Grid Security for the Cyber Science Infrastructure in Japan

28 March 2007, Academia Sinica, Taipei, Taiwan

Shinichi Mineo
(National Institute of Informatics)
Outline

- Introduction of CSI (Cyber Science Infrastructure) & NAREGI Grid Middleware
- A Use Case in NAREGI and its Security Model
- Security Features developed for NAREGI Middleware
- A plan of Authorization Service
- 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 Infrastructure

SuperSINET and Beyond: Lambda-based Academic Networking Backbone

- Hokkaido-U
- Tohoku-U
- Tokyo-U
- Nagoya-U
- Kyoto-U
- Osaka-U
- Kyushu-U
- NII
- (Titech, Waseda-U, KEK, etc.)

Restructuring Univ. IT Research Resources
Extensive On-Line Publications of Results

Industry/Societal Feedback

International Infrastructural Collaboration
Super SINET provides 10 Gbps Backbone
Cyber-Science Infrastructure for R & D

Cyber-Science Infrastructure (CSI)

- Deployment of NAREGI Middleware
- UPKI: National Research PKI Infrastructure
- SuperSINET and Beyond: Lambda-based Academic Networking Backbone
- Restructuring Univ. IT Research Resources
- Extensive On-Line Publications of Results

Industry/Societal Feedback

International Infrastructural Collaboration

NII-REO (Repository of Electronic Journals and Online Publications)
GeNii (Global Environment for Networked Intellectual Information)
Virtual Labs Live Collaborations

Cyber-Science Infrastructure

SuperSINET and Beyond: Lambda-based Academic Networking Backbone

GeNii (Global Environment for Networked Intellectual Information)
Virtual Labs Live Collaborations

UPKI: National Research PKI Infrastructure

Deployment of NAREGI Middleware

Restructuring Univ. IT Research Resources

Extensive On-Line Publications of Results

SuperSINET and Beyond: Lambda-based Academic Networking Backbone

Hokkaido-U
Tohoku-U
Tokyo-U
NII
Nagoya-U
Kyoto-U
Osaka-U
Kyushu-U
(Titech, Waseda-U, KEK, etc.)

NII-REO (Repository of Electronic Journals and Online Publications)
UPKI : Three Layer Architecture

**OpenDomain PKI**
- NII Pub CA
- Web Srv.
- S/MIME
- Web Srv.
- Other Pub CA

**Campus PKI**
- A Univ. CA
- Auth, Sign, Encrpt.
- EE
- Server, Super Computer
- Student, Faculty

**Grid PKI**
- A Univ. NAREGI CA
- Proxy
- EE
- Server, Super Computer
- Student, Faculty

**Future plan**
- Sign, Encrpt.
- Other Pub CA
- S/MIME

**Grid Computing**

Web Srv.
S/MIME
Web Srv.
Cyber-Science Infrastructure for R & D

Cyber-Science Infrastructure (CSI)

- NII-REO (Repository of Electronic Journals and Online Publications)
- GeNii (Global Environment for Networked Intellectual Information)
- Virtual Labs Live Collaborations
- Deployment of NAREGI Middleware
- UPKI: National Research PKI Infrastructure

SuperSINET and Beyond: Lambda-based Academic Networking Backbone

- Hokkaido-U
- Tohoku-U
- Tokyo-U
- NII
- Nagoya-U
- Osaka-U
- Kyoto-U
- Kyushu-U
- Titech, Waseda-U, KEK, etc.

Restructuring Univ. IT Research Resources Extensive On-Line Publications of Results

Industry/Societal Feedback

International Infrastructural Collaboration
NAREGI Software Stack
as of Beta ver. 2006
A Use Case: Job Submission with Reservation based Co-Allocation

WFT, PSE, GVS, GridRPC

Client

Workflow
Abstract
JSDL

Super Scheduler

Reservation, Submission, Query, Control...

Resource Query
DAI

Information Service

CIM
Resource Info.

Reservation based Co-Allocation

Concrete JSDL

Concrete JSDL

GridVM
Computing Resource

GridVM
Computing Resource

GridMPI

UR/RUS
Accounting
Requirements in AAA

- **Authentication**
  - PKI based user authentication
  - Compatible with GSI standards
  - Trust federation between CA’s
  - Developed NAREGI-CA to be deployed in UPKI

- **Authorization**
  - VO management for Inter-organizational collaboration
  - Interoperability with other Grid projects
  - Current Issues to be solved

- **Accounting**
  - ID federation for authn, authz, and charging
  - With privacy protection!
  - Future issues
Trust Chain supported by UPKI

CA for Campus PKI

CA for Grid PKI

Certs Inf.

ISSUE

CSR

EE Cert in IC Card

ISSUE

EE Cert for GRID

Campus PKI Domain

Grid PKI Domain
A virtual organization (VO) is a dynamic collection of resources and users unified by a common goal and potentially spanning multiple administrative domains.
VOMS-type VO Management
developed in EGEE

CA/RA -> CRL

DN, VO, Group, roll, capability -> MK-gridmapfile

DN > pseudo accounts

VOMS -> Gridmap file

User Cert, Proxy Cert + VO -> X.509AC

Policy Decision Point

User

EGEE Grid site

GRAM

LCAS

GACL

Grid Job Submission
VOMS-type VO Management adopted in NAREGI

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

NAREGI Grid site
Job Management in NAREGI

User -> Super Scheduler (SS) -> GridVM

Work Flow Description

Resource Reservation & Job Submission

User/Resource Information

Information Service (IS)
To Realize It ...

- In addition to the standard Grid Security,
- Super Scheduler (SS) must represent end users
  - Delegation of Proxy Certs to SS
- Reliable and easy key store and VO Attribute Control must be supported
  - Private key store and VOMS handling are troublesome for end users
Delegation of Proxy Certs to SS: using the Second MyProxy

- USER
- NAREGI Portal
- SS
- GridVM

Diagram:
- MyProxy
- MyProxy2
Delegation Procedure -1

1. Job-WF: Workflow Description
2. Job-Hash = hash (Job-WF)
3. Pass Phrase = Job-Hash
4. user-id = unique Id for Job-WF
5. myproxy-init(user-id, Pass Phrase)
6. send Job-WF
Delegation Procedure -2

⑦ subtract user-id from Job-WF
⑧ Pass Phrase=hash(job-WF)
⑨ myproxy-get-delegation(user-id, Pass Phrase)
Delete the used Proxy Cert
⑩ Globus Job submission

⑪ AuthN & AuthZ of users
⑫ Job submission to the local scheduler according to the Authz policy
Security model of Job Submission

Workflow Description

User on NAREI Portal -> Super Scheduler (SS)

Resource reservation & Job submission

Super Scheduler (SS) -> GridVM

MyProxy 2

User/Resource Information

Information Service (IS)

GSI

Receive Proxy Certs

Store Proxy Certs

GSI
Trust Chain in NAREGI Security Model

CA

EE Certificate

Proxy Cert

Signature

Job Description

User

MyProxy2

Proxy Cert

Proxy Cert

Proxy Cert

Hash Value

Super Scheduler

GridVM

Proxy Cert
Private key Store and VOMS Handling

1. Get EE Cert
2. Get Proxy Cert by proxy-init command
3. Request for Attr. Cert
4. Store in the Proxy Cert
5. Delegation to MyProxy
6. Get Proxy Cert from NAREGI Portal
7. Job Submission
Private Key Store and VO Attribute Control by End Users

- Difficult for end users to understand PKI and proper handling of certs
- High Risk in handling certs by end users themselves
- Prefer to use Grid computing without special environment such as GT
- Need Unique naming Method for proxy certs stored in MyProxy
NAREGI developed One-stop service by User Management Server (UMS)
Grid Job Submission using UMS

1. Log in to the Portal

2. Select menu to make Proxy Cert with VO attr. And store it to MyProxy

3. Store the Proxy Cert with VO Attri. To MyProxy2

4. SS analyzes WF and submits jobs
Now We are developing 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 XACLM 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
So far, we came...
Summary & Open Issues

- CSI is composed of High-speed Backbone NW, UPKI, Grid middleware and various services on it.
- NAREGI at first has developed reliable AuthN system to be deployed in UPKI.
- As VO mgt, VOMS has been adopted for interoperability with EGEE.
- Now NAERGI is developing 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.
- Security is a key issue for CSI, which will integrate the next generation peta-sale computing facilities to innovate Academia and Industry in Japan.
Cyber Science Infrastructure Plan Toward Petascale Computing

National Leadership System
(Next-generation Supercomputer)

Grid

Grid Interoperability and International Collaboration
- EGEE
- Tiergrid

National Infrastructure
(Institute, University)

Infrastructural middleware
(GRID, Infrastructure for certification, etc.)

Industry-university joint research VO

University/interuniversity research Institutes VO

Project VO

Virtual research environment for various fields

Development and Application of Advanced High-performance Supercomputer Project

NAREGI Grid Middleware
UPKI
(Inter-University Public Key Infrastructure)
(International Institute of Informatics)