On Certificate Issuance and User ID Management in the NAREGI Grid Middleware Integrating the Shibboleth

International Symposium on Grid Computing 2010
March 9, 2010
Academia Sinica, Taipei, Taiwan

Eisaku SAKANE¹, Manabu HIGASHIDA², Shinichi MINEO³ and Kento AIDA¹

¹National Institute of Informatics, Japan
²Osaka University, Japan
³RIKEN, Japan
Table of Contents

• Background
• Current situation and problems
• Design and implementation
• Discussion and future issue
• Summary
Background

- NII and 9 supercomputer centers constructed a grid environment on the SINET3 network and started pilot grid operation in April 2009.
- An application system for using the grid, called Grid Pack Application System, was established respecting the operation policy of each computer center.
  - registration of user account
  - grid certificate issuance
  - creating grid-mapfile at each center
- The system was confirmed for users concerned.
- With drastic increase of the number of users at starting production level grid services, several duties in the system will unravel.
Nine Computer Center Grid

- Resource provider
- Operation center

- Information Initiative Center, Hokkaido University
- National Institute of Informatics
- Information Technology Center, Nagoya University
- Research Institute for Information Technology, Kyushu University
- Academic Center for Computing and Media Studies, Kyoto University
- Cybermedia Center, Osaka University
- Cyberscience Center, Tohoku University
- Center for Computational Sciences, University of Tsukuba
- Information Technology Center, University of Tokyo
- Global Scientific Information and Computing Center, Tokyo Institute of Technology
Grid Middleware

• **NAREGI middleware 1.1**
  – developed by the CGRD, NII
  – composed of control nodes and computing nodes

• **computing nodes (operated in 9 computer centers)**
  – computing services
  – 8 Linux clusters (CentOS 5.2 + PBS Pro 9.1/OpenSUSE 10.3 + Sun Grid Engine 6.0)
  – 2 vector supercomputer (NEC SX)

• **control nodes (operated in NII).**
  – grid services (security, job brokering, information service, portal, ...)
  – Linux computing nodes (CentOS 5.2)
Grid Pack Application System

• A system for solving the following known problems
  – How do users apply accounts?
    • Users do not want to submit 9 application forms to computer centers.
  – How do users obtain grid certificates?
    • Users do not want to travel to NII (RA) for grid certificate issuance.
  – How do computer centers create grid-mapfile?
    • Computer centers cannot understand directly the subject DN of certificate.
Registration of User Account

User

Computer Center A

admin.

user account

account request

account request + G PID

Computer Center B ...

admin.

user account

offline communication

online communication
Certificate and Grid-mapfile

User → User (cert. request) → Computer Center A (LRA operator) (cert. request + GPID) → NII GOC (LRA admin.) → NAREGI CA system (cert.) → UMS (NAREGI Portal) → NAREGI CA system (cert.) → SVN repo. (GPID-DN list) → Computer Center B → User (cert. request) → User (F2F interview) → Computer Center A (LRA operator) (cert. request + GPID) → NII GOC (LRA admin.) → NAREGI CA system (cert.) → UMS (NAREGI Portal) → NAREGI CA system (cert.) → SVN repo. (GPID-DN list) → Computer Center B (computer admin.) → User (cert. request) → User (F2F interview) → Computer Center A (LRA operator) (cert. request + GPID) → NII GOC (LRA admin.) → NAREGI CA system (cert.) → UMS (NAREGI Portal) → NAREGI CA system (cert.) → SVN repo. (GPID-DN list) → Computer Center B (computer admin.) → User (cert. request) → User (F2F interview) → Computer Center A (LRA operator) (cert. request + GPID) → NII GOC (LRA admin.) → NAREGI CA system (cert.) → UMS (NAREGI Portal) → NAREGI CA system (cert.) → SVN repo. (GPID-DN list) → Computer Center B (computer admin.) → User.

Key:
- Green arrow: offline communication
- Blue arrow: online communication

Notes:
- UMS acct+passwd+license ID
- LRA operator
- LRA admin.
- computer admin.
- grid-mapfile
- GPID-LN list
- GPID-DN list
- offline communication
- online communication
Target Problem

• LicenseID notification
  – NII GOC notifies users of LicenseID.
    • sends users an email attached an encrypted archive including UMS account, password and LicenseID.
    • notifies users of the password of the encrypted archive by telephone.

• User identification with F2F interview

• Committing the subject DN and GPID of users to the repository

• With drastic increase of the number of user at starting production level service, these duties will be bottleneck of the procedure.
LicenseID Notification

It is expected that requests concentrate at the beginning of the fiscal year.
Target Problem (cont’d)

• LicenseID notification
  – NII GOC notifies users of LicenseID.
    • sends users an email attached an encrypted archive including UMS account, password and LicenseID.
    • notifies users of the password of the encrypted archive by telephone.

• User identification with F2F interview

• Committing the subject DN and GPID of users to the repository

• With drastic increase of the number of user at starting production level service, these duties will be bottle-neck of the procedure.

• How do we ease heavy duties in the operation?
Integrating with Shibboleth

• To solve the problem, we integrate the NAREGI middleware with the Shibboleth and improve current system.
  – Computer centers: Identity Provider
  – NAREGI CA: Service Provider
    • LicenseID
  – NAREGI Portal: Service Provider
    • operations on UMS
      – creating user account
      – storing user certificate
Automation of LicenseID notification

- User
- Computer Center A
  - Identification
  - ID/Password request
  - LicenseID request
  - ID/Password
  - Shibboleth Auth. Info.
- LRA operator
- LicensesID request
- Auth. server
- NII
  - LRA admin.
  - NAREGI RA SP
- LicensesID management system
Automatically Creating Account of UMS

User

Computer Center A

NAREGI Portal
SP

NII

UMS

Creating account

Registration of mapping info. (ePPN, account)

Certificate issuance

cert.

Registration of DN

UMS account management DB

Shibboleth Auth. Info.
Attrib: ePPN LicenseID, Passphrase

NAREGI CA system
Creating Grid-mapfile

Computer Center A

- computer admin.
- Query with ePPN
- DN
- grid-mapfile
- VOMS

NII

- UMS
- UMS account management DB

Computer Center B

- computer admin.
- Query with ePPN
- DN
- grid-mapfile
- VOMS
Identification with MICS Profile

- Is the user identification in conventional user application system sufficient to trust?
Conventional User Identification

• In conventional user identification, computer centers confirm
  – user information
  – approval of the chief person of the accounting section of the organization which the user belongs to.

• We think that the conventional user identification matches the identification obeying the MICS profile.
Discussion and Future Issues

• VO operation
  – Currently, there is one VO composed of
    • VO manager: NII GOC
    • Resource providers: 9 computer centers
  – What VO do computer center manage?

• Common rule in the Shibboleth federation
  – What requirements should IdP satisfy?
  – What requirements should SP satisfy?

• Evaluation of the proposed system.
Summary

• We reported a user application system of 9 computer center grid in Japan.
• The system eases heavy duties in previous application system.
• The system is implemented based on the NAREGI middleware integrating the Shibboleth.
• We will evaluate the proposed system at beginning of FY2010.