NAREGI CA

Masataka Kanamori
NAREGI
November 7, 2005

APGrid PMA

National Research Grid Initiative

Introduction

- NAREGI (National Research Grid Initiative)
  - a Japanese national Grid R&D project, covering the period of FY2003 to FY2007
- 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 on June 17, 2005.
  - NAREGI CA has offered its service since September 1, 2005.

APGrid PMA

National Research Grid Initiative

CP/CPS

- NAREGI CP/CPS:
  - current version: 1.0.1 (September 27, 2005)
  - OID: 1.2.392.00200181.1.1
  - conforms to RFC2527

- NAREGI CP/CPS is managed by the NAREGI PMA.
  - Changes in contents need to be approved by the NAREGI PMA, as described in section 8.

End Entity

- Grid Users, Servers and Services:
  - NAREGI partner research and development facilities and organizations
  - special users authorized to have a NAREGI certificate by the NAREGI project leader

Certificate Type

- User Certificate:

  C=JP, O=National Research Grid Initiative, OU=GRID,
  CN=Masataka Kanamori, Email=kanamori@grid.nii.ac.jp

- Grid Host:

  C=JP, O=National Research Grid Initiative, OU=GRID,
  CN=host/hoge.grid.nii.ac.jp

- Grid Service:

  C=JP, O=National Research Grid Initiative, OU=GRID,
  CN=ldap/hoge.grid.nii.ac.jp

Identification and Authentication

Prerequisite:

- NAREGI assigns each department head as a representative. (One representative per organization)
  - 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.
    - be signed by the representative on an application for requesting the issue of certificate.
    - submit in-person or mail (or FAX) the application to the user administrator.
  - User administrator confirms the application with the representative's signature on it

- Host and Service Certificate
  - An application is required to be submitted by a certificate user after obtaining the representative's approval in-person.

Certificate Restrictions

- Certificate Lifetime:
  - 10 years for NAREGI CA certificate
  - 1 year for each end entity certificate
    - User and server certificates should not be shared.

Certificate Revocation

- Certificates are to be revoked when …
  - the RA receives a revocation request from a user.
  - the user's key has been compromised or is suspected of being compromised.
  - the user information on the certificate is suspected of being incorrect.
  - a user resigns or leaves his/her job.
  - the CA private key has been compromised.
  - a user violates his/her obligations
    - as described in the CP/CPS Section 2.1.3.

Revocation Request Procedure

- Revocation Request from a user
  - User can choose between two methods, as follows:
    - Command-line UI and Web-based UI using encrypted communication between the user and the RA.
  - The RA confirms a revocation request by using the client certificate, and accepts it.
  - The RA sends a revocation request to the CA located in an independent network segment.
    - Communications between the RA and the CA are encrypted.
- The NAREGI CA chief officer can execute a revocation request on behalf of the user, if it is necessary.

CRL

- The NAREGI CA will …
  - revoke the certificate immediately after receipt and acceptance of the revocation request.
  - publish the CRL on the NAREGI CA web site immediately.
- A relying party can verify a certificate by retrieving the newest CRL on the web site.
- The issued CRL is valid for 30 days.
- The CRL will be reissued at least seven days before the previous one expires.

Physical Security

- CA Server :
  - dedicated machine in a locked cage with two keys
    - Two keys managed by two different CA operators.
  - The cage is located in a restricted machine room.
  - only connected to the RA server via an exclusive network using a private address.
    - CA server cannot be reached from the Internet.
- CA private key :
  - Protected by a FIPS 140-1 Level 3 compliant HSM.
  - is copied in a backup device with passphrase in a key-locked shelf.

Records Archival

- Types of Archive Data:
  - All issued certificates and CRLs
  - All enrollment requests and notifications between the NAREGI CA and users
  - Operation history of the CA key
  - Events of Interest, as described in CP/CPS 4.5.1
    - login, logout, reboot, access and error logs, etc…
  - Other documents about the NAREGI CA.
- The retention period is 3 years.
- Archived files are preserved in a key-locked shelf.

Key Pair

- The CA private key is generated by the HSM.
  - A user's key pair is generated on his/her PC by using a license ID.
    - The user's private key is not generated by the CA and the RA.

- Key Length:
  - CA Certificate: 2048 bits
  - End Entity: 1024 bits

License ID:
  - 24 characters
  - is provided from the RA for one-time authentication at the time of enrollment process of the user.

Contact Information

- About NAREGI CP/CPS

  National Institute of Informatics,
  Center for GRID Research and Development (NAREGI)
  e-mail: naregi-ca@grid.nii.ac.jp

- NAREGI Certification Authority

  https://www.naregi.org/ca/

Acknowledgments

- I used the IHEP Grid CA presentation as a reference in preparing this slides.
- These slides were supported by the NAREGI WP5 PKI group and the NAREGI PMA members.