NAREGI makes IT Safe
- Grid Security

As a basis of the Cyber Science Infrastructure

Shinichi Mineo
(National Institute of Informatics)

Outline

- Introduction of CSI: Cyber Science Infrastructure
- Concept of UPKI: National Research PKI Infrastructure
- Security Features developed for NAREGI Middleware
- Summary & Open Issues
Cyber Science Infrastructure for R & D

Cyber-Science Infrastructure (CSI)

- NII-REO (Repository of Electronic Journals and Online Publications)
- Virtual Labs
- Live Collaborations
- Deployment of NAREGI Middleware
- UPKI: National Research PKI Services
- Restructuring Univ. IT Research Resources
- Extensive On-Line Publications of Results

Industry/Societal Feedback

International Infrastructural Collaboration

SINET3: Lambda-based Academic Networking Backbone

- GeNi (Global Environment for Networked Intellectual Information)
- Cyber-Science Infrastructure (CSI)
- University of Hokkaido
- Tohoku University
- University of Tokyo
- University of Nagoya
- Osaka University
- Kyoto University
- University of Kyushu
- Titech, Waseda University, KEK, etc.

Cyber Science Infrastructure for R & D

SINET3: Science Information Network 3

- Innovative academic infrastructure for more than 700 universities and research institutions.
- Provides wide variety of services such as multi-layer transfer, VPN, QoS, and bandwidth-on-demand services and sufficient bandwidth with Japan's first STM-256 (40 Gbps) deployment.
- Enables quick service recovery by multiple-loop topology against link and node failures.
- Carries on its full-scale operations since June 2007.
UPKI : Three Layer Architecture
Concept of UPKI

- Open Domain PKI
  - Public Server Certification
  - Digital Signature/Encryption of e-mails by S/MIME
- Campus PKI
  - Identity Management
  - SSO for Web services
  - Wireless LAN roaming and VPN
- Grid PKI
  - Grid Services

UPKI Development Plan

- 2006FY
  - Gathering common interests and opinions, and feedback.
  - Interoperability check, knowledge transfer, publicity, tutorial works, …

- 2007FY
  - Insource model, multi-university cooperative model

- 2008FY
  - Insource model, multi-university cooperative model

- 2009FY and later
  - Deployment of campus PKI at each university
  - Connecting universities
  - Federation of applications etc.

- Campus PKI specification
  - Model design
  - Outsource model

- Campus PKI CP/CPS template
  - Outsource model
  - Insource model, multi-university cooperative model

- Developing, deploying and fostering new applications
  - Wireless LAN roaming
  - Single Sign On to Web Services
  - S/MIME

- Development of CA software package
  - Distribution and support for deployment of CA software package
UPKI Initiative

- Founded in 16 Aug 2006
- Sponsored by NII AAI TWG
- Mission
  - Gathering interests and opinions from academic and industry stakeholders.
- https://upki-portal.nii.ac.jp/

NII Public CA for Open Domain PKI

Now in Test Service
Campus PKI Operation Models

1. Full outsource

2. IA outsource

3. In source

NAREGI Software Stack
as of Beta ver. 2006
Requirements in Grid Security

- **Authentication**
  - PKI based user authentication
  - Compatible with GSI standards
  - Trust federation between CA's

- **Authorization**
  - VO management for Inter-organizational collaboration
  - Interoperability with other Grid projects

- **Accounting**
  - ID federation for authn, authz, and charging
  - With privacy protection!

Developed
NAREGI-CA to be deployed in UPKI

Developed VO based AuthZ

Future issues

Software Stack of NAREGI-CA

<table>
<thead>
<tr>
<th>UPKI interfaces</th>
<th>Command User Interface</th>
<th>Web User Interface</th>
<th>XKMS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RA: Registration Functions</td>
<td>Web Service Interface</td>
<td></td>
</tr>
<tr>
<td>LCMP</td>
<td>CP/CPS</td>
<td>Auth. Policy Extension (multi-domains)</td>
<td>Audit</td>
</tr>
<tr>
<td></td>
<td>Auth. Policy (single domain)</td>
<td></td>
<td>PMA</td>
</tr>
</tbody>
</table>

AICA (existing Certificate Authority Free Software)

| CP/CPS | Auth. Policy Extension (multi-domains) | Audit | PMA |

Free open source software Ver2.2 (Jan.24,2007) is available at http://www.naregi.org/download/
UPKI INTERFACE -1:
Distribution of RA using IC Cards

CA SITE

1. Issue IC Card for RA Admin
2. Pass it to RA Admin
3. Apply for Cert, Set Challenge PIN
4. Notified by e-mail
5. Accredit LRA via F2F

App Server

6. Create Account for LRA
7. Send a License ID
8. Set Info of LRA and Issue IC Card

LRA (Local RA)

9. Pass it to LRA
10. LRA Operation

UPKI INTERFACE -2:
Self-help Cert Issue using Challenge PIN

CA SITE

1. Apply for Cert, set Challenge PIN
2. Register RQ
3. Notify
4. F2F Inspection

INTERNET

5. Check the registered Info & Permit
6. Send a License ID
7. Input Challenge PIN & License ID
8. Authorization
9. Create Key pair & Send CSR
10. Get Subject Info & Issue a Cert

User

11. Download the Cert
UPKI INTERFACE -3: Interoperation with the Campus PKI

1. Register all the acceptable SDN Issued by Campus PKI
2. Apply for Cert using IC Card, set Challenge PIN
3. Check SDN & Register RA
4. Notify
5. Input Challenge PIN & License ID
6. Send a License ID
7. Create Key pair & Send CSR
8. Authorization
9. Check SDN & Register RQ
10. Get Subject Info & Issue a Cert
11. Download the Cert

User

INTERNET

CA SITE

APP Server

LDAP Server

LRA

CA Server

GRID CA

GRID RA

LDAP

GRID Services

Super Computers

Databases

Experiment Devices

User

CampusCA

Campus-Grid PKI Federation

Issue Certificate

Request Certificates (Using IC Cards as credentials)

Certificate for Grid System

Access

IC Card

Campus PKI

Grid PKI
VO based Authorization

A virtual organization (VO) is a dynamic collection of resources and users unified by a common goal and potentially spanning multiple administrative domains.

NAREGI adopts VOMS-type VO Management

- CA/RA
- CRL
- DN, VO info
- Information Service
- VOMS
- Account Mapping
- Gridmap file
- Grid VM
- Policy Decision & Enforcement Point
- Grid Job Submission
- Managed by the Super Scheduler
- User
- User Cert
- Proxy Cert + VO
- Policy Information Point
- GRAM
- Policy file
- AuthZ Service
AuthZ Service

Based on SAML 2.0 & XACML 2.0 with GT4.0 AuthZ Framework

- NAREGI’s XACML profile (A Plan)
  - Subject Attributes:
    - Maps of VOMS attributes in XACML Subject Attributes
    - Needs standardized attribute IDs for well-known types of credentials such as VOMS attribute certificate
  - Resource Attributes:
    - RAFM enables flexible resource attribute retrieval from the request message content to SP
    - To support for authorization for WS-Resource or finer-grained resource, this kind of mechanism is needed
  - Action Attributes:
    - Maps GT4.0 AuthZ Framework Property to an XACML Action Attribute
    - wsa:Action may also work well

Security Architecture - Overview

- CA
  - NAREGI-CA
- Credential Management
  - MyProxy
- VO Membership Management
  - VOMS
- Authorization
  - NAREGI-AuthZ (Prototype)
So far, we came...

Summary & Open Issues

- CSI is composed of High-speed Backbone NW, UPKI, Grid middleware and various services, integrating next generation peta-sale computing facilities.
- UPKI project has started to build national academic authentication and authorization infrastructure, on which Grid technology is widely used.
- NAREGI at first developed reliable AuthN system to be deployed in UPKI.
- Now NAREGI is developing VO based AuthZ service based on SAML 2.0 & XACML 2.0 with GT4.0 AuthZ Framework.
- ID mgt and Accounting are still remaining open issues to be designed jointly with all the stakeholders in CSI community.