Votopia is ready to serve

IRIS
(International Research center for Information Security)
http://www.iris.re.kr
ICU
(Information and Communications Univ.)
http://www.icu.ac.kr

April 30, 2002

Kwangjo Kim

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, Fangguo Zhang
- 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, Daeha Park, Seoungho Heo
- KISTI : Younghwa Cho, Jungkwon Kim, Jun Woo
- SECUi.COM : Kyongsoo Oh, Moonseok Seo, Wonkeun Hur, Hyunwon Ko
- MIC : Hyun Lee, Ee-Hwan Hwang and more
- Korean Press : INEWS24, Daily Econimics
- U. of Tokyo : Hideki Imai, Kazuguni Kobara
- NTT : Tatsuaki Okamoto, Atsushi Fujioka, Masayuki Abe, Koutarou Suzuki
- ORACLE, SUN

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 participation 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

- ❑ Celebrating or boosting 2002 FIFA World Cup Korea/Japan^{TM}
  - Period : May 31 ~ June 30, 2002
  - Place : Major cities in Korea and Japan
  - # of teams : 32 countries
- ❑ Korean and Japanese volunteers (non-commercial)
- ❑ Internet voting is as secure as manual voting using cryptography
- ❑ Independent with FIFA's MVP by press
- ❑ To spread the widely utilization of security technology like Public Key Infrastructure, *etc.*

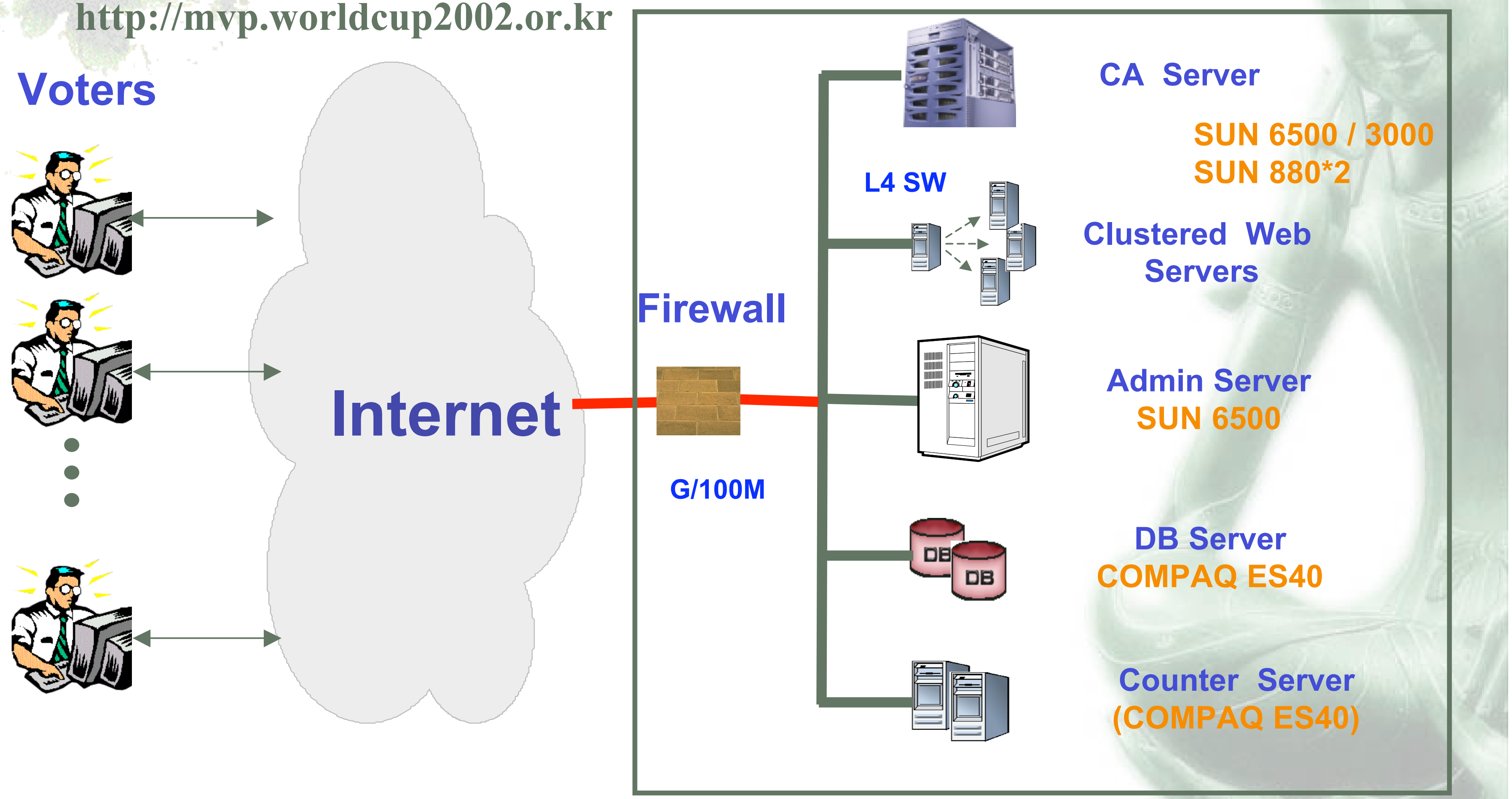
Cryptographic Req’t

- Basic
  - ✓ 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
  - ✓ 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 Req’t

- Server side
  - Network and computer security
    - Anti-hacking such as DDOS attack, etc
  - Large DB handling
  - Fault-tolerance and high reliability
  - Fast processing when registering and voting
- Client side
  - Fast and easy, user friendly web interface
  - No tamper-proof device provided
  - Various kinds of platforms, OS and browsers
  - Keep the privacy of voter
  - Remote identification

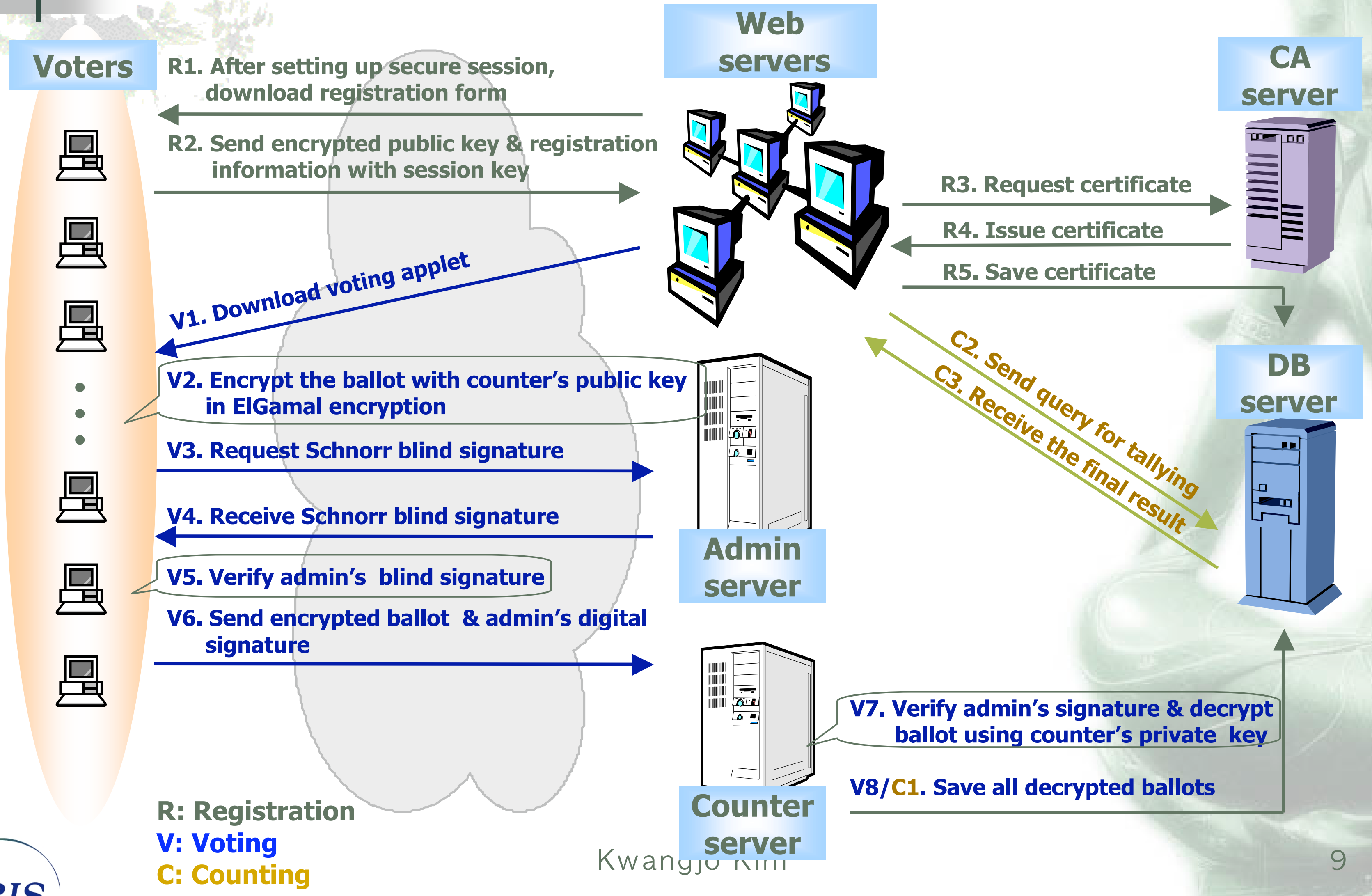
System Configuration



Implementation

- Client
  - Java, JLOCK+
  - MS Explorer 4.0 on Windows98 or higher
  - Korean, Japanese, English and Chinese
- Web, DB, Admin, and Counter Servers
  - Oracle DB, JDBC
  - Java, JSP, Tomcat, Apache, JSSWEB+
- Encryption and Certificate
  - ElGamal encryption and Schnorr (blind) signature
  - Simplified X.509v3 certificate issued by CA server

Flow of 3 main stages



Voters

Web servers

CA server

DB server

Admin server

Counter server

R1. After setting up secure session, download registration form

R2. Send encrypted public key & registration information with session key

R3. Request certificate

R4. Issue certificate

R5. Save certificate

V1. Download voting applet

V2. Encrypt the ballot with counter's public key in ElGamal encryption

V3. Request Schnorr blind signature

V4. Receive Schnorr blind signature

V5. Verify admin's blind signature

V6. Send encrypted ballot & admin's digital signature

V7. Verify admin's signature & decrypt ballot using counter's private key

V8/C1. Save all decrypted ballots

C2. Send query for tallying

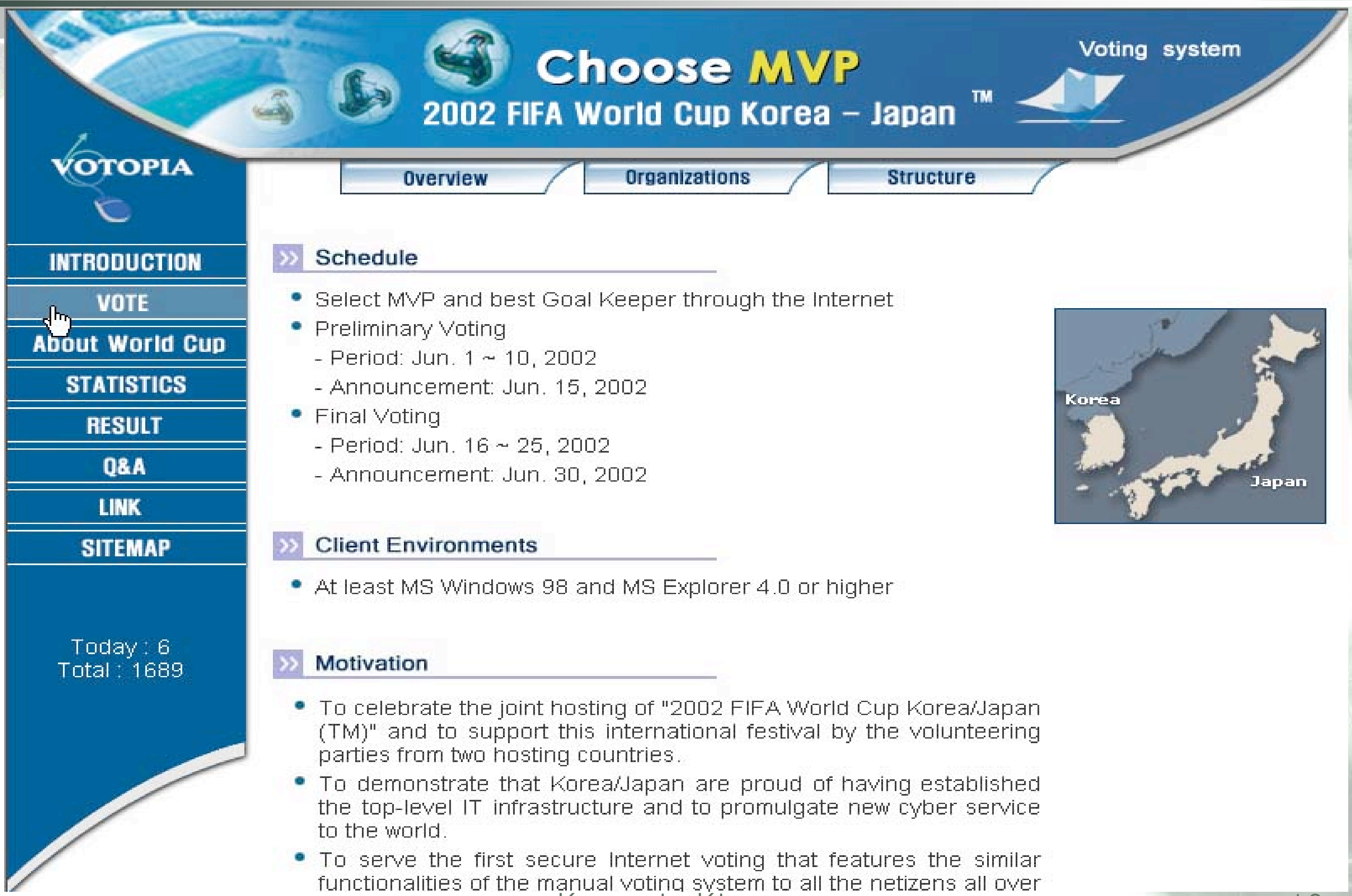
C3. Receive the final result

R: Registration

V: Voting

C: Counting

Home Page



Today : 6
Total : 1689

Schedule

- Select MVP and best Goal Keeper through the Internet
- Preliminary Voting
  - Period: Jun. 1 ~ 10, 2002
  - Announcement: Jun. 15, 2002
- Final Voting
  - Period: Jun. 16 ~ 25, 2002
  - Announcement: Jun. 30, 2002

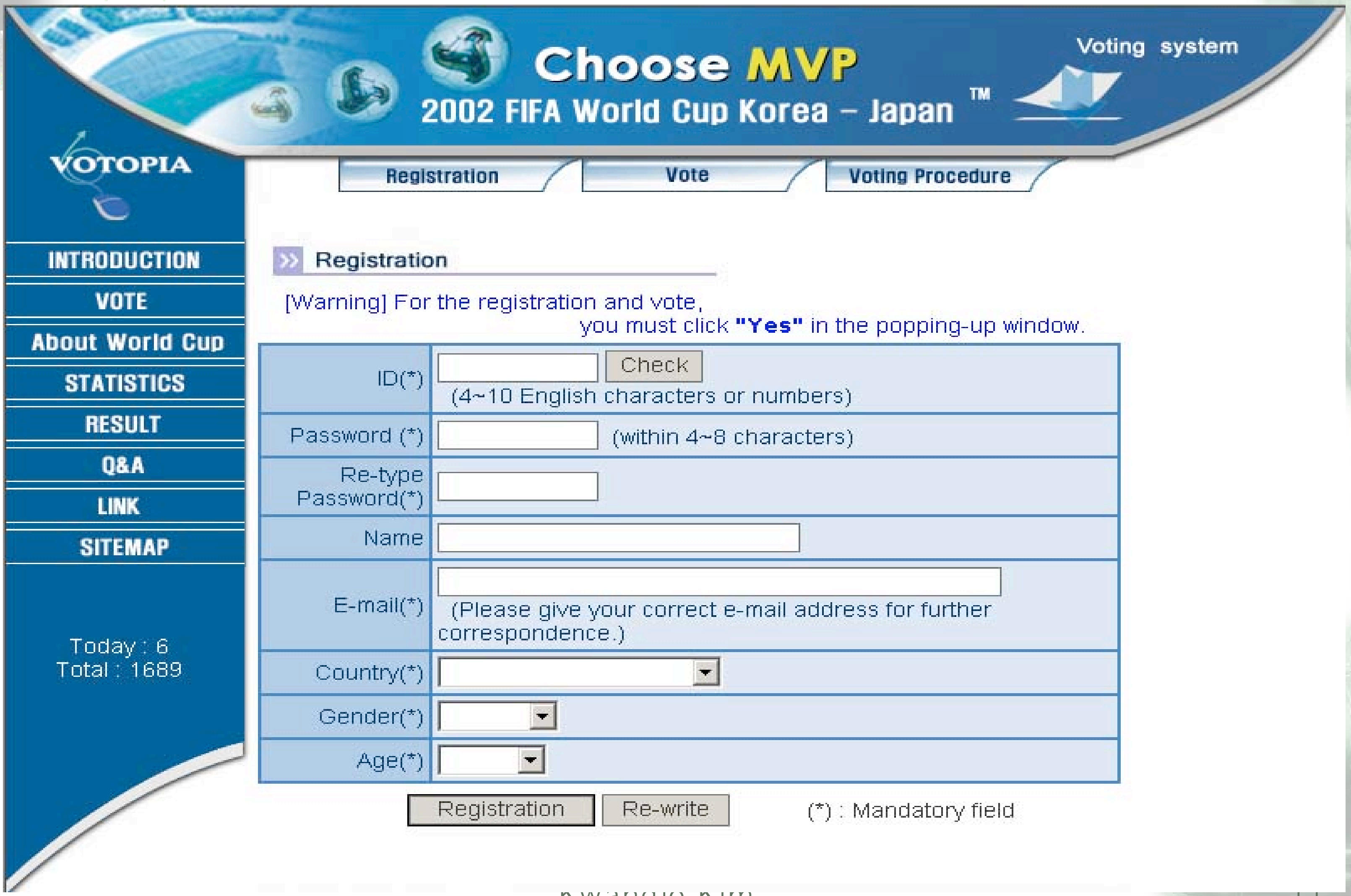
Client Environments

- At least MS Windows 98 and MS Explorer 4.0 or higher

Motivation

- To celebrate the joint hosting of "2002 FIFA World Cup Korea/Japan (TM)" and to support this international festival by the volunteering parties from two hosting countries.
- To demonstrate that Korea/Japan are proud of having established the top-level IT infrastructure and to promulgate new cyber service to the world.
- To serve the first secure Internet voting that features the similar functionalities of the manual voting system to all the netizens all over

Registration



Today : 6
Total : 1689

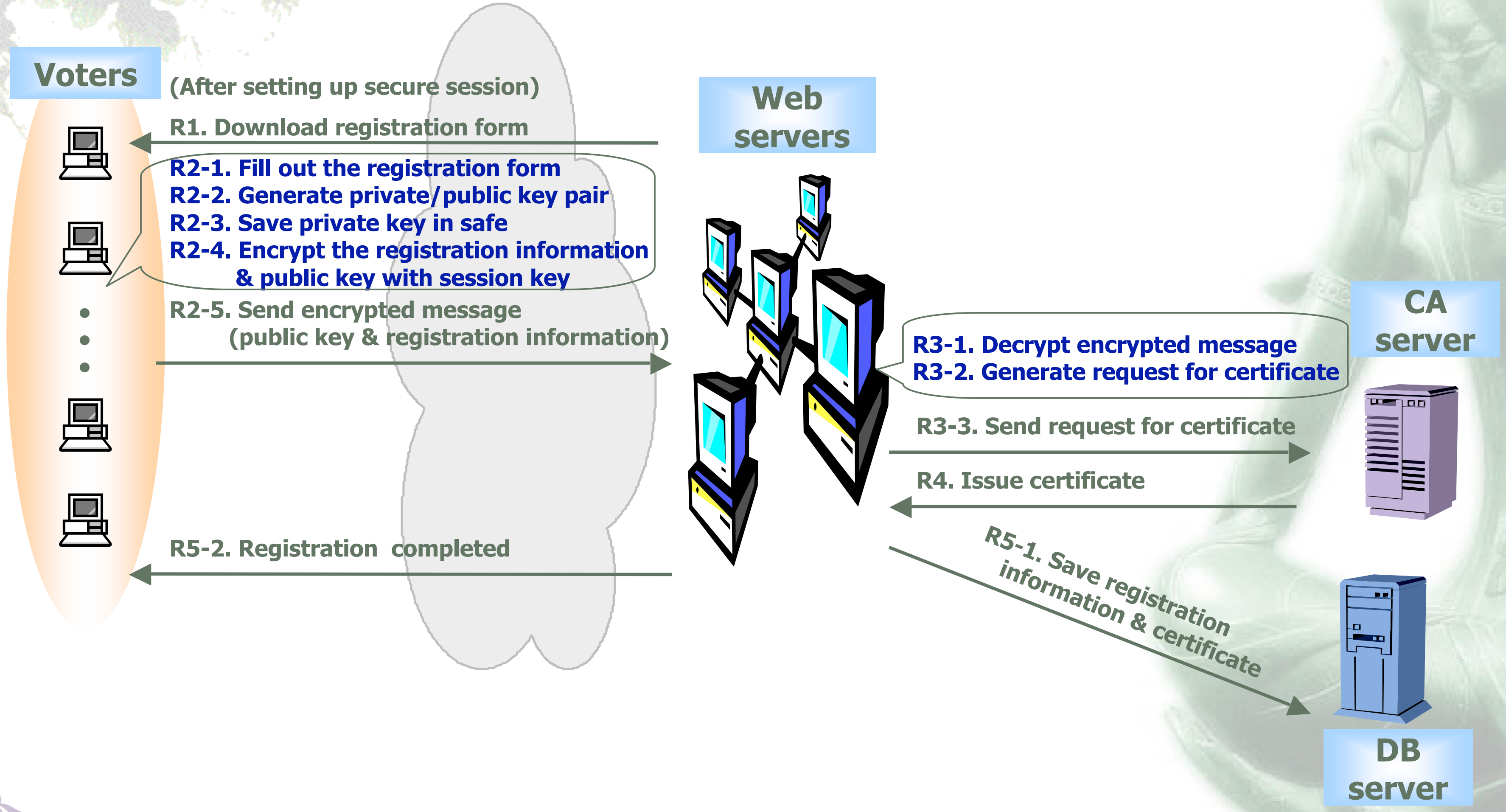
Registration

[Warning] For the registration and vote,
you must click **"Yes"** in the popping-up window.

ID(*)	Check (4~10 English characters or numbers)
Password (*)	(within 4~8 characters)
Re-type Password(*)	
Name	
E-mail(*)	(Please give your correct e-mail address for further correspondence.)
Country(*)	
Gender(*)	
Age(*)	

Registration Re-write (*) : Mandatory field

Registration Stage



Voters

(After setting up secure session)

R1. Download registration form

R2-1. Fill out the registration form
R2-2. Generate private/public key pair
R2-3. Save private key in safe
R2-4. Encrypt the registration information & public key with session key

R2-5. Send encrypted message (public key & registration information)

Web servers

R3-1. Decrypt encrypted message
R3-2. Generate request for certificate

R3-3. Send request for certificate

CA server

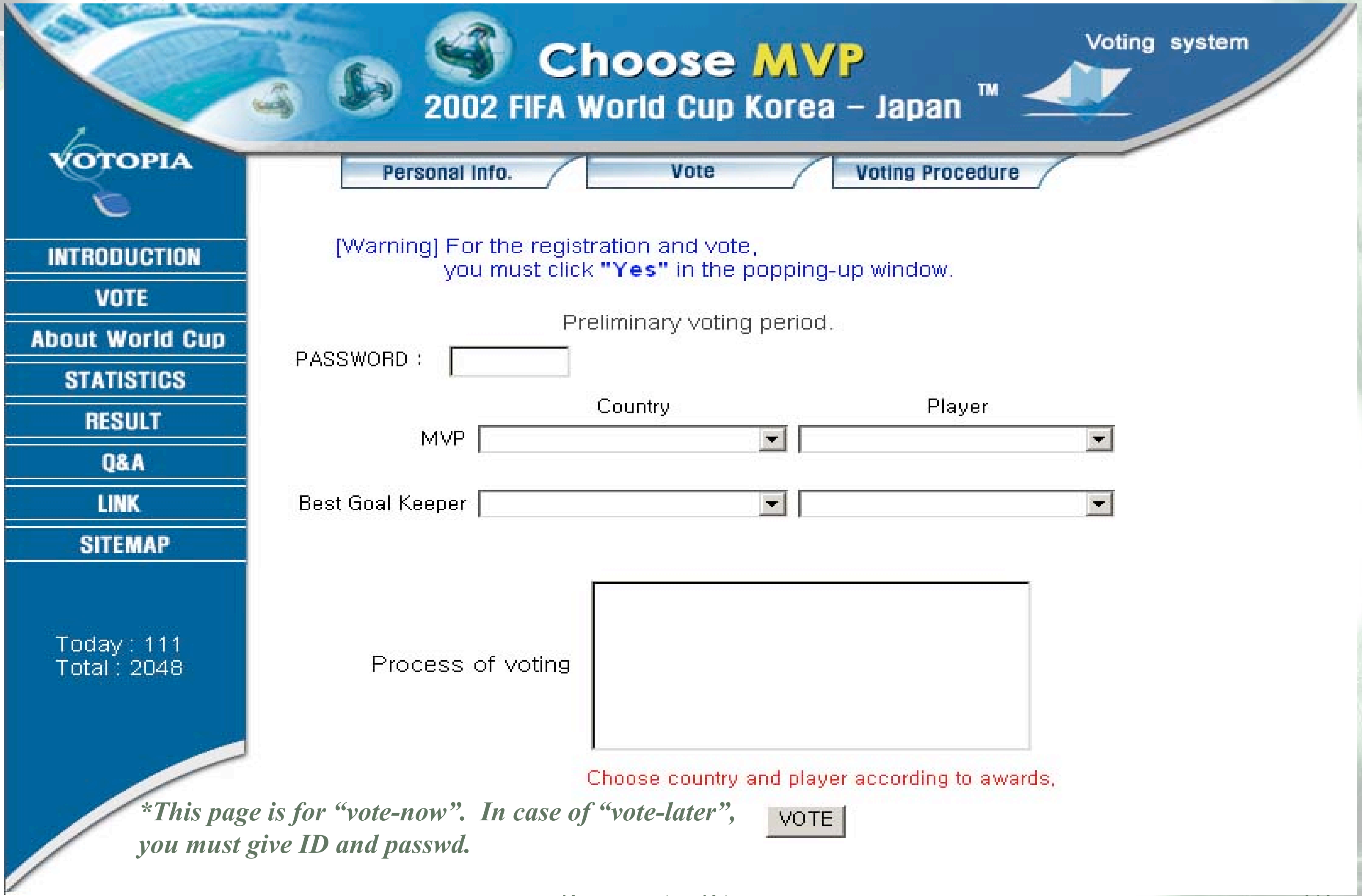
R4. Issue certificate

R5-1. Save registration information & certificate

DB server

R5-2. Registration completed

Voting



[Warning] For the registration and vote,
you must click "Yes" in the popping-up window.

Preliminary voting period.

PASSWORD :

	Country	Player
MVP		
Best Goal Keeper		

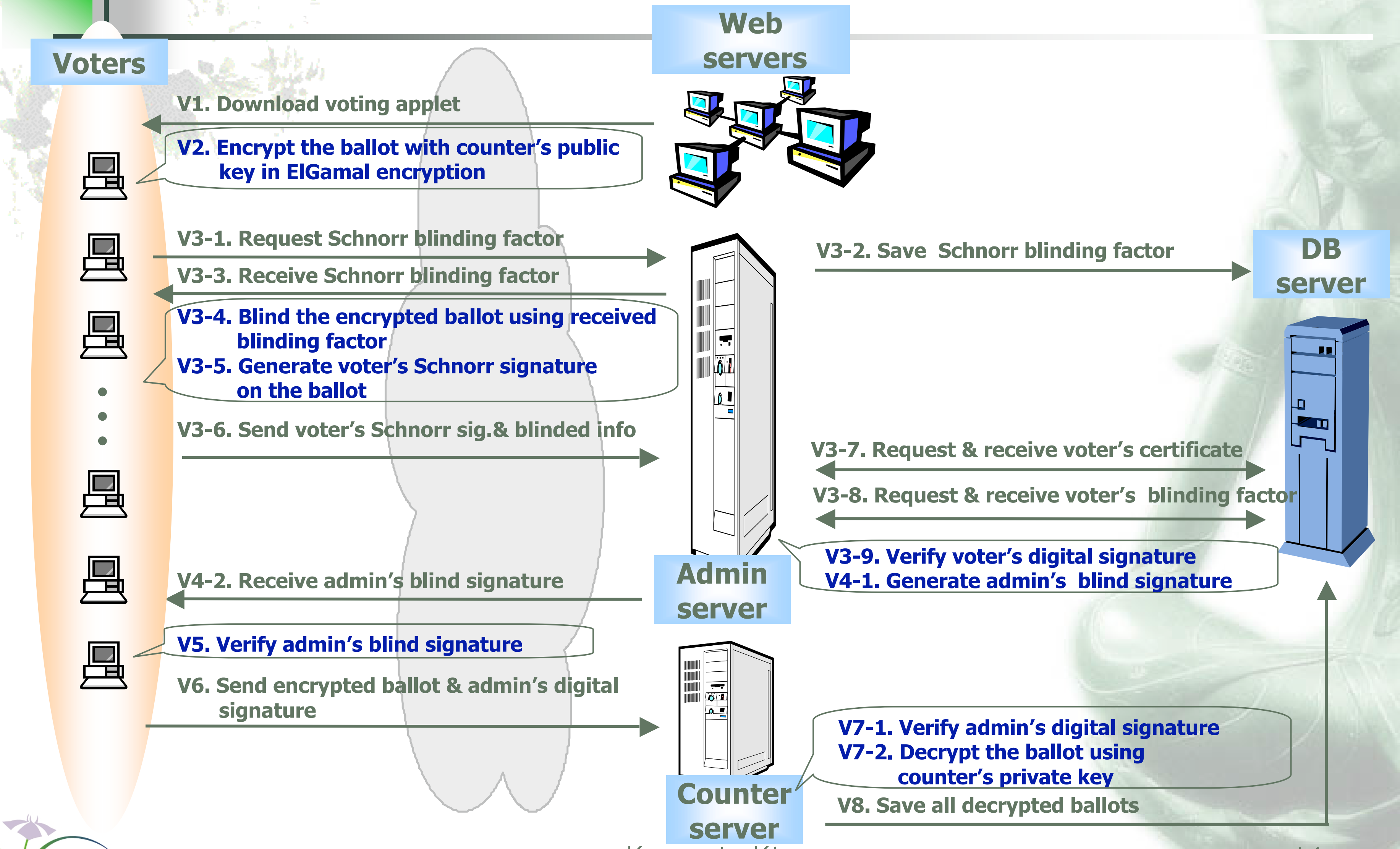
Process of voting

Choose country and player according to awards.

Today : 111
Total : 2048

*This page is for "vote-now". In case of "vote-later", you must give ID and passwd.

Voting Stage



Voters

Web servers

Admin server

DB server

Counter server

V1. Download voting applet

V2. Encrypt the ballot with counter's public key in ElGamal encryption

V3-1. Request Schnorr blinding factor

V3-2. Save Schnorr blinding factor

V3-3. Receive Schnorr blinding factor

V3-4. Blind the encrypted ballot using received blinding factor

V3-5. Generate voter's Schnorr signature on the ballot

V3-6. Send voter's Schnorr sig.& blinded info

V3-7. Request & receive voter's certificate

V3-8. Request & receive voter's blinding factor

V3-9. Verify voter's digital signature

V4-1. Generate admin's blind signature

V4-2. Receive admin's blind signature

V5. Verify admin's blind signature

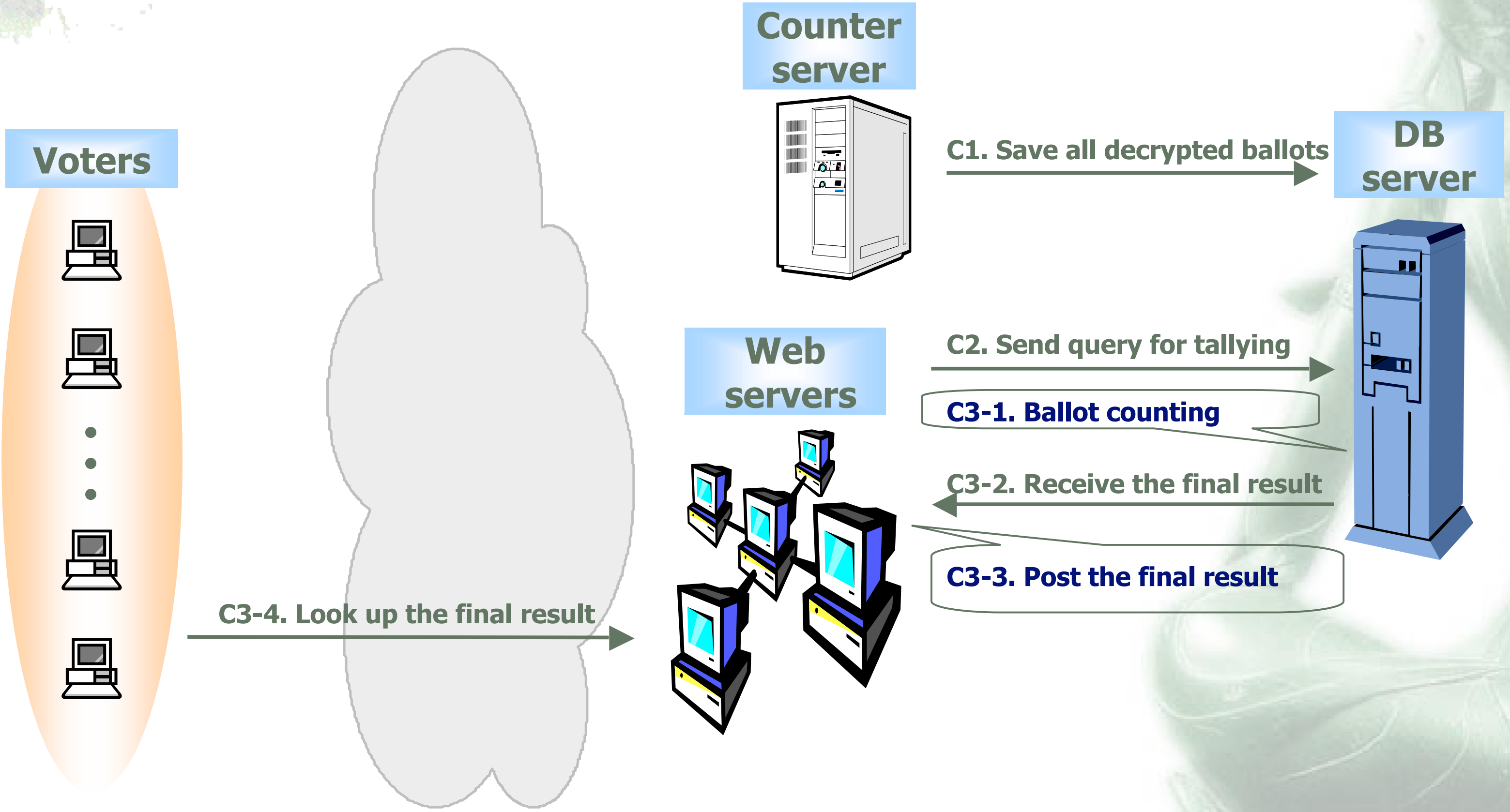
V6. Send encrypted ballot & admin's digital signature

V7-1. Verify admin's digital signature

V7-2. Decrypt the ballot using counter's private key

V8. Save all decrypted ballots

Counting Stage


Counter server
DB server
C1. Save all decrypted ballots
Voters
Web servers
C2. Send query for tallying
C3-1. Ballot counting
C3-2. Receive the final result
C3-3. Post the final result
C3-4. Look up the final result

Concluding Remarks

- 1st practice of *“cryptography is everywhere”* in the year 2002 not 2020 as T. Berson expected at Asiacrypt00.
- Enjoy e-voting without hacking
- Suggestions
  - Remote authentication of voters
  - Mobile voting
  - Shadow voting for IACR’s annual voting
- Web (http://mvp.worldcup2002.or.kr) Demonstration