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

Valerio Venturi[1], Morris Riedel[2], Shiraz Memon[2], Shahbaz Memon[2], Federico Stagni[1], Bernd Schuller[2], Daniel Mallmann[2], Bastian Tweddell[2], Alberto Gianoli[1], Sven van den Berghe[3], David Snelling[3], Achim Streit[2]

[1] National Institute of Nuclear Physics (INFN), Bologna, Italy
[2] Forschungszentrum Juelich (FZJ), Juelich, Germany
[3] Fujitsu Laboratories of Europe (FLE), London, UK

Abstract. In recent years, the Virtual Organization Membership Service (VOMS) emerged within Grid infrastructures providing dynamic, fine-grained, access control needed to enable resource sharing across Virtual Organization (VOs). VOMS allows to manage authorization information in a VO scope to enforce agreements established between VOs and resource owners. VOMS is used for authorization in the EGEE and OSG infrastructures and is a core component of the respective middleware stacks gLite and VDT. While a module for supporting VOMS is also available as part of the authorization service of the Globus Toolkit, there is currently no support for VO-level authorization within the new Web services-based UNICORE 6. This paper describes the evolution of VOMS towards an open standard compliant service based on the Security Assertion Markup Language (SAML), which in turn provides mechanisms to fill the VO-level authorization service gap within Web service-based UNICORE Grids. In addition, the SAML-based VOMS allows for cross middleware VO management through open standards.

1 Introduction

The concept of Virtual Organization (VO), defined as a dynamic collection of individuals, institutions, and resources, emerged as central within world-wide Grid and e-Science infrastructures that deal with the so-called 'Grid problem': flexible, secure, coordinated resource sharing across dynamic, multi-institutional collaborations [1]. Enabling VOs implies requirements for a highly dynamical fine grained access control over shared resources. Resource owners makes agreements with the VO on sharing their resources provided they have control on how the sharing is done.

Enabling VO management means providing instruments to facilitate the enforcement of such agreements. One such instrument is the the Virtual Organization Membership Service (VOMS) [2]. VOMS is an Attribute Authority

(AA) focused on VO management. It allows VO manager to assign attributes to users according to their position in a VO. With position we mean group or project membership, role possession, or generic key value pair attributes. On request VOMS releases signed assertions containing the above described attributes. These attributes are used at the resource level to drive authorization decisions. Thus VOMS supports dynamic, fine-grained access control needed to enable resource sharing across VOs.

VOMS is used for authorization in the EGEE [3] and OSG [4] Grid infrastructures and is thus a core component of the respective middleware stacks, the Lightweight Middleware for Grid Computing (gLite) and the Virtual Data ToolKit (VDT). In addition, a module for supporting VOMS is also available as part of the Globus Toolkit (GT) [5] authorization framework[4]. Hence, all these Grid middleware systems as well as production Grids provide sophisticated VO-level authorization. This can be significantly improved within UNICORE [6] Grids such as DEISA [7]. The absence of VO-level fine-grained authorization within UNICORE motivates our work to support VOMS authorization within the new Web services-based UNICORE 6 Grid middleware. The benefits are two fold. First, it fills the gap of having a VO-level authorization available within UNICORE Grids. Second, it lays the foundation for interoperability with other VOMS-based Grid infrastructures in terms of security and VO management.

This paper describes our work to make VOMS available under UNICORE 6 as it is developed within the Open Middleware Infrastructure Institute for Europe (OMII-Europe) [8]. The paper introduces VOMS and decribe its evolution towards an open standard compliant version based on the Security Assertion Markup Language (SAML) [9]. The core of the paper describes the usage of signed SAML assertions released by the VOMS server with the Web services-based UNICORE 6 Grid middleware. In details, it will describe how the assertions are transported in the Simple Object Access Protocol (SOAP) headers of message exchanges between UNICORE and its clients. In addition, the paper explains how the Extensible Access Control Markup Language (XACML) [10] of OASIS can be used in conjunction with VOMS and its SAML-based assertions to realize fine-grained authorization decisions within UNICORE.

The remainder of this paper is structured as follows. Section 2 presents the evolution of VOMS toward open standards and its adoption of SAML. How UNICORE 6 is capable of using VOMS as AA is described in Section 3, and in Section 4 we provide a use case scenario of how this newly developed VOMS support in UNICORE can be used by higher-level services. Related work is addressed in Section 5. The paper closes with some concluding remarks.

[4] http://dev.globus.org/wiki/VOMS

2 Evolution of Virtual Organization Membership Services

VOMS was originally developed in the framework of the European Data Grid and DataTag collaborations to solve the problem of granting Grid users authorization to access resources within a VO scope, enabling the high fine-grained, complex level of access control needed for sharing agreements in a VO. VOMS allows services to drive authorization decisions based on the position of the user in a VO. In the last years, VOMS has been developed within the EGEE project. It is a basic component of the EGEE Grid middleware, gLite and it is used in many Grids world-wide (OSG, D-Grid, NAREGI). A module for using VOMS for authorization is available with the Globus Toolkit.

In more detail, VOMS is a system for managing the user's membership and position in a VO, such for example as group membership and role possession. These information are used by Grid services to allow for access control. VOMS has a Web-based administrative interface as well as command-line tools to administer the VO: add and delete users, create groups, assign roles or other attributes. The core component is an AA that releases signed assertions containing user's attributes holding the position of the user in the VO. In the server that is used in production today, these attribute are carried in Attribute Certificates (ACs) compliant to RFC 3821 [11]. In the most adopted usage pattern, the AC is inserted in an extension of proxy certificates of the users, as shown in 1(a). When the user authenticates with the Grid services, the services extract the AC from the proxy and authorize the access to the resource based on the these attributes.

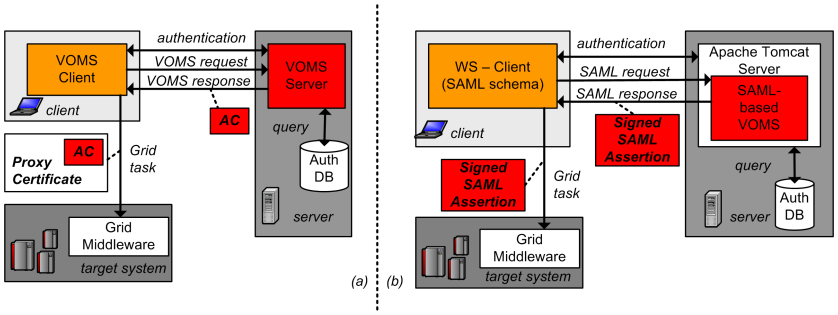

Fig. 1. VOMS server releases Attribute Certificates (a) or signed SAML assertions (b).

Within the OMII-Europe project, the VOMS server is being re-engineered to support standards emerging from the Grid community. The OGSA Authorization Working Group of the Open Grid Forum (OGF) has been working on recommendations for standardization of authorization related services. Following the work in the OMII-Europe project, the working group is defining a specification for a profile for attributes retrieval services based on OASIS SAML. The VOMS SAML Service implements that specification. The aim of the standardization activity in the OMII-Europe project is to have a VO management solution across different middleware distributions. The VO management services is part of a wider activity of re-engineering by the OMII-Europe project that aims at interoperability across of selected basic component of different grid middlewares such as UNICORE, gLite and GT. Components being re-engineered are for example Job Submission services (OGSA-BES [12]) and Data Access services (OGSA-DAI [13]).

The VOMS SAML Service is a Web service implementing protocols and binding defined in the SAML set of specifications [14] [15]. A prototype is available on the OMII-Europe Evaluation Infrastructure. The VOMS SAML Service uses Axis as SOAP implementation and can be deployed in a service container such as Tomcat. The package does not provide an API, with the aim of letting each consumer use their preferred Web services tools. The distribution comes with examples of consuming the service using popular SOAP implementations such as Axis, XFire, gSOAP, ZSI.

3 Using SAML-based VOMS with UNICORE 6

VOMS is used within gLite (EGEE), VDT (OSG), and GT (TeraGrid), mainly by using RFC 3821 compliant ACs within a proxy certificate of end-users. This usege pattern makes VOMS widely adopted with middlewares that uses proxy certificates, but not as widely adopted in middlewares using end-entity certificates such as UNICORE. Therefore, it becomes very helpful that the newly developed VOMS server is releasing SAML-compliant assertions that are independent from proxy certificates and thus can be used in environments that use end entity certificates. This paragraph describes how this is done in a way that VOMS can be used as AA for UNICORE Grids, including details about the authorization decisions based on VOMS attributes as shown in Figure 2.

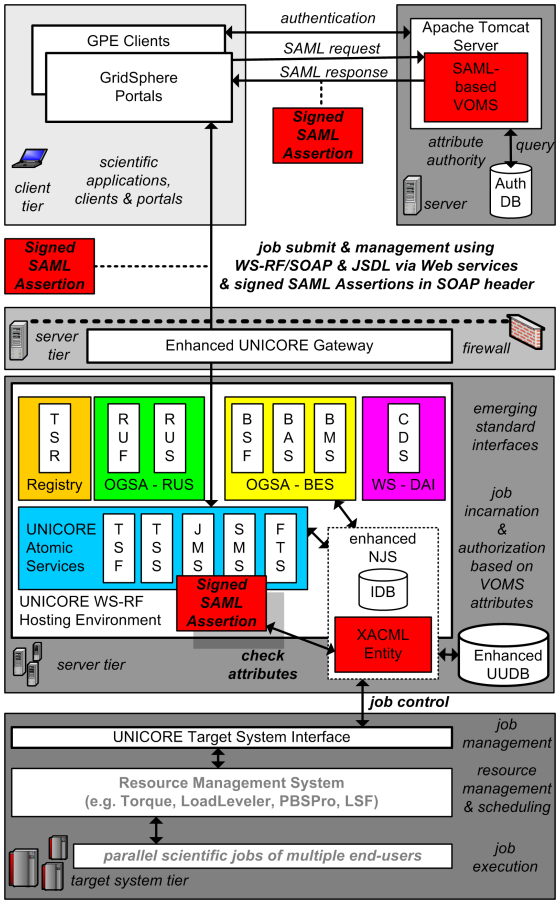

Fig. 2. VOMS acts as a AA for UNICORE 6 and releases signed SAML assertions with VOMS attributes. Based on these attributes, XACML policies are used to realize authorization decisions within the UNICORE 6 backend.

3.1 VOMS as Attribute Authority for UNICORE

Figure 2 shows how we have used VOMS as an AA for the Web service-based UNICORE 6 Grid middleware. The client retrieve a SAML assertion from the VOMS SAML Service. While proxy certificates proved a very effective way of tranporting ACs, we found that the most natural way of transporting SAML assertions is in the SOAP Header of Web services messages as shown in Figure 3. A similar mechanism is described in the OASIS Web Services Security set of specification.

```
<soap:Header xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 <wsa:To>http://...services/BESFactory?res=defaultbesfactory</wsa:To>
 <wsa:Action>http://.../BESFactoryPortType/CreateActivity</wsa:Action>
 <wsa:MessageID>...CBA4</wsa:MessageID>
 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="_ec36fa7c396ka4nqa91jst"
   IssueInstant="2007-04-22T14:34:10.059Z"
   Version="2.0"
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   CN=omii002.cnaf.infn.it,L=CNAF,OU=Host,O=INFN,C=IT
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   ...
  </ds:Signature>
  <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:SubjectConfirmation
    Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
   ...
  </saml:SubjectConfirmation>
  <saml:Conditions NotBefore="..." NotOnOrAfter="..." />
  <saml:AttributeStatement>
   ...
  </saml:AttributeStatement>
 </saml:Assertion>
</soap:Header>
```

Fig. 3. SAML-based assertions released from the VOMS server are transferred within the SOAP header of Web service message exchanges between UNICORE and its clients.

3.2 Authorization Decisions in UNICORE based on XACML

Figure 2 also shows how SAML assertions from the VOMS are used during authorization decisions in conjunction with XACML policies. UNICORE 6 incorporates a Policy Decision Point (PDP) that uses Extensible Access Control Markup Language (XACML) policies during authorization decisions in conjunction with the UNICORE User Database (UUDB). In the context of VOMS, these XACML policies can be used to make attribute-based authorization decisions based on SAML assertions released from the VOMS server and that are transported to UNICORE within the SOAP header. Part of these assertions are *saml:AttributeStatement* elements that provide values for Fully Qualified Attribute Names (FQANs) stating role possession or group/project membership as shown in Figure 4. Finally, the SAML-based assertions are signed with the certificate of the VOMS server, which can be verified at the resource level to check if the assertion comes from a trusted VOMS server.

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

Fig. 4. Simple example of an VOMS FQAN (group-membership-id with value omiieurope) encoded in an saml:AttributeStatement element within a saml:Assertion element. In this context an XACML policy can be defined within UNICORE that only allow members of the omii-europe group to access the requested service.

4 Use Case Scenario: Role-based Authorization in Collaborative Visualization and Steering Sessions

UNICORE 6 is easily extensible and allows for the development of higher-level services that work on top of the UNICORE Atomic Services (UAS) [16]. One of these services is the Collaborative Online Visualization and Steering (COVS) [17] Grid service that allow multiple participants sharing the same visualization session. COVS sessions support multiple roles for users and thus is a good proof of concept of how VOMS can be used for role-based authorization in UNICORE 6.

The master role is the initiator of a COVS session and is able to configure different setups during a session that can not be done by usual participants. A person that acts in this role uses the Grid middleware client and its COVS plugin to access the COVSFactory service. The COVSFactory service creates in turn a COVS session resource, which includes the startup of components realizing the communication between a parallel simulation on supercomputers or clusters and visualization clients. The participant role on the other hand is defined as any person that participates in a COVS session, which also includes the person in the master role. End-users that want to participate also use the Grid middleware client to join a COVS sessions, but are not allowed to create a session.

In this context, VOMS provides fine-grained authorization based on different roles or on group memberships. Therefore it can be used to control which users are able or not able to participate (e.g. a research group named astro-d configured within the VOMS server is allowed to share the view of a visualization or normal participants are usually not allowed to submit computational jobs). The VOMS server can release signed SAML assertions with role attributes checked at service-level at the COVSFactory and COVSSession service as shown in Figure 5.

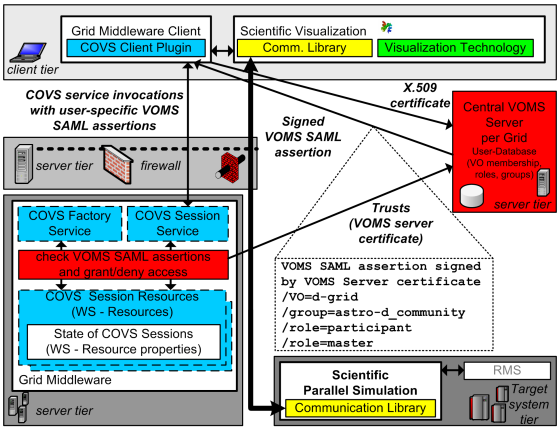

Fig. 5. Using the SAML-based VOMS to manage different roles in COVS sessions.

5 Related Work

The other main AA within Grids is Shibboleth, a tool that provides a federated single sign-on and attribute exchange framework, mainly used in the education community. GridShib is a software product that allows for interoperability between GT and Shibboleth, thus making the latter available for Grid authorization. GridShib project members are working on an OASIS standard for a deployment profile for X.509 subject to use with SAML 2.0. This profile complements the SAML specifications with indications on how to use SAML with X.509 certificates. Therefore, members from the GridShib and VOMS teams have agreed within the OGF OGSA Authorization WG that this specification in combination with SAML 2.0 is the specification for AA services. To sum up, it is expected that GridShib and VOMS follow the same standard interface for message exchanges as well as assertions and thus the work describes in this paper should work not only with VOMS but also with GridShib, except the different policy definitions that are dependent from the correspondent attribute formats. In addition, VOMS and Shibboleth use the same Internet2 OpenSAML toolkit source code. VOs and authorization based on information about the role of users within VOs are missing concepts in production UNICORE 5 today. UNICORE 5 also lacks support for using attributes of a user retrieved from his home institution. Overcoming these limitations is part of the IVOM project [18] that is part of the German D-Grid Initiative [19]. In contrast to our work that rely on UNICORE 6 and the SAML-based VOMS server, the IVOM project develops solutions for UNICORE 5 and the Attribute Certificate-based VOMS server.

6 Conclusions

An initial prototype of using the SAML-based VOMS in conjunction with UNICORE 6 was shown at OGF20 at the OMII - Europe booth and is currently further improved within the evaluation infrastructure of OMII-Europe.

This in particular fills the gap of UNICORE's limited VO-level authorization functionality since the new SAML-based VOMS server is independent from gLite and thus can be used by purely UNICORE Grids as Attribute Authority.

We have further shown that a VO is now capable to offer its end-users both high throughput computing resources (nodes in a farm running gLite) and high performance resources (supercomputers running UNICORE) if the middleware provide services that are compliant to emerging standards interfaces such as OGSA-BES or WS-DAIS. In other words, this work has a significant impact regarding the interoperability between UNICORE and gLite primary, but also Globus can be configured to use VOMS and thus VOMS can act as an AA for VOs to use cross-middleware Grid resources.

Finally, even if interoperability is technically possible, the adoption of these new developed components within production e-Infrastructures such as DEISA or EGEE is rather slow. However, it is expected that UNICORE 6 and thus the support for the new SAML-based VOMS server will considered as the next production version within these e-Infrastructures.

Acknowledgements

This work is partially funded by the OMII-Europe project under EC grant RIO31844-OMII-EUROPE, duration May 2006 - April 2008.

References

1. Foster, I., Kesselman, C., Tuecke, S.: The Anatomy of the Grid: Enabling Scalable Virtual Organizations. International J. Supercomputer Applications **15**(3) (2001)
2. Alfieri, R., Cecchini, R., Ciaschini, V., dell'Agnello, L., Frohner, Á., Lörentey, K., Spataro, F.: From gridmap-file to voms: managing authorization in a grid environment. Future Generation Comp. Syst. **21**(4) (2005) 549–558
3. Enabling Grid for E-sciencE, http://www.eu-egee.org/.
4. Open Science Grid, http://www.opensciencegrid.org/.
5. The Globus Toolkit, http://www.globus.org/toolkit.
6. Streit, A., Erwin, D., Lippert, T., Mallmann, D., Menday, R., Rambadt, M., Riedel, M., Romberg, M., Schuller, B., Wieder, P.: (UNICORE - From Project Results to Production Grids) Elsevier, L. Grandinetti (Edt.), Grid Comp. and New Frontiers of High Performance Proc., pages 357–376, 2005.
7. DEISA - Distributed European Infrastructure for Supercomputing Applications, http://www.deisa.org.
8. The Open Middleware Infrastructure Institute for Europe, http://omii-europe.org/OMII-Europe/.
9. OASIS Security Services (SAML) TC, http://www.oasis-open.org/committees/security.
10. OASIS eXtensible Access Control Markup Language (XACML) TC, http://www.oasis-open.org/committees/xacml.
11. S.Farrell, R.: An Internet Attribute Certificate Profile for Authorization (2002) http://www.ietf.org/rfc/rfc3281.txt.
12. OGSA Basic Execution Services WG, http://forge.gridforum.org/projects/ogsa-bes-wg.
13. Database Access and Integration Services (DAIS) , https://forge.gridforum.org/sf/go/proj1070.
14. Cantor, S., et al.: Assertions and Protocols for the Security Assertion Markup Language (SAML) V2.0 (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
15. Cantor, S., et al.: Bindings for the Security Assertion markup Language (SAML) V2.0 (2005) http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.
16. Riedel, M., Mallmann, D.: Standardization Processes of the UNICORE Grid System. In: Proceedings of 1st Austrian Grid Symposium 2005, Schloss Hagenberg, Austria, Austrian Computer Society (2005) 191–203
17. Riedel, M., Eickermann, T., Frings, W., Dominiczak, S., Mallmann, D., Dssel, T., Streit, A., Gibbon, P., Wolf, F., Schiffmann, W., , Lippert, T.: Design and evaluation of a collaborative online visualization and steering framework implementation for computational grids. (Proc. of the 8th IEEE/ACM International Conference on Grid Computing (Grid 2007), Austin, Texas, to appear)
18. Interoperability and Integration of VO-Management Technologies in D-Grid, http://www.d-grid.de/index.php?id=314&L=1.
19. D-Grid Initiative, http://www.d-grid.de/index.php?id=1&L=1.