--- Tsukuba-GAMA ---

Flexible Authentication and Credential Management for e-Science

N. YAMAMOTO, I. KOJIMA,
Y. TANAKA, and S. SEKIGUCHI
AIST, Japan

International Symposium on Grid Computing (ISGC) 2009
Apr. 21, 2009
GEO (Global Earth Observation) Grid

We are aiming at providing an e-Science infrastructure for worldwide Earth sciences communities to accelerate geosciences

Motivations

Grid implementations are very complicate for application users and developers
We could not apply Grid Security Infrastructure to specifications in the geosciences community

Our Solutions

We have been implementing Tsukuba-GAMA in order to satisfy their requirements

- web-portal based user interface
- flexible authentication methods
- adopting GSI for web-GIS applications
Requirements for Security

Not all services are freely accessible.
- commercial data
- Simulation on supercomputers

Security Infrastructure is necessary!
- Authentication: who are you?
- Authorization: what you can do?

Problems of traditional username/password approach
- Users need to manage username/password at site-by-site.
- Users need to login to each site.
- Service providers need to control access for individual users.
- Not enough secure to protect sensitive services.

Authentication: who are you?
Authorization: what you can do?

Users need to manage username/password at site-by-site.
Users need to login to each site.
Service providers need to control access for individual users.
Not enough secure to protect sensitive services.

http://www.geogrid.org/
Basic Functionalities for Geosciences

- **Search**
  - A uniform database interface that can handle heterogeneous databases

- **Transfer**
  - A third party delivery interface that can retrieve input data from data providing services

- **Process**
  - A uniform data processing service interface which can handle heterogeneous hardware resources

- **Security**
  - A flexible and robust authentication and authorization
Grid Security Infrastructure (GSI)
- Security infrastructure based on PKI and X.509 certificates.

GSI enables single sign on and credential delegation
- Users need to virtually login only once
- Users can access multiple databases via single query
- Third party data transfer enables computation to take input data from data servers on-demand.

However
- Users need to generate and manage certificates carefully
- Need to consider integration of existing technologies (e.g. OpenID) and standards (e.g. OGC Standards).

OGSA-DAI Client

Integration Framework with OGSA-DAI

Java Program

SQL

Globus

OGSA-DAI

OGSA-DAI

Database Server (PostgreSQL)

ASTER

MODIS

VOMS

VOMS

Transfer all data on-demand

Execute simulation

http://www.geogrid.org/
Search
  - **OGSA-DAI GLite**, which enables VOMS authorization, provides a uniform database interface

Transfer
  - **GridFFP** provides a third party file transfer in order to retrieve observation data

Process
  - **GRAM** provides a job execution service

Security
  - **GSI** provides a single sign on and delegation
  - **VOMS** reduces administrative cost
User interface is constructed as JSR168 portlet on GridSphere

- Access database using OGSA-DAI Java API
- Submit image analysis via GRAM
- Retrieve input data from GridFTP server
- GSI and VOMS
GAMA provides easy interface for GSI credential

- Users do not need to manage certificates.
- Added VOMS interface in GAMA authentication module

GAMA
(Grid Account Management Architecture)
by SDSC
(San Diego Supercomputer Center)

OGC Standard Services

Web Service Workflow Engines

Grid Environment

Sekiguchi et. al, *IEEE System of systems, 2008*
**Functionalities / Grid Solution**

- **Search**
  - *OGSA-DAI GLite*, which enables VOMS authorization, provides a uniform database interface

- **Transfer**
  - *GridFFP* provides a third party file transfer in order to retrieve observation data

- **Process**
  - *GRAM* provides a job execution service

- **Security**
  - *GSI* provides a single sign on and delegation
  - *VOMS* reduces administrative cost

- **Cannot adopt their authentication method**
  - only support username and password style

- **Cannot adopt standards in their community**
  - Application provider must use / modify their applications by using specified APIs

---

http://www.geogrid.org/
Our Solution: Tsukuba-GAMA

- Account Management
- MyProxy
- VOMS

Tsukuba-GAMA provides flexible and easy interface for GSI and VOMS.

- Enable to generate Grid credentials from various source of identities.
  - username/password
  - User certificates
  - external authentication
Authentication types

(a) GAMA style
- Username and Password

(b) Credential
- Globus User Certificate

(c) External Authentication
- OpenID
- Shibboleth

Account Management server

User DB

Credential Repository

External Authentication service

On-line CA (MyProxy CA)

VO Management Server (VOMS)

User Management System

http://www.geogrid.org/
GAMA Style
(Username and Password)

Globus User Certificate

External Authentication
(OpenID)
GAMA-style Account registration

- User Information
  - Account DB
  - Credential Repository

- CSR
- MyProxy CA
- MyProxy Registry
- Certificate Registry
- Store end-entity

User
GAMA Style
(Username and Password)

Globus User Certificate

External Authentication
(OpenID)
Credential authentication module

- Sign-on-tool generates proxy certificate on the portal server
  - using delegation protocol
- as JWS application

User → Sign-on-tool → Web Portal

Web Portal:
- Account DB
- Credential Repository

VOMS extension

VO member DB

http://www.geogrid.org/
GAMA Style
(Username and Password)

Globus User Certificate

External Authentication
(OpenID)
OpenID authentication module

1. User enters OpenID URL
2. User provides Password for OpenID
3. User requests short-lived credential from OpenID server
4. Web Portal provides access to VO member DB
5. MyProxy CA verifies user credentials
6. VOMS server assigns VOMS proxy
7. VO member DB provides access to VOMS proxy
8. Account DB and Credential Repository store user information

http://www.geogrid.org/
Tsukuba-GAMA provides authentication interfaces to generate VOMS-enabled proxy certificate on the web portal server by

- Username and Password
  - the end-entity stored in server-side

- Globus User Certificate
  - generate proxy certificate directly

- OpenID authentication
  - Short lived end-entity

VOMS-enabled services

- Search – OGSA-DAI/GLite
- Transfer – GridFTP (LCAS/LCMAPS)
- Process – GRAM (LCAS/LCMAPS)
There are many map contents
▶ provided by Google Map API, OpenLayers API (Ajax)

Many useful specifications discussed in OGC (Open Geospatial Consortium)
▶ RESTful application protocol
  @ http://servername/ogc?
  Service=WMS&Request=GetCapabilities

▶ direct access to service
  ▶ Client does not have any credential
OGCProxy is a broker portlet:

- forwarding users' requests to backend OGC services.
- providing freely development environment of client application.

ACL:
/testvo.geogrid.org/aster

VO Name: testvo.geogrid.org

Group: aster

https://portal/OGCProxy?
URL=https://gridsite/..../service

https://gridsite/..../service
Credential portlet allows the user to download VOMS-enabled proxy certificate as PKCS#12.
Tsukuba-GAMA provides authentication interfaces to generate VOMS-enabled proxy certificate on the web portal server in a single framework

- username and password
- Globus user certificate
- OpenID authentication

OGCProxy for existing Web-GIS application

- Ajax application works without any modification
- Any brokers for any application protocols

PKCS#12 download portlet

- The user access services directly
Thank you for your attention

http://www.geogrid.org/

naotaka@ni.aist.go.jp