

# KISTI Grid CA Status Report



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)

# 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/](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

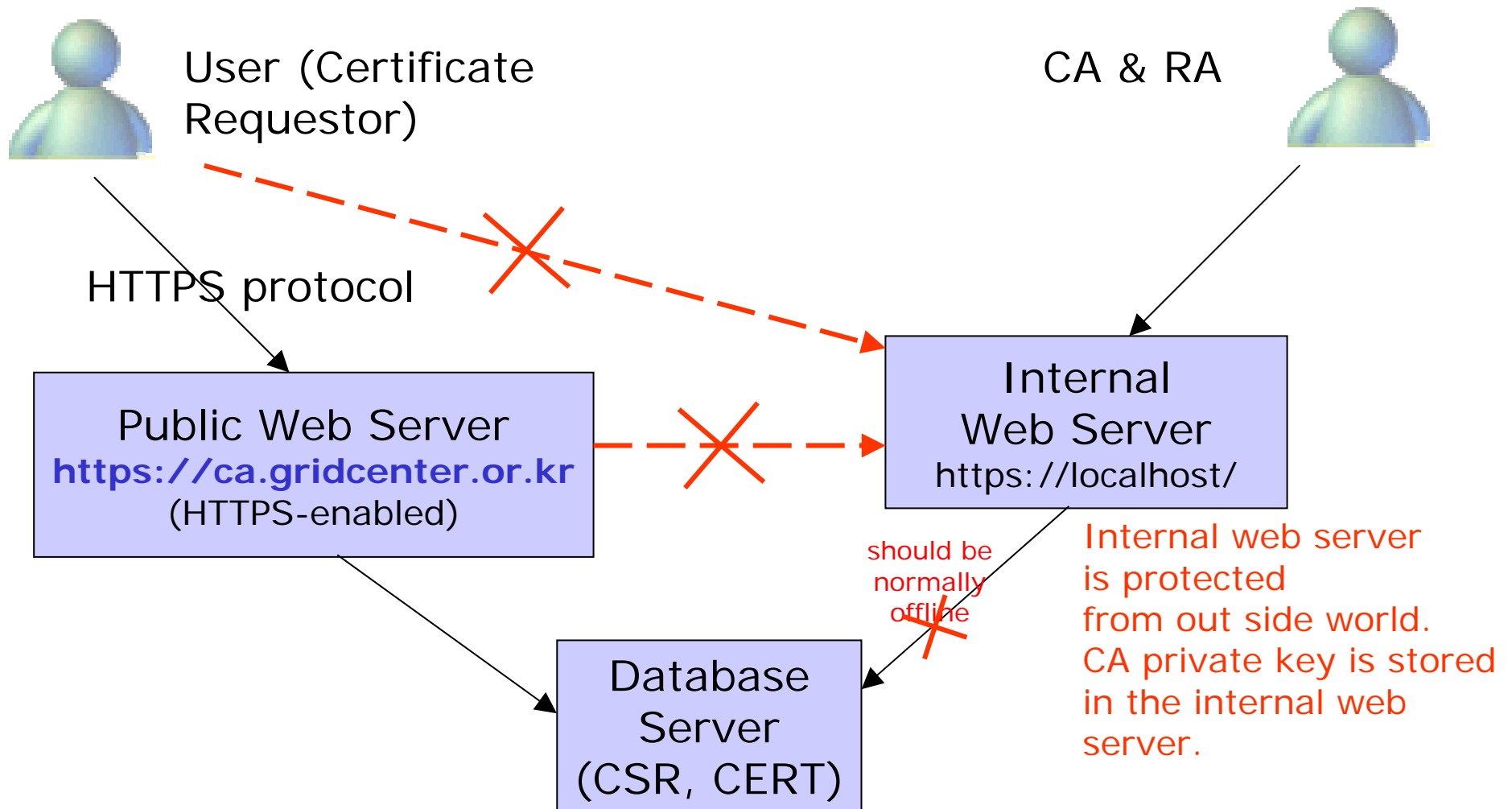
Features

- 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.kr/>
- Subscribers should send an email to [ca@gridcenter.or.kr](mailto:ca@gridcenter.or.kr) with his/her

Name, E-mail, Login ID, Organization



The screenshot shows a web browser window titled "https://ca.gridcenter.or.kr - GridCA - Register - Microsoft Internet Expl...". The page content includes a navigation menu with "Main", "Login", and "Registration" links. A message instructs users to read the CP/CPS document before registration and provides a link to "KISTI-GRID-CA-CP-CPS.pdf". It then asks for an email to be sent to "ca@gridcenter.or.kr" and lists the required information: Name, E-mail address, Login ID (2-20 characters), and Organization. A note at the bottom states: "\* If you are Korean, fill your information in Korean except login ID and e-mail address."

# KGridCA System Overview

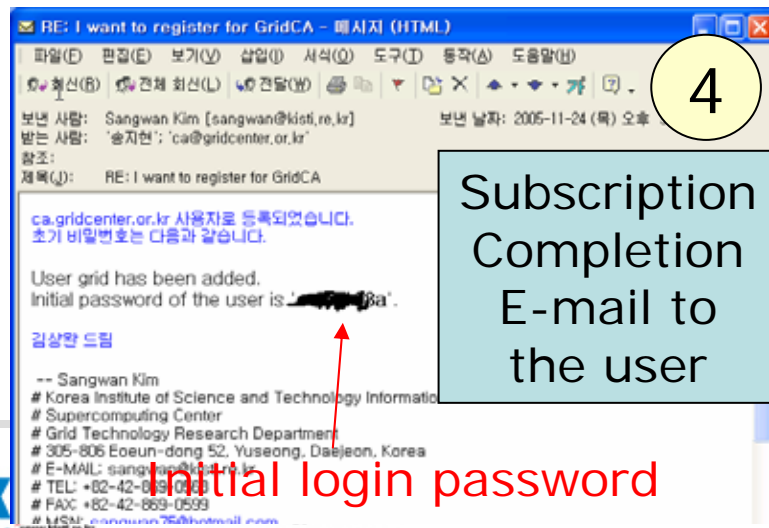
## • User Registration



Subscription Request E-mail

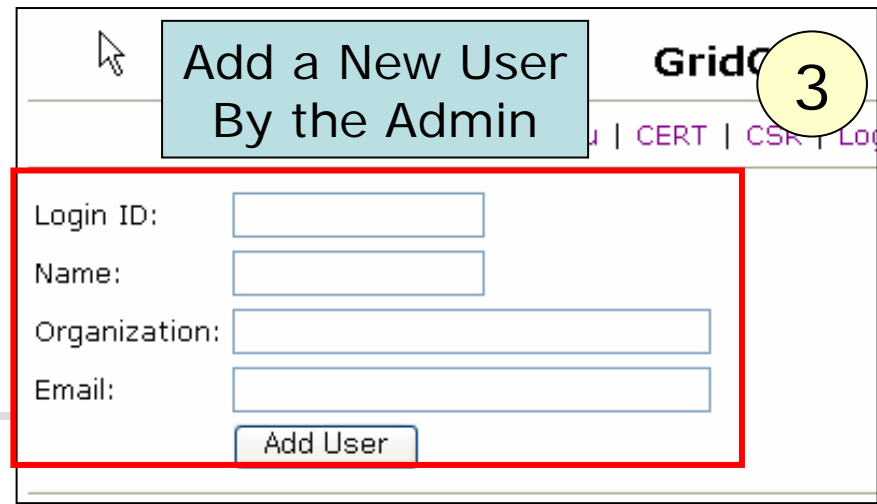


Administration Page



Subscription Completion E-mail to the user

Initial login password





# KGridCA System Overview

- Uploading CSR

1. Login as the registered user.

GridCA - Login - Microsoft Internet Explorer

주소(D) <https://ca.gridcenter.or.kr/GridCA/Login.php>

## GridCA - Login

[Main](#) | [Login](#) | [Registration](#)

User Name:

Password:

[\[\[Remember Password\]\]](#)

2004-06-07 11:54:54 KST[GMT+9]

# KGridCA System Overview

- Uploading CSR

## 2. Upload CSR as a text block or a file

The screenshot displays the 'GridCA - Upload CSR' web interface. At the top, there are navigation links: 'Menu | CERT | CSR | Logout'. Below this, two radio buttons allow selection between 'CSR Input Form' (selected) and 'CSR File Upload'. The 'CSR Input Form' view shows a text area containing a CSR request, starting with '-----BEGIN CERTIFICATE REQUEST-----' and ending with '-----END CERTIFICATE REQUEST-----'. An 'OK' button is located at the bottom left of the text area. The 'CSR File Upload' view shows a file selection dialog with the text 'Browse and select a CSR file to upload:'. The file path 'c:\temp\csr.pem' is entered in the text box, and a '찾아보기...' (Find) button is to its right. An 'OK' button is at the bottom center of the dialog.

# KGridCA System Overview

- Uploading CSR

## 3. CSR list & information

The image shows two side-by-side browser windows from Microsoft Internet Explorer. The left window, titled 'GridCA - CSR List', displays a table of CSR entries. The right window, titled 'GridCA - CSR View', shows the detailed information for a specific CSR entry.

**GridCA - CSR List**

ID	CSR Subject	Generation Time	Status	CERT
2	/C=KR/O=KISTI/CN=test <small>NEW</small>	2004-06-07 11:59:18	uploaded	null
1	/C=KR/O=KISTI/CN=aaaa	2004-06-01 11:37:38	issued	1

Displayed 2 / Total 2

2004-06-07 11:58:47 KST[GMT+9]

**GridCA - CSR View**

CSR Information

CSR ID 2

Subject /C=KR/O=KISTI/CN=test

CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBazCB1QIBADAsMQswCQYDVQQGEwJLUjEOMAwGA1UEChMFSDI1VEkxDTALBgNV
BAMTBHRlc3QwZ8wDQYJKoZIhvcNAQEBBQADgYODAMIGJAoGBAK2MvHgPPCzPzZ03
5+yORbx3tRmMCKvAtVdERhV5p5QXZ2jm+e070oy9En810vPZgrDm7cP302PK1PkL
wx9SBuld8jwHm17hN2uVMtrS5ROJL0sOmA4CYCKTz3dxL/b96eyKnjYsvREMMRx
7eg8PoHm/DRV5gHcnvDdxD7L1wTHAgMBAAGgADANBgkqhkiG9w0BAQFAA0BgQAT
o6BbWbujrgLTiOFiX7vFQfmNz1kQrTqjN6jLuHvGiXJuacFKyztUwqmJRdFiFUN7S
fZIsUNgjjpikuWa/29DNwi9QhzK8S1orgEQPtRvzNMShmBFCbwBIFj1h+11ALciY
nD+YU9TbVZ+VGmyOAYuUGes8nkmcZxSAVOMnguwuiw==
-----END CERTIFICATE REQUEST-----
```

[[asn1parse]] [[parse]] [[Download]]

Status CSR 2 is not signed yet.  
[[Send a request to the administrator]]

Delete [[Delete]]

**Click**

# KGridCA System Overview

- Uploading CSR

## 4. Request for signing certificate

GridCA - CSR View - Microsoft Internet Explorer

주소(D) https://ca.gridcenter.or.kr/GridCA/ListCSR.php?mode=view&id=2&sort=id&page=1

**CSR Information**

CSR ID	2
Subject	/C=KR/O=KISTI/CN=test
CSR	-----BEGIN CERTIFICATE REQUEST----- MII BAZCB1QIBADA sMqswCQYDVQQGEwJLUjEOMAwGA1UEChMFSOITVEKxDTALBgNV BAMTBHRlc3QwZ8wDQVJKoZl hvCNAQEBAQAgYDAMIGJAoGBAK2MvHgPPCzPzZ03 5+yORbx3tRmMCKYA tVdERhV5p5QXZ2j m+e070oy9En810vPZgrDm7cP3D2PK1PkL wx9SBu ldf8j wHm l7hN2uYMt rS5ROJL0s0mAA4CYCKTz3dxL/b96eyKnj VsvREMMRx 7eg8PoHm/ORV SgHcnvDdxD7L1wTHAgMBAAGgADANBgkqhki G9wOBAQQFAA0BgQAt o6bWbu jrgLT iOFi X7vFQfmNz1kQrTqj N6j LuHvGi xJuacFKyztUwqmJRdFi FUN7S fZl sUNgjj pikuW a/29DNw i9QhzKBSI orgEQPt RvzNM sHmBFCbwBIFj lh+ lIALci Y nD+YU9TbVZ+YGmyDAYuU6es8nkm cZxSAVOMmguwui w== -----END CERTIFICATE REQUEST----- [[asn1parse]] [[parse]] [[Download]]
Private Key	[[Download]]
Status	CSR 2 is not signed yet. [[Send a request to the administrator]]
Delete	[[Delete]]

2004-06-07 13:25:57 KST[GMT+9]

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

Microsoft Internet Explorer

An email requesting to sign this CSR has been sent to admin

확인

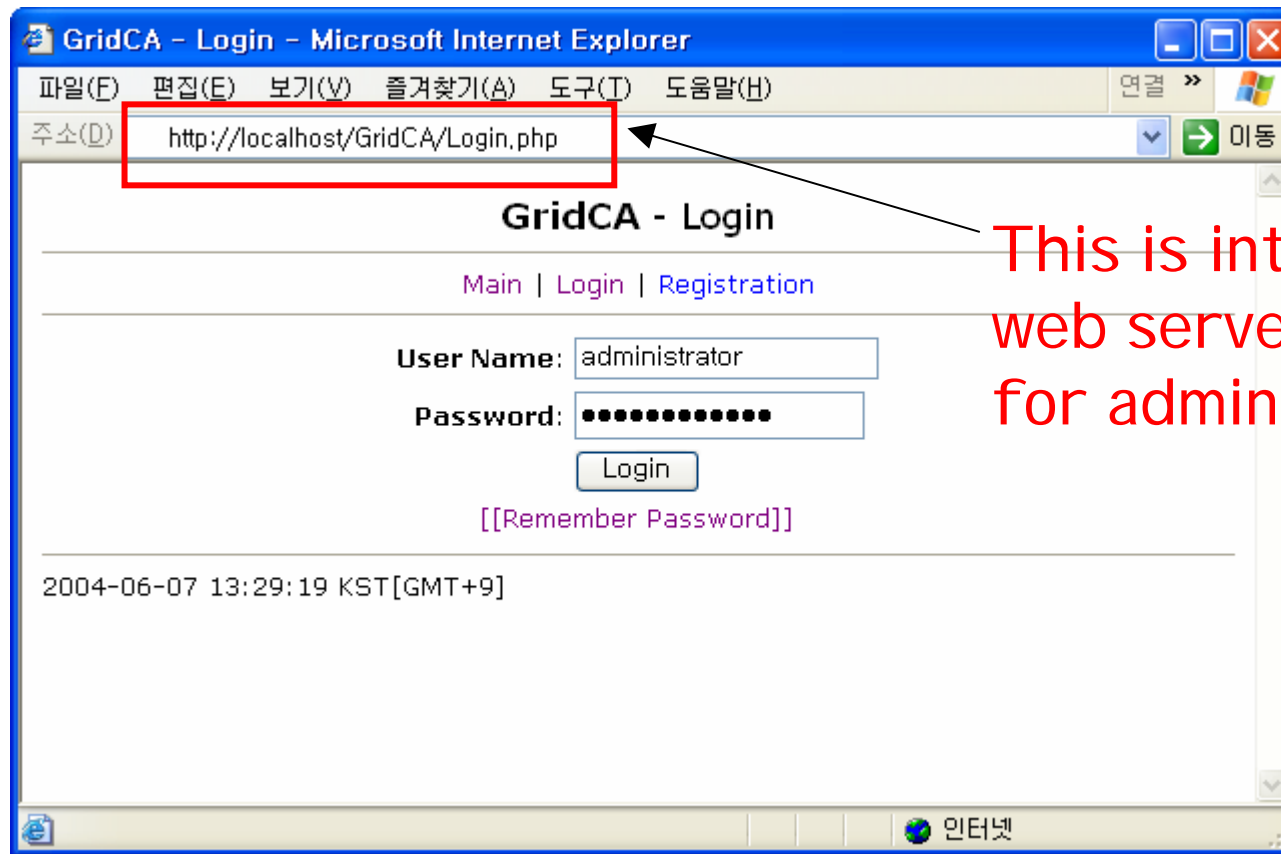
Click



# KGridCA System Overview

- Signing Certificate (by the admin.)

## 1. Login as the administrator



This is internal  
web server  
for administration

# KGridCA System Overview

- Signing Certificate (by the admin.)

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

ID	CSR Subject	Generation Time	Status	CERT	UID
2	/C=KR/O=KISTI/CN=test <b>NEW</b>	2004-06-07 11:59:18	<b>requested</b>	null	2
1	/C=KR/O=KISTI/CN=aaaa	2004-06-01 11:37:38	issued	1	2

Displayed 2 / Total 2

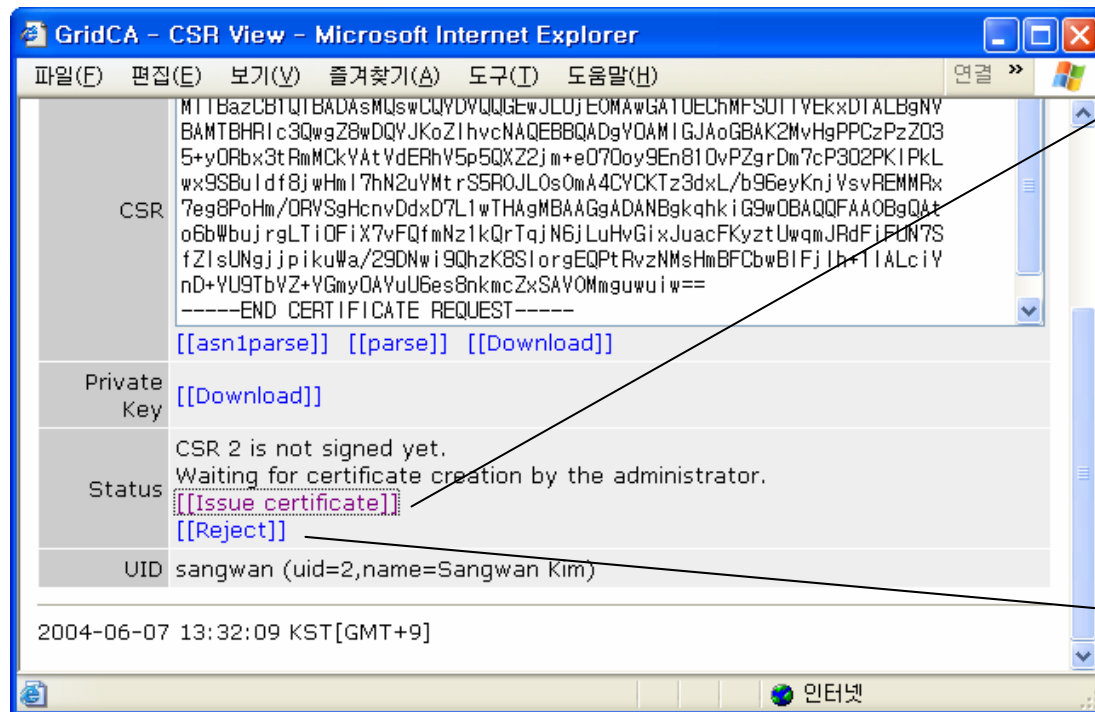
2004-06-07 13:30:02 KST[GMT+9]

# KGridCA System Overview

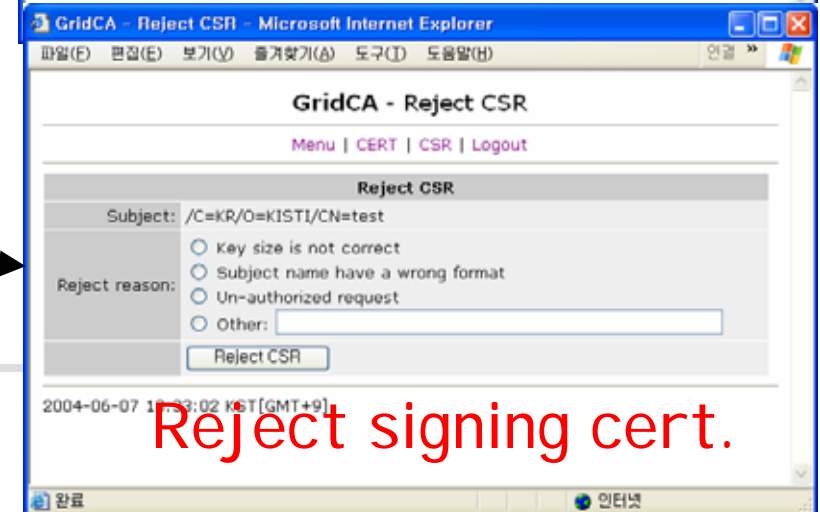
- Signing Certificate (by the admin.)

3. Issue a certificate or reject the CSR.

Based on the CSR. CA operator should check the suitability



Issue a certificate



Reject signing cert.

# 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 periodically 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 copied to the public web server using SCP(SSH).

# KGridCA System Overview

- CRL Generation

The image shows a screenshot of the KGridCA Administration Page and a terminal window. The Administration Page (labeled '1') has a sidebar menu with 'CRL (only for admin)' highlighted in red. The main content area (labeled '2') displays a list of certificates and a message: '47183fda: CRL has been generated.' Below this, two SCP commands are shown, which are highlighted in red and labeled 'Copy & Paste'. A terminal window (labeled '3') shows these commands being executed successfully.

**Administration Page**

- Certificate List
- Generate Self-Signed Root CA (only for admin)
- Certificate Signing Request (CSR)
- CSR List
- My Account
- Change passwords
- User List (only for admin)
- New User (only for admin)
- View Log (only for admin)
- Root CAs (only for admin)
- **CRL (only for admin)**

**GridCA - CRL**

Menu | CERT | CSR | Logout

```
000001 040620161048Z /C=KR/O=KISTI/CN=aaaa
000002 040811042223Z /C=KR/O=KISTI/CN=test
000003 010811042217Z /O=Globus/OU=gridcenter.or.kr/CN=Demo User
000004 040811042209Z /O=Globus/CN=host/nova01.gridcenter.or.kr
UUUUU5 U4U63U161635Z /O=KR/OU=KISTI/CN=host/erosU1.gridcenter.or.kr
000006 040630161640Z /O=KR/OU=Grid/CN=Globus
000007 041104061956Z /C=KR/O=KISTI/CN=host/eros01.gridcenter.or.kr
000008 050704061229Z /C=KR/O=KISTI/OU=Grid/CN=Globus
000009 050704064743Z /C=KR/O=KISTI/OU=Grid/CN=Sangwan Kim
00000a 050704064732Z /C=KR/O=KISTI/CN=host/eros02.gridcenter.or.kr
00000b 050818023133Z /C=KR/O=KISTI/CN=host/eros13.gridcenter.or.kr
```

47183fda: CRL has been generated.

**Copy & Paste**

```
scp /www/html/GridCA/tmp/gridca_0_1133195111/47183fda-2005-11-29.crl
ca.gridcenter.or.kr:/www/html/CRL/47183fda-2005-11-29.crl
scp /www/html/GridCA/tmp/gridca_0_1133195111/47183fda-2005-11-29.crl
ca.gridcenter.or.kr:/www/html/CRL/47183fda.crl
```

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

**Terminal:**

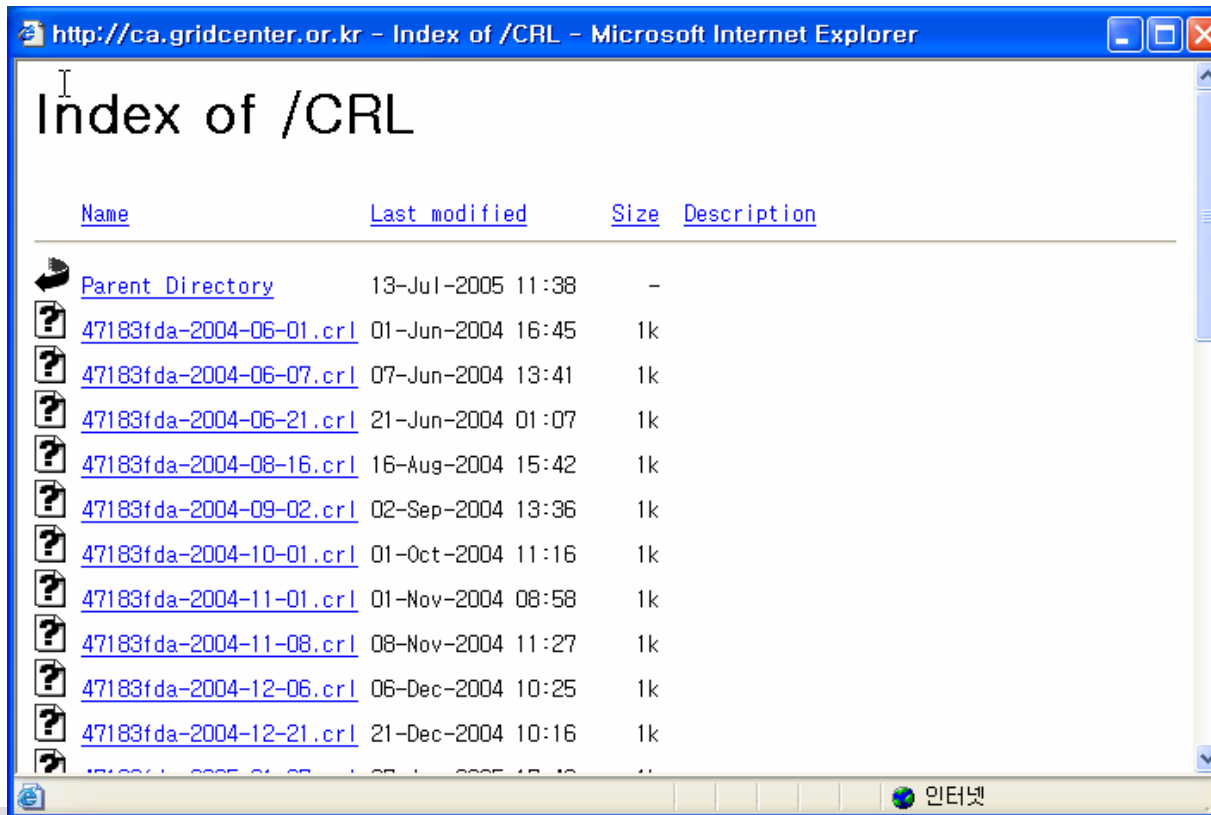
```
root@ [root@ ~]# scp /www/html/GridCA/tmp/gridca_0_1133195111/47183fda-2005-11-29.crl
ca.gridcenter.or.kr:/www/html/CRL/47183fda-2005-11-29.crl
47183fda-2005-11-29. 100% |*****| 3339 00:00
[root@ ~]# scp /www/html/GridCA/tmp/gridca_0_1133195111/47183fda-2005-11-29.crl
ca.gridcenter.or.kr:/www/html/CRL/47183fda.crl
47183fda-2005-11-29. 100% |*****| 3339 00:00
[root@ ~]#
```

# KGridCA System Overview

- CRL Distribution Point

History: [http\(s\)://ca.gridcenter.or.kr/CRL/](http(s)://ca.gridcenter.or.kr/CRL/)

Current: [http\(s\)://ca.gridcenter.or.kr/CRL/47183fda.crl](http(s)://ca.gridcenter.or.kr/CRL/47183fda.crl)





# Staffs & Hardware

# Staffs

Sangwan Kim

Jae-Hyuck Kwak



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 1<sup>st</sup> 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 4<sup>th</sup> 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?

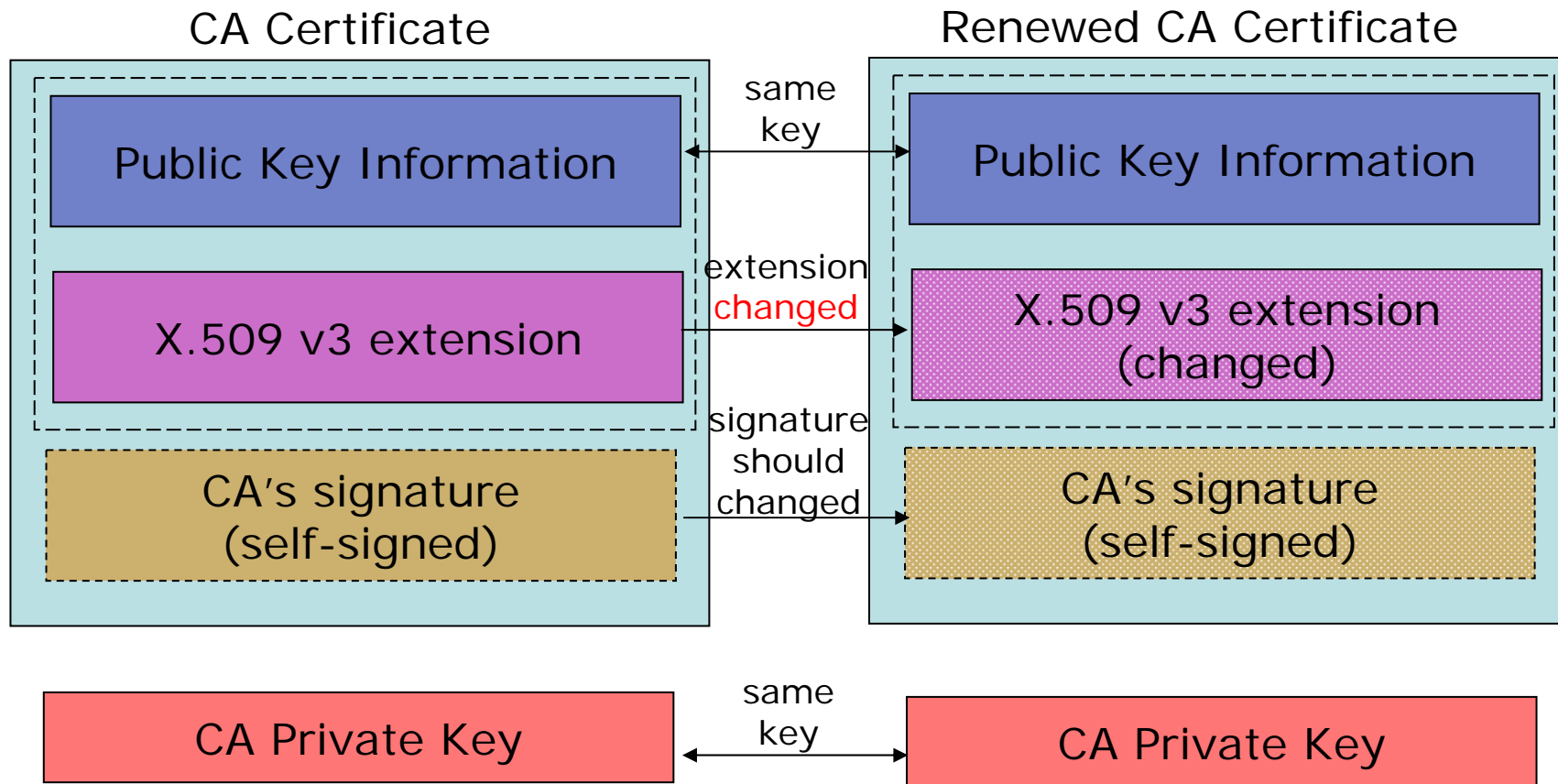
How can you do that?

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

The screenshot shows a web browser displaying the IBM z/TPF PUT 02 SSL User's Guide. The page title is "z/TPF PUT 02" and the sub-page is "SSL User's Guide". The main content area is titled "Renew a digital certificate".

**Renew a digital certificate**

Similar to a driver's license, a certificate specifies a period of time during which it is valid and has not expired. Any attempts to use a certificate for authentication before or after its validity or expiration period will not be successful. Therefore, mechanisms for managing the renewal of certificates are critical. For example, an administrator may want to be notified automatically when a certificate is about to expire so that an appropriate renewal process can be completed in a timely manner without causing any inconvenience to the certificate's subject. This renewal process can involve reusing the same pair of public keys and private keys, and just renewing the certificate or issuing a new key pair altogether.

The OpenSSL tool running on a platform other than the z/TPF system allows you to create a certificate request renewal using your existing certificate and key pair as input:

```
#!/openssl x509 -x509toreq -in mycert.pem -out renew.pem -signkey mykey.pem
Getting request Private Key
Enter PEM pass phrase:
Generating certificate request
```

The following shows the contents of the renew.pem file that was created:

```
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=US, ST=New York, L=Poughkeepsie, O=IBM, OU=TPF, CN=John Doe
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:a7:92:dd:6b:78:5a:45:69:69:c3:91:f8:05:a6:
        55:15:8c:fc:d9:75:68:61:26:80:ce:0c:dc:60:dd:
        55:f9:ef:08:42:10:10:1c:0b:14:6a:4a:0a:08:64:
        42:51:7a:c7:78:ee:2e:0c:1e:17:75:b4:a3:46:c8:
        79:fb:a2:23:11:3a:4f:f0:0e:ac:b1:d4:23:32:aa:
        25:57:cf:08:9a:50:d4:88:73:b6:97:24:6a:9f:f9:
        43:d8:fd:db:2a:f7:74:42:d8:e6:36:f2:b4:fe:fa:
```

The left sidebar contains a navigation menu with the following items:

- TPF Product Information Center Home
- z/TPF PUT 02
  - Introduction
  - Tasks
  - Concepts
    - Concepts and structures
    - Internet mail server
    - Migration
    - Program management
    - Programming services
    - Secure Sockets Layer
      - Getting started
      - SSL for the z/TPF system
      - SSL sessions
      - Shared SSL sessions
      - Cryptography standards
      - Digital certificates and authentication
      - Keys management and digital certificates
        - Create public and private key
        - Passwords for key files
        - Load key files to the z/TPF system
        - Create a digital certificate
        - Renew a digital certificate**
        - Revoke a digital certificate
        - Load digital certificates to the z/TPF system
      - Secure web server support
      - SSL daemon processes
        - Diagnostic tools
      - Performance and tuning
      - Supplements
    - Web services
    - XML4C Parser 3.5.1
    - Reference



# 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

