Outline

- Introduction
- Improvement from Previous Meeting
- Status from Previous F2F Meeting
- Future Plan
Recommendation from Previous F2F Meeting

- Replace signature algorithm MD5 by SHA1 for issued certificates.
  - New algorithm Start Running on Aug. 2008
- Move safe to DC3 area with limited access by ASGCCA Manager and DC Manager only
  - Unique key of lock kept by CA admin.
  - Entrance Guard System (EGS) will leave records for every DC pass in and out.
Updates from Last F2F Meeting

- New ASGCCA (Mercury) was online
- Modify request procedure for host certificates
- Improve request procedure of user certificate for more convenient
- Improve CA website for more readable
Updates from Last F2F Meeting (Cont.)

- Decommission old ASGCCA on Jun 16 2008
- Mercury (9cd75e87)
  - Subject= /C=TW/O=AS/CN=Academia Sinica Grid Computing Certification Authority Mercury
  - Start on Nov 27 2008 until 2027
• Modify request procedure for host certificates, so that non-ASGC certificates will not be kept anymore.
  
  • Main page: http://ca.grid.sinica.edu.tw/certificate/apply_host_cert/apply_host_cert.html
  
  • Improved instruction for requesting host certificates:
    • Step 1. Apply for ASGCCA User Certificate. (Required)
    • Step 2. On-line Create CSR from: Create CSR.
    • Step 3. Upload CSRs from: Upload CSR.
    • Step 4. Download certificates and put key pair into the machine.
From Last F2F Meeting (Cont.)

Request Host Certificate

Verify = SUCCESS
SerialNumber = 0158
Subject = /C=TW/O=AS/OU=GRID/CN=Jhen-Wei Huang 157071

Step 2-1: Fill in your request

1. Fill in the FQDN of host for your request. Example: ca.grid.sinica.edu.tw
2. Click "Add One" or "Add Five" to add text form if you have multiple request. Click "Delete" to delete text form. Make sure the JavaScript is enabled in your browser.
3. Click "Next" to continue request procedure.

Valid domain is required,
Verify via dig
(status: NOERROR or NXDOMAIN)
You want to request following host certificates this time.

1. Verify OK
   Subject = /C=TW/O=AS/OU=GRID/CN=ca.grid.sinica.edu.tw

2. Bad Hostname!
   Subject = /C=TW/O=AS/OU=GRID/CN=ca.grid.sinica.edu.tt

Unconfirmed request will not be created! Any problem please contact us.

Step 2-2: Please download Jhen-Wei_Huang_157071.tar.gz. There are configure files and a script in this tarball. Decompress this tarball and execute script on Unix-like machine directly. Finally, send created CSR file to us. You can execute `wget` to download tarball on the machine. Download Jhen-Wei_Huang_157071.tar.gz

Download compressed file, decompress it and execute script, then upload CSR file from Here
From Last F2F Meeting (Cont.)

- Improve procedure for user certificates, users don’t need key manager to assist in importing user certificates into Firefox. *(Simple to obtain user certificate)*
  - Import page: [http://ca.grid.sinica.edu.tw/certificate/request/import_cert.html](http://ca.grid.sinica.edu.tw/certificate/request/import_cert.html)
  - Improved User Interface for requesting user certificates:
    - Fill in [request form](http://ca.grid.sinica.edu.tw/certificate/request/import_cert.html) and meeting with local RA (Required for new member)
    - Online submit request and create CSR file from [Here](http://ca.grid.sinica.edu.tw/certificate/request/import_cert.html)
    - Import certificate into the browser from [Here](http://ca.grid.sinica.edu.tw/certificate/request/import_cert.html)
    - Convert certificate to PEM format for Grid usage *(Optional)*
5. For organization outside of Taiwan, select TW for country and AP for Organization

Country: TW
Organization: AS
Organizational Unit: GRID
First name: 
Last name: 
Email address: 
Length of key: High Grade
(At least 1024 bits)

Fill in user information for each request, need a valid email address used frequently

Submit Query

Academia Sinica Grid Computing Certification Authority

Fill in SN attached to the email from ASGCCA, system will import cert into the Firefox automatically

Import User Certificate

Fill in the serial number of your user certificate. You can find it in the email.

[Input field] [Import/Download Certificate]
From Last F2F Meeting (Cont.)

- Improve CA website for more readable, users can obtain useful information easily.
  - ASGCCA monthly report
  - FAQ
  - Lists of issued certificates
  - Certificates Statistics

<table>
<thead>
<tr>
<th>Serial</th>
<th>O</th>
<th>Common Name</th>
<th>Expiration Date</th>
<th>Revoked</th>
</tr>
</thead>
<tbody>
<tr>
<td>0210</td>
<td>AP</td>
<td>SANJEEV GAUTAM 186556</td>
<td>Sep 5 2009</td>
<td></td>
</tr>
<tr>
<td>020F</td>
<td>AP</td>
<td>Supriya DAS 181197</td>
<td>Sep 4 2009</td>
<td></td>
</tr>
<tr>
<td>020F</td>
<td>AS</td>
<td>registration.twgrid.org</td>
<td>Sep 3 2009</td>
<td></td>
</tr>
<tr>
<td>020D</td>
<td>AS</td>
<td>wds.twgrid.org</td>
<td>Sep 2 2009</td>
<td></td>
</tr>
<tr>
<td>020C</td>
<td>AS</td>
<td>cms.twgrid.org</td>
<td>Sep 2 2009</td>
<td></td>
</tr>
<tr>
<td>020B</td>
<td>AS</td>
<td>WeiLong Ueng 194701</td>
<td>Sep 2 2009</td>
<td></td>
</tr>
<tr>
<td>020A</td>
<td>AS</td>
<td>Jia-Ye Chen 140581</td>
<td>Sep 1 2009</td>
<td></td>
</tr>
<tr>
<td>0209</td>
<td>AP</td>
<td>dpms02.indiacms.res.in</td>
<td>Sep 1 2009</td>
<td></td>
</tr>
<tr>
<td>0208</td>
<td>AS</td>
<td>f-dpms10.grid.sinica.edu.tw</td>
<td>Aug 22 2009</td>
<td>V</td>
</tr>
</tbody>
</table>

Quarterly Breakup

- Number of Certificates
  - User Certificates
  - Host Certificates
  - Revoked Certificates

Academia Sinica Grid Computing
Future Plan

- Database for CA management
- Compatibility issue for different OS and Browsers
- Transition to on-line root CA from off-line
The End
Walk Through

- Homepage
  - http://ca.grid.sinica.edu.tw

- Apply for user certificate steps
  - http://ca.grid.sinica.edu.tw/certificate/request/request_user_cert.html

- Apply for RA status steps
  - http://ca.grid.sinica.edu.tw/certificate/request/request_ra.html

- Apply for host certificate steps
  - http://ca.grid.sinica.edu.tw/certificate/apply_host_cert/apply_host_cert.html
Apply for user certificate checklist

- Read and understand ASGCCA CP/CPS
- RA’s signature on application
- Fax the application and send an notify e-mail to asgcca@grid.sinica.edu.tw
- Generate CSR file via CA website