Trust Issues in Shibboleth-Enabled Federated Grid Authentication and Authorization Infrastructures Supporting Multiple Grid Middleware

Christian Grimm and Ralf Groeper
RRZN, Leibniz Universität Hannover
Hannover, Germany
{grimm, groeper}@rvs.uni-hannover.de

Siegfried Makedanz and Hans Pfeiffenberger
Alfred Wegener Institut
Bremerhaven, Germany
{siegfried.makedanz, hans.pfeiffenberger}@awi.de

Peter Gietz and Martin Haase
DAASI International GmbH
Tübingen, Germany
{peter.gietz, martin.haase}@daasi.de

Michael Schiffers
Ludwig Maximilian University Munich
Munich, Germany
schiffer@nm.ifi.lmu.de

Wolfgang Ziegler
Institute for Algorithms and Scientific Computing
Fraunhofer Gesellschaft
Sankt Augustin, Germany
wolfgang.ziegler@scai.fraunhofer.de

Abstract

In Germany's D-Grid project numerous Grid communities are working together to develop a common overarching Grid. One major aim of D-Grid is thus to integrate the existing Grid deployments and make them interoperable. The major challenge in this endeavor lies in the heterogeneity of the current implementations: Three Grid middleware and different VO management approaches have to be orchestrated to achieve the intended interoperability. This paper presents some of the findings of the IVOM project regarding VO management technologies. Furthermore, options are discussed for making Shibboleth federations and VO management systems interoperable so that attributes from both sources can be used for authentication and authorization in Grids. Finally two approaches, one using a so called "trust proxy" and one without trust proxying, are presented and support by current Grid middleware is discussed.

1. Introduction

The D-Grid subproject *Interoperability and Integration of VO management Technologies in D-Grid* (IVOM) [4] aims at evaluating currently deployed VO management technologies, assessing solutions developed by international VO management projects and designing a D-Grid wide VO management infrastructure based on these findings as well as identifying remaining gaps.

Germany's D-Grid initiative [3] consists of multiple community Grids from different fields of science and different industrial sectors. It is envisioned to use a common Grid infrastructure shared by all these community Grids, similar to using a common network, the internet. As a prerequisite, it is necessary to ensure that these Grids are interoperable among each other and, preferably, with international Grids for comparable communities. One challenge lies in the fact that the Globus Toolkit 4 [7], both in its web service and its pre-WS flavor, different versions of LCG/gLite [16] and UNICORE [17] are being used by German Grid communities. All of these have different authentication and authorization schemes.

Furthermore, a Germany-wide Shibboleth [13] federation mainly for academic use is being build by Germany's National Research and Education Network (DFN) [5]. Information about users stored in this federation can also be used for authentication and authorization on Grid resources as well as for VO management.

This paper first describes some challenges for authorization in Grids and presents principle approaches for conquering these challenges. Then, two of several identified implementations of these approaches are presented and discussed. Finally some related work is being presented and a conclusion drawn.

2. Challenges for Authorization in Grids

2.1 Identity- and Attribute-based Authorization

Many current authentication and authorization infrastructures (AAI) for Grids are using basic authorization mechanisms based on the *distinguished name* (DN) of the user's X.509 certificate. As the *grid security infrastructure* (GSI) [8] is based upon X.509 proxy certificates derived from X.509 user certificates the information about a user's DN is always available on Grid resources where the user himself or other Grid services acting on his behalf need to be authenticated and authorized. It was thus the obvious choice not only to authenticate the user based on this information but also to base authorization decisions on it as long as no further attributes describing the user, his roles and affiliations, are available on the resource. One implication of this authorization scheme is that the DNs of all users that potentially have access to a resource must be contained in a `grid-mapfile` and additionally a local account for each of these users must be available. It is obvious that such a solution is not very scalable for large amounts of users.

Attribute-based authorization needs at least two additional components compared to the identity-based approach: First it needs an *attribute authority* (AA) which issues such attributes in a trusted way and second it needs *policy decision points* (PDP) actually using these attributes for authorization decisions (see also the work in OGF's OGSA-Authz-WG [1]).

This approach is more scalable than the identity-based one, but at the current time it is widely deployed only by gLite-based Grids and limited to the hierarchical model of fully qualifies attribute names (FQAN), containing VO membership, groups, roles and capabilities within that VO. It does not allow for arbitrary attribute types such as nationality or affiliation to a real organizational unit to be managed or used for authorization.

2.2. Campus and VO Attributes

As we have identified a need for attribute-based authorization on Grid resources the next question that arises is, where these attributes are managed and who issues them in a trustworthy way so that Grid components can make authorization decisions based upon them. The first logical source of attributes is a VO management system such as VOMS [12] or myVocs [18]. These systems manage a list of members of a VO and the users' roles within that VO.

Additionally, there is another source of users' attributes which can also be used for authorization of users on Grid resources: As Shibboleth federations emerge to make users' attributes available across organizational boundaries, it is the next logical step to make these attributes available to Grid resources for both user management within Virtual Organizations and for authorization purposes on Grid resources. Such attributes can e.g. describe a user's affiliation to an institution or a project.

So there are now two attribute authorities instead of one: In addition to the existing Virtual Organization management systems there is the user's Shibboleth identity provider (IdP) at his home organization. These two attribute authorities issue different kinds of attributes:

Campus attributes are user attributes managed by their respective home institution. They identify and describe the user, e.g. by containing name, nationality or telephone number or his affiliation to organizational units and his roles within these units (e.g. professor at a faculty or student of a certain study course).

VO-Attributes describe membership, roles and capabilities within a VO. In this paper we assume that these attributes are managed by a dedicated VO management system, e.g. based on VOMS (with or without VOMRS [20]) or myVocs.

2.3. Trust Issues

In Shibboleth, trust is based on the respective federation policy and corresponding contracts between members and the federation. In addition special arrangements may be made between IdPs and Service Providers (SP). In practice, trust is utilized when an IdP releases user attributes at the request of a known SP and signs the assertion to confirm the reliability of the information contained. In other words: Information is requested, released and consumed in a bilateral, trustful communication process. VO management in Shibboleth as outlined above adds a third role to the process.

The Shibboleth-based VO management systems available today intermediate the user's IdP to a SP. This can be done in two ways, which are fundamentally different regarding trust issues:

(i) The home IdP's original assertion is transported to the Grid resources alongside the attributes asserted by the VO, thus preserving the different sources of authority.

(ii) The VO management service extracts the campus attributes and includes them in its own assertion together with the VO attributes. In this case the VO management service acts as a *trust proxy*. Regarding trust and responsibility the VO (or rather it's operating institution) would also be held accountable for the validity of campus attribute values.

The first solution has the advantage that the assertion the user's home IdP created is passed on unchanged and can be evaluated independently. We see this as the best practice currently feasible as all attributes will be issued and thus signed by their responsible authority.

The second solution leads to a core problem in distributed systems: *Who do you trust to say what about what or whom?* Here, the VO acts as if it were the authoritative source also for attributes stemming from a campus IdP. We consider this to be a bad practice and to be potentially dangerous for each VO provider as well as for the trust fabric of a federation in its entirety. As we will see later technical issues will, under some circumstances, force us to nevertheless offer such an approach to the D-Grid communities if no other solution is available.

3. Approaches for Combining Campus Attributes and VO Attributes in Grids

3.1 Prerequisites

The concepts presented in this paper rely on two main premises:

First, campus attributes are made accessible by a Shibboleth federation, i.e. by providing a Shibboleth IdP at each participating institution. In Germany the academic sector is building such an infrastructure, the DFN-AAI led by the German DFN Verein.

Second, VO management is done by using an appropriate VO management tool. Regarding authentication and authorization it is a basic requirement that the VO management tool can effectively act as an attribute authority, i. e. it can issue attributes in a trusted way.

Furthermore, the Grid middleware utilized must have components that are able to verify and evaluate the attribute assertions issued by the aforementioned attribute authorities to be able to make authorization decisions based upon them.

3.2. Shibboleth and VO Management

Shibboleth's federation model is two-tiered. The core concept of Shibboleth-based authorization is to have a single source of authority per user, which is the IdP, based on the identity management at the user's home institution. A Service Provider requiring a user's authentication and/or making an authorization decision based on the user's attributes may only request that user's attributes from a single Identity Provider.

With the wide acceptance of Shibboleth it was adapted in authentication and authorization realms outside the space of inter-institutional sharing of web resources. One such field is Grid AAI. The representation of Virtual Organizations in Shibboleth is a major issue for the integration of Shibboleth and Grid middleware. The "Grid problem" – as the specific challenge that underlies the Grid concept – has been identified as flexible, secure, coordinated resource sharing and problem solving among dynamic collections of individuals, institutions, referred to as Virtual Organizations (VO)[9].

A Virtual Organization is a source of authority of its own. Users have specific roles in it and it confers specific rights to users. So, to make a well-informed access control decision based on all available attributes of a user, a SP would have to request attribute assertions from the home institution *and* the VO. The current Shibboleth architecture does not support such attribute aggregation.

Therefore the additional source of authority had to fit into the given model. Based on previous work by Von Welch [22], the MAMS project [14] and the myVocs project four options were identified to achieve this:

(i) VO management at the home institutions, based on participant's agreement on attributes, VO-specific information is located at the member's home institution. It is a moot point if institutions would accept modifications in their identity management systems. However, the major problem is trust (see chapter Trust Issues below): the home IdP is generally not the authoritative source for this information.

(ii) The VO operates its own IdP including campus attributes of the users. This means extra work to run separate Identity Management (IdM) systems and services. This approach would undermine the advantages of the Shibboleth concept of identity federation.

(iii) Decentralized VO management: VO attributes are centrally managed by the VO and stored distributed in the institutional IdM systems. The Internet2 tools Grouper and Signet may be the appropriate provisioning tools in the future. This approach would need a new set of trust relations and associated policies, e.g. on attribute or namespace usage. A proof of concept is an open issue.

(iv) IdP Proxy: VO management hooks into the communication flow between IdP and SP by acting as a SP when facing the IdP and acting as an IdP when facing the SP. Thereby it gathers the user's home attributes, adds the VO-specific attributes and presents the resulting conglomerate assertion to the SP. This is the solution chosen by the developers of myVocs and IAMSuite [15], the MAMS VO system.

The management of Virtual Organizations was originally not on the agenda of the Shibboleth architects. This is currently changing, as a discussion about linking multiple attribute authorities has begun. It is especially encouraging to see this being discussed with special attention to trust issues [2]. This proposal about gathering attributes from a number of IdPs is applicable to the question of integrating VO management systems into the Shibboleth architecture.

3.3. Bridging Shibboleth and the GSI

GridShib [19] is a collection of software aimed at allowing Grid resources to make authorization decisions based on attributes managed by Shibboleth federations, i.e. by Shib-

Features	myVocs	VOMRS/VOMS
A. Profile		
1. Primary Grid ecosystem	Globus Toolkit GridShib	gLite Globus Toolkit
2. AAI base	Shibboleth	X.509 PKI
3. Release state (April 2007)	Beta	Stable
4. Software base	Sympa	VOMS
5. Maintainer	UAB	INFN
B. Interoperability with Grid Middleware		
1. Compatibility with GT2 /GT4 pre-WS Services	-	-
2. Compatibility with GT4 WS services with GridShib	X	X
3. Compatibility with gLite	-	X
4. Compatibility with Unicore5	-	-
5. Compatibility with Unicore6	X	X
6. Compatibility with GridShib	X	X
D. Interoperability with Short Lived Credential Services		
1. Supports own SLCS (one SLCS per VO server)	X	-
2. Supports central SLCS (e.g. EUGridPMA accredited DFN-SLCS)	X	X
E. Handling of IdP Assertions		
1. Attributes imported from IdP assertion to identify user	eduPersonPrincipalName, mail	n/a
2. Additional attributes imported from IdP assertion	all attributes released to myVocs by an IdP	n/a
3. Embedding of original IdP assertion in VO assertion	-	n/a
F1. Issuing of VO Attributes: SAML Assertions		
1. Issuing of VO assertions	X	n/a
2. Attributes used to represent VO membership	ePPN, mail from eduPerson; a custom "group" attribute in the format *role@vo*	n/a
3. Additional attributes included in VO assertion	-	n/a
F2. Issuing of VO Attributes: Attribute Certificates		
1. Support of Attribute Certificates	n/a	X
2. Representation of VO membership	n/a	FQAN
3. Additional attributes included	n/a	since VOMS 1.7: arbitrary Attribute-Value Pairs

Table 1. VO Management Systems Compared

boleth IdPs, being developed as part of the Globus Project. Furthermore it includes functionalities to enable users to access Grid resources without the need for long-lived certificates issued by a certificate authority (CA). The four main components of GridShib are:

GridShib for Globus: This component includes a Policy Decision Point (PDP) for web service-based components of the Globus Toolkit 4 such as WS-GRAM and RFT. This PDP makes authorization decisions based on Shibboleth attributes. It is not yet possible to make authorization decisions solely based upon Shibboleth attributes: As there is no concept in the Globus Toolkit similar to gLite's pool-accounts there is still need for a one-to-one mapping of Grid identities to local accounts. This shortcoming will be solved in the soon to be released Globus Toolkit 4.2.

GridShib for Shibboleth: This component has to be installed together with the Shibboleth federation's IdPs if attribute pull on the Grid resources is used. As we rely on attribute push solely in this paper this component will not be further considered.

GridShib CA: This component is a Shibboleth service provider (SP) used to issue short lived certificates (SLC), which users use instead of long-lived user certificates to access GSI-based Grid resources. A service issuing SLCs is called a short-lived certificate service (SLCS) or an online CA.

GridShib SAML Tools: These tools can be used to request SAML assertions from a SAML Attribute Authority (i.e. a Shibboleth IdP) and optionally bind them to X.509 proxy certificates. Using these tools it will be possible to push attributes within such a proxy certificate to the Grid resources. This solves the IdP discovery problem and eliminates the need to install the GridShib for Shibboleth software on the IdPs. If installed together with a GridShib CA the SAML tools can be used to embed a SAML assertion directly into the issued short lived certificate.

3.4. VO Management Suites

In IVOM we evaluated several VO management projects regarding their suitability for a VO management and authentication and authorization infrastructure combining Shibboleth-based campus attributes and self-managed VO attributes. An overview over the results is given in table 1. This table is part of a larger table including more features and VO management systems available in our IVOM working package 1 report [10].

3.5. Authentication and Authorization Without Trust-Proxying

As explained above, if trust proxying is not desired, the Grid resources making authorization decisions based on campus attributes must be able to consume and verify the original attribute assertion by the user's Shibboleth identity provider. Three conditions must be met to allow for this:

(i) The campus attributes must be available on the Grid resource. This means the attributes must be transported to the resource in some way. In Grids using the GSI, a chain of the user's proxy certificates is available on all Grid resources that received a request by or on behalf of the user. A proxy certificate is an ideal container for extensions containing attributes, as it is possible to push the attributes to all resources without any need for additional services or protocols. SAML assertions issued by Shibboleth identity providers can be embedded into proxy certificates using the GridShib SAML tools.

(ii) Upon successful transportation of the SAML assertion containing the user's attributes the Grid resource must be able to verify the attribute assertion. This does not only mean to cryptographically validate the identity provider's

signature but also to verify that a particular identity provider is the correct and responsible attribute authority for each attribute contained in the SAML assertion, i.e. that the IdP of institution A may not issue an attribute stating that a user is member of some other institution B. To be able to execute this verification process, the Grid resource needs the X.509 certificates of all identity providers together with the information about the scope of attributes for each IdP. This information is part of the Shibboleth federation's metadata, but not necessarily available on all Grid resources unless they are registered service providers of the Shibboleth federation.

(iii) The Grid resource must have a policy decision point capable of consuming the just received and verified attributes, i.e. in the case of campus attributes issued by a Shibboleth IdP SAML assertions.

3.6. Authentication and Authorization With Trust-Proxying

Doubts about sound principles put aside, the major advantage of using a trust proxy is that the Grid resources do not need to know all Shibboleth identity providers. Compared to the last section condition two is greatly simplified: Grid resources only need to know the entity acting as a trust proxy as this entity uses its private key to sign all campus attributes relayed through it. So the Grid resources only need exactly one X.509 certificate, that one belonging to the trust proxy, to validate pushed campus attributes.

If no policy decision point is available for SAML assertions, using a trust proxy can also solve that problem: As the attributes are re-signed anyway, the trust proxy can issue the attributes in a different container.

4. Example Workflows

4.1. Middleware Support

As already noted, Grid middleware must support validation and evaluation of the attributes contained in an attribute assertion. We currently have two types of attribute assertions: SAML assertions and Attribute Certificates. They are supported by the following Grid middleware:

SAML-Assertions: GridShib adds support for SAML assertions to the Globus Toolkit 4. UNICORE5 and gLite do not support SAML assertions. UNICORE is currently extended as part of the IVOM project to support SAML assertions coming from the IdP of a UNICORE user. The development includes an interface to GridShib delivering short lived certificates (SLC) and the modification of the UNICORE user database (UUDB), which is modified to extract assertions from the certificates and to act as a PDP.

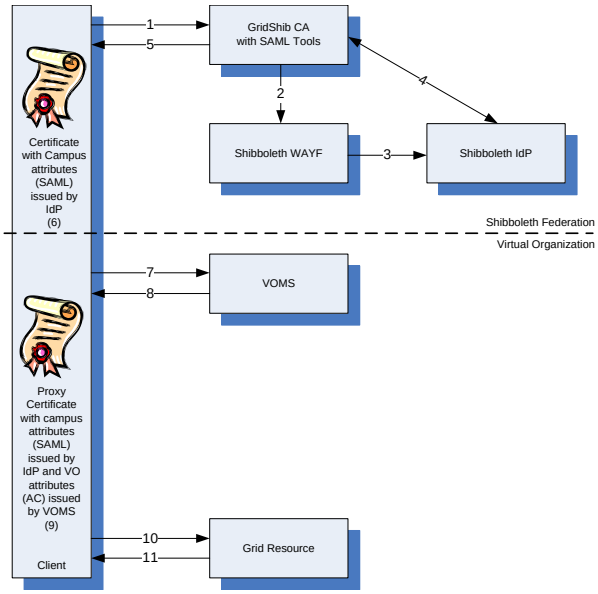

Figure 1. A workflow using VOMS without Trust Proxying

Attribute Certificates: a VOMS-PDP consuming Attribute Certificates is available as a technical preview for the Globus Toolkit, UNICORE will support Attribute Certificates. gLite does support Attribute Certificates, but only newer versions of the corresponding components do support generic attribute-value pairs instead of the hierarchic, fully qualified attribute names. Both versions of UNICORE currently do not support Attribute Certificates. As part of IVOM UNICORE is extended allowing the generation of Attribute Certificates from a users X.509 certificate using the VOMS `voms-proxy-init`. The UUDB is modified to extract the attributes from the certificates and acts as a PDP.

4.2. Using VOMRS/VOMS for VO Management Without Trust Proxying

gLite's Virtual Organization Membership Service (VOMS) [12] is a system for managing members of VOs. It features a database backend for storing the users and their attributes. It can store VO-membership attributes as well as Group, Role and Capability attributes used by gLite's Local Centre Authorization Service (LCAS) mechanism for authorization decisions. It is being accessed for VO management purposes using a Web front-end for both users to register themselves and for VO-Administrators to manage the VO-members. VOMS issues its attributes as Attribute Certificates which are commonly included into proxy certificates.

In D-Grid VOMS is used in conjunction with VOMRS for its currently more comprehensive set of features for VO administration. VOMRS itself however cannot issue any kind of attribute assertion, but it is capable of synchronizing into a VOMS database so that the attached VOMS can be used for issuing Attribute Certificates.

In Fig. 1 a typical workflow for a session of a Grid user without a long lived certificate for a VOMS-based Grid is depicted. In this case, VOMS is not used as a trust proxy, but the original SAML assertion of the user's home organization's IdP is preserved.

In step 1 the user contacts the online CA, in this case a GridShib CA, in order to obtain a short lived certificate. Steps 2 to 4 are a standard Shibboleth authentication and authorization procedure. Additionally, in step 4, the user's campus attributes are transferred from the IdP to the GridShib CA in form of a SAML assertion. The GridShib CA now embeds, using GridShib's SAML tools, this assertion in unaltered form into the certificate it issues in step 5. This means that the user now (step 6) owns a short lived certificate which already includes his campus attributes as an X.509 extension encoded as a SAML assertion.

In step 7 the user requests his VO attributes from the VOMS service, e.g. by using the `voms-proxy-init` command. In step 8 the VOMS service issues an Attribute Certificate containing these attributes which are embedded into a proxy certificate derived from the short lived certificate obtained from the GridShib CA. Now (step 9), the user has a proxy credential containing both, the short lived certificate containing his campus attributes and a proxy certificate derived from it containing his VO attributes.

The user can now access GSI-based Grid components using standard tools such as `globusrun-ws` in case of Globus Toolkit 4 (steps 10 and 11).

The advantages of using VOMS for VO management are its maturity and ongoing development. Initially, VOMS did not support arbitrary attribute-value pairs as Shibboleth does, instead it used a hierarchic model of Fully Qualified Attribute Names (FQAN). Current releases do already support generic attribute-value pairs and for future releases it is planned to be able to issue attributes in form of SAML assertions like Shibboleth. Currently VOMS only supports Attribute Certificates for issuing attributes.

4.3. Using myVocs for VO management With Trust Proxying

myVocs' design goal was to "extend the access to emerging Internet collaboration tools and build a system environment that respects VO defined roles and attributes while preserving valuable institutional identity assertions". myVocs thus manages attributes. It actually is a SAML-based Identity Provider proxy serving as a bridge between a federation

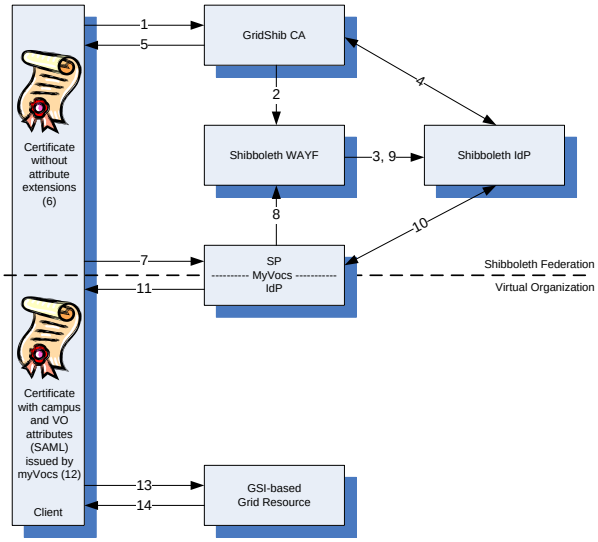

Figure 2. A workflow using myVocs with Trust Proxying

of Shibboleth Identity Providers and a federation of Shibboleth Service Providers for overcoming the somewhat unrealistic expectation that home organizations maintain their VO list of users. myVocs presents itself as a Shibboleth SP so that other services can rely on it to ensure that the user has been authenticated. The myVocs servers assert the attributes that the SPs in the VO need to base their authorization decisions upon.

In Fig. 2 a typical workflow for a session of a Grid user without a long lived certificate for a myVocs-based Grid is depicted. In this case, myVocs is used as a trust proxy. In step 1 the user requests a short lived certificate from an online CA, in this case the GridShib CA. Steps 2 to 4 are a standard Shibboleth authentication and authorization procedure. If the user is successfully authenticated and authorized the GridShib CA issues a short lived certificate and returns it to the user. As trust proxying is being used in this scenario, the issued certificate does not include any attributes yet (step 6).

In step 7 the user queries the myVocs service and is again, in steps 8 to 10, authenticated and authorized using Shibboleth. Furthermore, in step 10, attributes are released from the user's home organization's IdP to myVocs. If successfully authenticated and authorized, myVocs issues a SAML assertion in step 11 containing both, the user's campus attributes obtained in step 10 and his VO attributes managed by myVocs itself. In step 12 the user can now embed this SAML assertion to a proxy certificate derived from the short lived certificate obtained in step 5.

In step 13 the user accesses GSI-based Grid resources using standard tools such as `globusrun-ws` in case of

Globus Toolkit 4.

A user with a long-lived standard X.509 user certificate simply starts with step seven as he does not need to acquire a short lived certificate. Still, he needs to be member of some Shibboleth IdP of a supported federation as he needs to authenticate to myVocs.

myVocs allows several SPs (called VO SPs) to be aggregated into Virtual Organizations (VOs). myVocs considers VOs as people (more precisely: collections of attributes of people represented by lists), and the aggregated SPs as federated sets of distributed applications, the resources, accessible by this list of people. It is an important feature of myVocs that a single VO SP may serve multiple VOs and, hence, is supporting overlapping VOs. Like the IdPs, the VO SPs may reside in arbitrary administrative domains. Using off-the-shelf, open source software components (such as Shibboleth, MySQL, and Sympa), myVocs provides the "glue" that authorizes access to a VO SP based on the membership in some specific VO. The resources are protected by VO SPs which are mutually trusted by a VO IdP.

4.4. Comparison

As can be seen from Table 1, support for attribute-based authorization decisions in current Grid middleware is still limited. First of all it has to be noted that without a policy decision point able to validate and consume SAML assertions it is not possible to use campus attributes without trust proxying. As Shibboleth IdPs are only able to issue attribute assertions as SAML and any translation of these assertions in any other format would invalidate the IdP's signature these assertions need to be passed unaltered to the resource making the authorization decision. Currently SAML PDPs are avalilable for the Globus Toolkit as part of GridShib and this will presumably be part of Globus 4.2 to be released later this year. As myVocs also issues SAML assertions it will also be a supported VO management tool for SAML-compatible middleware regarding attribute-based authorization.

Attribute certificates as issued by VOMS containing generic attribute-value pairs are supported by gLite components using a version of LCAS/LCMAPS (Local Credential Mapping Service) currently being tested, a PDP for the Globus Toolkit 4 exists as a technology preview and UNICORE will also contain a VOMS-PDP.

In summary, the approaches using no trust proxy will in the short term only be available for UNICORE and the Globus Toolkit as there is no SAML-PDP currently available for gLite.

Based on these findings we have identified several currently available possible approaches for Shibboleth-enabled VO management. Two of them supported by the Globus Toolkit 4 and UNICORE are presented here: The first approach ist based on *VOMS* without trust proxying for Grid communities which do not want to rely on trust proxying. The SAML assertion containing the campus attributes has to be embedded into a proxy certificate by the user or into a short lived credential by the GridShib CA, both using the GridShib SAML tools. The VOMS will issue Attribute Certificates VO-attributes.

The second approach is based on *myVocs* as a trust proxy issuing SAML assertions containing both, campus-and VO-attributes. This approach will be supported by two Grid middleware in the mid-term, namely the Globus Toolkit 4 and UNICORE. This approach directly supports Grids being accessed by a web portal that is a standard Shibboleth service provider within the VO where the IdP part of myVocs is being used for authentication and authorization of Grid users.

5. Related Work

Some promising related work regarding trust proxying using VOMS is done by SWITCH as part of EGEE: The *Shibboleth Interoperability with Attribute Retrieval through VOMS* (VASH)[6] project aims at user-initiated transfers of Shibboleth attributes to a VOMS service. The VOMS service then issues these attributes together with VO attributes. At its current stage it is not evaluated whether the campus attributes stored within the VOMS are still valid, but in future releases this problem is going to be addressed by the developers. If the validity of the issued attributes can be verified upon issuing them as trust proxy, this approach will be reconsidered by the IVOM project for use in D-Grid. However, we cannot stress enough that we consider trust proxying in any way as a interim solution until it is possible to validate and consume original campus attribute assertions on all Grid resources.

Another work concerned with trust proxying is [11], where an approach using a central GridShib CA together with VOMS is presented. In this approach, the GridShib CA acts as a trust proxy, re-issuing the original SAML assertion within the issued short lived credential. This approach ensures that not all IdPs need to be known to the Grid resources but it requires both, SAML and Attribute Certificate support, to be available on the Grid resources.

A solution extending UNICORE6 for supporting SAML assertions is currently under development in the OMII-Europe project. The developments include both enhancements of UNICORE6 and a version of VOMS supporting SAML assertions [21].

6. Conclusion

In this paper we described the aim of the IVOM Project, presented some of its findings and identified several solu-

tions for the imminent challenges. Special focus is hereby on trust issues caused by the combination of campus attributes managed by a Shibboleth federation and VO attributes managed by a VO management system. Hereby we ensure interoperability in two directions: First, between Shibboleth federations and VO management systems and second between the three different Grid middleware used by D-Grid communities.

Currently, almost all solutions discussed appear to have weaknesses with respect to proper handling of trust issues or are not (yet) in a status lending itself to fast deployment. Future versions of SAML/Shibboleth as well as implementations of PDPs for all Grid middleware components for all necessary types of attribute assertions will address these issues. Trust proxying with all its implications may then not be needed any more. Meanwhile, any intermediate solution must also address the need of attribute consumers in Grids to recognize two chains of trust: The chain originating from the GridPMAs - as usual - and in addition the one of (national) Shibboleth federations. Also, either the Grid-service providers or their proxies must become partners in the appropriate federation - or attributes should not be delivered to them. If information present in VO membership, roles, etc. is to be used in other than Grid SPs, a proper (intermediate) contractual relation to the federation, fitting its policy, either as IdP or SP, must be found as well.

Acknowledgements

The IVOM work is funded by the BMBF, the German Federal Ministry of Education and Research (PT-IN grant FKZ 01AK810A - E).

References

[1] D. Chadwick. Functional components of grid service provider authorisation service middleware. Report of the OGF OGSA-Authz Working Group, October 2006.

[2] D. Chadwick, G. Inman, and N. Klingenstein. A conceptual model for attribute aggregation. [Online] http://www.jiscmail.ac.uk/cgi-bin/webadmin?A1=ind0707&L=shintau, July 2007.

[3] D-Grid. D-grid initiative. [Online] http://www.d-grid.de/index.php?id=1&L=1, 2007.

[4] D-Grid. Interoperabilität und Integration der VO-Management Technologien im D-Grid. [Online] http://dgi.d-grid.de/index.php?id=314, 2007.

[5] DFN – Deutsches Forschungsnetz. DFN-AAI - Authentifizierungs- und Autorisierungs-Infrastruktur im DFN. [Online] https://www.aai.dfn.de/, July 2007.

[6] P. Flury, V. Tschopp, T. Lenggenhager, and C. Witzig. Shibboleth Interoperability with Attribute Retrieval through VOMS. [Online] https://edms.cern.ch/cedar/plsql/doc.info?document_id=807849&version=2, January 2007.

[7] I. Foster and C. Kesselman. Globus: A metacomputing infrastructure toolkit. *The International Journal of Supercomputer Applications and High Performance Computing*, 11(2):115–128, Summer 1997.

[8] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A security architecture for computational grids. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pages 83–91, New York, NY, 1998. ACM Press.

[9] I. Foster, C. Kesselman, and S. Tuecke. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *International Journal of High Performance Computing Applications*, 15(3):200–222, 2001.

[10] P. Gietz, C. Grimm, R. Groeper, M. Haase, S. Makedanz, H. Peiffenberger, and M. Schiffers. Work package 1: Evaluation of international shibboleth-based vo management projects. [Online] http://www.d-grid.de/index.php?id=336&L=1, June 2007.

[11] R. Groeper, C. Grimm, S. Piger, and J. Wiebelitz. An architecture for authorization in grids using shibboleth and voms. Accepted Paper for the 33rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Special Session on Service Orientation, September 2007.

[12] INFN. Virtual Organisation Membership Service. [Online]. http://infnforge.cnaf.infn.it/voms/, May 2005.

[13] Internet2. Shibboleth Project - Internet 2 Middleware. [Online] http://shibboleth.internet2.edu/, 2007.

[14] Macquarie University. MAMS Project Overview Website. [Online] http://www.melcoe.mq.edu.au/projects/MAMS/, 2007.

[15] MAMS. IAMSuite Online Prototype. [Online] http://www.mams.org.au/IAMSuite, 2007.

[16] The EGEE Project. glite - ligthweight middleware for grid computing. [Online]. http://glite.web.cern.ch/glite/, 2007.

[17] UNICORE FORUM. Unicore. [Online] http://www.unicore.org/, 2007.

[18] University of Alabama at Birmingham, Advanced Technology Lab. The MyVocs Project. [Online] http://lab.ac.uab.edu/project/myvocs/.

[19] University of Chicago. GridShib: A Policy Controlled Attribute Framework. [Online] http://gridshib.globus.org/, 2007.

[20] USCMS VO Project. VOM Registration Service. [Online] http://www.uscms.org/SoftwareComputing/Grid/VO/, 2007.

[21] Valerio Venturi et al. Using saml-based voms for authorization within web services-based unicore grids. In *Proceedings of the 3. UNICORE summit*, 2007. to appear.

[22] V. Welch. Gridshib: Grid-shibboleth integration (identity federation and grids. [Online] http://grid.ncsa.uiuc.edu/GridShib/presentations/GridShib-uk-april05.ppt, April 2005.