New open source CA development as Grid research platform.

National Research Grid Initiative in Japan

Takuto Okuno.
About NAREGI PKI Group (WP5)
To develop CA and RA server software that supports grid environment.

To develop CA/RA policy and authentication service policy satisfied with basic assurance level by GGF.

To experiment the operation of PKI authentication service (CA server software and CP/CPS) for UNICORE and Globus grid environment.

To consider multi domain policy, and create an authentication mechanism for such environment.

It was necessary for developing new CA software to satisfy our functional and security requirement.
NAREGI Registration Sequence

1. Prepare LicenseIDs
2. User registration
3. Submit a licenseID and request to issue a certificate
4. Request to revoke a certificate
5. Request to update a certificate
6. grid-mapfile generation

End user
Host administrator

Certificate Request
Apply certificate operation

Site Administrator (LRA)

LicenseIDs Request
Issue a LicenseID

Might be face to face.

Issue LicenseIDs

Telephon, Mail and so on.

CA Administrator

Issue LicenseIDs

RA Server
Accept a user request
(issue,revoke,update)

NAREGI site

base grid-mapfile publish

User site

Download a base grid-mapfile and generate mapfile for local site

Via command line or WEB (Online)
## NAREGI CA – roadmap & function layer

|---------------------|----------------|------------|

### Command User Interface

- LCMP
- RA

### Web User Interface

- Service Interface for Account management
- Web Service Interface (Java API)

### Service Interface for VO Management

- XKM S

### Based on AiCA (Open Source)

- CP/CPS
  - Authentication Policy (single domain)
  - Extended Authentication Policy (multi domain)

---

**NAREGI AUTHENTICATION SERVICE**

**NW Infrastructure**
NAREGI CA – server components

CA Server
- aicad
- aicrlpub

RA Server
- aienroll
- airad
- enroll (apache CGI)
- gridmapgen

LDAP Server

CA Administrator

User

PKI utilities
- certview
- certconv

CA management tools
- aica

Collaborate with Grid Service, S/MIME, Group ware and so on.

WEB
- HTTP
- LCMP

- email

- certreq
CD contents

- README (Overview, install, etc..)
- LICENSE
- Release NOTE
- naregi-ca-1.0.tar.gz
  - Source files
  - CP/CPS, Administrator Guide, etc..
- naregi-project
  - naregi_pre.pdf (about NAREGI)
  - wp5_pre.pdf (about NAREGI Work Package 5)
### Available Cryptographic and Hash algorithms

<table>
<thead>
<tr>
<th>Public key cryptography</th>
<th>RSA (with key generation)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSA (with parameter generation)</td>
</tr>
<tr>
<td></td>
<td>Elliptic Curve DSA (with parameter generation)</td>
</tr>
<tr>
<td>Symmetric cryptography</td>
<td>DES( ECB, CBC, CFB)</td>
</tr>
<tr>
<td></td>
<td>Triple-DES( ECB, CBC)</td>
</tr>
<tr>
<td></td>
<td>RC2( ECB, CBC)</td>
</tr>
<tr>
<td>Hash</td>
<td>MD2, MD5, SHA1</td>
</tr>
<tr>
<td></td>
<td>HMAC (key hash)</td>
</tr>
<tr>
<td>Available PKI files</td>
<td></td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Certificate</td>
<td>X509 DER, PEM (*.cer, *.pem)</td>
</tr>
<tr>
<td></td>
<td>PKCS#7 DER ( *.p7b )</td>
</tr>
<tr>
<td></td>
<td>PKCS#12 DER ( *.p12, *.pfx)</td>
</tr>
<tr>
<td>Private Key</td>
<td>PKCS#1 PEM (*.key, *.pem)</td>
</tr>
<tr>
<td></td>
<td>PKCS#8 DER (*.key, *.pem)</td>
</tr>
<tr>
<td></td>
<td>PKCS#12 DER (* .p12, *.pfx)</td>
</tr>
<tr>
<td>CRL</td>
<td>X509 DER, PEM (*.crl, *.pem)</td>
</tr>
<tr>
<td></td>
<td>PKCS#7 DER ( *.p7b)</td>
</tr>
<tr>
<td>Cross certificate pair</td>
<td>X509 DER, PEM (*.ccp, *.pem)</td>
</tr>
<tr>
<td>Certificate Signing Request</td>
<td>PKCS#10</td>
</tr>
<tr>
<td></td>
<td>DER, PEM (*.crl, *.pem)</td>
</tr>
</tbody>
</table>
Appendix. grid-mapfile generation

Generate a grid-mapfile from a global mapfile and local users.csv file.

Users.csv

Create a file that defines a licenseID and local account name mapping.

Site Administrator

Inform a licenseID

User

Issue or revoke a certificate. Input licenseID and subject DN

RA Server

Issue or revoke a certificate

CA Server

Generate a grid-mapfile that includes a licenseID and a subject DN mapping.

LCMP

http download

(1) (2) (3) (4) (5) (6) (7)
Appendix. NAREGI Authentication Service

NaReGI Auth.
Policy Domain

User
Proxy

User

Resource

Process

Other Auth.
Policy Domains

Resource

Process

Create

Create

JOB Request

JOB Request

Delegate

Validate

Validate

Cert

Cert

CSR

CSR

RA

RA

CA

CA

Collaboration

Collaboration
# NAREGI CA – development roadmap

<table>
<thead>
<tr>
<th>In 2003</th>
<th>In 2004</th>
<th>In 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>• LCMP protocol definition</td>
<td>• Optimize performance (10k certificates/h)</td>
<td>• XKMS</td>
</tr>
<tr>
<td>• NAREGI CA development</td>
<td>• LCMP Java API</td>
<td>• Feedback / improve server operation</td>
</tr>
<tr>
<td>• Start trial CA operation</td>
<td>• Service Interface for account management</td>
<td></td>
</tr>
</tbody>
</table>