Future Generation Computer Systems 25 (2009) 275–280

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

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

ARTICLE INFO

Article history:
Received 29 November 2007
Received in revised form
14 April 2008
Accepted 14 May 2008
Available online 25 May 2008

Keywords:
Attribute-based authorisation
VO-management
VOMS/VOMRS
GridShib
Shibboleth

ABSTRACT

In Germany's D-Grid project numerous Grid communities are working together to provide a common overarching Grid infrastructure. The major aims of D-Grid are the integration of existing Grid deployments and their interoperability. The challenge 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.

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 [1,2]) 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 different Grids, whether they are 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. Not only they differ in their VO-philosophies but also in their authentication and authorization schemes. Harmonizing these schemes over the emerging 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 access 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 has 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 the previous and the 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

☆ 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.

* Corresponding address: RRZN and L3S, Universität Hannover, Schlosswender Str. 5, 30159 Hannover, Germany.
E-mail address: groeper@rvs.uni-hannover.de (R. Groeper).

0167-739X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2008.05.008

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 is now 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 Identity 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 of 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 Security 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 easy to observe that there is no common attribute encoding supported by *all* middleware implementations. In what follows, 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