VOMS/VOMRS Utilization patterns and convergence plan

A. Ceccanti[1], V. Ciaschini[1], M. Dimou[2], G. Garzoglio[3], T. Levshina[3], S. Traylen[2], V. Venturi[1]

1: *INFN-CNAF*, 2: *CERN*, 3: *Fermilab*

E-mail: `andrea.ceccanti@cnaf.infn.it, vincenzo.ciaschini@cnaf.infn.it, maria.dimou@cern.ch, garzogli@fnal.gov, tlevshin@fnal.gov, steve.traylen@cern.ch, valerio.venturi@cnaf.infn.it`

Abstract.
    The Grid community uses two well-established registration services, which allow users to be authenticated under the auspices of Virtual Organizations (VOs). The Virtual Organization Membership Service (VOMS), developed in the context of the Enabling Grid for E-sciencE (EGEE) project, is an Attribute Authority service that issues attributes expressing membership information of a subject within a VO. VOMS allows to partition users in groups, assign them roles and free-form attributes which are then used to drive authorization decisions. The VOMS administrative application, VOMS-Admin, manages and populates the VOMS database with membership information. The Virtual Organization Management Registration Service (VOMRS), developed at Fermilab, extends the basic registration and management functionalities present in VOMS-Admin. It implements a registration workflow that requires VO usage policy acceptance and membership approval by administrators. VOMRS supports management of multiple grid certificates, and handling users' request for group and role assignments, and membership status. VOMRS is capable of interfacing to local systems with personnel information (e.g. the CERN Human Resource Database) and of pulling relevant member information from them. VOMRS synchronizes the relevant subset of information with VOMS. The recent development of new features in VOMS-Admin raises the possibility of rationalizing the support and converging on a single solution by continuing and extending existing collaborations between EGEE and OSG. Such strategy is supported by WLCG, OSG, US CMS, US Atlas, and other stakeholders worldwide. In this paper, we will analyze features in use by major experiments and the use cases for registration addressed by the mature single solution.

1. Introduction

Resource sharing in current production Grid deployments, like OSG [1] and EGEE[2], is mainly regulated according to membership in Virtual Organizations (VOs). Within VOs, a varying number of participants with various degrees of prior relationships join in order to share resources in a highly controlled fashion. The Virtual Organization Membership Service (VOMS) currently represents the key element in enabling VOs, by providing the bases for attribute based authorization in production Grids. Current production Grid middleware also provide two well-established VOMS registration and administration services that allow a potential user to become part of a specific VO:
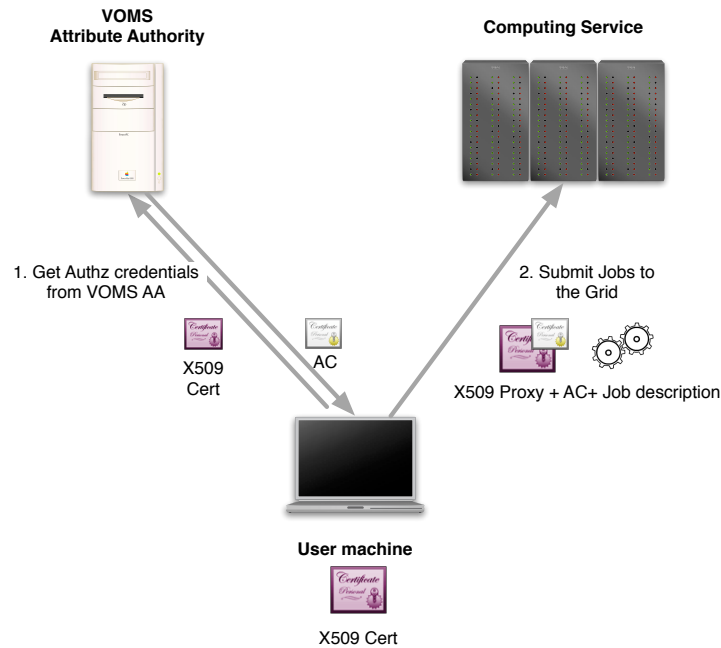
Figure 1. VOMS User interaction.

- **VOMS-Admin**, the main VOMS administrative application, that implements a complete VOMS management tool and provides a streamlined registration service, mainly used by smaller VOs;
- **VOMRS**, a more sophisticated registration service, developed on top of the management services exposed by VOMS-Admin, typically used by bigger VOs (e.g., the four major LHC experiments (ATLAS, ALICE, CMS and LHCb))

In this paper, we introduce the main features of the two services and describe and motivate a convergence plan that will produce a unified and more mature solution for VO registration and management.

2. VOMS
The Virtual Organization Membership Service (VOMS) [3] has been developed with the aim of supporting the dynamic, fine grained access control needed to enable resource sharing across virtual organizations (VOs). VOMS allows to manage authorization information within the scope of a VO. This information is then used for enforcing the agreements established between VOs and resource owners.

The main idea of VOMS is to augment user's credentials with additional attributes, thus allowing services to retrieve them and take authorization decisions on their basis. In a typical Grid job submission scenario, a Grid user first requests his/her bag of VOMS trusted attributes from the VOMS service and the submits a job to the Grid together with the bag of received attributes. These attributes will then be used to authorize operations according to the user position in the VO context (see figure Figure 1).

VOMS currently defines three types of attributes:

- *Groups* reflect the VO internal structure by defining a tree where membership in a subgroup implies membership in a parent group. Group membership in VOMS cannot be repudiated, so any user will receive all the attributes describing its group membership for any request;
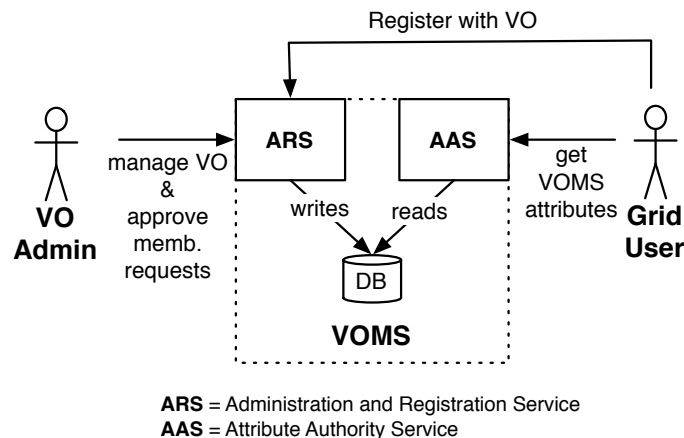
Figure 2. The VOMS software architecture.

- *Roles* are used to assign *special* privileges to users in the context of a specific VOMS group. Roles are issued by VOMS only on explicit user's request.
- *Generic attributes* are (name, value) pairs which can be used to represent user attributes that do not directly relate to the organizational structure of the VO (its groups and roles), but identify some other property on which authorization decisions can be taken.

The VOMS software may be roughly divided in two different sub-packages, according to their main usage (see Figure 2): an Attribute Authority Service (AAS) and a Registration and Administration Service (RAS). The AAS' main responsibility is to issue attributes to authenticated users while the RAS deals with VO structure and user membership management tasks.

2.1. The VOMS Attribute Authority Service

The VOMS AA can issue attributes in two different formats: X.509 Attribute Certificates (AC)[4], and SAML Attribute Assertions (SAML AA)[5].

The X509 AC attribute authority is composed of two elements: a unix daemon, called `vomsd`, and a client, `voms-proxy-init`. Each VO runs its own daemon, whose task is to authenticate client requests for attributes and issue signed Attribute Certificates (ACs) to authenticated VO members. `voms-proxy-init` is the command line interface by which user request attributes from the VOMS server.

The SAML attribute authority service, developed during the OMII project [6] and recently incorporated in the VOMS-Admin code base, exposes an interface according to SAML protocols [5] and bindings [7] that SAML-speaking clients can contact to obtain VOMS attributes. The VOMS SAML endpoint in described in greater detail in [8].

2.2. The VOMS Administration and registration services

The VOMS Administration and registration Services are responsible for VO creation, upgrade and management.

VO Administrators use the administration services to define the VO structure (i.e., its groups and roles), assign VO members the appropriate attributes and manage who is allowed to perform administrative operations on the VO.

The Administration service implements an authorization framework based on X.509 certificates [9] to allow the execution of VO management operations only to trusted users. In particular, the frameworks has Access Control Lists (ACLs) that define the trusted user's

capabilities and allow the implementation of delegation of administrative tasks among groups of VO administrators. For instance, it's possible to grant an administrator the right to assign membership to users only for a specific group.

All the Administration service management operations are exposed through a Web Service interface, to foster interoperable integration with other applications and middleware components (e.g., VOMRS). The web service interface is also the one contacted by the Administrative service command line tools.

VOMS-Admin Registration service consists of a registration web page where aspiring VO members can submit their personal information and request VO membership. Such request is then evaluated by VO managers and, if deemed appropriate, the user becomes part of the VO and is assigned VOMS attributes.

2.2.1. Implementation Details The VOMS Administration and registration services are implemented in the Java programming language as a J2EE Web application that runs on top of the Apache Tomcat container [10]. The administration services are accessible either through a web based interface or using a command line client (`voms-admin`) that enables the scriptability of repetitive administration tasks.

The `voms-admin-configure` python script manages the creation, upgrade and configuration of VO instances.

3. The JSPG's Virtual Organisation Management Policy

The Joint Security Policy Working Group (JSPG) [11] is a joint group of experts that makes recommendations regarding security issues for its primary stakeholders, i.e. the WLCG and the EGEE project.

In order to regulate security aspects of VO registration management, the JSPG has defined a set of requirements that VO registration services must implement to be deemed compliant with the JSPG Virtual Organisation Management Policy.

The current version of the Virtual Organisation Management Policy, accessible on the JSPG's wiki can be summarized as follows:

- The registration service supports multiple administrative roles (e.g., VO Manager, Institute representative) that can be assigned the responsibility to carry out specific actions during the VO management and user registration process;
- In order to become part of the VO, aspiring members must sign and agree with the VO and Grid Acceptable Use Policies (AUPs);
- The registration service must provide the tools to manage the versioning and evolution of the AUPs by administrators and the corresponding acceptance by the users;
- The registration service must support suspension, expiration and renewal of VO user's membership;

Currently, VOMS-Admin registration service is not compliant with the above requirements, since:

- it does not implement support for management and versioning of Grid and VO AUPs;
- it does not support suspension, expiration and renewal of VO membership.

To address these and other limitations of the VOMS-Admin registration service, a more mature and flexible registration tool, VOMRS, has been developed at Fermilab. Its main features are described in the next section.

4. The Virtual Organization Management Registration service (VOMRS)

The Virtual Organization Management Registration Service (VOMRS) [12] was developed to address the end-to-end needs for VO membership registration and user groupings within the Worldwide LHC Computing Grid (WLCG) and Fermilab contexts. When work on VOMRS started, VOMS-Admin was already widely in use, but was lacking some important registration features that were commonly required by the various big VOs. For example, VOMS-Admin did not provide support for a VO to request its members to sign the authorization usage policy or did not allow members to request group/group role affiliation. It was lacking the ability to temporarily suspend membership in a VO as well as to collect arbitrary personal information from a member during the registration. The goal of VOMRS was to build a more sophisticated registration service on top of VOMS-Admin VO management services.

The project was initiated in early 2003 and the first production release was available in March of 2004. Some of the requirements collected were incorporated into the VO Membership Management Policy document from the JSPG. Subsequent development of VOMRS was done in compliance with the expanding JSPG requirements.

4.1. Main features

VOMRS implements a sophisticated registration workflow and notification engine. It supports a hierarchy of administrators. Each type of administrators has well defined responsibilities. For example, a Representative is responsible for approving a users request to become a member of a VO and a Group Manger has the responsibility of granting a user membership to a group. The VO Admin, instead, has the ultimate control on all the actions supported by VOMRS.

VOMRS allows for the creation of Groups that may have an Open or Restricted access. If a Group has an Open access, a member does not need administrative approval to join the group. VOMRS supports interfaces to link a Group Role to a specific Group. A Group Role may also have an Open access if its Group has Open access as well.

According to the JSPG requirements, a VO should request its members to sign an Acceptable Usage Policy(AUP) during the registration process and to re-sign it every few years or every time that the AUP changes. VOMRS can prompt a user to sign an AUP during the registration, keeping track of the signing date and of the AUP version.

The registration process consists of two phases. During the first phase, a user fills out a web form with personal information, selects its affiliated institution, and an institution Representative. Information about the user credentials are automatically obtained from the browser. The second phase starts after a user gets email notification of the initial registration and proceeds with email confirmation and AUP signing. After approval from the Representative, a member can request approval to add additional certificates and/or apply for membership to specific Groups / Group Role. Such membership can be approved or denied by the hierarchy of administrators.

A user's membership status could be in four states:

- *Approved*, for members in good standing
- *Denied*, for an applicant that has been rejected by its Representative
- *Suspended*, for a member that has some outstanding issues with his/her membership.
- *Expired*, for a member whose association with the affiliated institution has been ended, or this signature on the AUP has expired

A member can register multiple certificates and each certificate also could have the four states mentioned above.

Each action performed by VO administrators and members is recorded in the VOMRS database and it is registered as a VOMRS event. VOMRS can be configured to send relevant

event notifications to members and administrators. Members can subscribe to get events relevant to their membership status. Administrators can subscribe to get notification about pending members' requests, addition/removal of group and group roles, and other relevant events. Members and administrators can register for events from a list.

An important feature of VOMRS is the ability to interface third-party systems to get/push relevant membership information. This is achieved by registering the third-party system interface with the event notification mechanisms of VOMRS. This mechanism is used to synchronize VOMRS with VOMS. In particular, an instance of VOMS is registered with VOMRS, so that all events related to changes of membership are pushed to VOMS through the VOMS-Admin API.

VOMRS can also pull information from third-party systems during the process of registration. Currently, VOMRS is interfaced with the CERN HR database and the Fermilab directory service. This approach allows not only for the verification of users information from a trustworthy source, but it also avoids the duplication in the VOMRS database of sometimes sensitive information about a member.

4.2. Deployments

The VOMRS service is written in Java. The Web user interface uses JavaScript. All the configuration scripts are written in python and the configuration files are in XML format. VOMRS supports both Oracle and MySQL rdbms.

Currently VOMRS is deployed on several sites. The list includes CERN, Fermilab, Desy, Texas Tech University, University of Melbourne, Juelich Research Center and other organizations. Four major LHC experiments such as ATLAS, ALICE, CMS and LHCb are using VOMRS installed at CERN as their VO registration service. They are using VOMRS instances that are configured to interface CERN HR database. Dteam, Geant4, Unosat and other smaller VOs are also using VOMRS installations at CERN. There are multiple instances of VOMRS at Fermilab as well. Fermilab, DZero, OSG VOs make use of these installation.

4.3. The VOMRS/VOMS Synchronization process

Figure 3 shows the VOMRS/ VOMS synchronization process as implemented today. Tipically, when VOMRS is used for registration, the VOMS-Admin registration service is turned off. Users request VO membership contacting the VOMRS service. These requests are then authorized by VO administrators also via the VOMRS service.

VOMRS keeps information about VO structure, members and pending registration requests in a relational database. This information needs to be periodically synchronized with VOMS so that changes in VO structure and membership are properly mirrored to the VOMS database. The synchronization process leverages VOMS-Admin web service interface to define the structure of the VO and manage user certificates and attribute assignments.

4.4. Commitment for support

VOMRS is a VO registration service used in production by several VO and sites. It provides the means to communicate with VO members and to assign grid privileges to them. Through the use of the administrative hierarchy, VOMRS allows for delegation of responsibilities within the VO, while still providing a high level of control over privileges granted. It meets the needs of a wide variety of VOs and is fully compliant with JSPG requirements. Though active development has been stopped for the last two years, the Fermilab Computing Division is committed to fully supporting it, while it is in use.
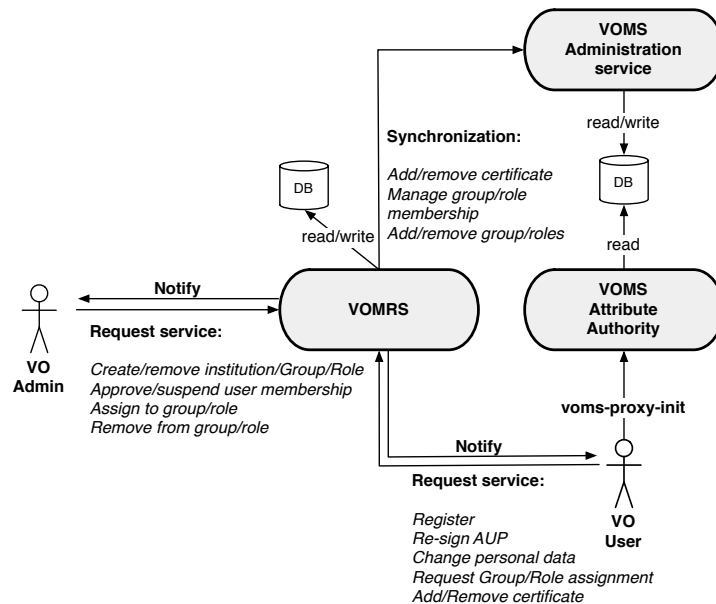
Figure 3. The VOMRS/VOMS synchronization process.

5. VOM(R)S Convergence

Starting with version 2.5, VOMS-Admin will be fully compliant with the JSPG VO Membership Management Policy. The compliance with these requirements has been requested by many VOs that currently rely on VOMS-Admin for registration but would like to have some of the features that are currently only implemented in VOMRS (AUP management and membership suspension) without having to install and maintain also a VOMRS installation.

VOMS-Admin compliance with JSPG requirements will however bring a significant feature overlap with VOMRS. For this reason, the VOMS and VOMRS team met during 2008 to devise a plan to converge on a single VO registration solution that would have all the main features currently implemented in VOMRS but also the benefit of a single registration service.

The main benefits of the convergence are:

- No parallel development will be required to keep VOMS and VOMRS features synchronized. Currently, every evolution of VOMS and VOMS-Admin needs to be *back-ported* to VOMRS, with considerable development and testing effort. Such back-porting will not be needed when all the needed registration functionality will be implemented in VOMS-Admin, since evolution of the registration service will be part of core VOMS evolution;

- A simplified deployment. Maintaining two parallel services (and their databases) that have more or less the same features impose a significant overhead on service deployers.

5.1. The convergence schedule
The convergence schedule agreed by the VOMS and VOMRS development team is presented in this section and summarized in Table 1.

5.1.1. Phase I - JSPG requirements compliance
Phase one will implement the compliance of VOMS-Admin with the JSPG VO Membership Management policy (sec. 3). The main new features are described hereafter:

Phase	Description	Deadline	Funding
Phase I	JSPG compliance	June 2009	EGEE
Phase II	Migration of essential VOMRS features	Jan. 2010	INFN
Phase III	Interface with third party directory services	Spring 2010	INFN
Phase IV	Validation, testing and collection of user's feeback	?	?
Phase V	Development of migration tools and migration of existing data from VOMRS to VOMS-Admin	?	?

Table 1. The VOMRS/VOMS convergence schedule.

AUP support   VOMS-Admin will implement versioned support for VO and Grid Acceptable usage policies (AUPs). AUPs' acceptance will be requested from users at the following times:

- at VO registration time,
- at membership renewal time,
- when a new version of the AUP is introduced in the system,
- on trusted VO administrator request.

The VOMS-Admin web interface and configure scripts have been extended to include support for AUP management and acceptance tasks.

Membership expiration, suspension, removal   VOMS-Admin will keep track of VO membership lifetime, by adding a validity field to membership records. It will be possible for administrators to change/extend this validity period, possibly requesting AUPs reacceptance from users.

Multiple certificate per user support   Starting with version 2.5, VOMS-Admin introduces support for multiple certificates per membership. These certificates will share the VOMS attributes assigned to the user, (i.e. groups, roles and generic attributes), so a user will be able to contact VOMS with different personal certificates and get back the same set of VOMS attributes. Finally, administrators will have the ability to suspend certificates for a user without suspending his/her membership. A user authenticated through a suspended certificate will not obtain any VOMS attribute but a warning message set by the VO administrator (or by the service itself) explaining the reason behind the suspension.

Group/Role membership requests   Besides the functionality requested to become JSPG compliant, VOMS-Admin will also add the ability for VO members to request group/role membership via VOMS-Admin's web interface. Such request will then be evaluated by a trusted VO administrator and will result in possible assignment of the requested attributes.

All these enhancements (being part of the EGEE-III project description of work) have already been developed and are currently under testing by the VOMS team. The VOMS-Admin 2.5 release providing these features is expected to be released to certification in June 2009.

5.1.2. Phase II - Migration of essential VOMRS features   Phase II will migrate priority VOMRS features, important for VOMRS clients, to the VOMS-Admin code base:

Configurable Group and roles membership access   VOMS-Admin will implement the possibility to configure Group and Roles as either `open` or `restricted`. User membership requests for `open` groups/roles will be automatically approved by the system, while requests for `restricted` groups will need the intervention of a VO administrator.

Ability to attach a description field to Group and Roles   It will be possible to associate a textual description to group and roles. This description will be presented to users when requesting Group/Role membership and will be shown together with other group/role information in the VOMS-Admin web interface.

Institution and institute representatives management   VOMS-Admin will provide the tools to manage the list of Institutions that are trusted by the VO. This institution list will be then presented to the aspiring VO users at registration time, so that they can select the Institution they belong to. It will also be possible to define an Institute representative for each institution that will be queried by the system to confirm the validity of the personal information submitted by users as well as their entitlement to be part of the VO.

Rationalization of the web interface   VOMS-Admin web interface will be evolved to incorporate some functionality now existing only in VOMRS, such as the ability to execute multiple management operations with a single click of a mouse (e.g., deletion of group of users, assignment of group of users to a specific group etc.). Better support for sorting VO member's information will also be implemented.

Dynamic list of collected personal information   It will be possible to optionally configure VOMS-Admin to collect and store personal information besides the minimum information needed for JSPG compliance. The visibility of this information will be configurable by the user to be either public or accessible only by VO administrators.

Selection and notification of VO-related interesting events   VO administrators will have the possibility to select which type of notifications they receive as consequence of interesting VO-related events (e.g., user requests, group and roles management actions etc...) The granularity of this selection will however be more coarse-grained with respect to currently available VOMRS implementation.

A VOMS-Admin release implementing these features is scheduled for the beginning of 2010.

5.1.3.   Phase III - Interface with third party directory services Phase III will implement the ability for VOMS-Admin to gather information from external data sources during VO membership registration and validation. In particular, a pluggable framework will be designed and implemented to be general enough so that different kind of external data sources (e.g., LDAP directories,relational databases) may be integrated in the VOMS-Admin workflow by writing data source specific plugins. A plugin for interfacing with the CERN HR database will be developed and tested during this phase of the convergence plan.

This phase marks the end of the core development work for the VOM(R)S convergence and include robustness and scalability testing of the new VOMS-Admin service. Backwards compatibility with existing services and clients will also be assessed at this time.

A VOMS-Admin release implementing this features is scheduled for the foreseen end of the EGEE-III project, i.e. Spring/Summer 2010. Funding for phase two and three of the convergence plan will be provided by INFN.

5.1.4. Phase IV & V - Validation and Migration for existing VOMRS installations   Phase four of the convergence plan will focus on validation of the whole set of new features by members of the VOMS development team and external testers (e.g., the VOMRS development team or service early adopters). Feedback gathered from this validation steps by the end users will probably involve more development on the VOMS-Admin code base to properly meet user requirements. The outcome of will be a certified version of VOMS-Admin that exposes all the main VOMRS functionality.

The last phase of the convergence plan will focus the development of VOMRS/VOMS migration tools. Such tools will be used to migrate existing VOMRS installations willing to migrate their VO management infrastructure to VOMS admin.

It is still unclear how these last phases' effort will be funded so no reliable conclusion date can be given at this time.

6. Conclusions

In this paper we have presented a plan for merging in a single product the two main VOMS administration and registration services in use today: VOMS-Admin and VOMRS. This convergence, supported by WLCG, OSG, US CMS, US Atlas, and other stakeholders worldwide, yields many benefits, such as a unified coherent interface towards VO management and registration services, simplified development and maintenance of the service code base and more rational and manageable service deployment.

The convergence plan is articulated in five phases, with the major part of the development work (the first three phases) scheduled for completion by the end of the EGEE-III project. As of today it is unclear how the effort for the last phases of the convergence will be funded. We are however positive that the interest in this convergence will draw funding to this project out of future National and European Grid initiatives or organizations (e.g., INFN, Fermilab, CERN) interested in a mature, full-fledged VO registration and management software.

References

[1] The Open Science Grid project URL `http://www.opensciencegrid.org/`
[2] The Enabling Grids for EsciencE project URL `http://www.eu-egee.org/`
[3] Alfieri R, Cecchini R, Ciaschini V, dell'Agnello L, Frohner Á, Lörentey K and Spataro F 2005 *Future Generation Comp. Syst.* **21** 549–558
[4] Farrell S and Housley R 2002 An Internet Attribute Certificate Profile for Authorization RFC 3281 (Proposed Standard) URL `http://www.ietf.org/rfc/rfc3281.txt`
[5] Cantor S, Kemp J, Philpott R and Maler E 2005 Assertions and protocols for the oasis security assertion markup language (saml) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
[6] The OMII project URL `http://omii-europe.org/`
[7] Cantor S, Hirsch F, Kemp J, Philpott R and Maler E 2005 Bindings for the oasis security assertion markup language (saml) v2.0 http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf
[8] Venturi V, Stagni F, Gianoli A, Ceccanti A and Ciaschini V 2007 *e-Science and Grid Computing, International Conference on* **0** 545–552
[9] Tuecke S, Welch V, Engert D, Pearlman L and Thompson M 2004 Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile RFC 3820 (Proposed Standard) URL `http://www.ietf.org/rfc/rfc3820.txt`
[10] Apache Tomcat URL `http://tomcat.apache.org/`
[11] The Joint Security Policy Working Group URL `http://www.jspg.org/`
[12] The Virtual Organization Management Registration Service URL `http://www.uscms.org/SoftwareComputing/Grid/VO`
All the URLs listed in this bibliography have been accessed on May 14, 2009.