AIST GRID CA Updates

APGrid PMA meeting, Nov. 29, 2005

Yoshio Tanaka (yoshio.tanaka@aist.go.jp)
Grid Technology Research Center,
AIST, Japan
Outline

- Introduction of AIST and AIST GRID CA
- Current status of AIST GRID CA
  - Number of issued certificates
  - Subscribers
- Details of CA operation
  - Staffs
  - Hardware / Equipments / Facilities / Physical access
  - Events recorded and archives
- Detailed flow for issuing certificates
- Other issues (if you have)
AIST: National Institute of Advanced Industrial Science and Technology

- One of the largest Nat’l Labs in Japan
- Research topics include
  - Environment
  - Material
  - Bio/Life science
  - Standards (JIS/OSI)
  - Geographical survey
  - Semiconductor device
  - Computer Science
  - etc.
- 3,500 employee + 3,000 staff
- roughly $1,400M USD/FY2002

7 other campuses across Japan

Tsukuba

Narita

Tokyo
Grid Technology Research Center

Establishment
- Since Jan. 1, 2002
- 7 years term
- 24th Research Center of AIST

Location
- Tsukuba Central
  Umezono 1-1, Tsukuba
- Tokyo Office
  @ Akihabara cross field
  @ 30 people for software development

Engaged in developing grid middleware, applications and system technologies
Research $$ approx. 1000M JPY

<table>
<thead>
<tr>
<th></th>
<th>2002/1</th>
<th>2003/1</th>
<th>2004/1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Researchers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full time</td>
<td>14</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>Fellowship</td>
<td>1</td>
<td>9</td>
<td>12</td>
</tr>
<tr>
<td>Collaborators</td>
<td>7</td>
<td>32</td>
<td>33</td>
</tr>
<tr>
<td>Sub total</td>
<td>22</td>
<td>60</td>
<td>65</td>
</tr>
<tr>
<td>Staff</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administration</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Support</td>
<td>5</td>
<td>9</td>
<td>8</td>
</tr>
</tbody>
</table>

One of the world’s foremost GRID Research Center, the largest in Japan
Director: Satoshi Sekiguchi

<table>
<thead>
<tr>
<th>Team</th>
<th>Leader</th>
<th>Focus Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid Diversification Team</td>
<td>Satoshi Itoh</td>
<td>R&amp;D of Middleware and Applications for Business on Grid. Grid PSE Builder</td>
</tr>
<tr>
<td>Data-Intensive Computing Team</td>
<td>Isao Kojima</td>
<td>Data Grid / Database and Grid (OGSA-DAIS, etc.)</td>
</tr>
<tr>
<td>E-Science Team</td>
<td>Mitsuo Yokokawa</td>
<td>E-Science</td>
</tr>
<tr>
<td>Cluster Technology Team</td>
<td>Tomohiro Kudoh</td>
<td>Interconnection, GFarm</td>
</tr>
</tbody>
</table>
Current status of AIST GRID CA

Number of issued certificates

- **Globus User**
  - valid: 39  revoked: 12

- **Globus Host**
  - valid: 582  revoked/expired: 20

- **Globus LDAP**
  - valid: 103  revoked: 16

- **UNICORE User**
  - revoked: 1

- **UNICORE Gateway**
  - revoked: 1

- **UNICORE NJS**
  - revoked: 1

Subscribers

- **GTRC/AIST researchers**
- **University students and graduates in Japan**
- **Two foreign researchers**
  - 1 is in Vietnam and the other is in Singapore
Details of CA operation – staffs –

Yoshio Tanaka
Yousuke Noguchi
Mototsune Omura
Satoshi Sato
Naoki Fukaumi
Motokuni Tsushima

Security Officer

Private Key Management

User Administrator

CA Operator

RA Operation
IA Operation
OS Maintenance

CA System Administration

HelpDesk

Certificate Request

Host Administrator
Certificate User

Accept CSR, revocation, registration, user administration

Certificate Request

Role
:Staff

All staffs
Details of CA operation – hardware / equipments / facilities / physical access –

**RA server**
- Sun Fire V120, Solaris 9
- connected to the Internet
  - Only the necessary ports for RA operation are opened. The other ports are filtered by the firewall.
- UPS is supplied

**CA server**
- Sun Fire V120, Solaris 9
- Only a connection to the RA server is allowed
- UPS is supplied
- HSM for private key protection
  - Chrysalis-ITS LunaCA3 (CHR-LUNACA3)
    - FIPS 140-1 Level 3 compliant
- Tape drive with auto loader for daily backup
  - Used for daily backup of CA and RA servers
Details of CA operation – hardware / equipments / facilities physical access – (cont’d)

- **Web server (repository)**
  - Sun Fire V100, Solaris 9
  - connected to the Internet
    - Reasonable port filtering.
  - UPS is supplied
  - NAS storage for daily backup

- **CA room**
  - Dedicated to the CA operation.
  - Limited person can enter.
    - Security Officer
    - CA Operators
    - Three staffs in General Administration Department of AIST.
  - Two doors protected by electric key.
Details of CA operation – hardware / equipments / facilities physical access – (cont’d)

Physical access

- A CA operator is not allowed to enter the room alone and need to enter the room with the other CA operator.
- If a CA operator needs to enter the room alone, he must notify the fact to the user administrator by Emails before and after entering the room.
- All events about the access to the room must be recorded in the paper sheets prepared in the room. The events include the names of CA operators, date and time of entering/leaving the room, and the purpose of the access to the room.
- The filled sheets will be kept in a safe box.
Details of CA operation – events recorded and archives –

- **CA system logs**
  - Access and operation logs to the CA daemon process
  - Error logs for accesses and operations to the CA daemon process
  - Operation logs of the CA daemon process

- **RA system logs**
  - Access and operation logs to the RA daemon process
  - Error logs for accesses and operations to the RA daemon process
  - Logs of issued certificates
  - All issued CRLs
  - The date of issuance of CRLs

- **Unix system logs**
  - shutdown/boot/reboot logs of the CA server and the RA server
  - login/logout/sudo logs of the CA and the RA server
  - other logs archived by UNIX operating of the CA and the RA server
    - authlog, cronlog, daemonslog, errorlog, log, logrotate.status, maillog, messages, sulog, syslog, tripwire/report
    - dumplog and rsynclog are archived only for the CA server
Details of CA operation – events recorded and archives – (cont’d)

- **Logs of physical access to the CA room**
  - Paper sheets which record all events about the access to the CA room.
  - Access logs to the CA room those are recorded by the General Administration Department of AIST.

- **Emails**
  - All emails received by the AIST GRID CA
  - All emails received by the AIST GRID RA
  - All emails of system-logs sent from the CA and the RA servers

- **Other documents**
  - A list of email addresses of end entities
  - All issued certificates
  - for each approved request, how the request was approved
  - for each rejected request, how the request was rejected
  - official documents if they are used for identification of entities
  - All versions of the CP/CPS
  - All versions of the Certificate and CRL Profile
  - Internal documents for the operation of AIST GRID PKI Service
  - All Audit reports
detailed flow for issuing certificates

1. Send a request to the RA by email

2. Identification by face-to-face meeting
   3. Give some notes

4. Instruct CA operators to issue a LICENSE ID by a signed email

5. Send a LICENSE ID (18 chars) by an encrypted email

6. Send a password for decrypting the encrypted LICENSE ID by a fax

7. Send a CSR with the LICENSE ID via ssl

8. Verifies the LICENSE ID

9. RA server sends a CSR
10. CA server signs the CSR
11. CA server sends a issued certificate. All communications are encrypted

12. Send a issued certificate via ssl

13. CA operators check the subject DN of the issued certificate (compare with the username/hostname in the application form.)