KISTI Grid CA Status Report

APGrid PMA
Asia-Pacific Grid Policy Management Authority

2st APGrid PMA Meeting
Oct. 15. 2006
Osaka University Convention Center, Osaka, Japan

KISTI Supercomputing Center
Grid Technology Research Team
Sangwan Kim (sangwan@kisti.re.kr)

KISTI Korea Institute of Science and Technology Information

Supercomputing Center
Extending the Horizon of Science and Technology

Contents

- Introduction of KISTI Supercomputing Center
- KISTI Grid CA Operation
  - ▶History of KISTI Grid CA Operation
  - ▶KGridCA: KISTI Grid CA Software
- Staffs & Hardware
  - ▶Staffs
  - ▶Hardware
  - ▶Physical Accesses
  - ▶Events record and archival
- KISTI CA Audit Results
- Certificate Renewal
- Update Plans

Introduction

Introduction to KISTI

- KISTI - Korea Institute of Science and Technology Information
  - ▶ Korea Institute of Science and Technology Information(KISTI) is a research institute in Korea, which is located in the Daedeok Science Town, in Daejeon City.
  - ▶ KISTI's pivotal roles are establishing a national knowledge information infrastructure for science and technology in Korea. KISTI's major functions are:
    - - Knowledge Information Portal: collection, management, and diffusing system of science and technology information
    - - Value-added Information: in-depth analysis and feasibility study
    - - Knowledge Infrastructure: **Advancement of supercomputer and research network**.
      (→ Supercomputing & High-Performance Network)

http://www.kisti.re.kr

Korea

South Korea

Introduction to KISTI Supercomputing Center

- KISTI Supercomputing Center(KSC) is the largest public provider of supercomputing resources and high performance research network in Korea.
- The missions of KSC are to advance the national information infrastructure by providing leading-edge computational resources and networks to advance computational science and computational techniques, and to assist scientific communities and industry in exploiting the computational resources for the growth of their competitiveness worldwide.

KISTI Web Site http://www.ksc.re.kr

KISTI Grid CA Operation

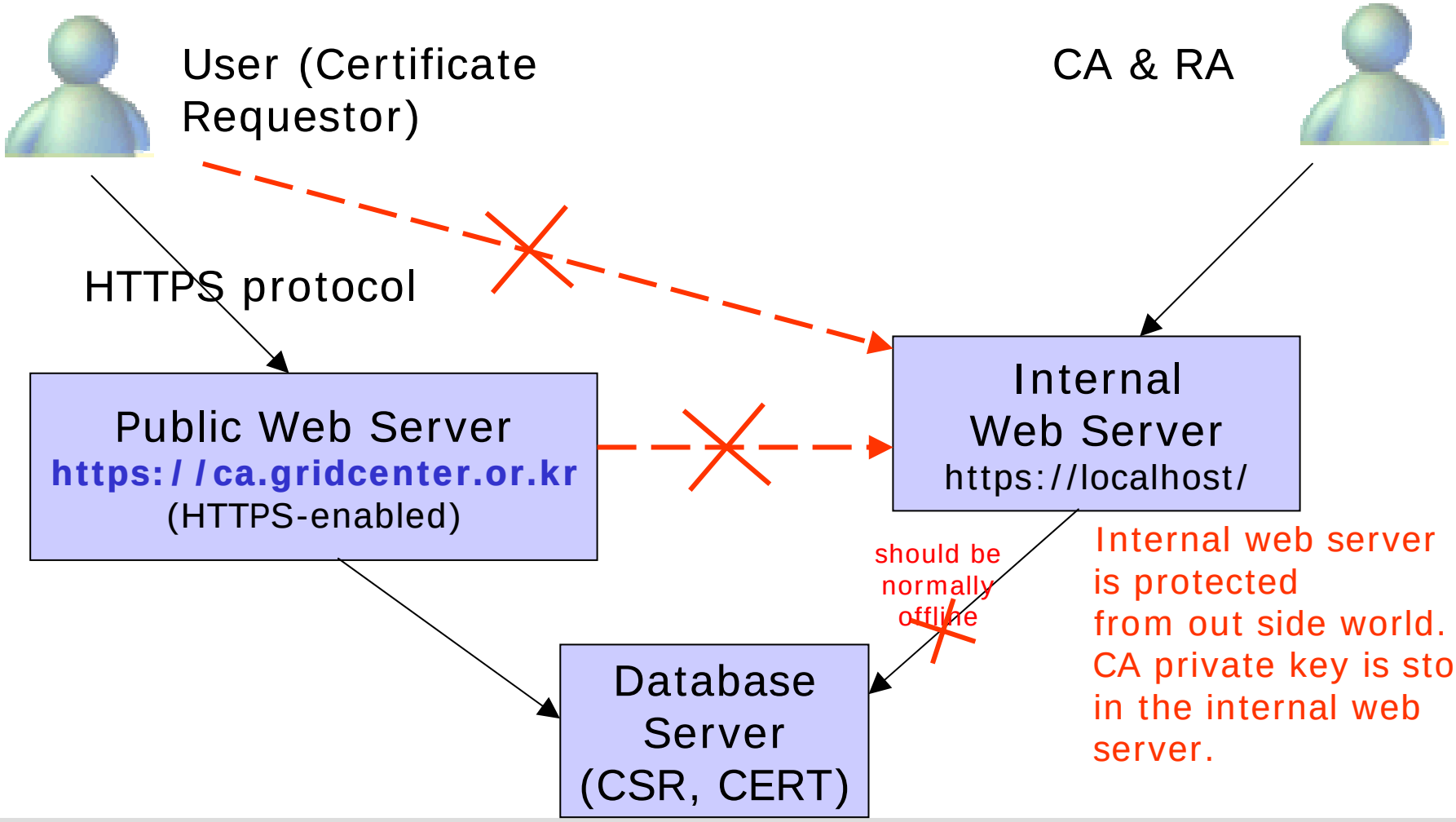
History of KISTI Grid CA Operation

- **K*Grid Project** started from 2002 in Korea.
- Experimental CA System (no operation anymore)
  - ▶Operation started from April, 2002
  - ▶Web-based System
  - ▶Statistics (by June 2004)
    - # of users (subscribers) : more than 390 users
    - # of issued certificates : more than 3000 certificates
- Production Level CA System
  - ▶Web-based System: http(s)://ca.gridcenter.or.kr/
  - ▶Service started from June, 2004
  - ▶Statistics (by Sep. 2006)
    - # of users (subscribers) : more than 50 users
    - # of issued certs : more than 340 certs.

KGridCA: KISTI Grid CA Software

- KGridCA
  - ▶Certificate Authority management system
  - ▶OpenSSL and Web-based system
    - openssl command line program front-end
  - ▶Features
    - Certificate management (CSR upload, Issuing Certs, revoking, etc)
    - Email notification (on an event of signing request, issuing certificate)
    - Certificate revocation & CRL generation
  - ▶Requirements
    - OpenSSL command line tool, MySQL, PHP-enabled Apache web server

KGridCA System Overview

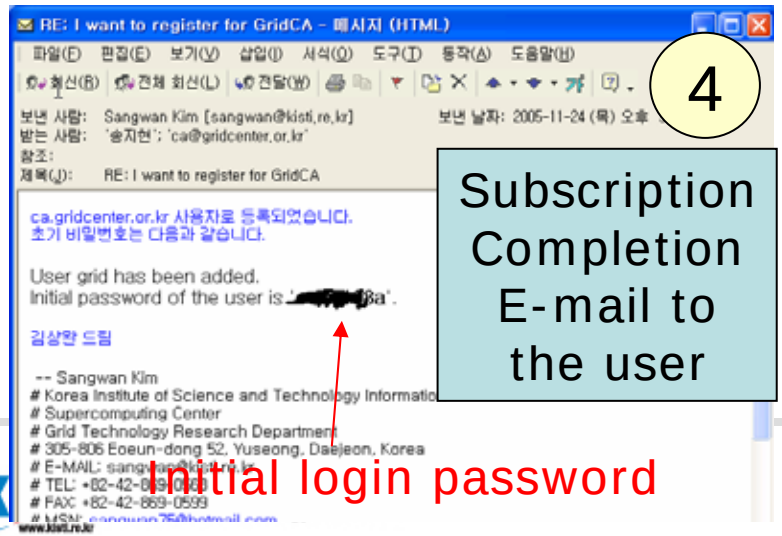


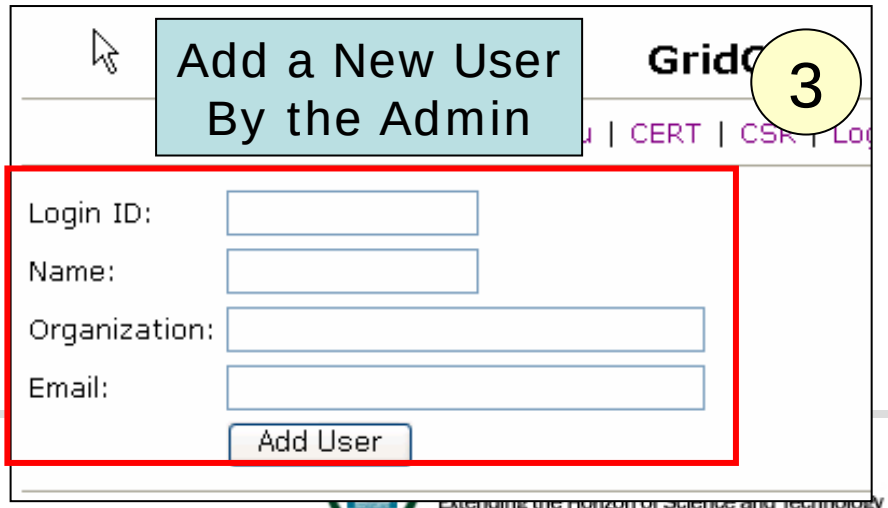
KGridCA System Overview

- User Registration
  - To subscribe as an user of KISTI CA, he/she should register as a user of a web site http://ca.gridcenter.or/
  - Subscribers should send an email to ca@gridcenter.or.kr with his/her
    - ▶ Name, E-mail, Login ID, Organization

KGridCA System Overview

- User Registration

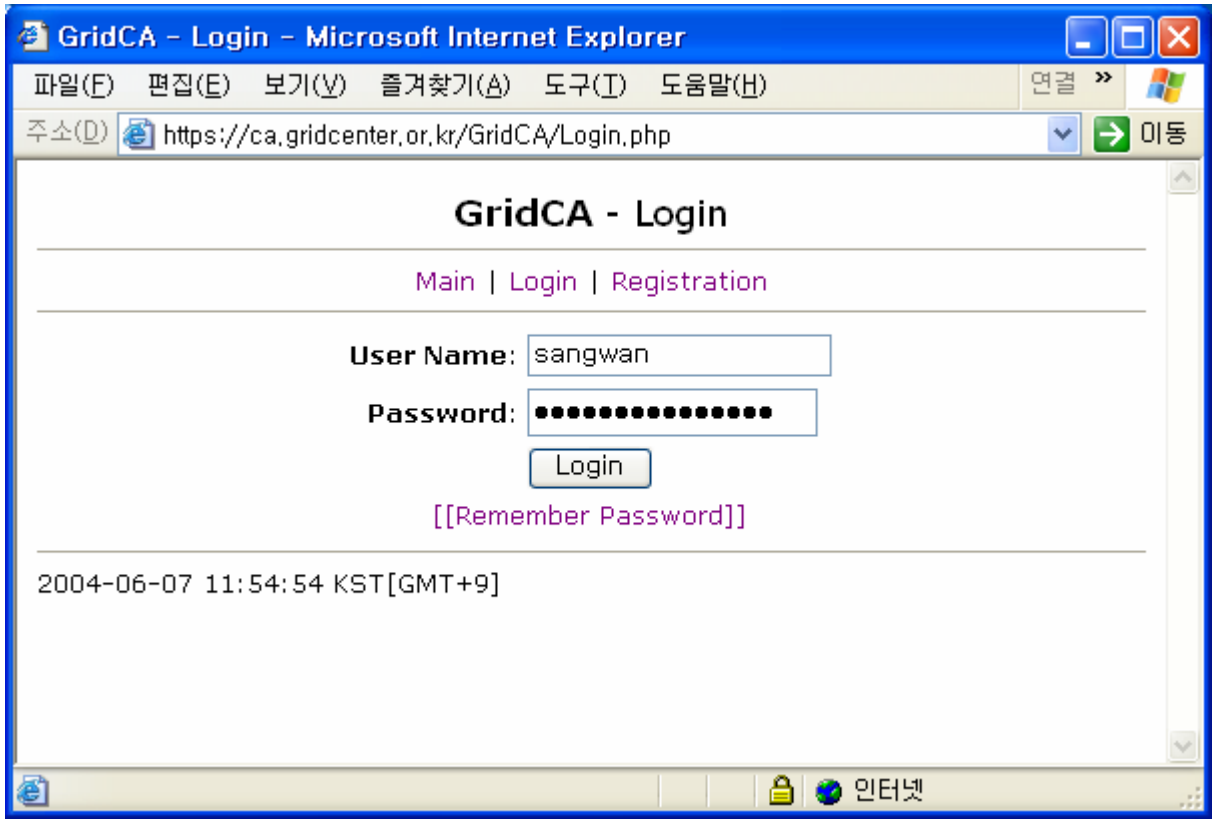




KGridCA System Overview

- Uploading CSR

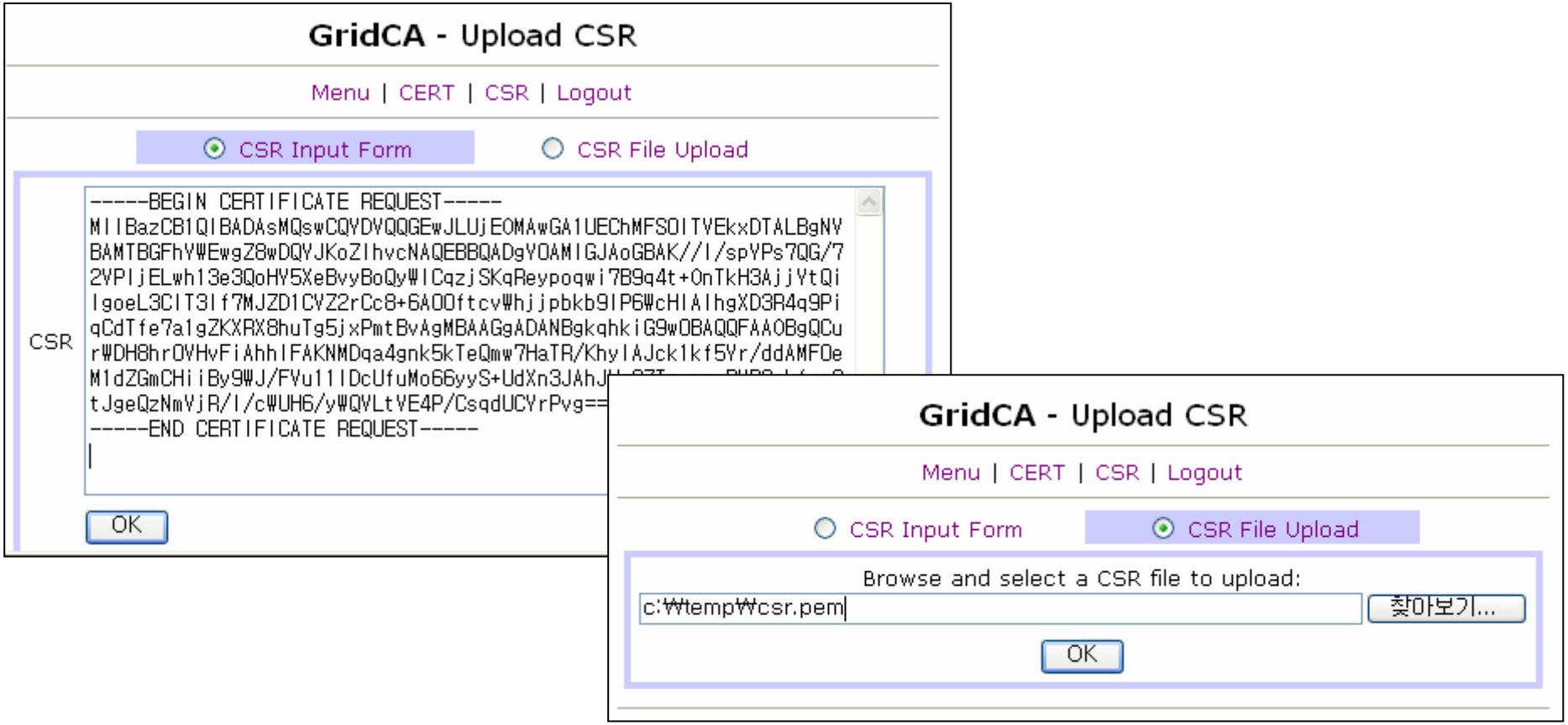
1. Login as the registered user.



KGridCA System Overview

- Uploading CSR

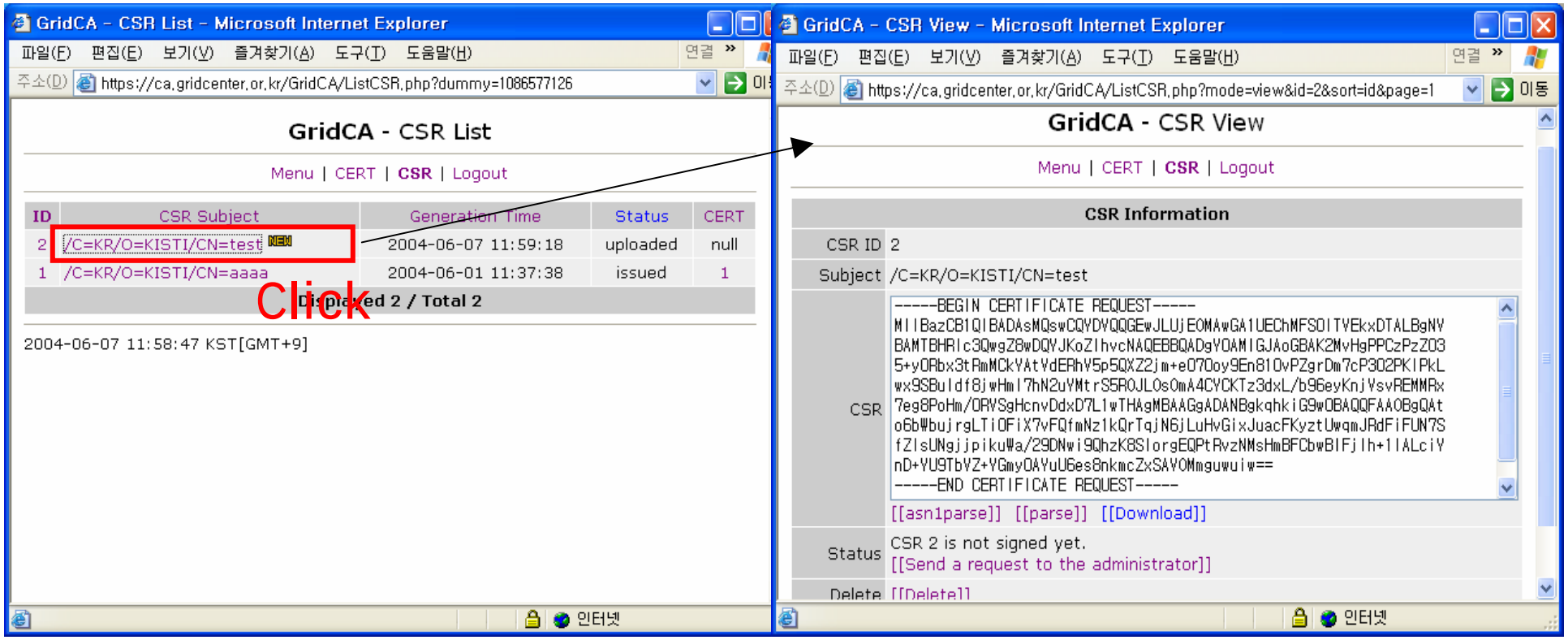
2. Upload CSR as a text block or a file



KGridCA System Overview

- Uploading CSR

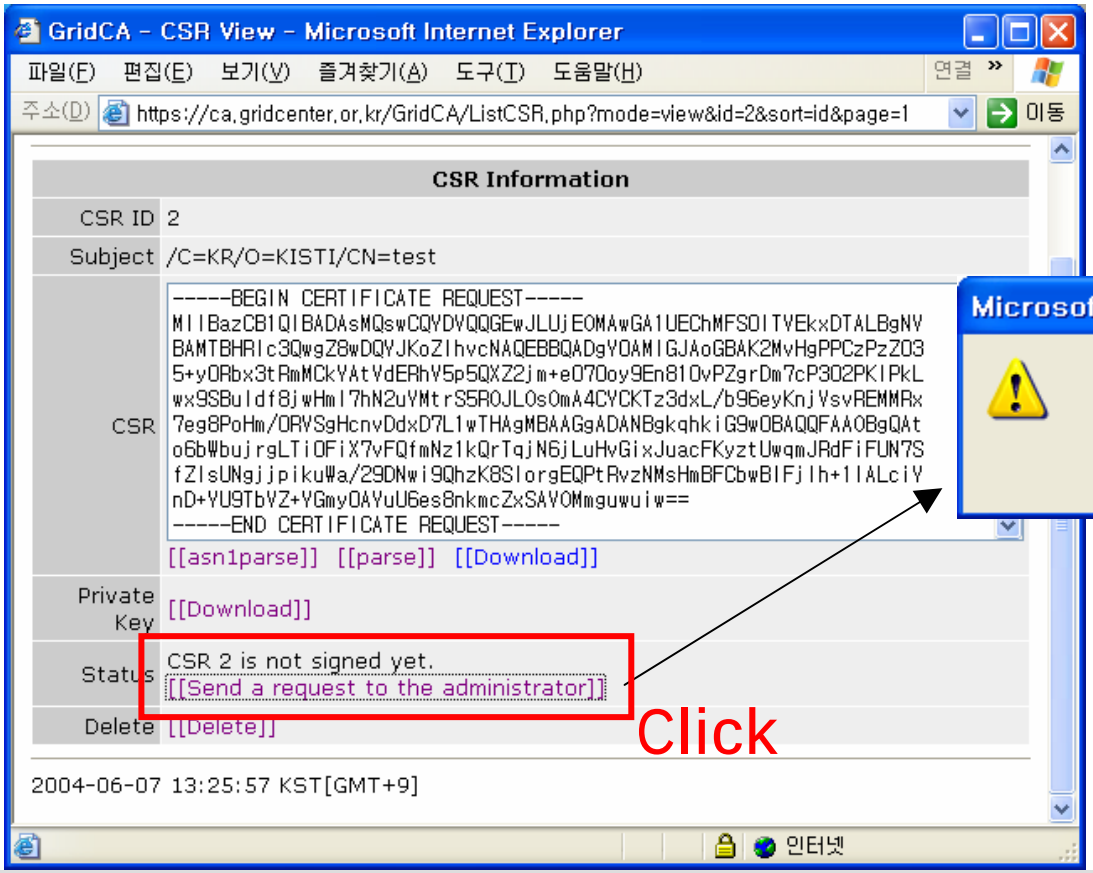
3. CSR list & information



KGridCA System Overview

- Uploading CSR

4. Request for signing certificate

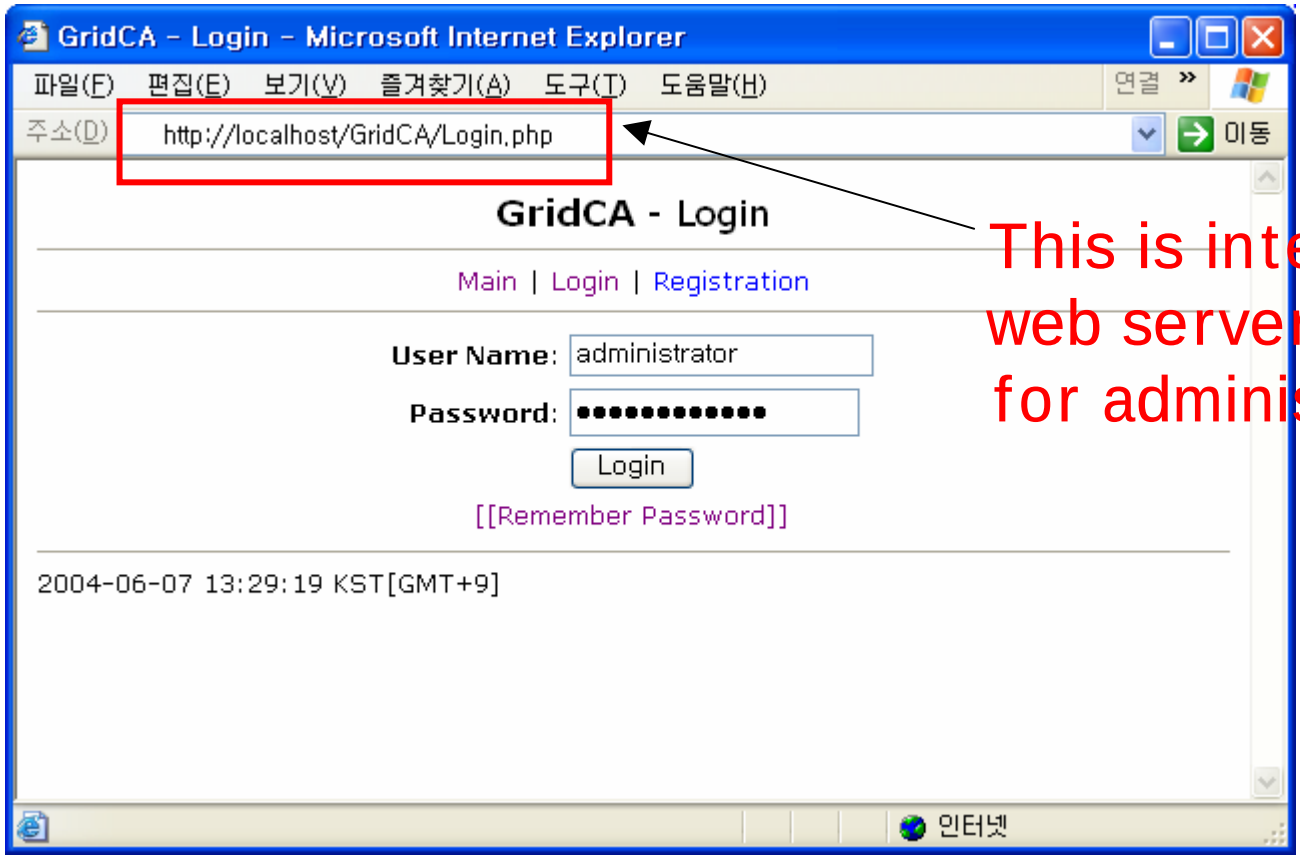


- Email Notification
(An email is sent
to the administrator)

KGridCA System Overview

- Signing Certificate (by the admin.)

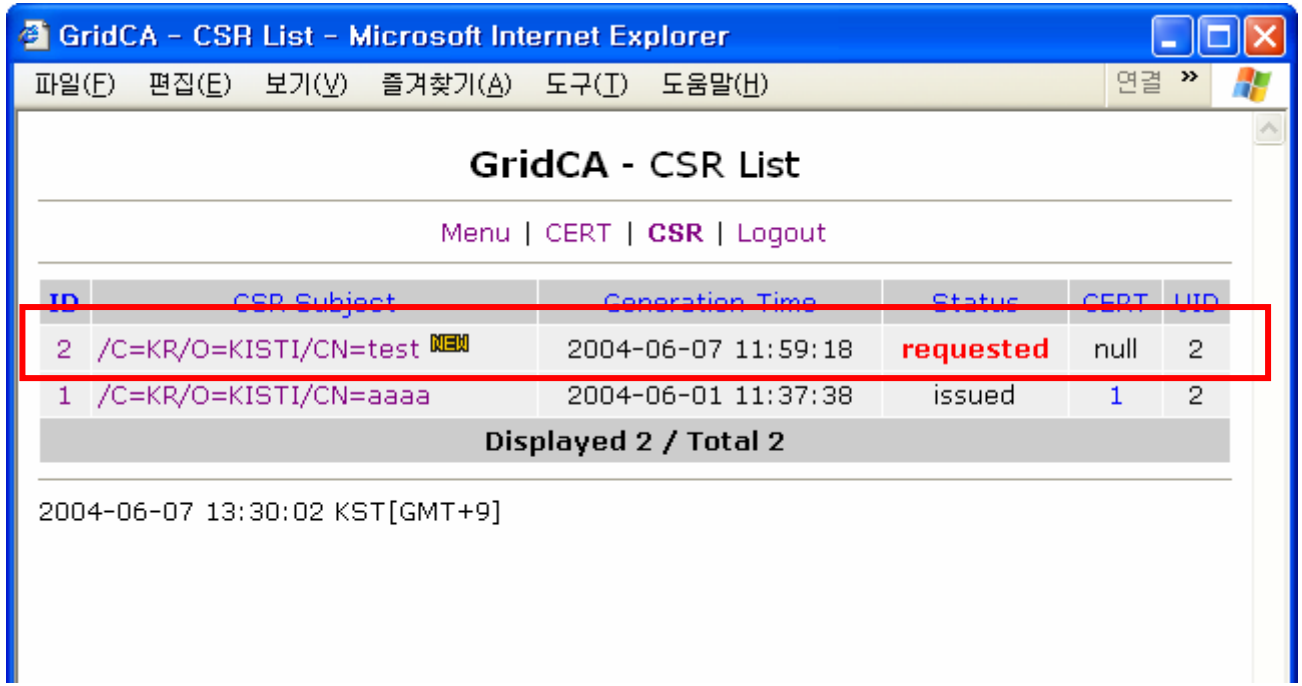
1. Login as the administrator



KGridCA System Overview

- Signing Certificate (by the admin.)

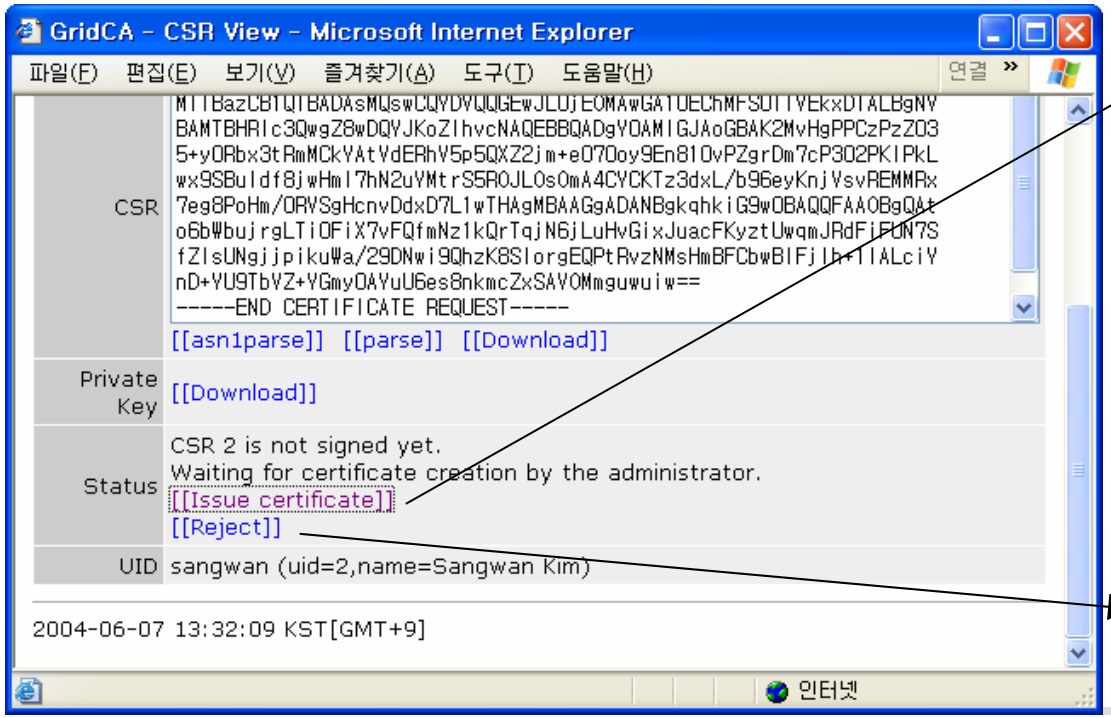
2. CSR list (CSRs requested by the requestor are highlighted)

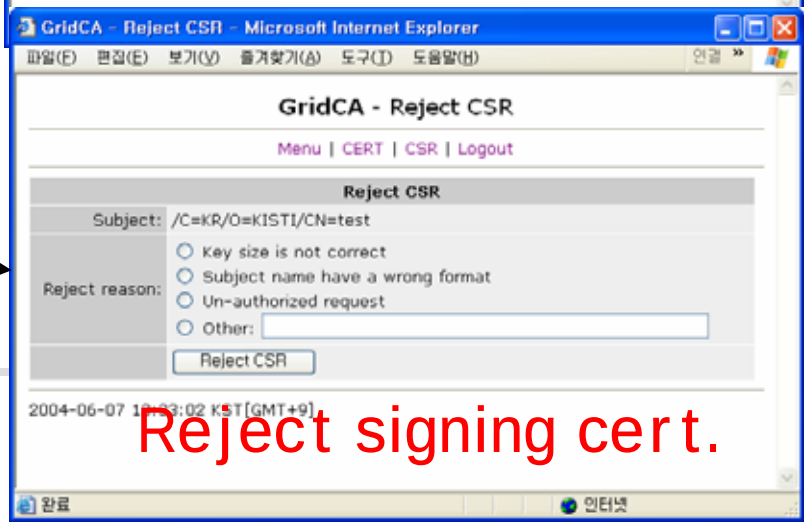


KGridCA System Overview

- Signing Certificate (by the admin.)

3. Issue a certificate or reject the CSR.
   Based on the CSR. CA operator should check the suitability





Korea Institute of Science and Technology Information

KGridCA System Overview

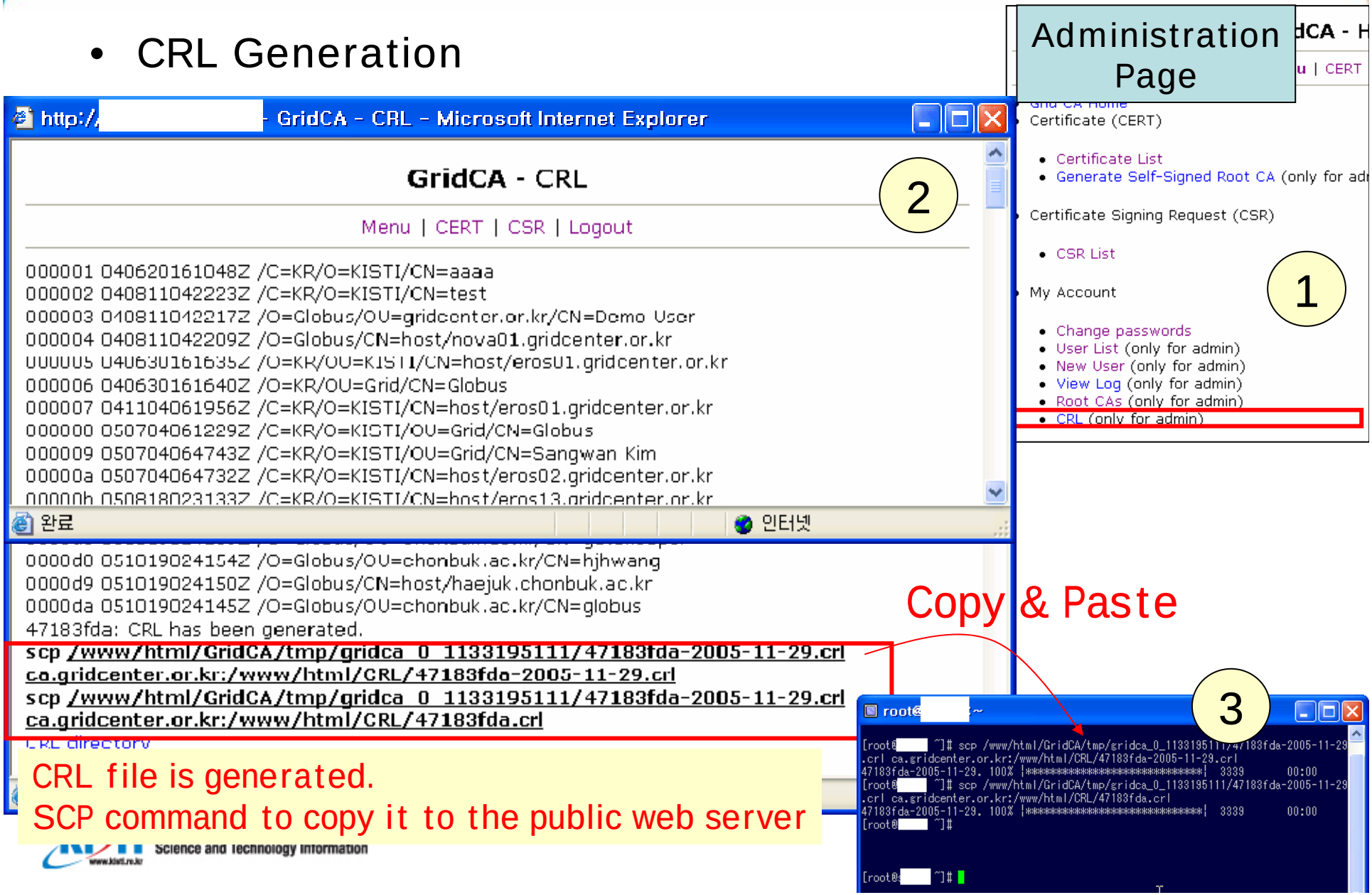
- Email Notifications
  - ▶A certificate signing request from the requestor is sent to the administrator email.
  - ▶If a certificate is signed(or rejected) by the admin, a notification email is sent to the requestor's email.
  - ▶If a certificate owner requests to revoke a certificate, a notification message is sent to the admin's email.

KGridCA System Overview

- Information Repository
  - ▶All CSR, Certificates, users' login information are stored in the database server, which priodically backed up to a safe place.
  - ▶CA private key is stored in the internal web server. Accesses to the internal web server are not allowed from Internet or the public web server.
  - ▶A CRL is issued at the internal web server and copyed to the public web server using SCP(SSH).

KGridCA System Overview

- CRL Generation

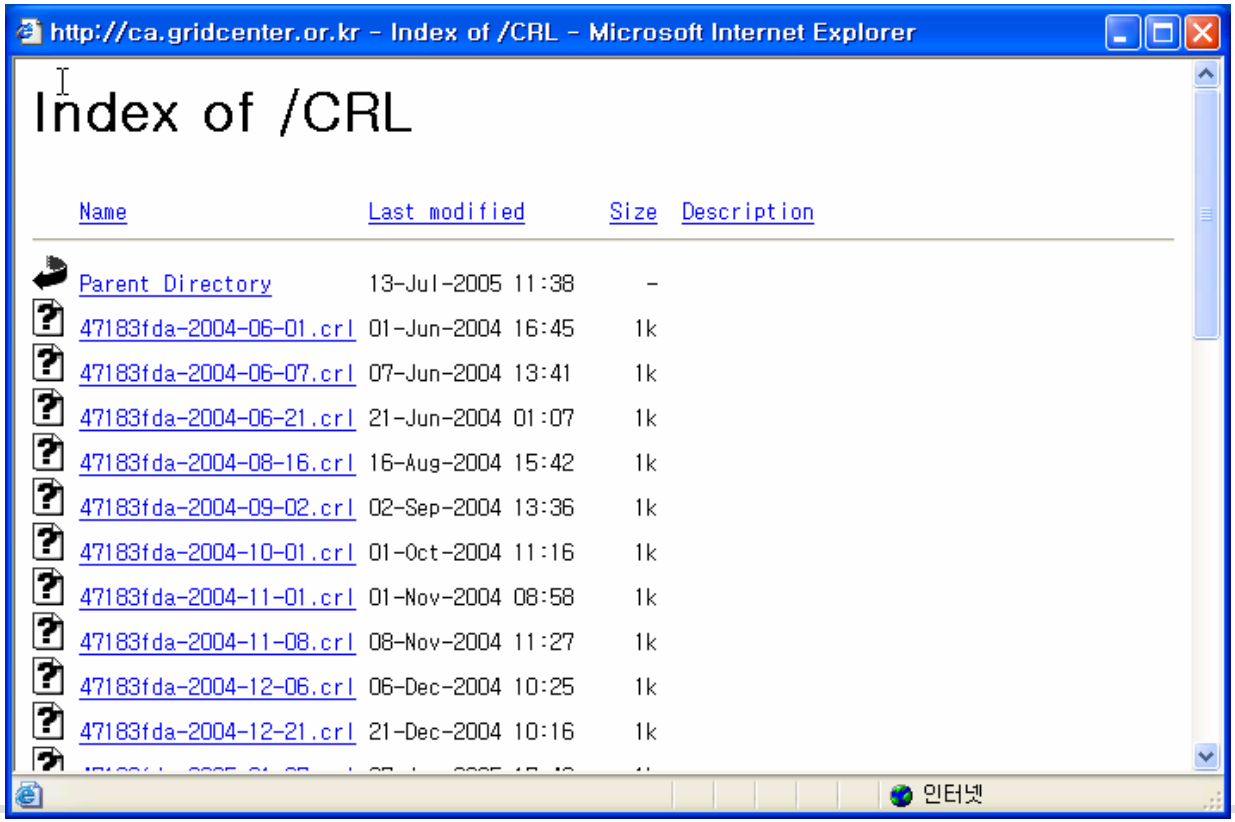


CRL file is generated.
SCP command to copy it to the public web server

Science and Technology Information

KGridCA System Overview

- CRL Distribution Point
  - ▶ History: http(s)://ca.gridcenter.or.kr/CRL/
  - ▶ Current: http(s)://ca.gridcenter.or.kr/CRL/47183fda.crl



Staffs & Hardware

Staffs

Grid Technology Research Team Members

Hardware

- ca.gridcenter.or.kr (public web server)
  - Intel Pentium4 1.6GHz, 512MB RAM
  - RedHat Linux 9
  - PHP4-enabled Apache web server 1.3.29
- Internal web server
  - AMD Athlon 2800+, 512MB RAM
  - RedHat Linux 9
- MySQL database server
  - The same machine as the public web server
- No HSM (Hardware Security Module) with KISTI Grid CA
  - We have a HSM equipment managed by other team in KISTI. We can share the equipment for KISTI CA.
  - But currently we have insufficient man power to set up it and we don't feel necessity of HSM equipment.

Physical Accesses

- ca.gridcenter.or.kr (public web server)
  - ▶Machine Room on the 1st floor in KISTI building, which is locked with a key
  - ▶Only accessible by some system admins. (4-5 staffs)
- Internal web server
  - ▶Office Room on 4th floor in KISTI building
  - ▶In my desktop which is accessible by any KISTI staffs
- MySQL database server
  - ▶The same machine as the public web server

Events record and archival

- User login, CSR uploading, certificate issuing, certificate revoking request, certificate revoking are logged in a database table by the KGridCA software.
- System log(login/logout/reboot etc) of the CA machine is not archived yet.

KISTI CA Audit

KISTI CA Audit by APGrid PMA

- Date of audit: Sep. 21, 2006, 10:00-13:00
- Auditor: Yoshio Tanaka (ApGrid PMA chair)
- Participants: Sangwan Kim
- Where?: KISTI Supercomputing Center, Korea (Yoshio Tanaka visited KISTI for auditing)
- How the audit performed?
  - ▶Interview
  - ▶Material check: KISTI CP/CPS documents
  - ▶Inspection: machine rooms at KISTI building

KISTI CA Audit Results

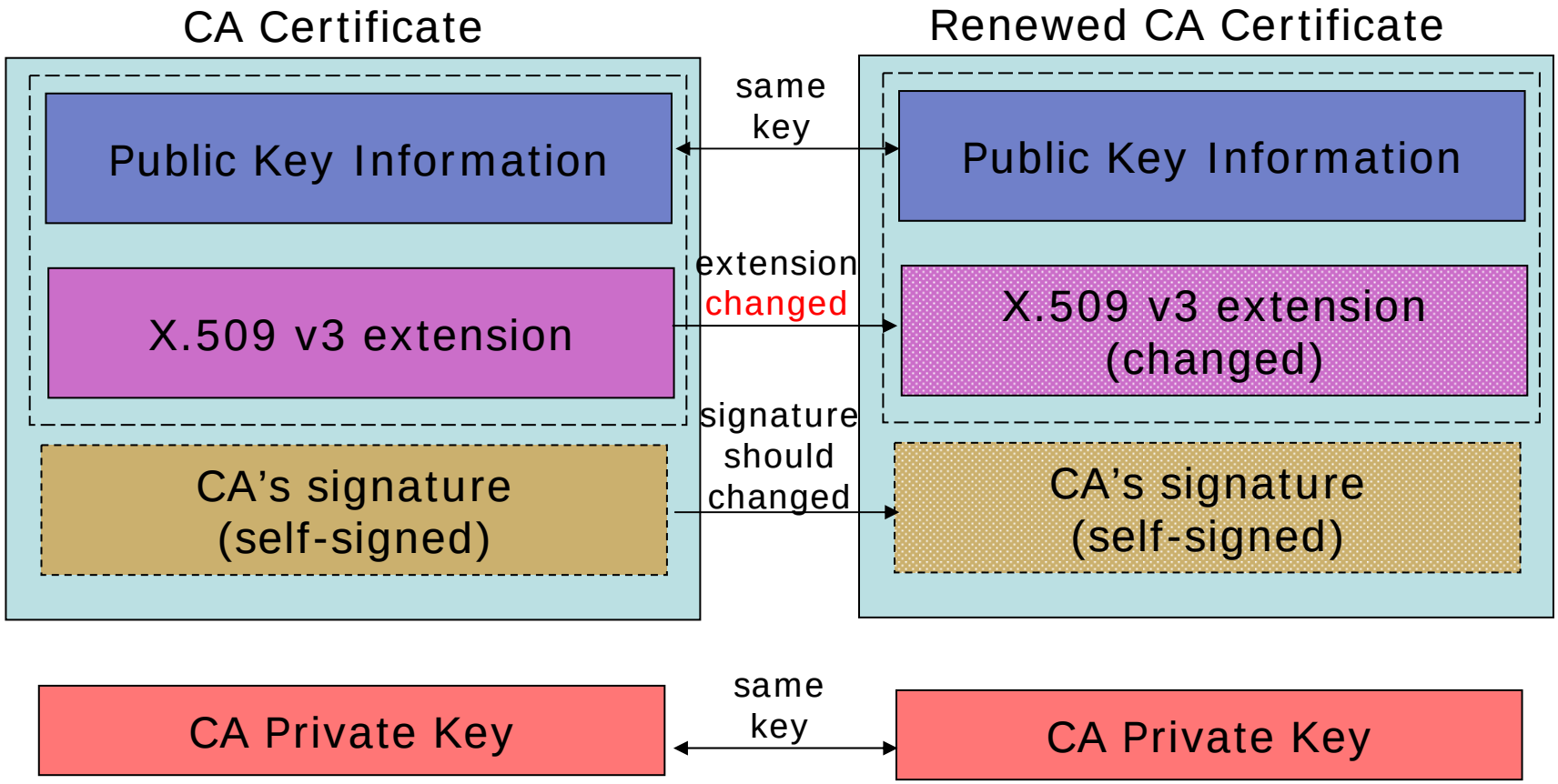
- Problems of KISTI CA
  - ▶X.509 v3 extension
    - Certificate Policies extension is missed in the CA cert.
    - basicConstraints, keyUsage is not marked as critical (for both CA and end entity cert)
  - ▶KISTI CA is being operated by only one staff (Sangwan Kim).
    - For backup, CA must be operated by multiple staffs
  - ▶CPS document should describe more details about
    - Operational audits (section 4.5)
    - CPS and CP change control procedures, publication and notification policies (section 8)
    - Procedure for CA private key backup and recovery should be described in the CPS (section 5.1 and 6.2)

KISTI CA Audit Results

- Problems of KISTI CA (cont.)
  - ▶Personal identification and authorization
    - Personal identification
      - ▶Currently, KISTI CA issues certificates to domestic grid research. We can not enforce too strong operational policy.
      - ▶Face-to-face meeting is nearly impossible in our case.
    - Multiple user certificates per one person
      - ▶A person can issue
    - Certificate requestor has the authority on host of host certificate he requested?
      - ▶How can you do that?
  - ▶System login/logout/reboot log should be archived
    - For general system security, system log should be kept more carefully.

Certificate Renewal

How to renewal CA certificate without changing the key of the CA?



Certificate Renewal

How to renewal CA certificate without changing the key of the CA?

- Generate a new certificate request renewal using the existing certificate and key pair as input:

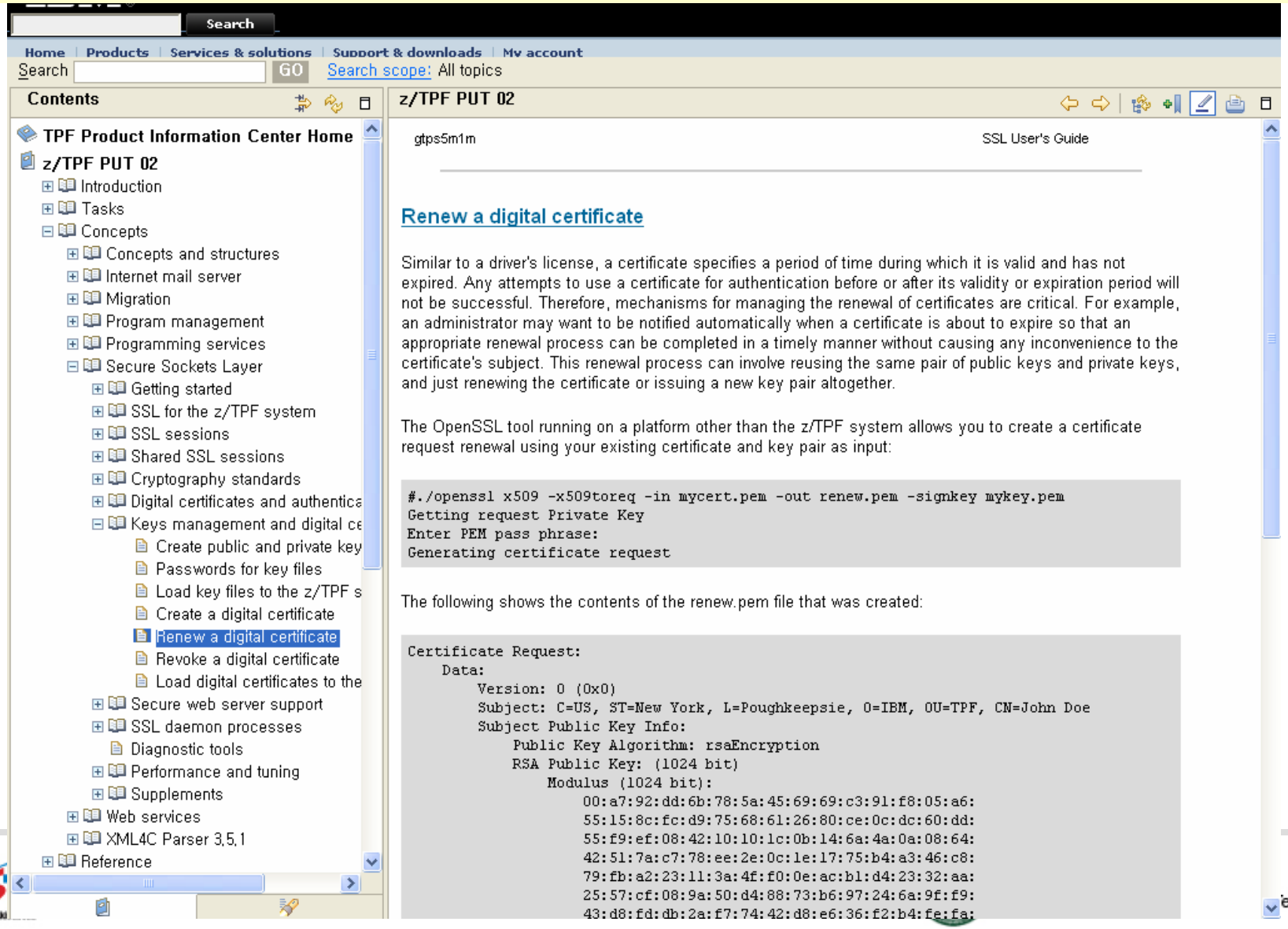
```
openssl x509 -x509toreq -in cacert.crt -signkey cakey.key \
  -out renew.pem
```

- Sign the renewal certificate request to generate a new CA certificate:

```
openssl x509 \
  -extfile  openssl.cnf \
  -extensions  v3_ca \
  -CA cacert.crt -CAkey cakey.key \
  -set_serial 0 -days 365 \
  -req -in renew.pem -out newcacert.pem
```

Certificate Renewal (FYI)

http://publib.boulder.ibm.com/infocenter/tpfhelp/current/index.jsp?topic=/com.ibm.ztpf.doc_put.02/gtps5/gtps5m1m.htm



X509 Extension

How to add X509 v3 extension to a certificate?

- In the OpenSSL configuration file, edit the extension section for adding additional x509 extensions:

```
[ v3_ca ]
basicConstraints = critical,CA:TRUE
keyUsage = critical,keyCertSign,cRLSign
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
crlDistributionPoints=URI:http://ca.gridcenter.or.kr/CRL/
subjectAltName=email:ca@gridcenter.or.kr, URI:http://ca.gridcenter.or.kr/
issuerAltName=email:ca@gridcenter.or.kr, URI:http://ca.gridcenter.or.kr/
certificatePolicies=1.3.6.1.4.1.14305.1.1.1.1.3
```

Update Plans

- Update the CA certificate.
  - ▶to be approved by APGrid PMA members
- Change CP/CPS document
  - ▶ to be approved by APGrid PMA members
- Enhance the system security
- Multiple-person operation
- Backup and archiving

Thank You