GRID Authorization Framework
for
CCLRC Data Portal

Ananta Manandhar
Large scale resource sharing between trusted and untrusted Organizations.

Researchers are interested to use the Grid if they can access the resources that they require.

Resource providers are keen to host resources in the Grid but would want the control over their resources.

- Control
- Reliability
- Manageable

Missing any one of these three would make a Resource provider wary in Collaborating.
Data Portal

Broker application that provides a web based interface to access data located in multiple facilities
Validating who the user says he is

- Use of Certificate
- Use of delegation features of GSI Architecture

Managing what the user is allowed to do

- Grid Map Files
- CAS
- VOMS
- PERMIS
- Akenti
Requirements

• Scalable
  Ability to manage increase in users and resources as collaborations between other organizations increase

• Manageable and maintainable
  Adding, removing and modifying user privilege need to be kept easy and intuitive

• Preferably under the control of the resource end
  Organizations prefer to have control over who have access over their data.
Requirements 2

• Minimum intervention at the Data Portal Layer
  To keep the points of Security consideration as low as possible.

• Ability to utilize existing Access Control Models
  Many resource providers already have existing access control mechanisms that are reliable and proven.

• Future integration capabilities with other Grid Related Applications
Globus CAS

• Presence of a Community authorization server.
• Resource Providers Grants Privileges to CAS
• Privileges of the user are stored in CAS
• User request CAS to receive CAS credential
  • CAS credential is a GSI proxy certificate signed by CAS server with policies and privileges of the user included in an extension.
• User presents CAS credential for Resource provider in place of proxy certificate.
• Presence of a central publicly accessible LDAP sever hosting Attribute Certificates

• Organization’s Privilege Allocator create Authorization Certificates for users and stored in publicly accessible LDAP Directories

• Also Authorization policy description are created and stored in publicly accessible LDAP directories.

• While querying a resource
  • User presents its certificate
  • The Resource’s Access Decision Framework retrieves the user’s Attribute certificate and the policy definition from the LDAP server and enforces the privileges
Classifies authorization information into two categories

- General information regarding the relationship between the user and the Virtual Organization
- Information regarding what the user is allowed to do at the Resource Provider

Relationship between VO and user is specified as group and role by VOMS server (coarse grained)

Information regarding what the user is allowed to access is maintained by the Resource provider. (fine grain)
Authorization Framework

- **Authorization Server**
  - Request Authorization Token
  - Return Authorization Token
  - Get Policy Attributes for DN
  - Manage User Policies and Policy Description

- **User Privilege Database**

- **Management Interface**
  - Super Admin
  - Admin

- **Certificate Store**

- **Access Adapter**
  - Resource 1
  - Resource 2
  - Resource n

- **VO**
  - Request result (Proxy Cert + Authorization Token + query)
Authorization Token Server

Web Service Interface

Get Authorization Token (Proxy Cert, Request Parameters)

Authorization Token Generator

User Privilege Interface

Get DN Privileges for DN

Certificate Store

User Privilege Store

Management Interface

Admin

Type 1
Authorization Token

```
<attributeCertificate>
  <aclInfo>
    <version>0.1</version>
    <holder>user DN</holder>
    <issuer>issuer DN</issuer>
    <issuerName>issuerName</issuerName>
    <issuerSerialNumber></issuerSerialNumber>
    <signatureAlgorithm>MD5withRSA</signatureAlgorithm>
    <validity>
      <notBefore></notBefore>
      <notAfter></notAfter>
    </validity>
    <attributes>
      <DPView>value</DPView>
      <wrapperGroup>value</wrapperGroup>
      <dataAccessGroup>value</dataAccessGroup>
    </attributes>
  </aclInfo>
  <signature>
  </signature>
</attributeCertificate>
```
Implications with adding Authorization Framework

Organization’s Perspective

The organization would only have to maintain the user’s group membership to the organization and host an Authorization Token generation server.

Data Portal Perspective

It would have to request for Proxy certificate from MyProxy Certificate and an Authorization Token from Organization’s authorization server on behalf of the user and forward these certificates along with the user’s query.

User’s Perspective

Would need have to have membership with the Organization and will have to request for a Authorization token at the start of the session before being able to query the organization’s resources.

Resource Provider’s Perspective

The Resource Provider would need to maintain the group mapping to its local access control mechanisms and be able to verify the authenticity of the Certificates.
• Formalize the format and structure of Authorization Token

• Look into the possibilities of replacing web service interface with Grid Service interface and other communication protocols

• Look in feasibility of using authorization token in HPC portal.
**Summary**

- Better trust for resource providers
- Better manageability for organizations
- Use of existing access control mechanisms
- GSI delegation would remain unaffected
Questions ?