omii europe

open middleware infrastructure institute

Cross Middleware VO Authorization

Alberto Forti on behalf of the VOMS team

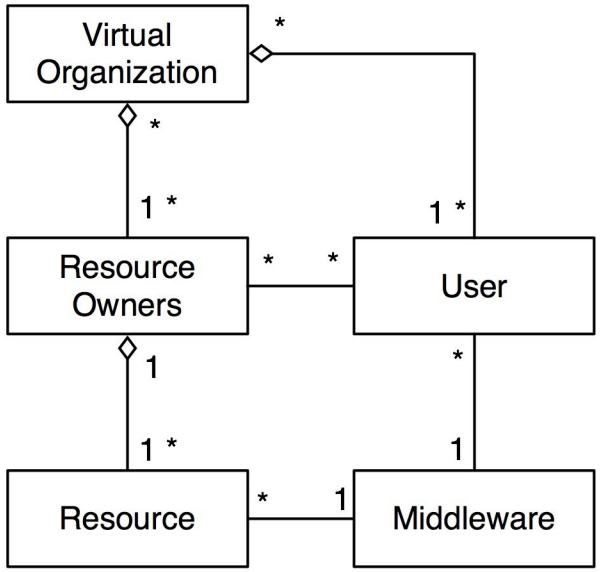
CHEP 2007

Outline

- **Virtual Organization management**
- **VOMS**
- **Authorization standards in the Grid community**
- **Evolution of VOMS towards AuthZ standards**
- **Use cases : Integration of VOMS in UNICORE**

Virtual Organizations

- **The ‘Grid problem’ : coordinated resource sharing across dynamic collections of individual, institution and resources, what we call Virtual Organizations**
- **Resources owners share their resources within the VO**
- **Resources may deploy any grid middleware**
- **Users may use any grid middleware**



Virtual Organization Management

- **Resource owners share their resource subject to the fact that they maintain control over how the sharing is done**
- **Resource owners make sharing agreements within the VO**
- **Enabling VO management means providing the instruments to facilitate the enforcement of such sharing agreements**
- **Since the shared resources may deploy any middleware, standards are key enabler of VO management**

VOMS

- The Virtual Organization Membership Service is a tool for doing VO management
- Originally developed in the framework of the European Data Grid and DataTAG collaborations, now maintained in the EGEE project
- Core components for authorization of middleware stack as gLite (EGEE) and VDT (OSG), module available for using it with the GT authorization framework
- Used in many Grid Infrastructures worldwide: EGEE, OSG, D-Grid, Naregi

VOMS

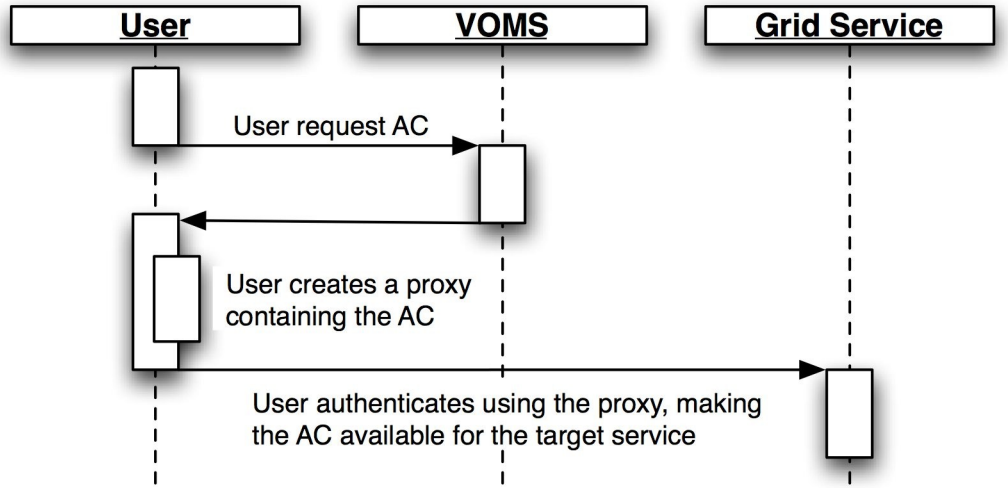
- **VOMS allows to assign to users attributes expressing their position in the VO**
  - With position we mean groups users are in, roles they have, or any other attributes (funding agency)
- **These attributes are used by Grid services exposing resources for access control**
- **This allows the enforcement of the agreement between Resource Owners (ROs) and the VO**
  - A RO may share some resources subject to the fact that users in a group are given preference

VOMS Attribute Authority

- **The main VOMS component is an Attribute Authority (AA) that releases signed assertions containing users attributes**
- **The current AA uses Attribute Certificates (ACs) according to RFC 3821**
  - Does not expose a web service interface
  - Uses proprietary xml messages
  - Uses GSI for securing communications

VOMS Attribute Authority

- **In the most popular usage pattern the AC retrieved from the VOMS AA is inserted by the users in their proxy certificates**
  - Using provided CLI clients or API
- **After authentication with a Grid service, the AC is thus available for the service to drive authorization**



Authorization Standards

- **OGF OGSA AuthZ working group**
- **Leverages on existing standardization efforts in the Web Service community and profile them for use with OGSA Grid Services**
- **Currently working on three components**
  - Attribute Authority (SAML)
  - Authorization Service (SAML XACML)
  - Credential Validation Service (SAML)
- **VOMS implements the AA**
  - Currently working on finalizing the profile but agreements settled

SAML

- **The Security Assertion Markup Language (SAML) defines a framework for exchanging security information between online business partners**
- **An XML based framework for communicating user authentication, entitlement, and attribute information**
- **Developed by the Security Services Technical Committee of OASIS (the Organization for Advancement of Structured Information Standards)**
- **History**
  - SAML V1.0 OASIS standard in November 2002
  - SAML V1.1 followed in September 2003
  - SAML V2.0 OASIS standard since November 2005

SAML Components

- **Assertions**
  - Supplies statements made by a SAML authority
  - Attributes assertions asserts that a specified subject is associated with the supplied attributes
  - Authorization and Authentication assertions
- **Protocols**
  - Request/response protocols that allow to request assertions from SAML authorities
- **Bindings**
  - Mapping from SAML request/response messages into standard messaging or communication protocols
    - **SOAP**

VOMS SAML Service

- **In the OMII-Europe project, VOMS is being extended to support authorization standards emerging from the Grid community**
- **A VOMS SAML Service is being developed that retain the same functionalities of the current AA**
  - Exposes a web service interface according to the SAML spec
  - Uses SAML Assertions instead of AC
- **Can be deployed to any J2EE service container**
- **Aim at being middleware independent**
  - Enforce the idea that VO management is a task that is inherently middleware independent

SAML Assertions

- **Example SAML Assertions released by the VOMS SAML Service (some parts are missing for brevity)**

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" … >
 <saml:Issuer>/C=IT/O=INFN/OU=Host/L=CNAF/CN=datatag6.cnaf.infn.it</saml:Issuer>
 <saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:x509SubjectName">
   CN=Morris Riedel,OU=ZAM,OU=Forschungszentrum JuelichGmbH,O=GridGermany,C=DE
  </saml:NameID>
 </saml:Subject>
 <saml:Conditions NotBefore="..." NotOnOrAfter="..." />
 <saml:AttributeStatement>
  … shown below …
 </saml:AttributeStatement>
</saml:Assertion>
```

SAML Attributes

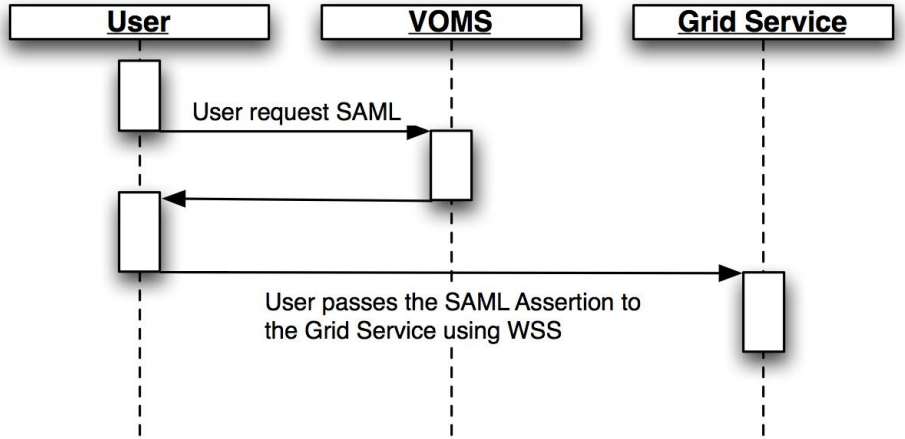
- **Example VOMS attributes express as SAML Attribute elements**

```
<saml:AttributeStatement>
<saml:Attribute Name="group-membership-id" NameFormat="urn...">
 <saml:AttributeValue type="xs:string">
    /vo
 </saml:AttributeValue>
 <saml:AttributeValue type="xs:string">
    /vo/group
 </saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

- **Coherent with the current FQAN format /vo/group**
- **The format for the SAML Attribute and AttributeValue elements is work in progress, a VOMS SAML profile is being finalized**

VOMS SAML Service Usage

- **The coupling of AC and proxy certificates has proved a very efficient way of making attributes available for services**
- **A requirement was to support middleware not using proxy certificates**
- **The possibility explored was to use WS-Security**
  - WS-Security SAML Token Profile



VOMS for UNICORE 6

- **Since UNICORE 6 does not use proxy certificates, using VOMS for authorization was a good proof of concept for the aim of supporting multiple usage pattern**
- **The flow is as depicted above**
  - A UNICORE client (either using GPE clients or the Gridsphere portal) gets a SAML Assertion from the VOMS SAML service
  - When contacting UNICORE services, the client passes the assertion in the header of the SOAP message, according to WSS
  - The UNICORE service can use the attributes to drive authorization
- **Prototype demonstrated at OGF 20 May 2007 in Manchester**

Future plans

- **Service to a production level**
- **Feedback profile describing our implementation ot the OGF OGSA AuthZ WG**
- **VOMS SAML Profile**

- valerio.venturi@cnaf.infn.it