Votopia will be coming soon

ICU

(Information and Communications Univ.)
韓國情報通信大學校, http://www.icu.ac.kr

IRIS

(International Research center for Information Security)
國際情報保護技術研究所, http://www.iris.re.kr

Jan. 31, 2002

Kwangjo Kim, 金 光 兆

Internet Voting

- Why do we consider ?
  - Anyone can vote
  - Every country wants to be e-government
  - Anywhere from home, office, overseas, etc.

  -> Solution for the problem of decreasing the partici pation rate by the manual voting

- What are the problems ?
  - Digital divide (Slow Internet, PKI is not ready, etc)
  - Difficult identification in non face-to-face situation
  - Undetectable coerced or collaborated voting

Motivation & Contributions

- □ Celebrating or boosting 2002 FIFA World Cup Korea/Japan^{TM}
- □ Trial of Internet voting to the worldwide s cale by Korea and Japan joint teams
- □ Participation based on volunteership (non -commercial)
- □ Secure voting system to the real life usin g PKI
- □ Independent with FIFA’s MVP by press

Similar Approaches

- MIT-Caltech Task Force
  - Panic in Florida 2000 Presidential Election
  - Reliable electronic voting system
- CyberVote
  - Internet voting system with fixed and mobile terminal
  - 3-year(‘01-’03) R&D program by European Commission
- Electronic Voting system in Belgium
  - DOS system designed by Quisquater
  - Served in 1995
  - 3 Million voters
- Other systems

Cryptologic 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)

Security & Performance Requirements

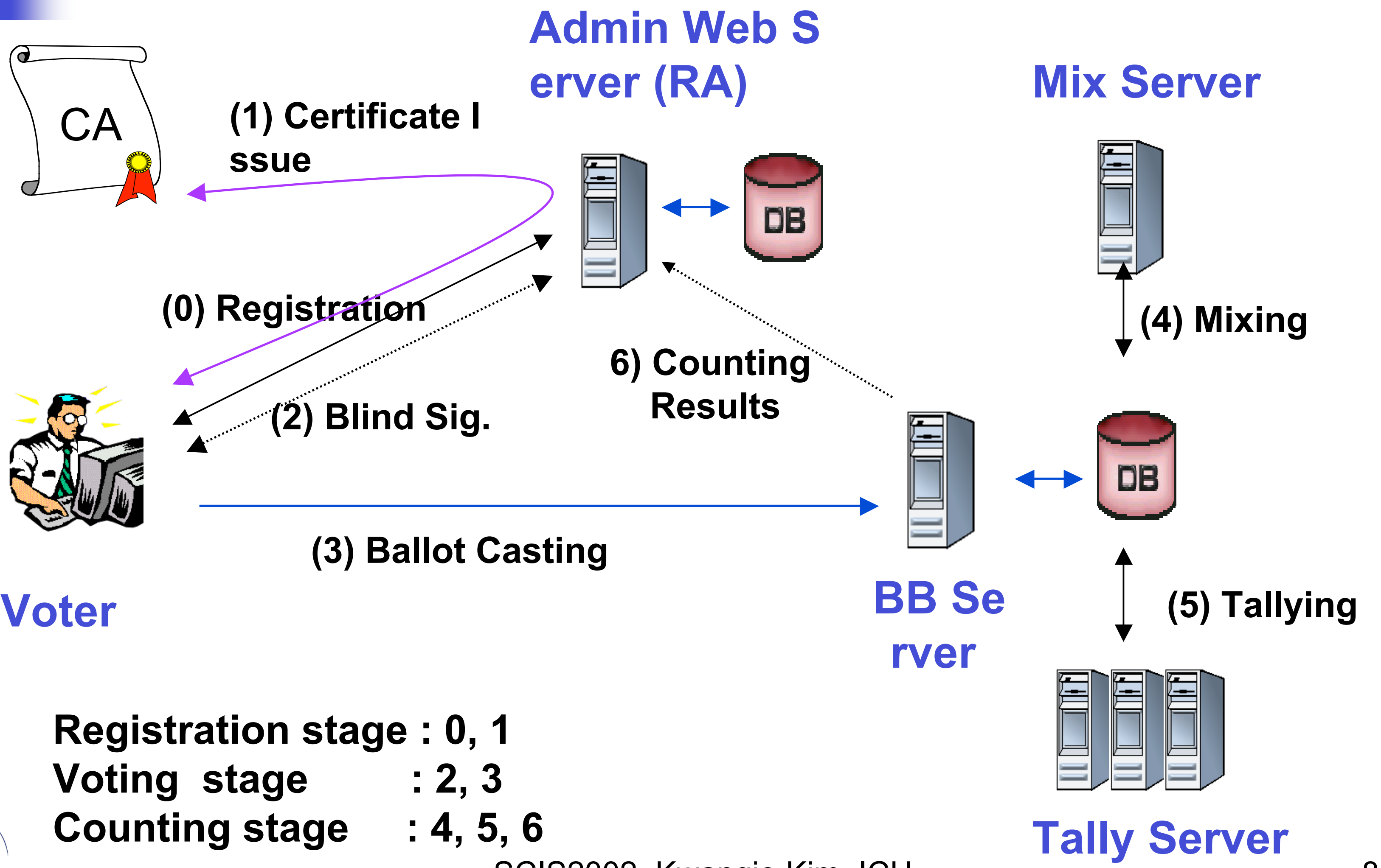
- Server side
  - Network and computer security
    - Anti-hacking such as DDOS attack, etc
  - Huge memory up to 10 M voters and reliable connection
  - Fault-tolerance and high reliability
  - Reasonable time (< 10 sec) of registration and voting
- Client side
  - Fast and easy, user friendly
    - Web Interface
  - No tamper-proof device provided
  - Various kinds of platforms, OS and browsers
  - Don’t disturb voter’s privacy

Secure 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

System Configuration



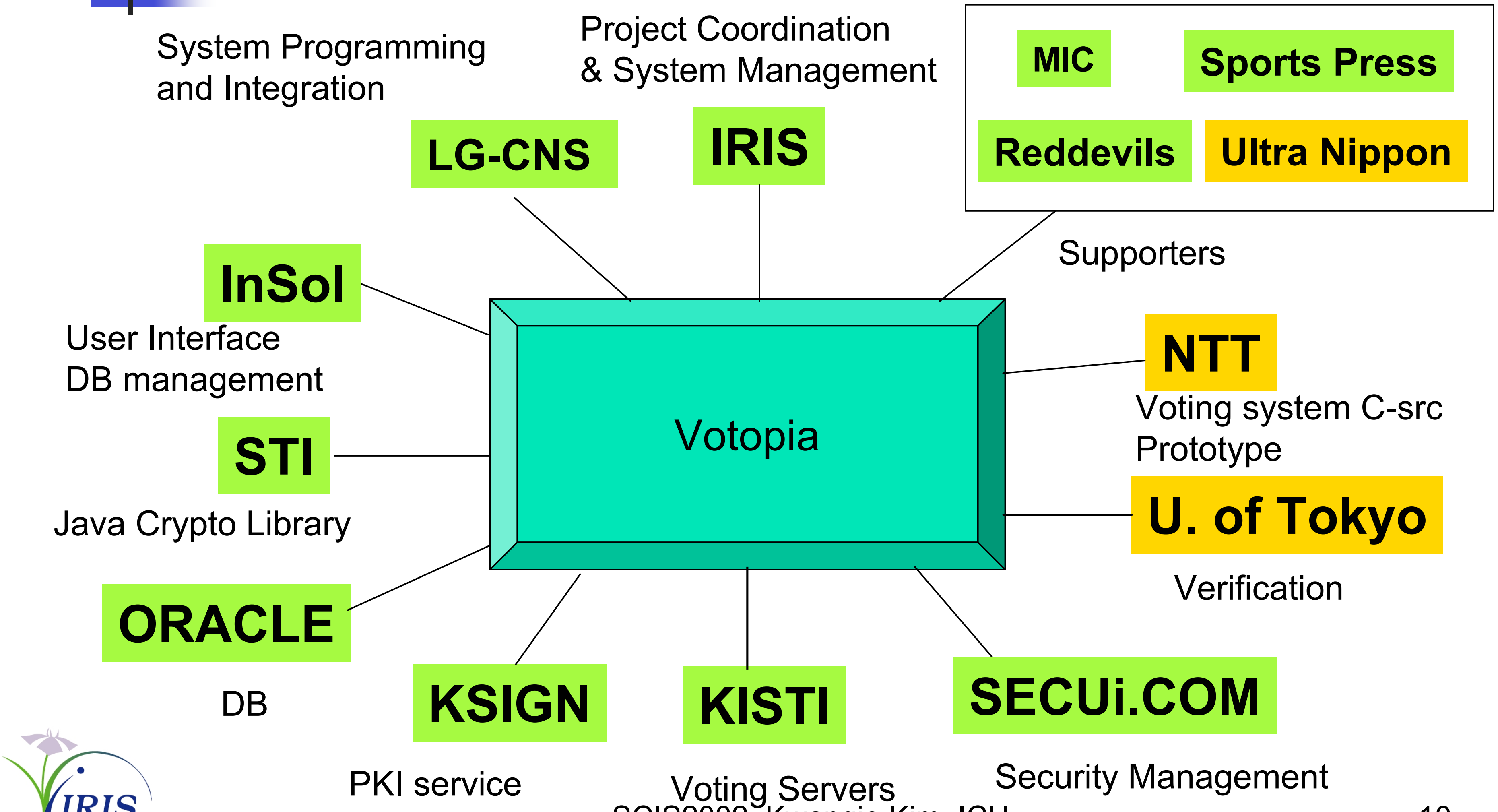
Registration stage : 0, 1
Voting stage : 2, 3
Counting stage : 4, 5, 6

Implementation

- Voting scheme : extension of NTT C prototype
  - Txt-based to Web interface
  - Add encryption function and PKI
  - C-library change from UCB to V5
  - DB update from Berkeley to Oracle
- Public-key Infrastructure
  - Needed for “one certificate - one vote” principle
  - Simplified X.509v3 certificate for one-time use
  - ElGamal encryption and Schnorr blind signature

Partners

🟩 Korean 🟨 Japanese



Votopia

LG-CNS

System Programming and Integration

IRIS

Project Coordination & System Management

MIC

Sports Press

Reddevils

Ultra Nippon

Supporters

InSol

User Interface DB management

STI

Java Crypto Library

ORACLE

DB

KSIGN

PKI service

KISTI

Voting Servers

SECUi.COM

Security Management

NTT

Voting system C-src Prototype

U. of Tokyo

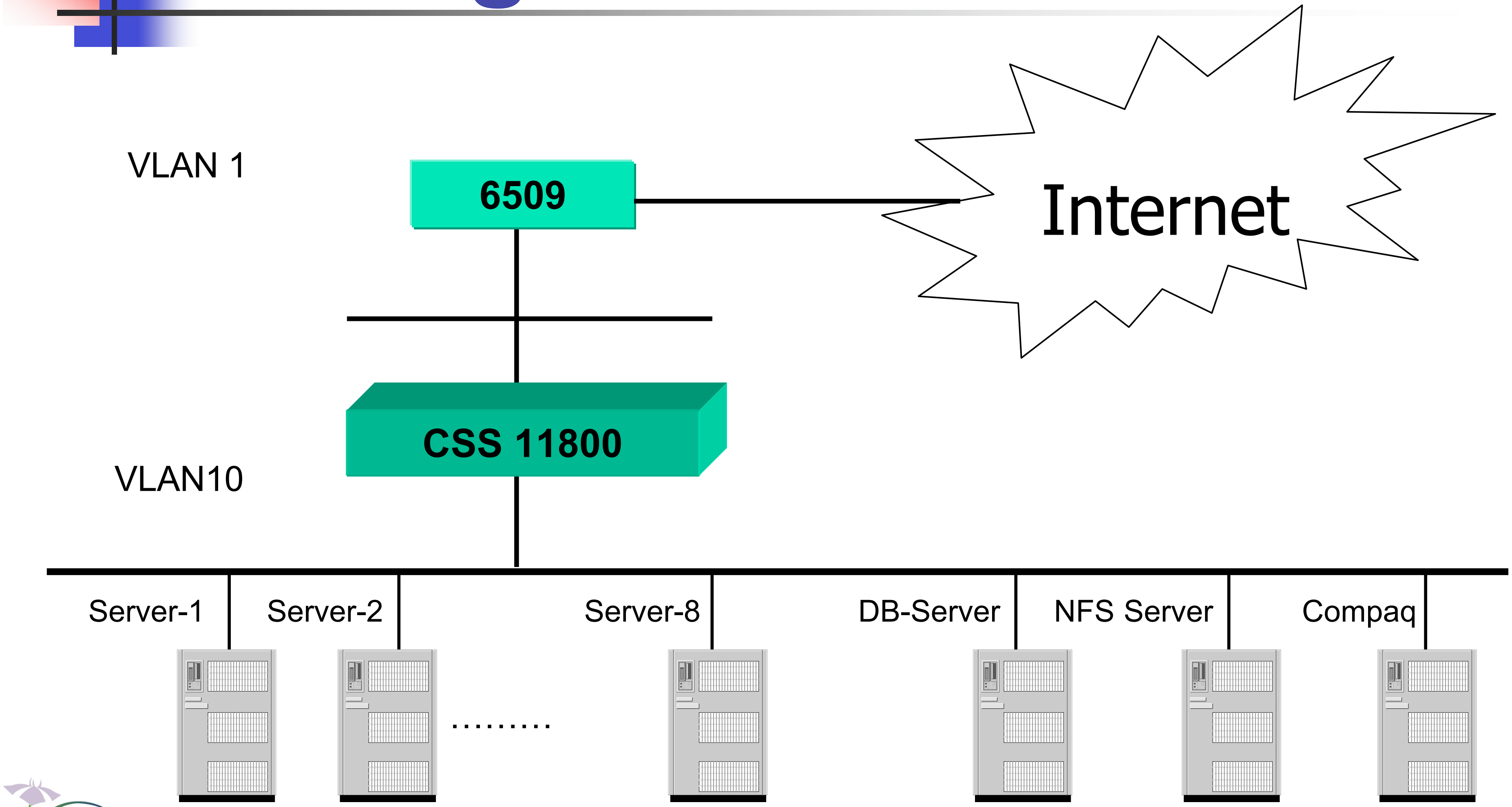
Verification

Contributors

- IRIS : Kwangjo Kim, Byoungcheon Lee, Jinho Kim, Myoungsun Kim, Hyunrok Lee, Jaegwan Park, Manho Lee, Wooseok Ham, Jongseung Kim, Hyunggi Choi, Kyuseok Ham, Vo Duc Liem, Xie Yan
- LG-CNS : Daehun Kim, Minhyung Kim, Jongyoon Choi
- Insolsoft : Mina Jung, Junghan Kim, Sunjoo Hyun
- KSIGN : Ki-Yoong Hong, Jadong Ku, Eunsong Lee, Jinsoo Lim
- STI : Donnie Choi, Seoungho Heo
- KISTI : Younghwa Cho, Jungkwon Kim, Jun Woo
- SECUi.COM : Kyoungsoo Oh, Moonseok Seo, Wonkeun Hur, Hyunwo n Ko
- MIC : Hyun Lee, Kwanghyun Seo

- U. of Tokyo : Hideki Imai, Kazuguni Kobara
- NTT : Tatsuaki Okamoto, Atsushi Fujioka, Masayuki Abe, Koutarou S uzuki

Voting Servers



Level of voting

- Plain mode
  - Web interface by Java and JSSWEB+
  - Minimum secure voting by Explorer 4.0 over
- Cipher Mode I
  - Plain mode +
  - Encrypted voting is guarded by blind signature
  - Fast tallying without mix-net
- Cipher Mode II
  - Plain mode + OMAFO99
  - Meet most cryptographic requirements

* Depending on the allowable capability of voting serve r and Internet

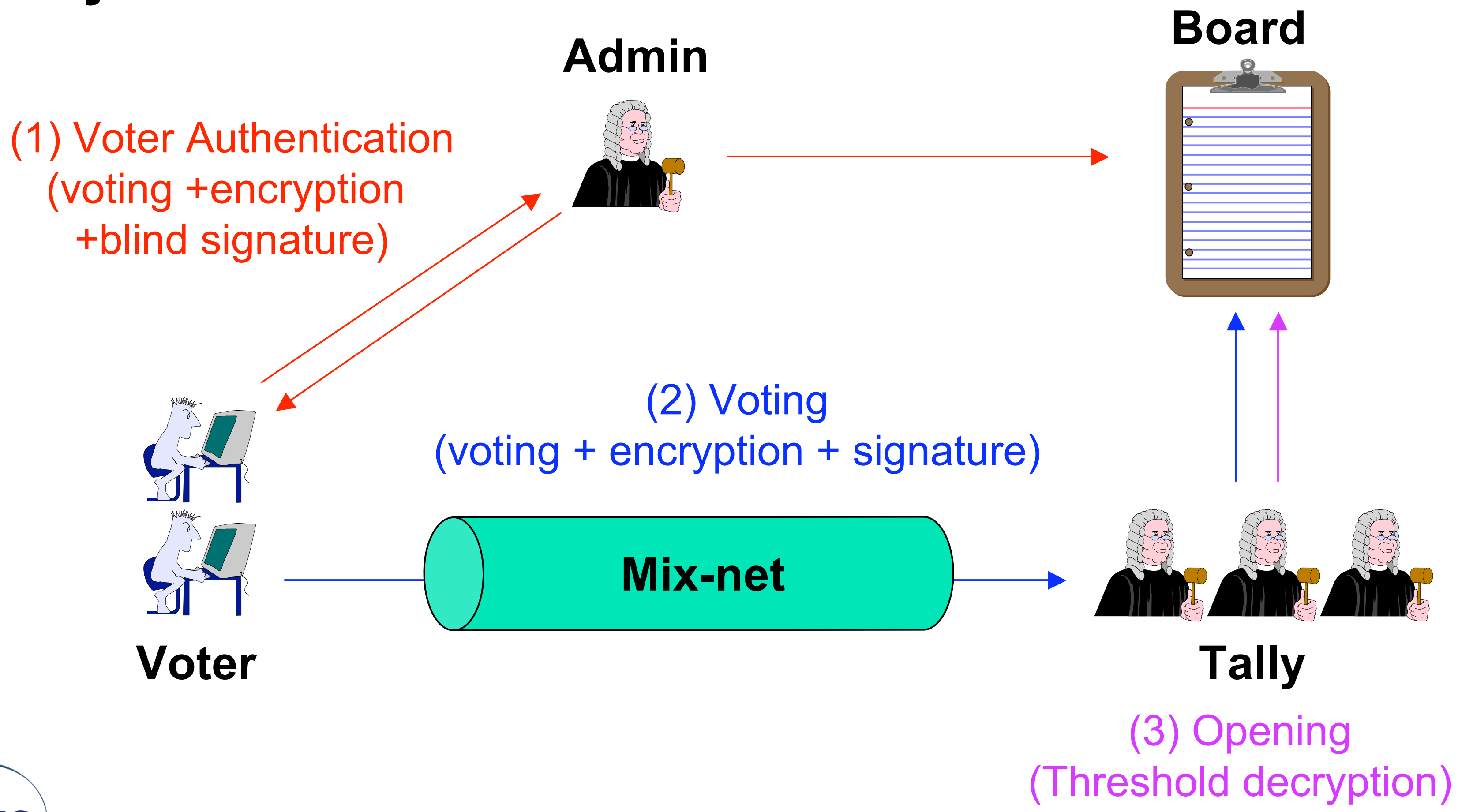
Time Schedule

- 2002 FIFA World Cup Korea/Japan™
  - Period : May 31 ~ June 30, 2002
  - Place : Major cities in Korea and Japan
  - Participants : 32 teams from the world
- 2 times Voting
  - Best 10 MVPs and goal-keeper
  - Preliminary Voting
    - Period/ Result : June 1 ~ 10, 2002 (10 days) / June 15
  - Main Voting
    - Period /Res ult: June 16 ~ 25/ June 30 (Just after final game)
- Web-page
  - http://mvp.worldcup2002.or.kr

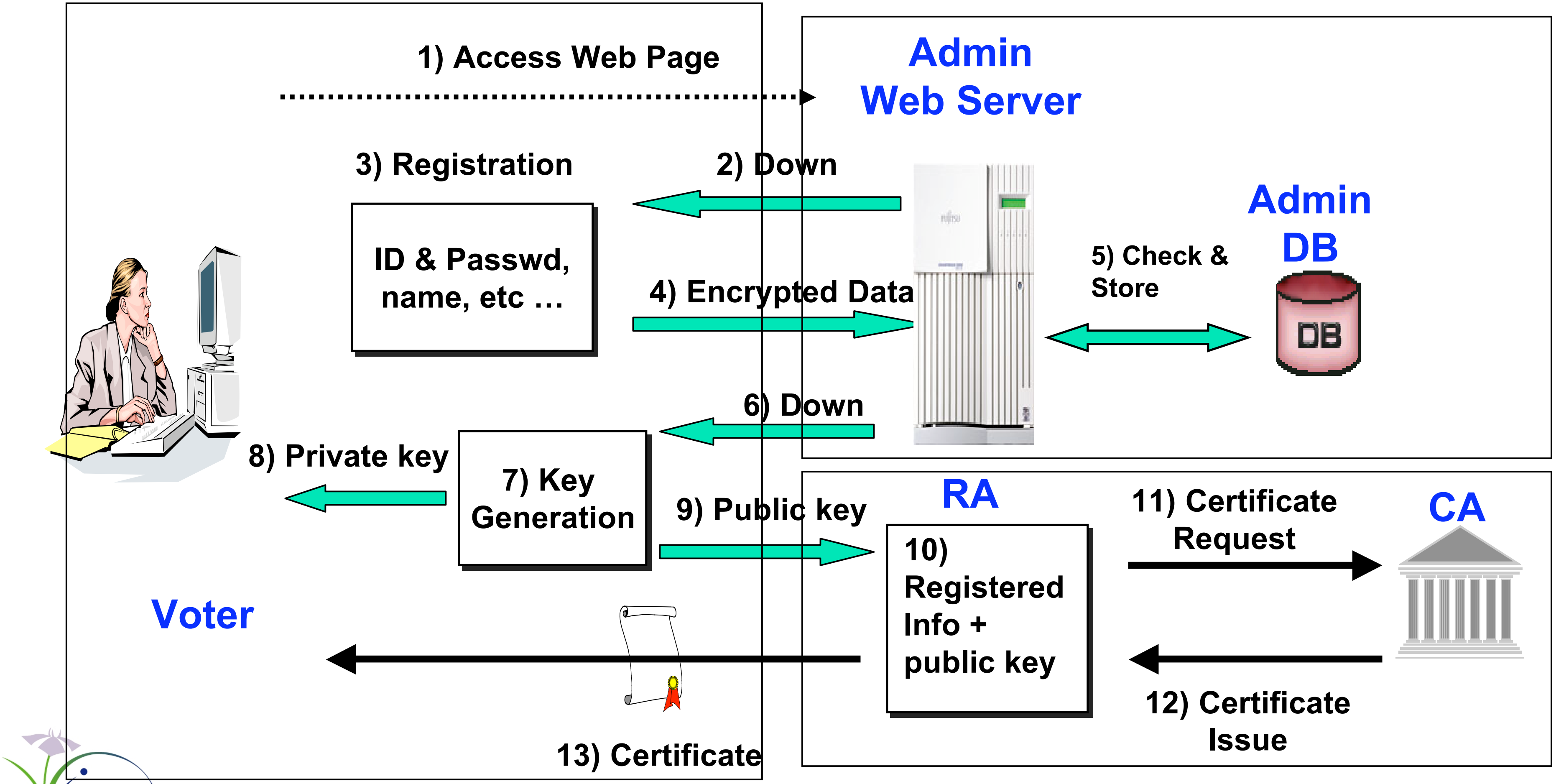
Conclusion

OMAFO99 scheme

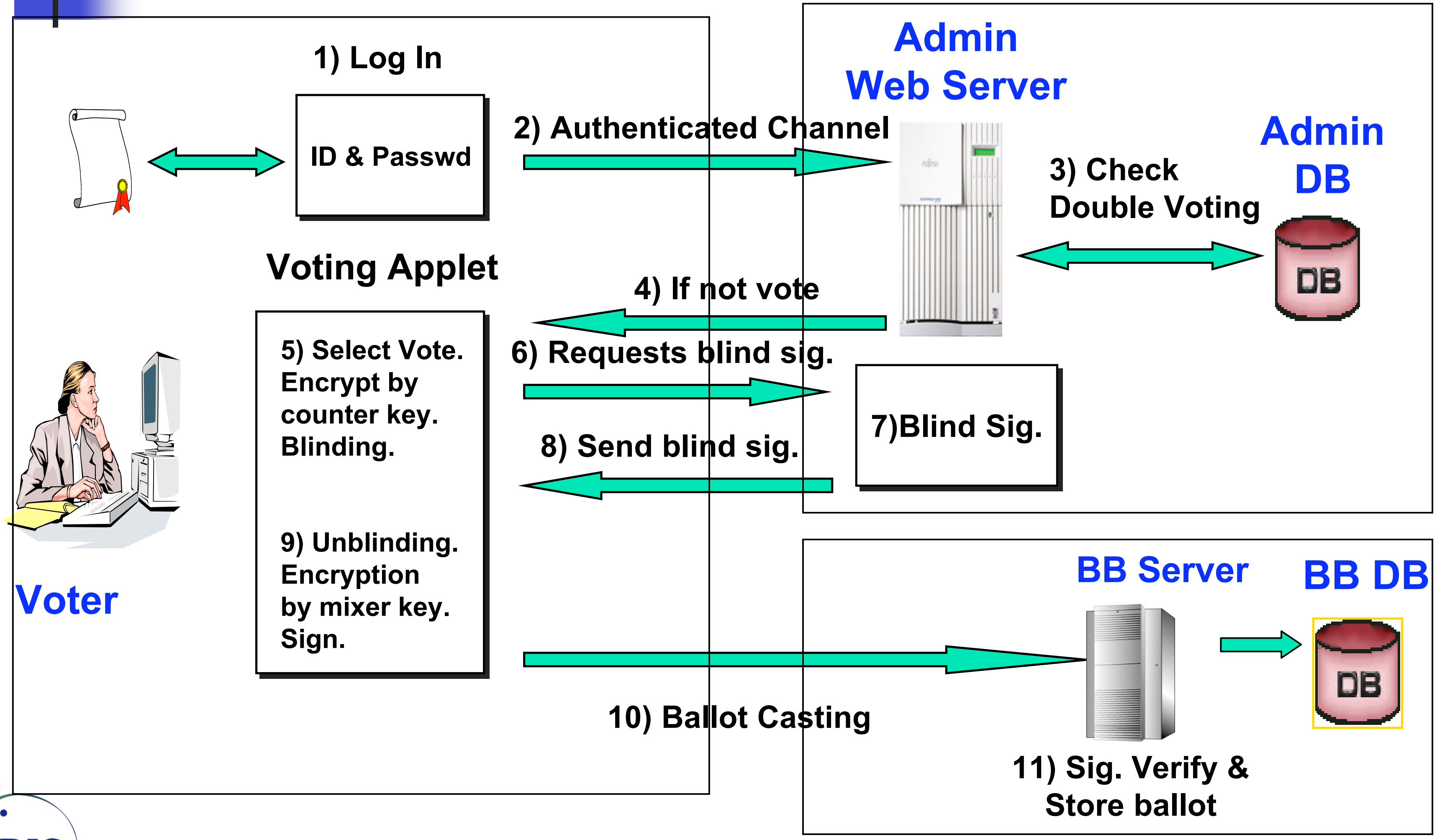
- **System overview**



Registration stage



Voting Stage



1) Log In

ID & Passwd

2) Authenticated Channel

Admin Web Server

Admin DB

3) Check Double Voting

Voting Applet

4) If not vote

5) Select Vote.
Encrypt by counter key.
Blinding.

6) Requests blind sig.

7)Blind Sig.

8) Send blind sig.

9) Unblinding.
Encryption by mixer key.
Sign.

Voter

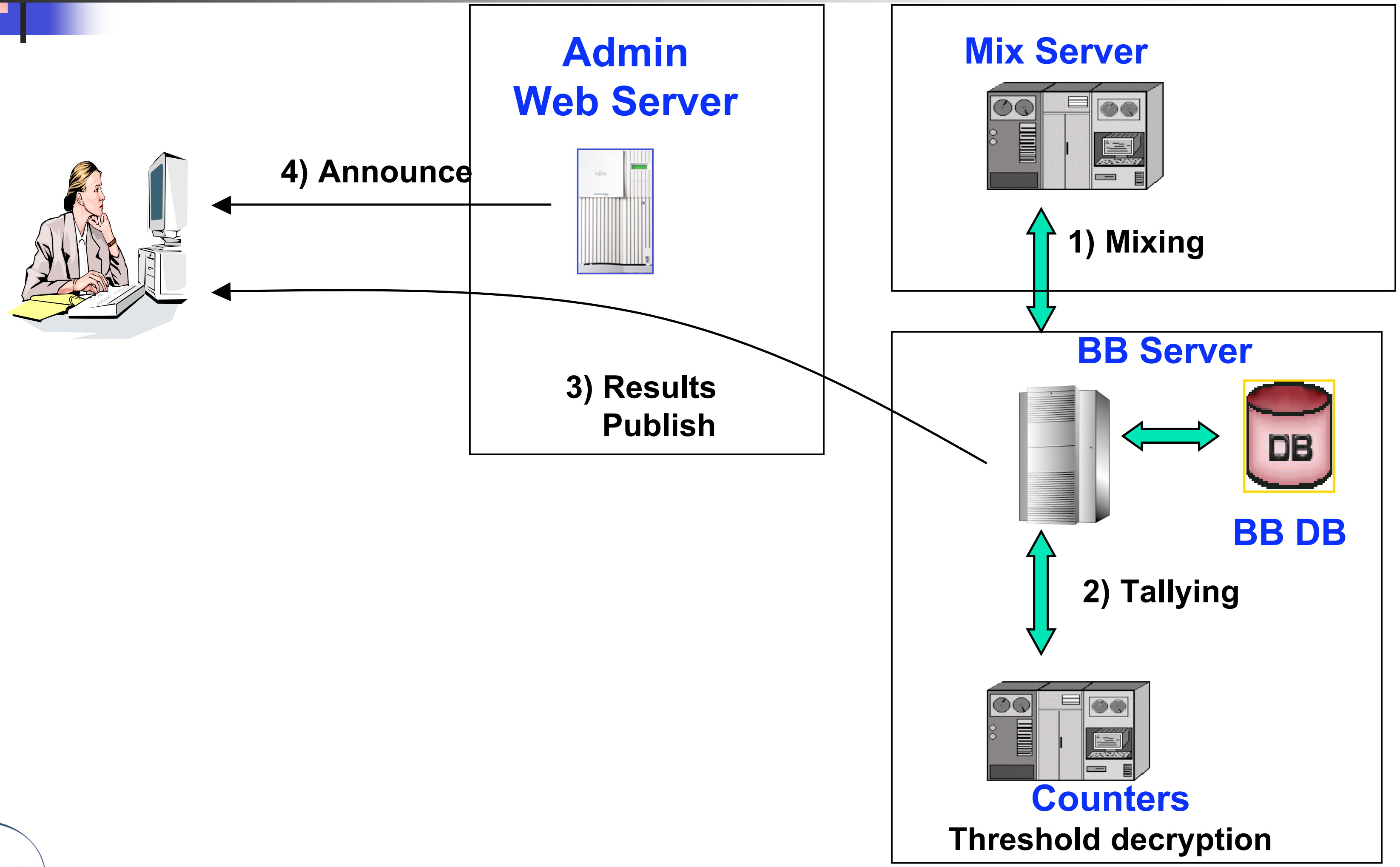
BB Server

BB DB

10) Ballot Casting

11) Sig. Verify & Store ballot

Counting Stage



Admin Web Server

Mix Server

BB Server

BB DB

Counters

Threshold decryption

1) Mixing

2) Tallying

3) Results Publish

4) Announce