A Concept for Attribute-Based Authorization on D-Grid Resources ⋆

Ralf Groeper [a], Christian Grimm [a], Siegfried Makedanz [b], Hans Pfeiffenberger [b], Wolfgang Ziegler [c], Peter Gietz [d], Michael Schiffers [e]

[a] *RRZN and L3S, Leibniz Universität Hannover, Hannover, Germany*

[b] *Alfred Wegener Institut, Bremerhaven, Germany*

[c] *Fraunhofer Institute SCAI, Department of Bioinformatics, Sankt Augustin, Germany*

[d] *DAASI International GmbH, Tübingen, Germany*

[e] *Ludwig Maximilian University Munich, Munich, Germany*

Abstract

In Germany's D-Grid project numerous Grid communities are working together to providing a common overarching Grid infrastructure. The major aims of D-Grid are the integration of existing Grid deployments and their interoperability. The challenge in this endeavor lies in the heterogeneity of the current implementations: Three Grid middleware stacks and different Virtual Organization management approaches have to be embraced to achieve the intended goals. In this article we focus on the implementation of an attribute-based authorization infrastructure that not only leverages the well-known VO attributes but also Campus attributes managed by a Shibboleth federation.

Key words: Attribute-Based Authorisation, VO-Management, VOMS/VOMRS, GridShib, Shibboleth

⋆ Some of the work reported in this paper is funded by the German Federal Ministry of Education and Research through the IVOM project as part of the D-Grid initiative under grant #01AK800A and #01AK810.

1 Introduction

The D-Grid subproject *Interoperability and Integration of Virtual Organization Management Technologies in D-Grid* (IVOM) aims at evaluating currently deployed management technologies for Virtual Organizations (VO, (1)) by assessing solutions developed by international VO management projects and at designing a D-Grid wide VO management infrastructure based on these findings to close gaps identified earlier in D-Grid.

Germany's D-Grid initiative consists of multiple community Grids from different fields of science and different industrial sectors (18). It is envisioned to use a common Grid infrastructure shared by all such community Grids, similar to using the Internet as a common networking infrastructure. As a prerequisite, it is necessary to ensure the interoperability among the different Grids be them D-Grid ones or international ones. One major challenge in this context relates to the interoperability of the underlying middleware technologies which in D-Grid are the Globus Toolkit 4, both in its Web Service (WS) and pre-WS flavor, LCG/gLite, and UNICORE. They not only differ in their VO-philosophies but also in their authentication and authorization schemes. Harmonizing these schemes over the emergent Germany-wide Shibboleth federation provided by the German National Research and Education Network (DFN) is a major objective of the IVOM project. The goal is to base the authentication of users and the authorization of accesses to Grid resources on the information provided by both, the standard VO-management mechanisms and the new Shibboleth federation. The need for such fine-grained attribute-based authorization decisions has been identified by both the D-Grid communities using the resources and the resource providers (RP) providing them (8).

To achieve these goals the IVOM project developed a two-step roadmap to enhance the existing D-Grid infrastructure with the necessary features. In this paper we will develop this roadmap in section 5. Before presenting the roadmap we will address campus attributes and VO attributes and how these can be encoded in section 2. In section 3 we analyze previous and ongoing work related to issues addressed in this paper before we discuss the requirements for an attribute-based authorization in D-Grid in section 4. Section 6 presents open issues which need to be elaborated on in the future. Finally section 7 concludes the paper.

2 Campus- and VO-Attributes and Their Encodings

Shibboleth federations have emerged to make user attributes available across organizational boundaries (but not across federations). The next logical step

will now be to make these attributes available to Grid resources for both user management processes within VOs and for authorization purposes on Grid resources. Consequently, this would lead to two distinct attribute authorities participating in the management of Grid user attributes: the traditional VO management systems such as VOMRS/VOMS (12; 13) and the user's home organization's Shibboleth Identity Provider (IdP). These two authorities issue different kinds of attributes:

(1) *Campus attributes* are user attributes managed by their respective home institution. They identify and describe the user by e.g. stating his name, nationality, telephone number, his affiliation to organizational units, and his roles within these units, e.g. professor at a faculty or student of a certain study course. These attributes are managed and issued by the Shibboleth federation's Idenitity Providers.
(2) *VO attributes* on the other hand describe users by their memberships, roles, and capabilities he has within a VO. These attributes are managed and issued by a dedicated VO management system such as VOMS (with or without VOMRS support).

Both types of attributes need to be encoded in some way to be transferred to the Grid resources, regardless whether they are being pushed to the Grid resources in a job context or pulled by the resources when needed. In (7) we concluded attribute push by embedding them into proxy certificates as the method-of-choice. The two prevailing encodings for embedding attributes within proxy certificates are Secure Assertion Markup Language (SAML) assertions and Attribute Certificates (AC), the first being an XML-based standard by OASIS (11), the latter being specified in RFC 3281 (4). While ACs are a Grid-specific solution relying on VOMS as attribute authority, SAML is a widely accepted XML-based standard used by many projects, especially by Shibboleth.

For transporting attributes both methods are feature-wise equally suited. The bottom line is that it depends on the capabilities of the producers and consumers, i.e. the issuers of assertions and the Grid resources, which method to prefer. The following table from (7) relates the standards for attribute encoding to the main VO management technologies (for further discussions we refer to (7)):

Component	Supported Attribute Encodings
VOMS	attribute certificates (SAML-assertions planned)
myVocs	SAML-assertions
GridShib CA	SAML-assertions obtained from Shibboleth IdPs

In the next table we relate attribute encodings to the different Grid middleware implementations used in the German D-Grid infrastructure (7). It is easily observable that there is no common attribute encoding supported by *all* middleware implementations. In the following we present a solution which helps closing this gap.

Middleware	Supported Attribute Encodings
Globus Toolkit 4 (pre-WS)	none, only X.509 DNs
Globus Toolkit 4 (WS)	optional Policy Decision Points (PDP) for SAML and attribute certificates exist and are planned to be part of GT4.2
LCG/gLite 3.0	gLite components can consume attribute certificates, containing Fully Qualified Attribute Names (FQAN). The current release does not support arbitrary attribute-value pairs. Support is currently in testing stage.
UNICORE 5	SAML and attribute certificates (developed by the IVOM project)
UNICORE 6.1	SAML and attribute certificates

3 Related Work

A considerable set of products and concepts is emerging from investigating the integration of X.509-based Grid environments with Shibboleth/SAML setups. In (7) we have provided a survey of these technologies and both Shibboleth-based and Public Key Infrastructure (PKI)-based VO management systems. Furthermore, we assessed their suitability as integration and management tools in Grids and the given constraints. We have especially evaluated the work performed by SWITCH for integrating gLite and Shibboleth (14), the GridShib activities (5), the MAMS project (9), myVocs (10), PERMIS (6), VOMS (13) and VOMRS (12).

For a detailed discussion of the related work the reader is referred to (7). The findings in (7) can be summarized as follows:

GridShib had a head start in the field of Grid and Shibboleth integration and maintains a lead over the peer projects. It currently offers the broadest set of solutions and is the best starting point for Grid and Shibboleth integration, given it becomes part of the Globus ecosystem.

myVocs: While myVocs is restricted regarding both the attribute handling and the user/administrator support, it is however flexible enough to pave the way for a VO management in Grids utilizing Shibboleth-based federations of IdPs and Grid Service Providers. Bridging collections of IdPs and SPs is a requirement when transparently managing VOs in non-trivial configurations. myVocs supports this objective. Combined with functionalities from other projects myVocs would be a first-choice candidate to proceed further. However, it's approach implies some serious trust issues by using trust proxying (15) and the software is not yet mature enough for productive use in D-Grid.

IAMSuite, developed by the MAMS project, is not yet available as a software product and can therefore not be recommended for a production environment.

VOMS is a mature and stable VO-Management system developed as part of the gLite middleware. It is used in production environments, especially in the High Energy Physics communities, for several years and is thus the de-facto standard in VO management based on public key infrastructures (PKI). Furthermore it is being actively enhanced with new features such as support for arbitrary attribute-value pairs, which is an essential feature for flexible VO management. The importance of VOMS is also reflected by the ongoing integration of Attribute Certificates in additional Grid middleware stacks such as Globus Toolkit 4. It has though to be considered that VOMS itself does not offer the integration of Shibboleth-based Campus attributes, which is an essential goal of the IVOM project. Means would still have to be found to combine VOMS with Shibboleth, e.g. by using GridShib or an approach similar to the VOMS Attributes From Shibboleth (VASH) (14) service by SWITCH.

VOMRS offers only a subset of the features of VOMS, but implements them in a more streamlined way, thereby lessening the burden imposed on VO administrators. However, VOMRS can be used as a front-end of a VOMS server, offering the complete functionality of VOMS and VOMRS' streamlined VO management workflows.

PERMIS is a system for policy-based authorization, which already has a longer history. Support for Grid infrastructures in general and GridShib especially has however been introduced rather recently. PERMIS provides all components needed for establishing and maintaining an authorization infrastructure to be used in, but not limited to, Grid environments.

4 Requirements for Attribute-Based Authorization in D-Grid

As can be derived from section 2 and the analysis in (7), none of the currently available solutions for authorization on Grid resources utilizing both

Campus- and VO attributes does support all three middleware implementations used in D-Grid. Consequently, the integration of SAML-based authentication and authorization is an ongoing research question in several Grid middleware projects. Besides the Globus project with GridShib, EGEE gLite and UNICORE are working on support for SAML assertions and callouts in their next releases. However, since the release date of a SAML-aware gLite is unclear, we are forced:

- to recommend intermediate solutions – which will most probably become obsolete soon – to those D-Grid community projects which are in need for an attribute based authorization mechanism now (8), and
- to select a combination of schemas, standards, and candidates for successful and timely development as a proper foundation for a future stable D-Grid VO management platform.

The former, preliminary, solution may be needed to be implemented in some cases even if it is not completely conforming to the intended architecture yet. We should bear in mind, though, that there is a clearly expressed caveat regarding multiple changes related to transitions from FQANs to attribute-value pairs and from attribute certificates to SAML assertions in the near future. The latter refers to the target technologies for the upcoming work on implementing an architecture for VO management in D-Grid which integrates and facilitates interoperation between *any* middleware implementation used in D-Grid, and, possibly, beyond.

Due to the insufficient support of SAML in current production releases of all three middleware implementations used in D-Grid it is not possible today to deploy an interoperable infrastructure that

- delivers Campus- and VO attributes to Grid resources *and*
- supports all D-Grid middleware implementations, *and*
- avoids serious trust issues as imposed by using trust proxying (15) or delivering potentially outdated attribute values.

However, it is already possible to use VO attributes managed and issued by VOMS encoded as Attribute Certificates on all three middleware implementations: gLite does support VOMS as it stems from the gLite software suite; a VOMS PDP is available for the Globus Toolkit 4; a PDP for UNICORE 5 has been developed by the IVOM project and will be part of upcoming UNICORE releases. Based on the community requirements sampled by IVOM we can weight VO attributes to be the most important carrier of authorization information whereas the use of Campus Attributes will mainly be restricted to user identification purposes.

The path to attribute-based authorization in D-Grid to be presented in the next section is intended as a guideline for those D-Grid communities that wish

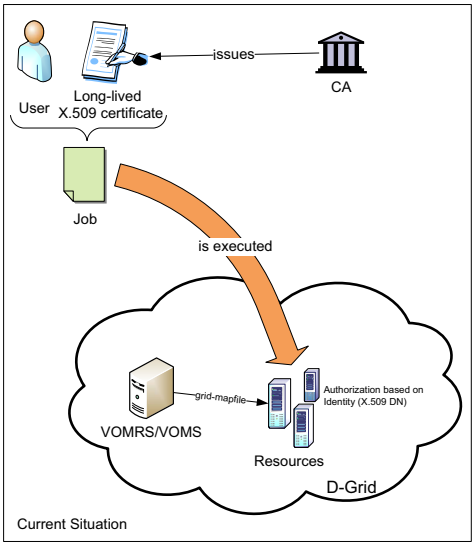

Fig. 1. Current Situation: Identity-Based Authorization in D-Grid

to utilize D-Grid resources or make their own resources available to members of other communities. The D-Grid partners maintaining parts of the infrastructure are advised to implement this proposal and can thus serve as a reference for the D-Grid communities. By this approach, the communities may evaluate the proposed solution in a live environment before adopting it for their own resources.

5 A Two-Step Roadmap Towards Attribute-Based Authorization in D-Grid

In this section we develop a two-step roadmap towards attribute-based authorization. For doing so we first assess the current situation in the D-Grid, list then the prerequisites, and finally define the two steps of our proposed roadmap.

5.1 State-of-the-Art: Idenitity-based Authorization in the D-Grid Infrastructure

The current Authentication and Authorization Infrastructure (AAI) deployed in D-Grid consists of a simple authorization mechanism based on the Distinguished Name (DN) of the user's X.509 certificate (see figure 1). Authentication on Grid resources 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 users themselves – or other Grid services acting on their 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 and his entitlements are available or necessary 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 mapped onto a local system account. It is obvious that such a solution does not scale well when dealing with large numbers of users.

In D-Grid, VO membership information is maintained in a VOMRS/VOMS server combination. However, the VOMRS/VOMS setup is not used to issue attribute assertions D-Grid-wide but for creating and distributing the information necessary for identity-based authorization. In the case of Globus and gLite this is the grid-mapfile, for UNICORE-based resources a so called UUDB is created.

5.2 Prerequisites for Attribute-Based Authorization

Attribute-based authorization needs at least two additional components compared to the identity-based approach: First it needs an Attribute Authority (AA) which issues attributes in a trusted way and second it needs Policy Decision Points (PDP) on the Grid resources for authorization decisions based on these attributes. Regardless of these components, the concept for VO-management systems proposed in this paper relies on two further premises, which are D-Grid inherent:

(1) Campus attributes are made accessible by a Shibboleth federation, i.e. by providing a Shibboleth Identity Provider (IdP) at each participating institution. In Germany the academic sector is building up such an infrastructure, the DFN-AAI led by Germany's National Research and Education Network (DFN-Verein).
(2) VO management is performed 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 AA, i.e. it can issue attributes in a trusted way. Currently, VO management in D-Grid is operated using a combination of VOMRS and VOMS.

Furthermore, it is assumed that the Grid middleware provides components that are able to verify and evaluate the attribute assertions issued by the aforementioned AAs. Availability of PDPs for Attribute Certificates and SAML Assertions has already been discussed in chapter 2.

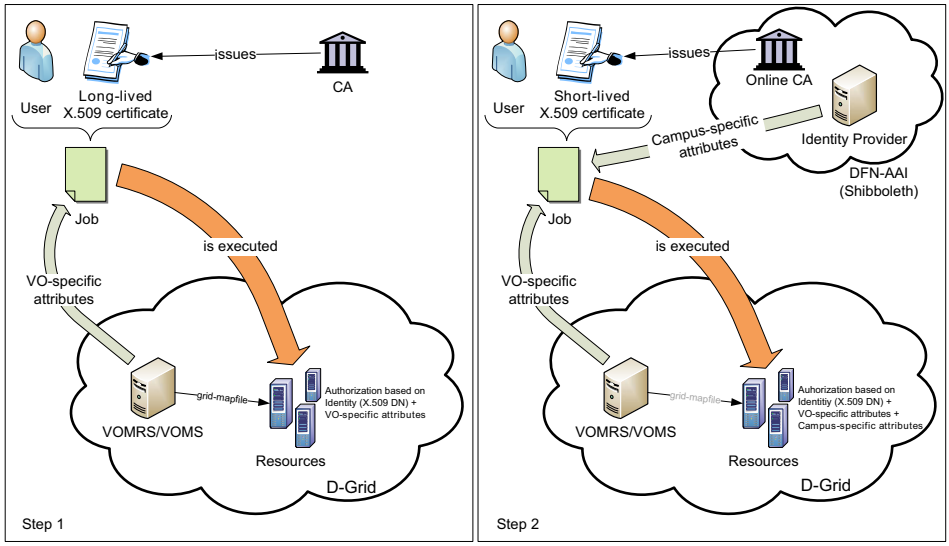

Fig. 2. Adding Support for VO- and Campus Attributes

5.3 Step 1: Adding VO Attributes to Authorization on D-Grid Resources

The first step towards attribute-based authorization depicted in the left half of figure 2 utilizes the existing VOMRS/VOMS combination already deployed in D-Grid to enable authorization on Grid resources based on VO attributes. It is necessary to deliver these VO attributes stored in VOMRS/VOMS databases to the Grid resources to allow authorization decisions on the resources based on these attributes. This is possible by embedding an Attribute Certificate or – when the SAML-enabled VOMS is available and deployed – SAML assertions into the proxy certificate used for job submission. The proxy certificate is derived from the long-lived certificate depicted in figure 2. As pointed out earlier, only VOMS is capable of issuing Attribute Certificates; VOMRS is just a front-end to VOMS. The use of VOMS in combination with VOMRS assures that step 1 is compatible to the current implementation of VO management in D-Grid and it ensures a smooth migration to attribute-based authorization without sacrificing current deployments.

The additional components – compared to the current deployment – and their availability status are:

VOMS. A VOMS server is already deployed within D-Grid. When the SAML-enabled VOMS becomes available we recommend upgrading to that version.

gLite. No additional software is necessary as gLite supports attribute certificates containing Fully Qualified Attribute Names (FQAN) describing VO memberships, groups, roles and capabilities within that VO instead of generic attribute-value pairs out of the box. If FQANs will be considered not sufficient compared to generic attribute value pairs in the future, an attribute certificate PDP currently being developed by SWITCH (14)

that is able to consume attributes certificates containing generic attribute value pairs needs to be deployed until both VOMS and gLite (possibly using gJAF (17)) support SAML assertions. When available, we suggest to issue VO attributes as SAML assertions.

Globus Toolkit. Depending on the use of the SAML-enabled VOMS, either the VOMS PDP or GridShib for Globus needs to be installed on all WS-based Globus components such as WS-GRAM, RFT or OGSA-DAI. It is advisable to use SAML assertions and thus GridShib for GT as soon as possible as the VOMS PDP is not actively in development in contrast to the very active GridShib project. The pre-WS components of GT4 do not provide any kind of attribute-based authorization and this is not expected to change short-term. Therefore we cannot provide support for attribute-based authorization on these components in D-Grid.

UNICORE. Both an attribute certificate PDP and a SAML PDP for UNICORE 5 have been developed as part of the IVOM project. A SAML-PDP for UNICORE will soon be available for UNICORE 6.1. We recommend to use SAML-assertions instead of attribute certificates when both the SAML-enabled VOMS and UNICORE with SAML support are available.

5.4 Step 2: Adding Campus Attributes to Authorization on D-Grid Resources

As explained earlier in this document it is envisioned to use not only VO attributes for authorization but also Campus attributes. Although mechanisms for managing and issuing Campus attributes are available today (e.g., Shibboleth) and the transport of such attributes within proxy certificates is already state-of-the-art with existing software (e.g., the GridShib SAML tools which are part of GridShib), the full support for this requirement still depends on the support for SAML assertions on the Grid resources themselves. In the right half of figure 2 the additional features compared to step 1 are depicted. An Online CA issues short-lived X.509 certificates with embedded Campus attributes managed within the DFN-AAI. Authentication to the Online CA is implemented by using a Shibboleth Service Provider that is part of the DFN-AAI. The subsequent steps for job submission, including the addition of VO attributes from the VOMS into the proxy certificate, are identical to step 1. However, the Grid resources are presented *two* attribute assertions in the certificate associated to the job.

When assessing the support for Campus Attributes in the D-Grid middleware implementations we need to consider that these attributes will be SAML-encoded, as they are issued by Shibboleth IdPs. We thus need SAML PDPs on all Grid resources that need to base authorization decisions on these attributes. The availability of SAML PDPs for Grid middleware implementations used in D-Grid has already been discussed in step 1. For this step to be deployable,

the DFN-AAI is required to be in operation and all Grid users that have to be authorized based on Campus attributes are required to be registered on their home organization's Shibboleth Identity Provider within the DFN-AAI. Also, for users without long-lived certificates, within the Shibboleth federation an EUGridPMA accredited Online CA must be implemented and its CA certificate must be among the trusted CAs on the D-Grid resources. Currently, DFN is planing to implement and operate such an Online CA.

In the long term, a one-to-one mapping of Grid users to local accounts may not be possible any more, e.g. because the maximum number of local accounts for standard Linux systems has been reached. The solutions laid out in this paper also pave the way for different mapping schemes that are not based on grid-mapfiles or their respective equivalents but solely upon attributes describing the user. This is denoted by greying out the grid-mapfile in the right half of fig. 2. As the user's X.509 distinguished name will still be present on all Grid resources, it will still be possible to relate any operation on a Grid resource to the identity of the submitter of the job.

5.5 Assessment

The solution presented above is not only scalable for large numbers of users without supplying each with a personal long-lived X.509 certificate, it also solves the interoperability problem when using VOMS with the planned Online CA by DFN. Short lived certificates acquired from the Online CA by using the DFN-AAI for authentication can be used to derive proxy certificates in which attribute certificates or SAML assertions issued by VOMS can be embedded. From a technical perspective it does not matter whether a user issues a job with a proxy certificate derived from a long-lived user certificate issued by a Grid CA or a short lived certificate issued by an Online CA as both are standard X.509 certificates. It is thus not mandatory that every Grid user is in possession of a personal long-lived user certificate.

6 Future Work

The main issue concerning SAML-encoded Campus attributes that needs to be solved in the future refers to attribute verification: All Grid resources containing a PDP based on the aforementioned attributes must be able to verify that the attributes (in either format but especially in the form of SAML assertions) describe the same subject that issued the Grid job, i.e. the user who is authenticated by the X.509 DN taken from the proxy credential. As the SAML assertion is not bound to that X.509 DN, means have to be found to

create, maintain and provide such a binding, e.g. by adding the X.509 DN to the Campus Attributes or, vice versa, the Shibboleth identity to the VO attributes. This problem does not arise when short-lived certificates issued by the Online CA are used. As the Online CA binds the Campus Attributes directly to the issued certificate, the mapping between the user's X.509 identity and his Shibboleth identity is guaranteed by the Online CAs signature on the issued certificate.

Regarding the attribute schema, it would seem to be obvious to use the eduPerson schema (3), since this is the de-facto standard for expressing attributes in Shibboleth federations like DFN-AAI (16). An additional controlled vocabulary pertaining to Grid resources in particular is desired and should be developed in D-Grid, in close collaboration with all D-Grid communities and Resource Providers. It is obvious that encoding and transport standards from the OASIS family of Web Services standards, in particular SAML, is preferable when all components offer support for them.

7 Conclusions

In this document we have described both Campus- and VO attributes and ways for delivering them from their respective attribute authorities to Grid resources. In the IVOM project we discussed different solutions based on different software packages, especially regarding support by the three Grid middleware implementations used in D-Grid. Based on these findings, we developed a two-step roadmap starting from the currently deployed identity-based authorization mechanism.

Step 1 adds support for authorization decisions based on VO attributes whereas step 2 additionally adds support for Campus attributes. For both steps we have identified lacking software components, mainly SAML PDPs, and described the architectures of the proposed authorization schemes once these components become available. As VO attributes are considered more important for authorization in D-Grid, we propose a VOMS-based authorization scheme in step 1 that can be extended in the future when the identified software becomes available by extending the features added in the previous step.

However, support for attribute-based authorization on Grid resources is still limited by the respective software availability. Most components either offer no support at all, or support is only announced for the future, or it is in testing stage. This situation will, however, change in the near future, as many international Grid projects actively work on similar challenges.

Acknowledgments

The authors would like to thank the developers of Shibboleth and GridShib, people from the Swiss science network, SWITCH, as well as all international reviewers of our IVOM work package reports for their helpful comments.

References

[1] I. Foster and C. Kesselman and S. Tuecke: The Anatomy of the Grid: Enabling Scalable Virtual Organizations, Lecture Notes in Computer Science, Volume 2150, 2001.

[2] I. Foster, C. Kesselman. The Grid: Blueprint for a New Computing Infrastructure, Morgan-Kaufman, 1999

[3] EDUCAUSE/Internet2: Object Class eduPerson. `http://www.educause.edu/eduperson/`, last visited 31 Aug 2007.

[4] S. Farrell, R. Housley. An Internet Attribute Certificate Profile for Authorization. IETF Request for Comments 3281, April 2002.

[5] GridShib Project, `http://gridshib.globus.org/`, last visited 15 Aug 2007.

[6] PERMIS Project, `http://sec.cs.kent.ac.uk/permis/index.shtml`.

[7] IVOM Work Package 1 Report: Evaluation of International Shibboleth-Based VO Management Projects, Version 1.2. June 2007. `http://dgi.d-grid.de/fileadmin/user_upload/documents/DGI-FG1-IVOM/AP1-Report-v1.2.pdf`

[8] IVOM Work Package 2 Report: VO-Management Requirements from a Community Perspective, Version 1.0. August 2007 `http://www.d-grid.de/fileadmin/user_upload/documents/DGI-FG1-IVOM/requirements-v1.0.pdf`

[9] MAMS Project Overview Website, `http://www.melcoe.mq.edu.au/projects/MAMS/`, last visited 10 Aug 2007.

[10] myVocs `http://myvocs.org/`, last visited 10 Aug 2007.

[11] OASIS Security Services (SAML) TC, `http://www.oasis-open.org/committees/security/`, last visited 10 Aug 2007.

[12] VOM Registration Service, `http://computing.fnal.gov/docs/products/vomrs/vomrs1_3/wwhelp/wwhimpl/js/html/wwhelp.htm`, last visited 10 Aug 2007.

[13] VOMS, `http://vdt.cs.wisc.edu/components/voms.html`, last visited 10 Aug 2007

[14] P.Flury, V.Tschopp, T.Lenggenhager, C.Witzig. Shibboleth Interoperability with Attribute Retrieval Through VOMS. April 2007. `https://edms.cern.ch/file/807849/2/EGEE-II-MJRA1.5-807849-v0.95.doc`, last visited 29 Nov 2007.

[15] C. Grimm, R. Groeper, S. Makedanz, H. Pfeiffenberger, P. Gietz, M. Haase, M. Schiffers and W. Ziegler: Trust Issues in Shibboleth-Enabled Federated Grid Authentication and Authorization Infrastructures Supporting Multiple Grid Middleware, Proceedings IEEE eScience 2007, International Grid Interoperability and Interoperation Workshop, Bangalore, India, Dec 2007.

[16] P. Gietz, J. Lienhard, S. Makedanz, B. Oberknapp, H. Pfeiffenberger, J. Rauschenbach, A. Ruppert, R. Schroeder. DFN-AAI - Technische und organisatorische Voraussetzungen - Attribute. November 2006. `https://www.aai.dfn.de/fileadmin/documents/vertraege/attribute.20061130.pdf`, (in German), last visited 18 Mar 2008.

[17] Yuri Demchenko. gLite Java Authorisation Framework (gJAF) and Authorisation Policy Coordination. Presentation at the EGEE06 Conference, Geneva, Switzerland, September 2006.

[18] Heike Neuroth, Martina Kerzel, Wolfgang Gentzsch. German Grid Initiative D -Grid. Niedersächsische Staats- und Universitätsbibliothek, 2007, ISBN 3938616997, (in German).