Academia Sinica Grid Computing Certification Authority Mercury (ASGCCA)

5th APGrid PMA Meeting

Biopolis, Singapore

Eric Yen

September 16, 2008

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

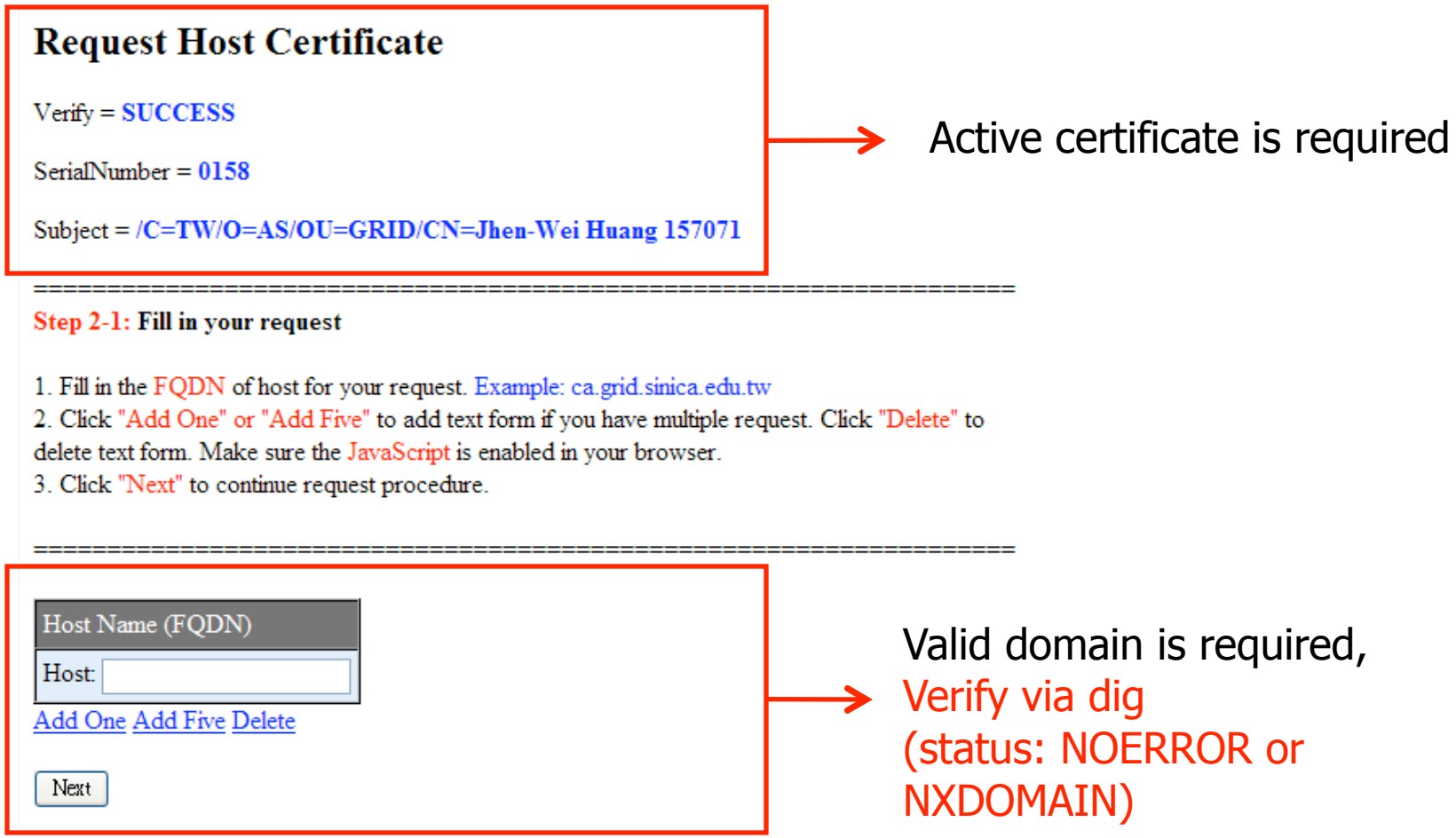
Updates from Last F2F Meeting (Cont.)

- 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
  - Signing Policy: http://ca.grid.sinica.edu.tw/publication/signingpolicy.txt
  - CA Certificate & CRL: http://ca.grid.sinica.edu.tw/publication/index.php
  - Certificates Statistics: http://ca.grid.sinica.edu.tw/publication/newCRT/newcerts/status.php

From Last F2F Meeting (Cont.)

- 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.)



Active certificate is required

Valid domain is required,
Verify via dig
(status: NOERROR or NXDOMAIN)

From Last F2F Meeting (Cont.)

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

→ Only validated request will be approved

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
  - Improved User Interface for requesting user certificates:
    - Fill in request form and meeting with local RA (Required for new member)
    - Online submit request and create CSR file from Here
    - Import certificate into the browser from Here
    - Convert certificate to PEM format for Grid usage (Optional)

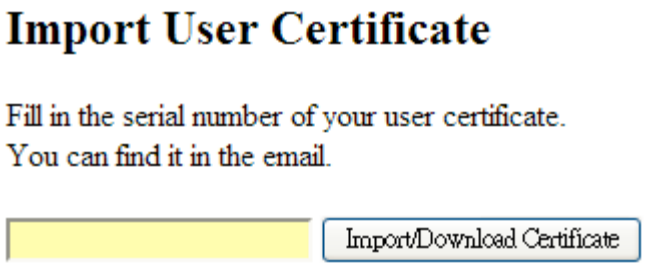
From Last F2F Meeting (Cont.)

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: (At least 1024 bits) High Grade
Submit Query
Academia Sinica Grid Computing Certification Authority

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

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



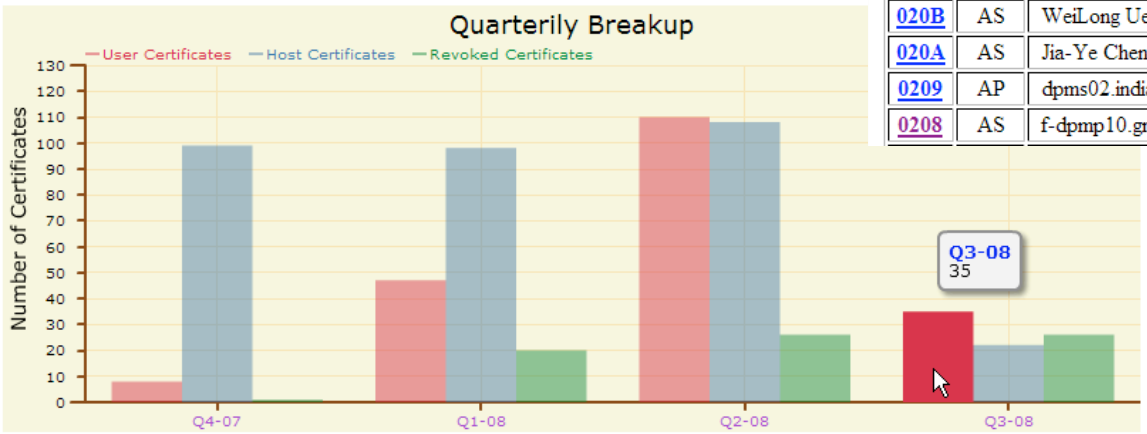
From Last F2F Meeting (Cont.)

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

Issued List

(Signed by Mercury)

Serial	O	Common Name	Expiration Date	Revoked
0210	AP	SANJEEV GAUTAM 186556	Sep 5 2009	
020F	AP	Supriya DAS 181197	Sep 4 2009	
020E	AS	registration.twgrid.org	Sep 3 2009	
020D	AS	wds.twgrid.org	Sep 2 2009	
020C	AS	cms.twgrid.org	Sep 2 2009	V
020B	AS	WeiLong Ueng 194701	Sep 2 2009	
020A	AS	Jia-Ye Chen 140581	Sep 1 2009	
0209	AP	dpms02.indiacms.res.in	Sep 1 2009	
0208	AS	f-dpmp10.grid.sinica.edu.tw	Aug 22 2009	



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