UNICORE SUMMIT

3rd UNICORE Summit, Rennes, 28.08.2007

omii europe
open middleware infrastructure institute

Using SAML-based VOMS for Authorization within Web Services-based UNICORE Grids

Valerio Venturi, Morris Riedel, Shiraz Memon, Shahbaz Memon, Frederico Stagni, Bernd Schuller, Daniel Mallmann, Bastian Tweddell, Alberto Gianolli, Sven van de Berghe, David Snelling, Achim Streit

Outline

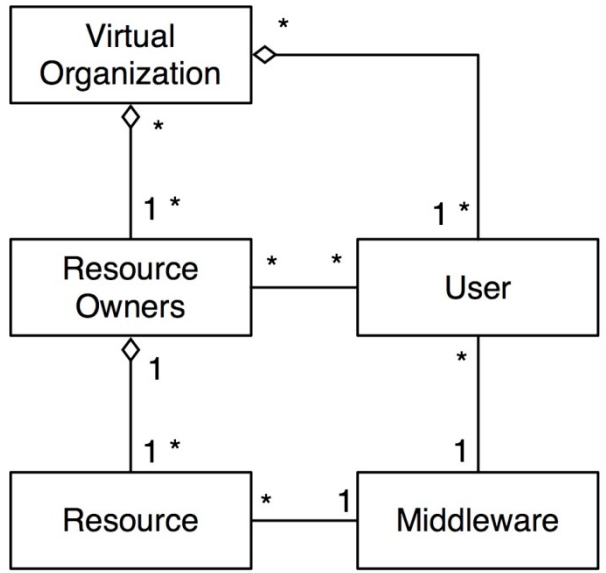
- **Virtual Organizations and their management**
- **The VOMS Technology**
  - VOMS Functionality, Admin Tool, Attribute Authority
- **Authorization standards in the Grid**
  - OGF OGSA-AuthZ, SAML, XACML
- **VOMS SAML Service**
  - Deployment, SAML assertions & attributes
- **Integration of VOMS in UNICORE 6**
  - SAML VOMS AA
- **Roadmap and Use cases in context of UNICORE**
- **Related Work and Conclusion**

Virtual Organizations

- **The 'Grid problem' :**
  - Coordinated resource sharing across dynamic collections of individuals, institutions and resources,
    - **Grids are doing this in flexible Virtual Organizations (VOs)**

[2] Foster et al.

- **Resource owners (ROs) share their resources within the VO**
- **Resources are exposed/accessed by different Grid middleware systems**
- **Users may use any Grid middleware they prefer**
- **Users may or may not have relationships to resource owners**



Virtual Organization Management

- **Resource owners share their resource**
  - But only due to the fact that they maintain control over how the sharing is done (e.g. WHO is allowed to access)
  - Resource owners make sharing agreements within the VO
- **Enabling VO management means…**
  - Providing tools that deal with highly dynamic VO administrations
  - Providing the instruments to facilitate the enforcement of such sharing agreements
- **Today: Shared resources are exposed/accessed by different Grid middleware systems (in different e-Infrastructures)**
  - Common open standards are key enabler of cross-Grid VO management and Grid/e-Infrastructure interoperability

The VOMS Technology

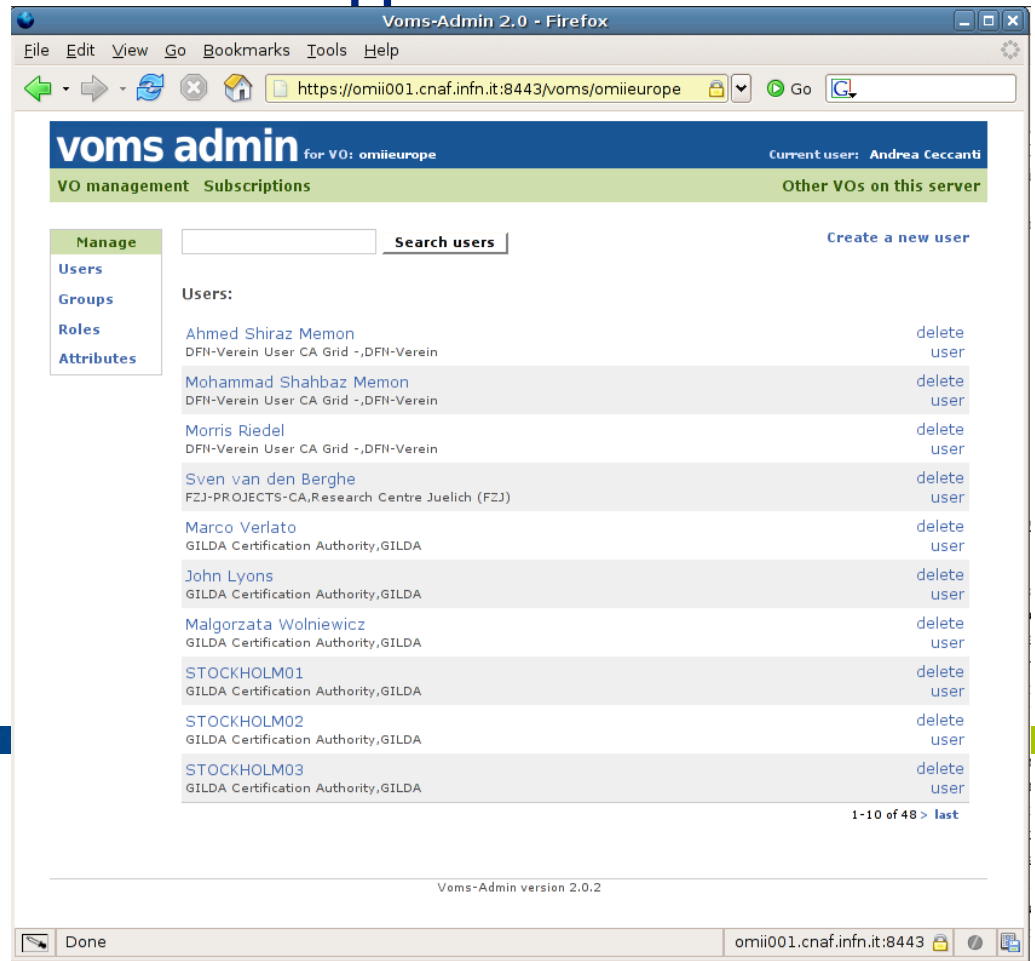
- **VOMS = Virtual Organization Membership Service** [3] Alfieri et al.
  - A tool for doing VO management
  - Originally developed during the European Data Grid and DataTAG collaborations
  - Production version maintained in the EGEE project
  - New open standards integration within OMII-Europe
- **Core components for authorization in middleware stacks**
  - gLite (EGEE) and VDT (OSG)
  - Module available for using it with the Globus Toolkit authorization framework
- **Production version used in Grid Infrastructures worldwide**
  - EGEE, OSG, D-Grid, NAREGI, …

VOMS Functionality

- **VOMS allows to assign users in a VO attributes regarding their 'position' in a VO**
- **Position (attributes) means…**
  - Groups of an user (e.g. LHC, DECI)
  - Project Membership (e.g. OMII-Europe)
  - Roles of an users (e.g. administrator)
  - Any other attributes (e.g. funding_agency_x)
- **These attributes are used for access control by Grid services that are exposing resources**
  - Allows enforcement of agreements between ROs and the VO
  - Resource owners share resources for dedicated groups/project/roles or any other type of defined attributes

VOMS Admin Tool

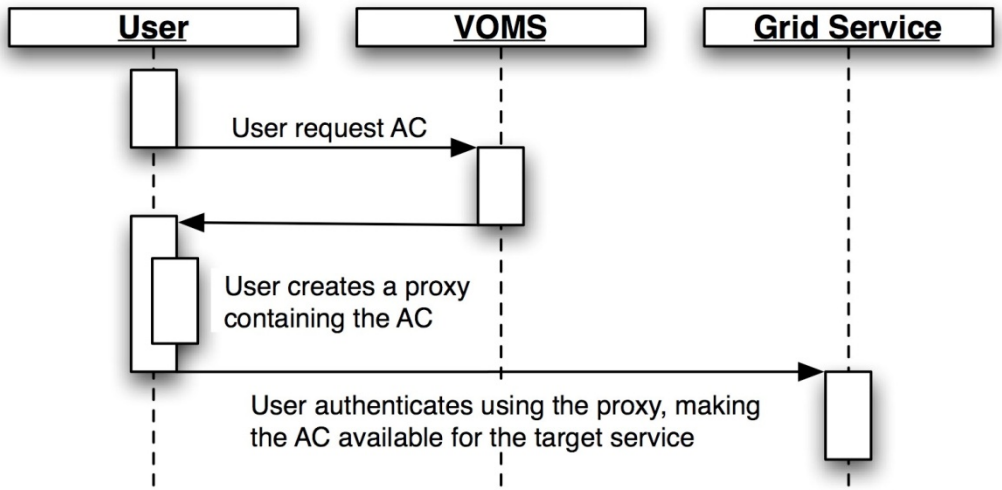
- **Tool allows VO managers to perform administrative operations**
- **A Web service interface is available exposing such operations for easy development of custom admin applications**
- **A ready-to-use Web application enabling …**
  - Users to register
  - VO managers to manage subscriptions
  - VO managers to create and manage groups and assign roles/group membership



omii europe
open middleware infrastructure institute

VOMS Attribute Authority

- **VOMS is an Attribute Authority (AA) that releases signed assertions containing users attributes (groups/roles, etc.)**
- **'AC VOMS' uses Attribute Certificates (ACs) (RFC 3281)** **[1] Farrel et al.**
  - No use of Web services, use of proprietary xml messages
  - Uses GSI for securing communications
- **Mostly, the AC retrieved from the VOMS AA are inserted into the proxy certificates of the user**
- **After authentication with a Grid service, the AC is available for the service to use it for authorization**



Authorization Standards in the Grid

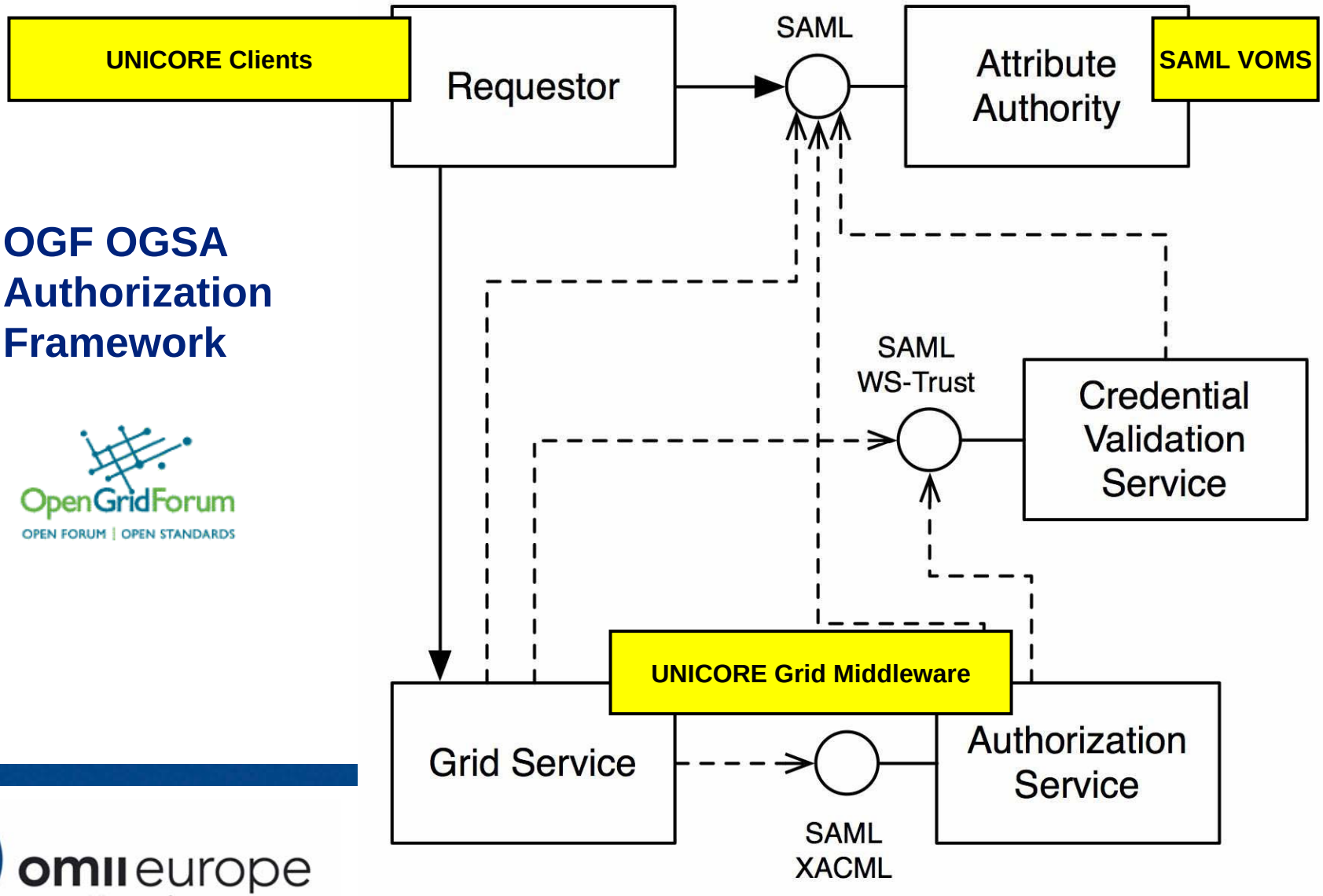
- **OGF OGSA - Authorization (AuthZ) working group**
- **Goal: Leverage existing standardization efforts in the Web Service community and adapt them to Grid Services**
- **Currently focussing on three technologies**
  - Attribute Authority
    - **Based on OASIS Security Assertion Markup Language (SAML)**
  - Authorization Service
    - **Based on OASIS SAML and OASIS Extensible Access Control and Markup Language (XACML), SAML profile for XACML**
  - Credential Validation Service
    - **Based on OASIS SAML**
- **New 'SAML VOMS' implements the SAML-based AA**
  - Working on finalizing the profile but agreements settled

Link to Talk:
Kenneth Klingenstein
Takeaways Open Standards:
SAML & XACML

[6] OASIS Security TC

Overview: Services in Context

- **OGF OGSA Authorization Framework**



OpenGridForum
OPEN FORUM | OPEN STANDARDS

omii europe
open middleware infrastructure institute

SAML (in short) [4] OASIS Security TC

- **XML-based Framework for exchanging security information**
  - User authentication, entitlement, and attribute information
- **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**
  - Protocols that allow to request assertions from SAML authorities
- **Bindings**
  - Mapping from SAML request/response messages into standard messaging or communication protocols (e.g. SOAP)

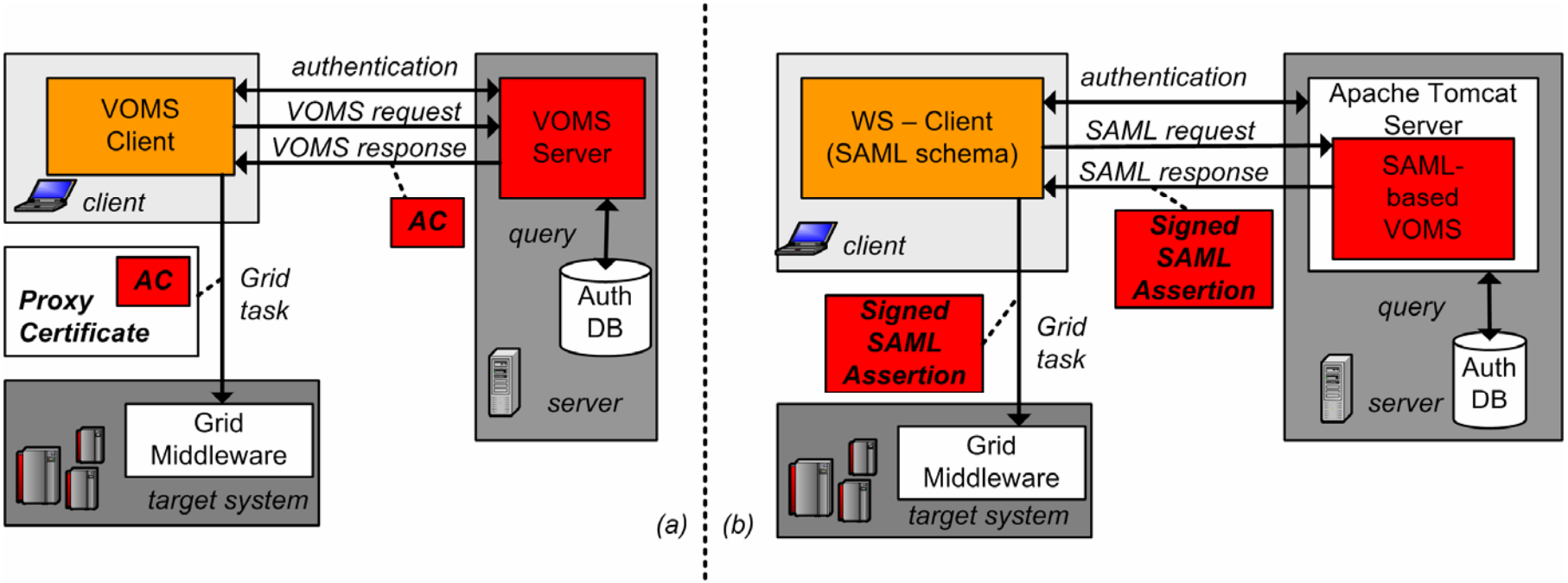
SAML Assertion

<xml>
…
</xml>

VOMS SAML Service (aka SAML VOMS)

- **VOMS has been extended to support authorization standards emerging from the Grid community**
- **The VOMS SAML Service retains the same functionalities of the production AC VOMS**
  - Exposes a Web service interface according to SAML
  - Uses SAML Assertions instead of ACs
- **Can be deployed to any J2EE service container**
  - Apache Tomcat, JBoss, etc.
- **Goal of standard-integration: Grid middleware independence**
  - Enforce the idea that VO management is a task that is inherently Grid middleware independent
  - Allows for cross-Grid VO management

VOMS AC and VOMS SAML Comparison



Proprietary AC VOMS request protocol

New standardized SAML REQUEST looks like this:

```
<wsdl:portType name="AttributeAuthorityPortType„>
   <wsdl:operation name="AttributeQuery">
     <wsdl:input message="tns:AttributeQueryRequest"/>
     <wsdl:output message="tns:AttributeQueryResponse"/>
   </wsdl:operation>
</wsdl:portType>
```

According to:
[5] Randall et al.
„SAML profile for X.509 „ specification

SAML Assertions

- **Example SAML Assertions released by the VOMS SAML Service (some part are missing for brevity)**
- **SAML Assertion indicates for "WHO/WHAT" the assertion is valid (saml:Subject)**

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" … >
    <saml:Issuer> … </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 ASSERTION

Subject Morris Riedel (confirmed per X.509 certificate)

SAML Attributes

- **We have 'Morris Riedel' as subject (user)**
  - So what attributes he has…?!
- **Example VOMS attributes expressed as SAML Attributes…**

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

SAML ASSERTION

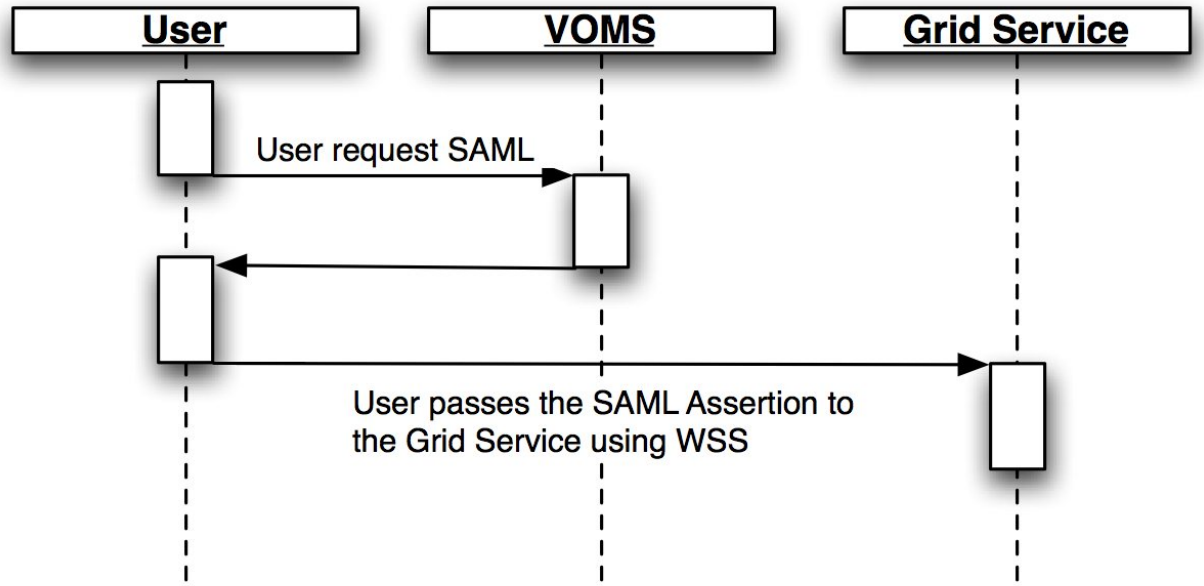
Subject Morris Riedel (confirmed per X.509 certificate)

Attribute /omiieurope (confirmed by VOMS server)

- **Hence: The user is in the omiieurope project**
- **The format for the attributes is going to change…**
  - A VOMS SAML profile is being finalized

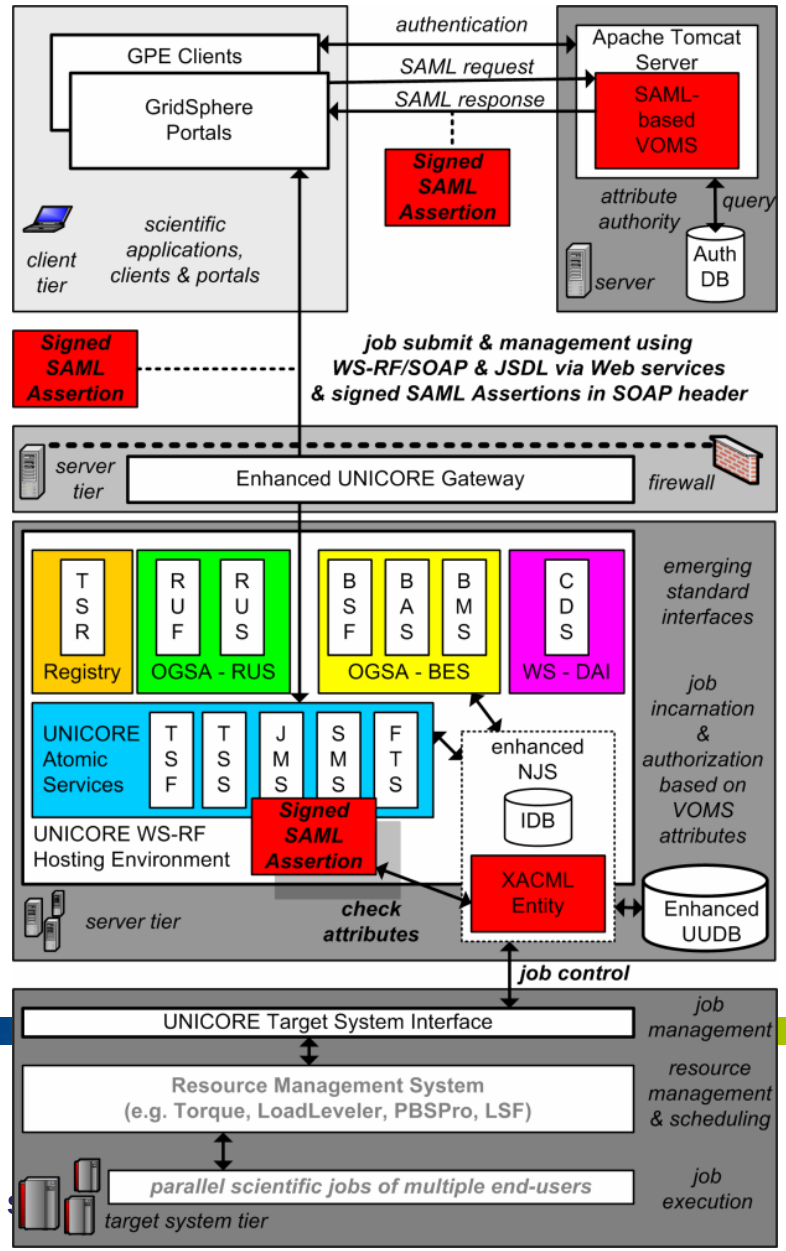
SAML VOMS using WS-Security extensions

- **The coupling of AC and proxy certificates has proved a very efficient way of making attributes available for services**
  - E.g. used in proxy-based gLite and Globus Toolkits
- **Requirement from UNICORE community:**
  - Support Grid middleware not (natively) using proxy certificates
- **SAML assertions in WS-Security extensions (SOAP headers)**



SAML VOMS AA for UNICORE 6

- **UNICORE 6 Client-side**
  - Gridsphere portal or GPE Clients
  - Get a SAML Assertion from the VOMS SAML service
  - SAML assertion is signed by the VOMS SAML service
- **When contacting UNICORE 6…**
  - Client puts the SAML assertion into the header of the SOAP message
  - (using WS-Security extensions)
- **UNICORE 6 Server-side**
  - Grant/Deny access based on SAML assertions of users



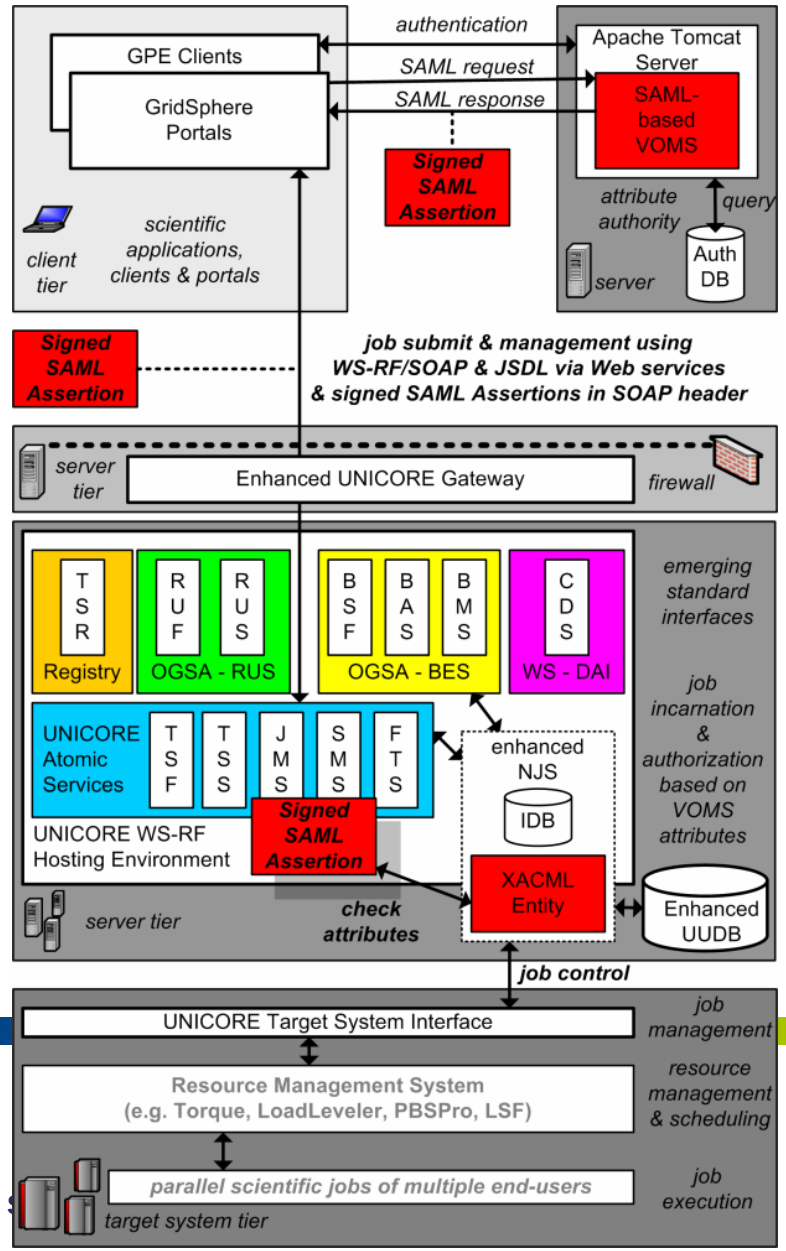
omii europe
open middleware infrastructure institute

Prototype on UNICORE@SourceForge „VOMS-enabled OGSA-BES“

Example of Messages to UNICORE 6

SAML-based SOAP Message to UNICORE 6

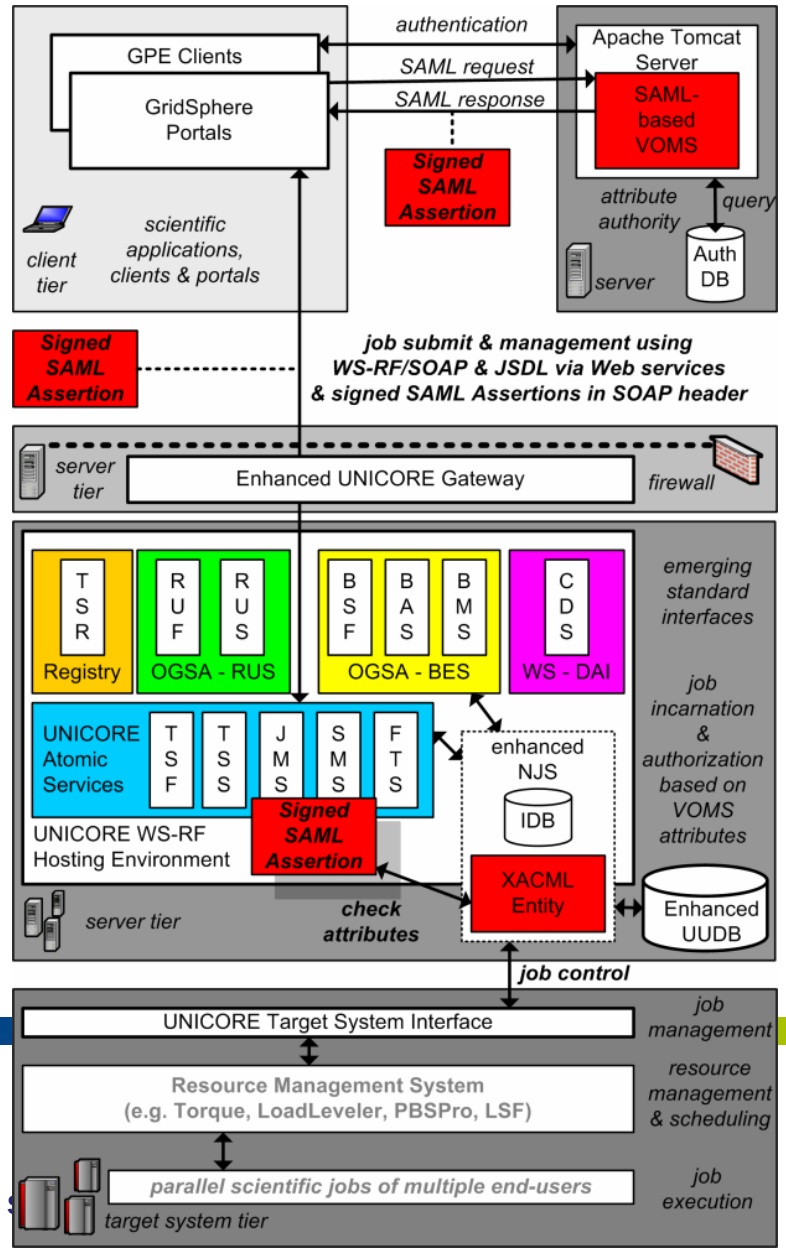
```
<soap:Envelope xmlns:soap="...„>
  <soap:Header>
    <wsse:Security wsse="...„>
      <saml:Assertion xmlns:saml="...">
      ....
      </saml:Assertion xmlns:saml="...">
    </wsse:Security>
  </soap:Header>
  <soap:Body>
  ...
  </soap:Body>
</soap:Envelope>
```



Prototype on UNICORE@SourceForge „VOMS-enabled OGSA-BES“

Attribute-Based AuthZ in UNICORE 6

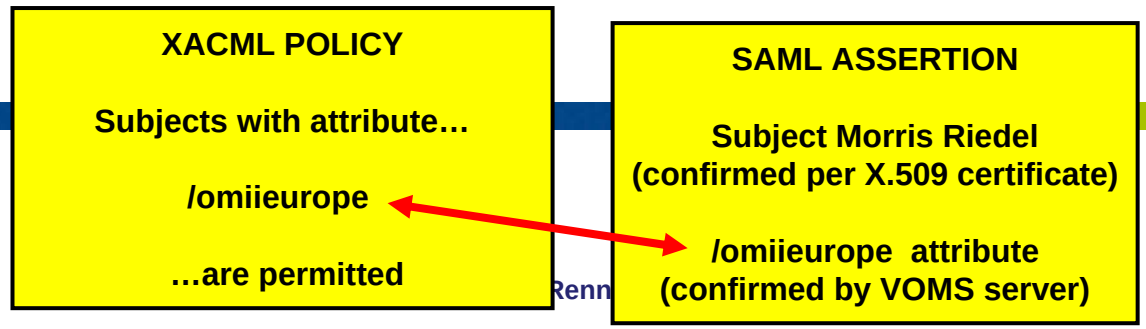
- **UNICORE 6 incorporates a Policy Decision Point (PDP) that uses XACML policies to make authorization decisions**
- **The relevant UNICORE 6 service extracts the VOMS attributes from the SAML Assertion in SOAP header**
  - SAML assertion is used for a request to the PDP along with the action and resource description
  - The PDP check against its set of policies to decide whether the user is allowed to perform the requested action or not



Prototype on UNICORE@SourceForge „VOMS-enabled OGSA-BES“

XACML Policy Example

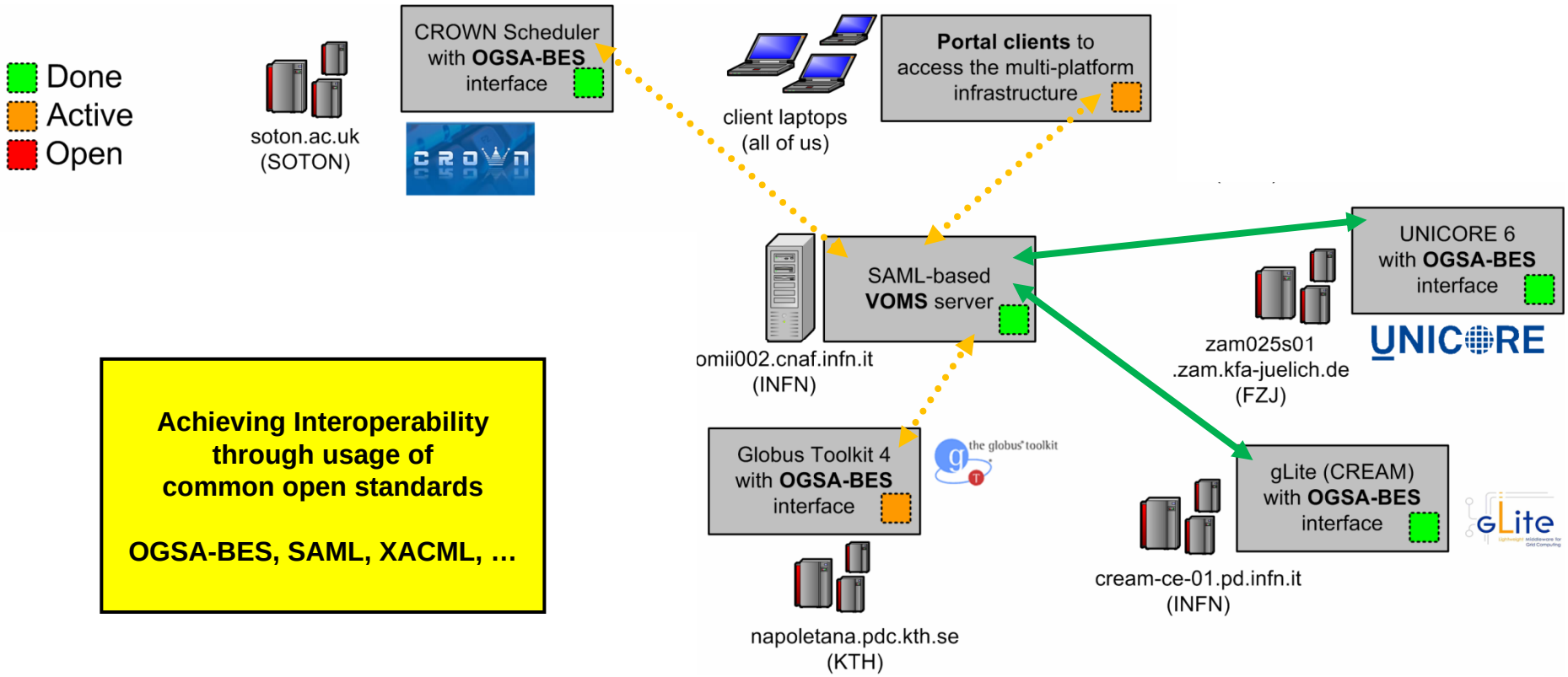
```
<Rule Effect="Permit" RuleId="allow-omiieurope-members"
      xmlns:xacml="urn:oasis:names:tc:1.0:policy"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <Description>Allow users in the omiieurope VO access any service</Description>
   <Target>
      <Subjects>…</Subjects>
      <Resources>…</Resources>
      <Actions>…</Actions>
   </Target>
   <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
         <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="group-membership-id" />
      </Apply>
      <AttributeValue
     DataType="http://www.w3.org/2001/XMLSchema#string">/omiieurope</AttributeValue>
   </Condition>
</Rule>
```



Roadmap and Use case OGSA-BES

- **Production SAML VOMS support is planned for End 2007**
  - Aligned with UNICORE 6.1, starting with delegation scenarios now
- **Production Client integration**
  - GridSphere, but also UNICORE Rich Client Platform Client
  - GPE Support is still matter of ongoing discussions
- **Use case: OGF OGSA – Basic Execution Service (OGSA-BES)**
  - Interface for job submission and management
  - Implemented on top of UNICORE 6 backend (XNJS)
- **Jobs submission requests to the UNICORE OGSA-BES were allowed or denied after possession of groups in a VO**
  - Using the VOMS SAML service as AA
- **Prototype of VOMS integration demonstrated at OGF 20**

OMII-Europe multi-platform Grid infrastructure (proves open standards actually work!)



Towards technical e-Infrastructure interoperability

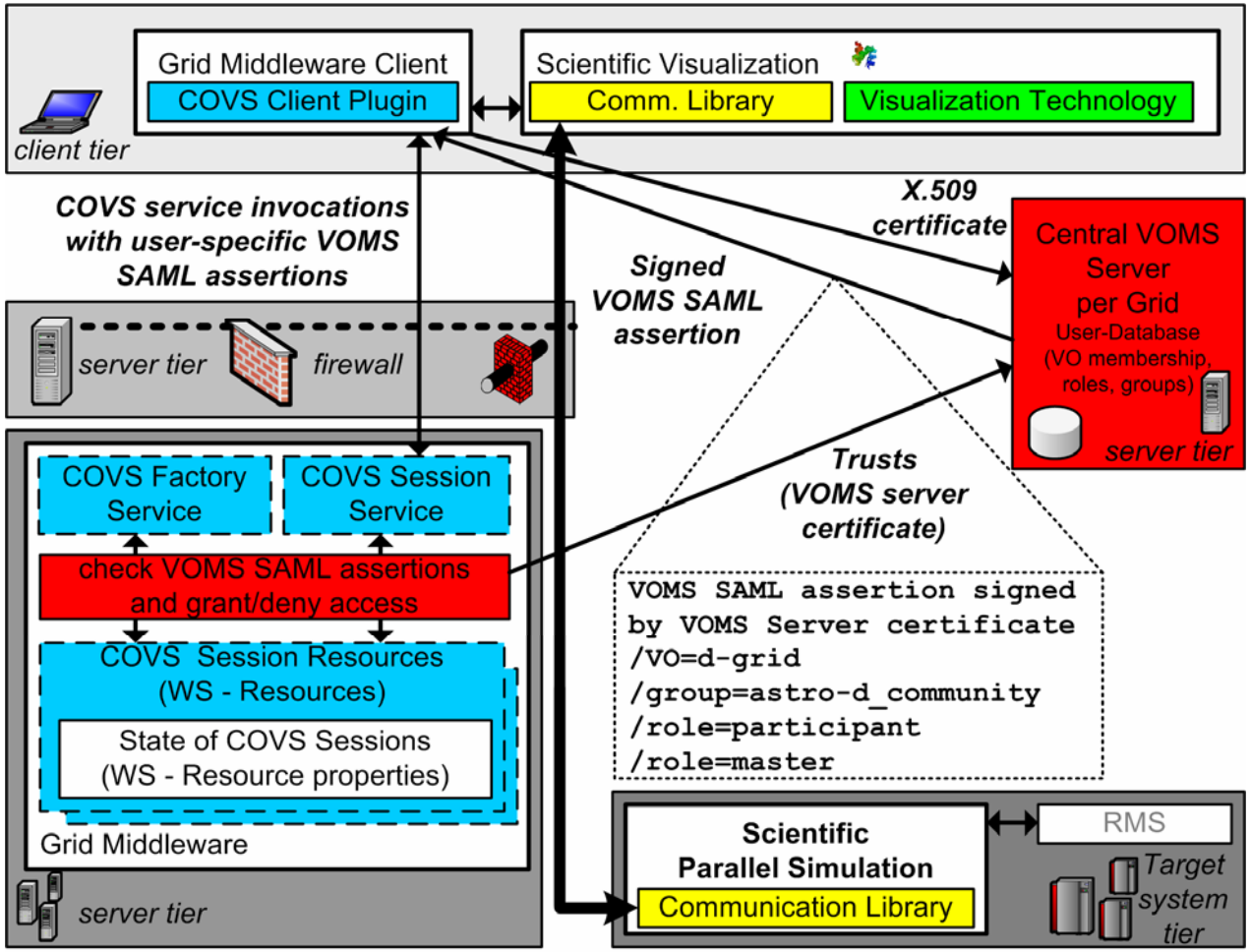
Use Case : RBAC for COVS (planned)

- **UNICORE 6 allows the developments of higher-level application services that work on top of UASs**

  [7] Riedel et al.

  – The Collaborative Online Visualization and Steering (COVS) service allows participants sharing the same visualization session
- **COVS sessions require roles for users to be authorized to the different actions in a visualization session**
  – E.g. add/remove participants of a collaborative session
- **VOMS provides the fine grained access control based on group membership and role-based Access Control (RBAC)**
  – Participant are divided in groups (within D-Grid Astro VO)
  – Assigned roles within groups imply different allowed actions
    - **Start/stop session, steer session, add/remove participants, etc.**

Use Case : RBAC for COVS (planned)



Related Work

Link to talk from Kenneth Klingenstein (Internet-Scale Identity and Collaboration)

- **Shibboleth**
  - Attribute-based authorization framework (among the others)
  - Widely used especially in the education community
  - Also based on SAML
- **IVOM: Interoperability and Integration of VO Management Technologies in D-Grid**
  - Providing VO management solutions for UNICORE 5
  - Focus on the problem of aggregating attributes coming from different sources (e.g. Shibboleth and VOMS as AAs)
  - Using both AC VOMS and soon also SAML VOMS
  - Ongoing collaboration between OMII-Europe VOMS activity and German IVOM project

Link to talk from Wolfgang Ziegler (Attributes and VOs: Extending the UNICORE Authorisation Capabilities)

Conclusion

- **Different versions of VOMS are available soon**
- **AC VOMS (Attribute Certificate-based VOMS)**
  - Releases RFC3821 compliant certificates
  - AC VOMS is used in production and will be still supported
- **SAML VOMS (SAML-based VOMS)**
  - Developed in OMII-Europe
  - Releases signed SAML assertions
  - Intended to be the successor of AC VOMS in production soon
  - Grid middleware independent
- **UNICORE integration with VOMS**
  - Production release at the end of year 2007 (with UNICORE 6.1)
  - Usable by many clients: GridSphere portals, UNICORE RCP, …

References

[1] S. Farrel, R. Housley. *An Internet Attribute Certificate Profile for Authorization.* IETF RFC 3281, April 2002. http://www.ietf.org/rfc/rfc3281.txt.

[2] I. Foster, C. Kesselman, and S. Tuecke. The anatomy of the grid: Enabling scalable virtual organizations. *International J. Supercomputer Applications, 15(3):200–222, 2001.*

[3] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A´ . Frohner, K. Lo¨rentey, and F. Spataro. From gridmapfile to voms: managing authorization in a grid environment. *Future Generation Comp. Syst., 21(4):549–558, 2005.*

[4] OASIS. Oasis security assertion markup language (saml) tc. http://www.oasisopen. org/committees/tc home.php?wg abbrev=security, 2005.

[5] R. Randall, R. Philpott, R. Metz, T. Wisniewsky, S. Cantor,and P. Madsen. Saml attribute sharing profile for x.509 authentication-based systems. www.oasisopen. org/committees/download.php/18058/, 2006.

[6] OASIS. Oasis extensible access control markup language (xacml) tc. http://www.oasis-open.org/committees/xacml, 2005.

[7] M.Riedel et al. Requirements and Design of a Collaborative Online Visualization and Steering Framework for Grid and e-Science Infrastructures. In Proc. of German e-Science Conference, Baden-Baden, 2007.

Questions

Morris Riedel
m.riedel@fz-juelich.de

Valerio Venturi
valerio.venturi@cnaf.infn.it