Overview

• OSG & EGI Authorization Models
• Authorization Interoperability Profile
• Implementations, Status, and Plans

Keith Chadwick for the AuthZ Interop team
Grid & Cloud Computing dept.,
Computing Sector, Fermilab

ISGC 2012
Feb 27, 2012
The Collaboration

Ian Alderman\textsuperscript{9}
Mine Altunay\textsuperscript{1}
Rachana
Ananthakrishnan\textsuperscript{8}
Joe Bester\textsuperscript{8}
Keith Chadwick\textsuperscript{1}
Vincenzo Ciaschini\textsuperscript{7}
Yuri Demchenko\textsuperscript{4}
Andrea Ferraro\textsuperscript{7}
Alberto Forti\textsuperscript{7}
Gabriele Garzoglio\textsuperscript{1}
David Groep\textsuperscript{2}
Ted Hesselroth\textsuperscript{1}
John Hover\textsuperscript{3}
Oscar Koeroo\textsuperscript{2}
Chad La Joie\textsuperscript{5}
Tanya Levshina\textsuperscript{1}
Zach Miller\textsuperscript{9}
Jay Packard\textsuperscript{3}
Håkon Sagehaug\textsuperscript{6}
Valery Sergeev\textsuperscript{1}
Igor Sfiligoi\textsuperscript{1}
Neha Sharma\textsuperscript{1}
Frank Siebenlist\textsuperscript{8}
Valerio Venturi\textsuperscript{7}
John Weigand\textsuperscript{1}

\textsuperscript{1} Fermilab, Batavia, IL, USA
\textsuperscript{2} NIKHEF, Amsterdam, The Netherlands
\textsuperscript{3} Brookhaven National Laboratory, Upton, NY, USA
\textsuperscript{4} University of Amsterdam, Amsterdam, The Netherlands
\textsuperscript{5} SWITCH, Zürich, Switzerland
\textsuperscript{6} BCCS, Bergen, Norway
\textsuperscript{7} INFN CNAF, Bologna, Italy
\textsuperscript{8} Argonne National Laboratory, Argonne, IL, USA
\textsuperscript{9} University of Wisconsin, Madison, WI, USA
The Authorization Model

- The EGEE (EGI) and OSG security model is based on X509 end entity and proxy certificates for single sign-on and delegation
- Role-based access to resources is based on VOMS Attribute Certificates
- Users push credentials and attributes to resources
- Access privileges are granted with appropriate local identity mappings
- Resource gateways (Gatekeeper, SRM, gLExec, …) i.e. Policy Enforcement Points (PEP) call-out to site-central Policy Decision Points (PDP) for authorization decisions
Status of the Adoption of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware

Authorization Infrastructure (the OSG case)

VO

VO Services

VOMRS → VOMS

Site Services

GUMS

SAZ

PDP

Grid Site

PEPs

WN

Storage

Data Access (UID/GID)

Submit request with voms-proxy

register

get voms-proxy

VO

VO Services

VOMRS → VOMS

Site Services

GUMS

SAZ

PDP

Grid Site

PEPs

WN

Storage

Data Access (UID/GID)

Submit request with voms-proxy

register

get voms-proxy

Legend

AuthZ Components

Not Officially In OSG

VCI Management Services

AuthZ Components

Not Officially In OSG

VCI Management Services
Goals for Interoperability

• Agree on common **PEP to PDP call-out protocol** and **implementation** in order to…
  1. …share and reuse software developed for EGI and OSG,
  2. …give software providers (external to the Grid organizations) reference protocols to integrate with both Grids infrastructures,
  3. …enable the seamless deployment of software developed in the US or EU in the EU or US security infrastructures.
AuthZ Interoperability Activities

• 2008
  ▪ **Release XACML profile** document: 1+ yr collaboration (OSG, EGEE, Globus, and Condor)
  ▪ **Implementation and integration** of XACML AuthZ modules with principal PDPs and PEPs in OSG and EGEE
  ▪ Demonstrated interoperability of OSG vs. EGEE deployments in ad-hoc scenarios – **Goal 3**

• 2009
  ▪ Discussion on evolutions of the profile in the context of Argus
  ▪ **Argus extends** the interoperability **profile**
  ▪ External software providers use the profile as reference on authorization for the Grid Domain. TechX: SVOPME project. Globus: GT5 – **Goal 2**

• 2010
  ▪ Consolidation of **additional** OSG PDPs and PEPs
  ▪ Start migration of PEPs to LCAS / LCMAS (Nikhef, NL) as common code base – **Goal 1**

• 2011
  ▪ Tune client parameters to sustain **authz tsunami**
  ▪ **Extend profile** with proxy validity attributes
  ▪ Begin **OGF standardization** – **Goal 2**

• 2012
  ▪ Work on profile extension for **Cloud Authorization**
Status of the Adoption of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware

Overview

✓ OSG & EGI Authorization Models

➢ Authorization Interoperability Profile
  • Implementations, Status, and Plans

ISGC 2012
Feb 27, 2012
Keith Chadwick for the AuthZ Interop team
Grid & Cloud Computing dept.,
Computing Sector, Fermilab
Request/Response Attribute Categories

- Request is made with
  - Subject attributes
  - Action attributes
  - Resource attributes
  - Environment attributes

- Response is made with
  - Permit, Deny, or Indeterminate
  - Obligation attributes
## Request Attributes (see profile doc for full list)

<table>
<thead>
<tr>
<th>Subject:</th>
<th>Action:</th>
</tr>
</thead>
</table>
| • Subject-X509-id  
  • String: OpenSSL DN notation  
• Subject-VO  
  • String: “CMS”  
• VOMS-FQAN  
  • String: “/CMS/VO-Admin” | • Action-id (enum type)  
  • Queue / Execute-Now / Access (file)  
• Res. Spec. Lang.  
  • RSL string |

<table>
<thead>
<tr>
<th>Resource:</th>
<th>Environment:</th>
</tr>
</thead>
</table>
| • Resource-id (enum type)  
  • CE / SE / WN  
• Resource X509 Service Certificate Subject  
  • resource-x509-id  
• Host DNS Name  
  • Dns-host-name | • PEP-PDP capability negotiation.  
  • PEP sends to PDP supported Obligations  
• Enables upgrading of the PEPs and PDPs independently  
• Pilot Job context (pull-WMS)  
  • Pilot job invoker identity  
• Policy statement example: “User access to the WN execution environment can be granted only if the pilot job belongs to the same VO as the user VO” |
## Obligation Attributes

<table>
<thead>
<tr>
<th><strong>UIDGID:</strong></th>
<th><strong>Path restriction:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• UID (integer): Unix User ID local to the PEP</td>
<td>• RootPath (string): a sub-tree of the FS at the PEP</td>
</tr>
<tr>
<td>• GID (integer): Unix Group ID local to the PEP</td>
<td>• HomePath (string): path to user home area (relative to RootPath)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Secondary GIDs:</strong></th>
<th><strong>Storage Priority:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• GID (integer): Unix Group ID local to the PEP (Multi recurrence)</td>
<td>• Priority (integer): priority to access storage resources.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Username:</strong></th>
<th><strong>Access permissions:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Username (string): Unix username or account name local to the PEP.</td>
<td>• Access-Permissions (string): “read-only”, “read-write”</td>
</tr>
</tbody>
</table>
Overview

- OSG & EGI Authorization Models
- Authorization Interoperability Profile
- Implementations, Status, and Plans

ISGC 2012
Feb 27, 2012

Keith Chadwick for the AuthZ Interop team
Grid & Cloud Computing dept.,
Computing Sector, Fermilab
Implementations

- **SAML v2 - XACML v2 profile**
  - OpenSAML (Java); Globus XACML (C)

- **Authorization Callout Modules and PDPs**
  - LCAS / LCMAPS (L&L) - SCAS plug-in → SCAS (EGI)
  - PRIMA - gPlazma plug-in → GUMS / SAZ (OSG)

- **Resource Gateways**
  - Computing Element
    - Pre-WS and WS Gatekeepers 4.2 / 5.2
  - Storage Element
    - SRM / dCache; BeStMan; xrootd; GridFTP
  - Worker Node
    - gLExec
SAML Callout Structure in OSG
Minimal Code Sharing

Legend:
- Cmpnt
- EGEE Comp. used in OSG
XACML Callout Structure in OSG
Transitioning: Using also EMI Code

Legend: Cmpnt, EGEE Comp. used in OSG
XACML Callout Structure in OSG
Using only EMI Code

Legend:
- **Cmpnt**: EGEE Comp.
- **used in OSG**:
Measured Performance

Tuning PEP / PDP connection parameters to sustain authorization “tsunami”*

- Socket connection timeout > 21 s (set to 30 s)
- Sysctl parameter 'net.core.somaxconn' = max expected job connections (set at 4096 per server)
- Apache parameter 'ListenBacklog' = same value as above (GUMS only)
- Tomcat parameter 'acceptCount' = same (SAZ only)
- Apache ‘MaxClients’ = 32 (GUMS only)

* https://twiki.grid.iu.edu/bin/view/Documentation/Release3/InstallGlexec#Engineering_Considertations
Status and Plans

- rpm-based VDT packages L&L / XACML call-out for easy deployment
- Major OSG sites fully or partially migrated
- Working with OGF on standardization of the profile
- Looking for collaborators to extend the standardized profile in support of Cloud Authorization
  - Goal: reuse stable fine-grain role-based site-central Grid AuthZ infrastructure for Cloud deployments at sites
Conclusions

• An EGEE, OSG, Globus, and Condor collaboration has released in 2008 an Authorization Interoperability profile and XACML implementation
• Effort on OGF standardization and extension for Cloud computing
• Call-out module implementations are integrated with major Resource Gateways
• Performance tuned to support the authorization needs of major OSG Grid sites
• The major advantages of the infrastructure are:
  1. share and reuse software developed for EGI and OSG
  2. give software providers reference protocols to integrate with both Grids infrastructures
  3. when using the same release of the protocol, enable the deployment of software developed in the US or EU in the EU or US security infrastructures