 2, 3
Counting stage : 4, 5, 6

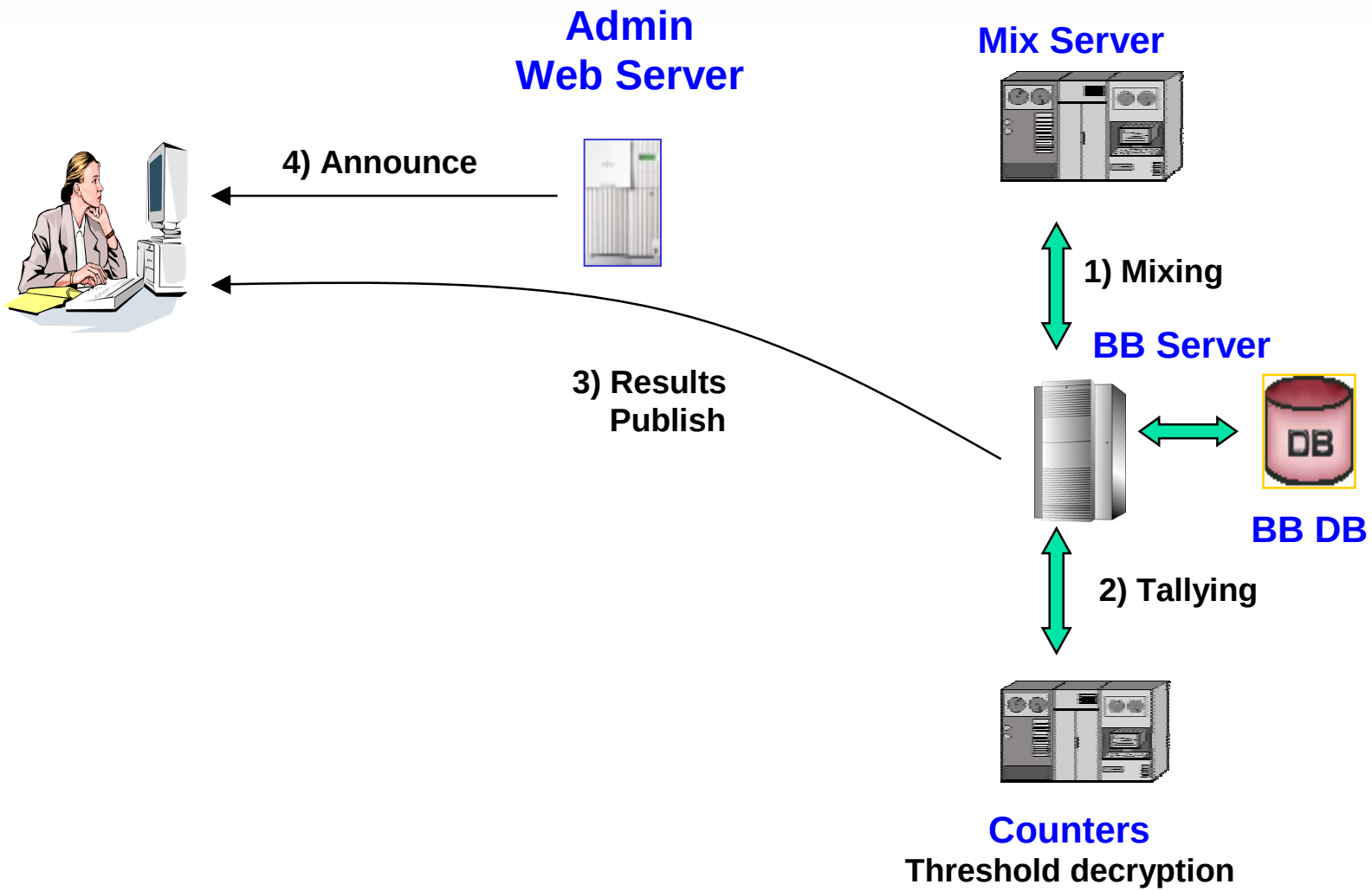
Registration stage



Voting Stage



Counting Stage



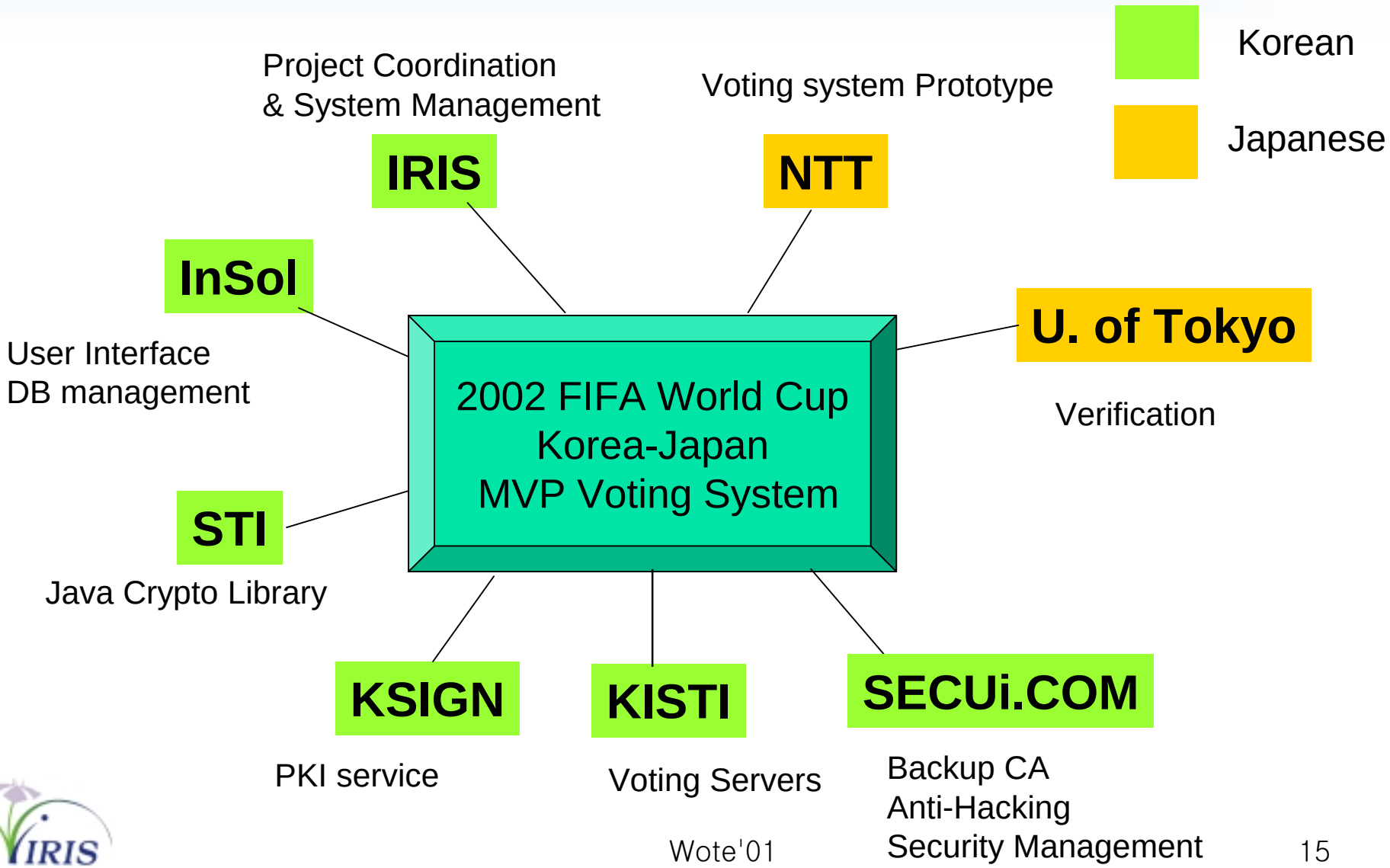
5. Implementation

- **Public-key Infrastructure**
  - Needed for “one certificate - one vote” principle
  - simplified X.509v3 for one-time use
- **Web Interface**
  - User Friendliness
- **A huge number of data handling**
  - KISTI – Computing Power Support
  - Mix Server and Counting Server

Detailed Implementation

- **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
- **Cryptographic algorithms**
  - AES
  - ElGamal public key cryptosystem
  - Schnorr type blind signature

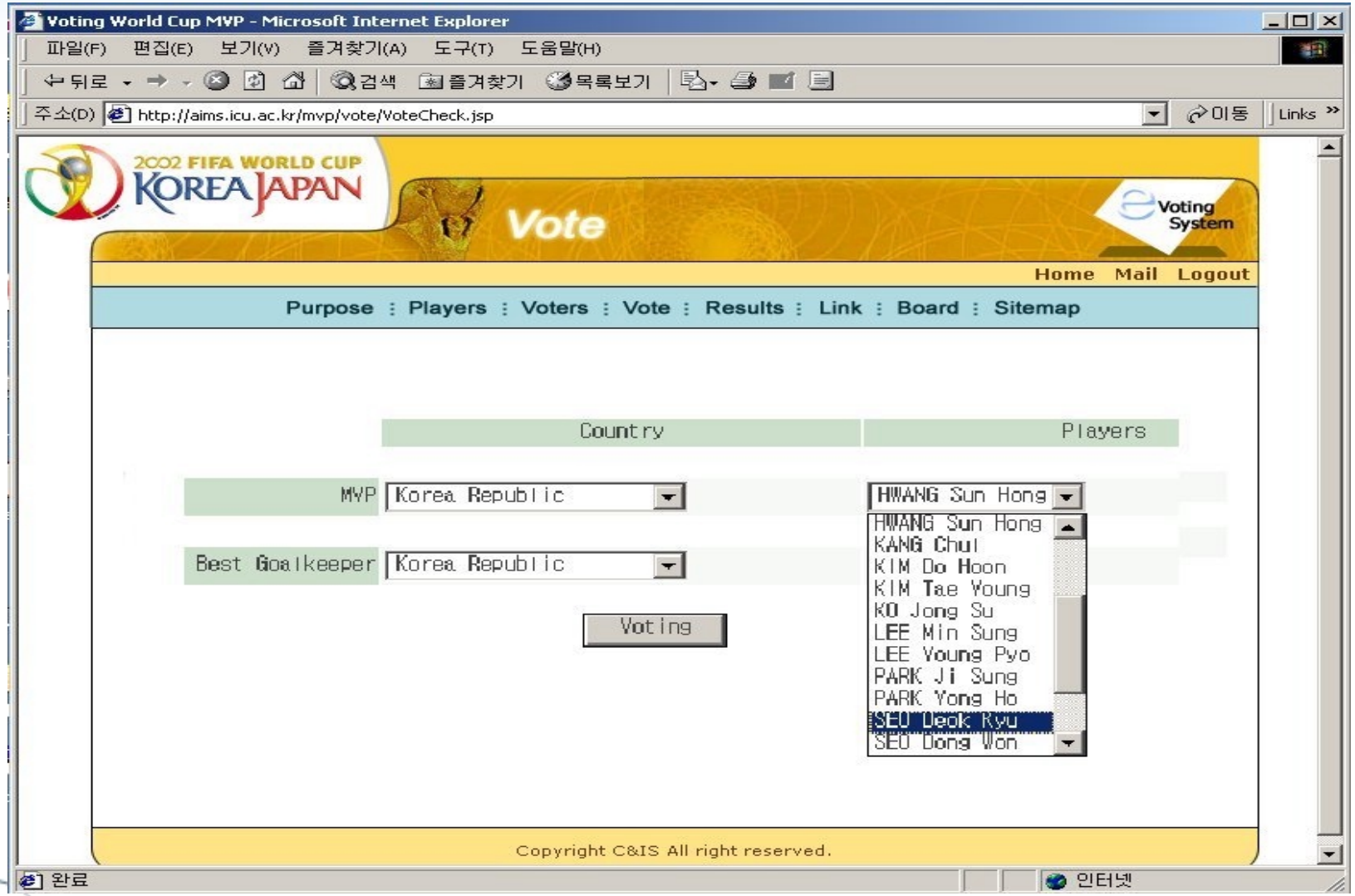
Job


Korean
Japanese
Project Coordination
& System Management
IRIS
Voting system Prototype
NTT
InSol
User Interface
DB management
U. of Tokyo
Verification
2002 FIFA World Cup
Korea-Japan
MVP Voting System
STI
Java Crypto Library
KSIGN
PKI service
KISTI
Voting Servers
SECUi.COM
Backup CA
Anti-Hacking
Security Management

6. Application-Votopia

- **2002 FIFA World Cup Korea-Japan™**
  - May 31 ~ June 30, 2002
  - Major cities in Korea and Japan
  - 32 teams from the world
- **Candidates**
  - After 1st round, 16 teams
  - MVP and best goal-keeper
- **Voting period**
  - July 1 ~ 10, 2002 (10 days)
- **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
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 Ryu
SEO Dong Won
Best Goalkeeper
Korea Republic
Voting
Copyright C&IS All right reserved.
완료
인터넷

7. Summary

- **Design & Prototyping 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
- **Left problems**
  - Multiple registration, # of voters,
  - Social engineering, political problem, etc

Questions