

NAREGI CA Updates

- APGrid PMA 1st F2F Meeting in Beijing -

Masataka Kanamori (kanamori@grid.nii.ac.jp)
Center for Grid Research and Development,
National Institute of Informatics (NII)
November 29, 2005



National Research Grid Initiative

Outline

2

- Introduction of NAREGI(NII) and NAREGI CA
- Current status of NAREGI CA
 - Number of issued certificates
 - Subscribers
- Details of NAREGI CA operation
 - staffs
 - hardware / equipment / facilities / physical access
 - Events recorded and archives
- Detailed flow for issuing certificates
- Useful Links



National Research Grid Initiative



NAREGI CA

- NAREGI CA, managed by NAREGI, issues:
 - client certificates for NAREGI members and partners.
 - server certificates for NAREGI computing resources and partner computing resources.
- Brief History
 - NAREGI PMA (Policy Management Authority) was established in June 17, 2005.
 - NAREGI CA has offered its services since September 1, 2005.



National Research Grid Initiative

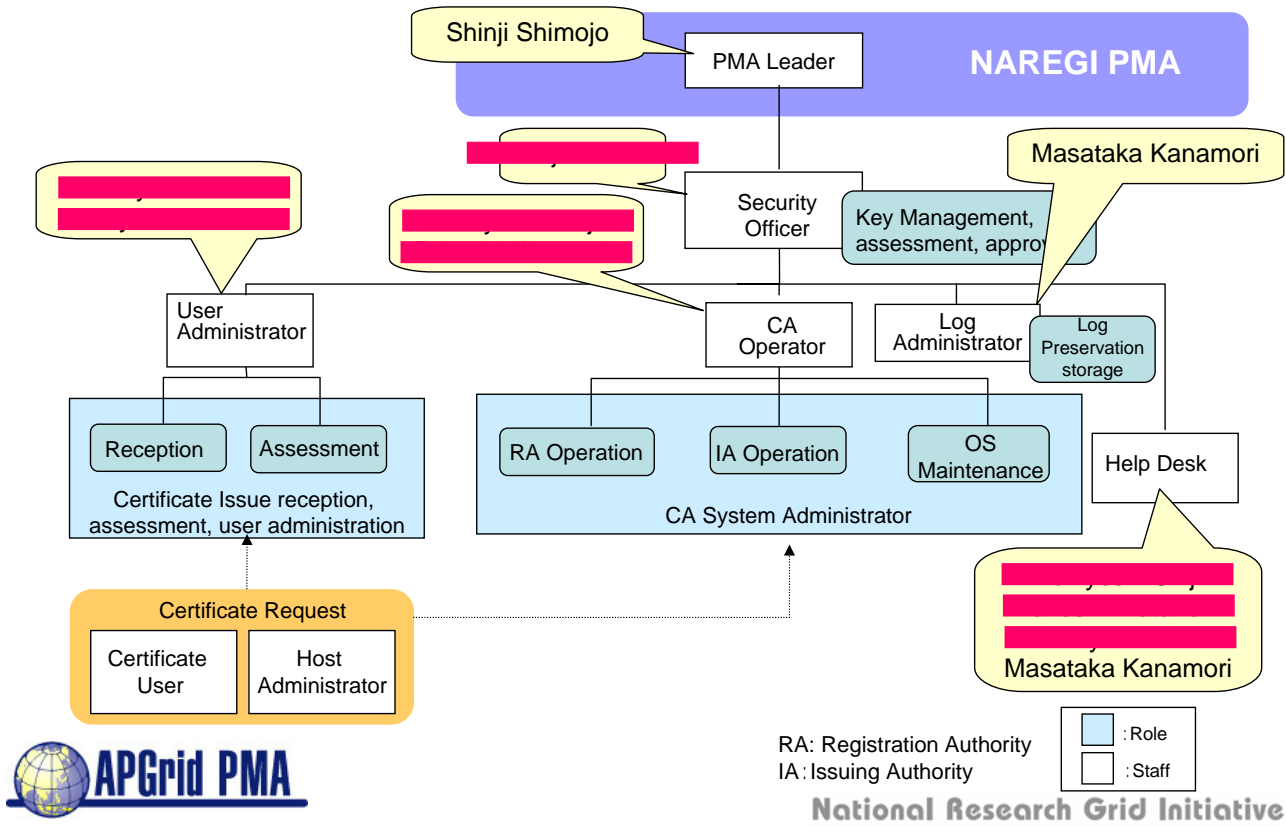


Current Status of NAREGI CA

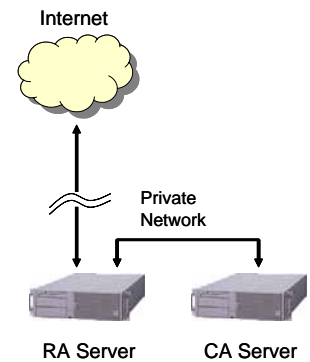
- Number of issued certificates
 - Server Certificates *(Sep. 1, ~ Nov. 24, 2005)*
 - Globus: 519
 - Unicore: 481
 - Client Certificates
 - Globus: 5
 - Unicore: 1
 - Subscribers
 - Users: 5
- Now In preparation for
- deployment of server certificates issued by NAREGI CA
 - registration of a department head, following later



National Research Grid Initiative



- CA server
 - NEC Express 5800, RedHat 8
 - Tape drive for weekly backup
 - dedicated machine in a key-locked cage
 - only connected to the RA server via an exclusive network using a private address.
 - HSM for private key protection
 - LUNA CA (FIPS 140-1 Level 3)
- RA server
 - NEC Express 5800, RedHat 8
 - Tape drive for weekly backup
 - Connected to the Internet with appropriate ACLs.
- Web server (repository)
 - Fujitsu PRIMEPOWER 200, SunOS
 - protected by a firewall device, has a reachability to the Internet



- Machine Room
 - protected by an IC card key and limited persons can enter.
 - CA cage stored the CA server is located with two keys
 - Two keys managed by two different CA operators.
 - The cage can access
 - Security Officer
 - CA Operators
 - CA operators must record their working events in the machine-room log books.
 - e.g., Data and time of entering/leaving the machine room.
 - Machine room log books are stored in a key-locked shelf.
- Physical Access
 - Only CA operators are authorized to enter the machine room when they operate the NAREGI CA.

Physical Security (1/2)





(Photographed by CA operators)

National Research Grid Initiative

Details of NAREGI CA operation – events recorded and archives – (1/2)

- CA system logs
 - access logs to the CA server daemon
 - logs of issued / revoked certificates and CRLs
 - error logs about the CA server daemon
 - access and operation logs to the CA server
 - access and operation logs to the HSM
- RA system logs
 - access logs to the RA server daemon
 - error logs about the RA server daemon
 - access and operation logs to the RA server
 - logs of issued / revoked certificates and CRLs
- Unix system logs
 - System information logs of the CA and the RA server.



Details of NAREGI CA operation – events recorded and archives – (2/2)

13

- Logs of physical access to the machine room and the CA cage
 - Working books which record
 - date and time of entering/leaving the machine room and the CA cage
 - working purpose
 - CA operator's name
 - Once a CA operation is completed, CA operators should record it in the working books along with security officer's signature
 - Other documents
 - official documents, e.g.,
 - system applications to issue user's system account
 - certificate applications from users
 - registration applications for department heads
 - Internal documents for the operation of NAREGI PKI Service
 - Internal documents for NAREGI PMA members
 - NAREGI PMA meeting materials and scripts
 - All versions of the CP/CPS
 - NAREGI Certificate and CRL Profile
- stored in a key-locked shelf controlled by a log administrator.



National Research Grid Initiative



Identification and Authentication

14

Prerequisite:

- NAREGI assigns each department head as a representative (One representative per organization)[11 people, Nov 23, 2005]
 - Representatives, who should be well-known at NAREGI, must present an enrollment application with his/her signature to a user administrator.
- User Certificate:
 - Subscriber must
 - meet in person with the representative of the user's organization in order to verify the user's identity
 - get a certificate application signed by the representative
 - submit in person or mail (or FAX) the application to the user administrator
 - User administrator confirms the application by ensuring that a representative's signature is on it
- Host and Service Certificate
 - An application can be submitted by a certificate user after obtaining the representative's approval in person



National Research Grid Initiative

Useful Links

- <http://www.nii.ac.jp/>
 - about the National Institute of Informatics (NII)
- <http://www.naregi.org/>
 - about NAREGI
- <https://www.naregi.org/ca/>
 - about NAREGI CA
- <http://www.tokyometro.jp/e/index.html>
 - subway maps are available in 8 languages
- <http://www.jorudan.co.jp/english/norikae/e-norikkeyin.html>
 - easy to find your transfer stations



National Research Grid Initiative

