THE VIRTUAL ORGANIZATION MANAGEMENT REGISTRATION SERVICE

L. Bauerdick, I. Fisk, A. Heavey, T. Levshina, P. Mhashilkar, R. Pordes, J. Weigand, S. White,
D.Yocum, FNAL, Batavia, IL 60510, USA
A.Sill, Texas Tech University, Lubbock, TX 79409
G. Carcassi, BNL , Upton, NY 11973-5000

Abstract

Currently, grid development projects require end users to be authenticated under the auspices of a "recognized" organization, called a Virtual Organization (VO). A VO establishes resource-usage agreements with grid resource providers.

The Virtual Organization Management Registration Service (VOMRS), developed at Fermilab, provides a comprehensive set of services that facilitates management of VO membership and privileges. It implements a registration workflow that requires email verification of identity, VO usage policy acceptance, membership approval by designated VO representatives or administrators, and allows for management of multiple grid certificates, and the selection of group and role. VOMRS maintains a VO membership status and a certificate level status for each member, allowing for VO-level control of a member's privileges and membership.

VOMRS is capable of interfacing to local systems with personnel information (e.g., the CERN Human Resource Database), and pulling relevant member information from them. VOMRS membership data can be configured to synchronize with the VOMS system (developed jointly for DataTAG by INFN and for DataGrid by CERN) with all approved members' certificates and privileges.

The current architecture and state of deployment will be discussed.

VOMRS SCOPE

VOMRS offers a comprehensive set of services that facilitates secure and authenticated management of VO membership, grid resource authorization and privileges. It implements a registration workflow providing means for collaborators to register with a Virtual Organization (VO). VOMRS supports management of multiple grid certificates per member and permits VO-level control of a member's privileges. It offers a subscription service that sends email notifications when selected changes are made to information about a member's VO membership status and/or when actions are required by members or administrators. VOMRS supports VO-level control over the trusted set of Certificate Authorities (CA). It provides the capability to delegate responsibility among several VOMRS administrators for approval of VO membership, group membership and group roles. It is capable of interfacing with other third-party systems allowing membership information shared.

VOMRS Place in Grid World

The VO management and authorization infrastructure consists of several independent modules:

VOMRS [1]

- The registration service

VOMS [2]

- The EGEE VOMS Admin service provides the distributed storage of member DN, CA, groups and roles, and a means to handle this data.
- The DataTag VOMS Core service generates extended proxy upon member’s request which include group and role as extended attributes.

Prima [3]

The PRIMA authorization module provides fine grain authorization utilizing the extended attributes of the VOMS proxy.

- On the Compute Element (CE) node through a Globus gatekeeper callout.
- On the Storage Element (SE) node through the gPlazma system.

GUMS) [4]

- Provides site-consistent user and group assignment
- Interfaces and extensions to the data storage systems
- Some additional security service deployed at the gird site (e.g. SAZ [5] at Fermilab) that provides additional level of authorization control to site grid resources

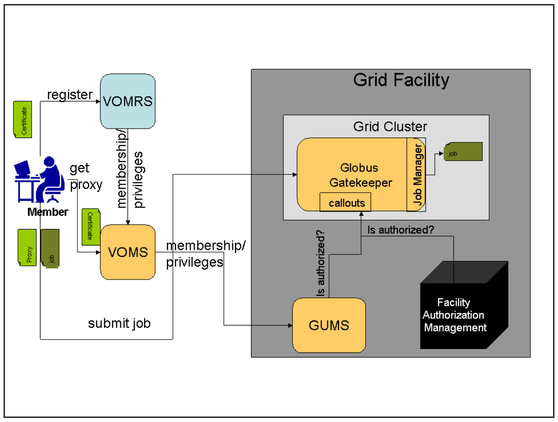


Figure 1 illustrates the interactions between VO management and grid authorization modules

VOMRS Entities

There are several concepts and definitions that are used in the VOMRS project in addition to the standard terminology such as Grid, VO, Certificate, Grid resource, Grid job, etc. The most important entities and their usage within VOMRS are listed below:

- Certificate Authorities: VOMRS allows management of CAs accepted by the VO. It offers a consistent way of handling membership status for members whose certificate's CA have become obsolete or invalid.
- Groups and Group Roles: VOMRS supports hierarchy of groups. It provides a interface to manage groups and group roles.
- Institutions and Sites: VOMRS provides interface to manage Institutions and Sites. It requires member affiliation with an Institution and provides the capability to establish an expiration date on each member.
- Personal Data: VOMRS supports real time editing of personal data collected during the registration process. It distinguishes between private and public data, persistent and non persistent data. VOMRS is configurable allowing each VO to specify the registration stage that personal data is collected and whether the information is obtained from the user or from a third-party source (e.g. CERN Human Resource Database).

VOMRS Administrators

VOMRS allows for delegation of responsibilities within the VO. The following administrators are distinguished within VOMRS:

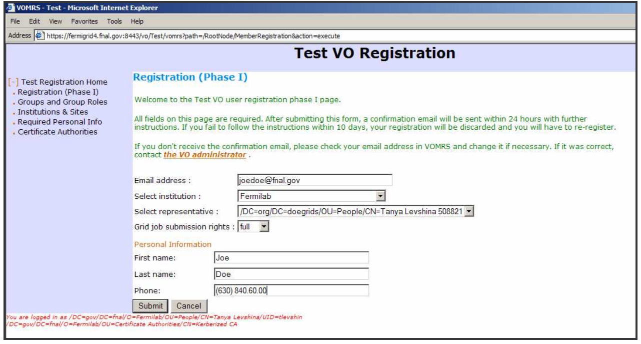
- A VO Admin is responsible for maintaining the VOMRS. A VO admin manages data pertaining to institutions, sites, CAs, members' privileges, and can modify the set of personal information required by the VO.
- A Representative is responsible for approving or denying applicant requests for VO membership based on personal knowledge of each individual applicant's identity and institutional affiliation.
- A Group Owner and a Group Manager are responsible of managing the group's membership and group roles. A Group Manager can create new subgroups and/or group roles.
- A Site Admin and a Local Resource Provider are able to access members' information.

Membership registration

In order to access VOMRS a user is required to have a valid certificate whose CA is recognized by the VO. The registration process consists of two steps.

Phase I

During Phase I a new user fills out personal information, selects a Representative from the list of available Representatives and provides her/his email address. Figure 2 shows the example of Phase I of WEB UI.



https://fermigrid4.fnal.gov:8443/vo/Test/vomrs?path=/RootNode/MemberRegistration&action=execute

Test VO Registration

Registration (Phase I)

Welcome to the Test VO user registration phase I page.

All fields on this page are required. After submitting this form, a confirmation email will be sent within 24 hours with further instructions. If you fail to follow the instructions within 10 days, your registration will be discarded and you will have to re-register.

If you don't receive the confirmation email, please check your email address in VOMRS and change it if necessary. If it was correct, contact *the VO administrator* .

Email address : joedoe@fnal.gov
Select institution : Fermilab
Select representative : /DC=org/DC=doegrids/OU=People/CN=Tanya Levshina 508821
Grid job submission rights : full

Personal Information
First name: Joe
Last name: Doe
Phone: (630) 840.60.00

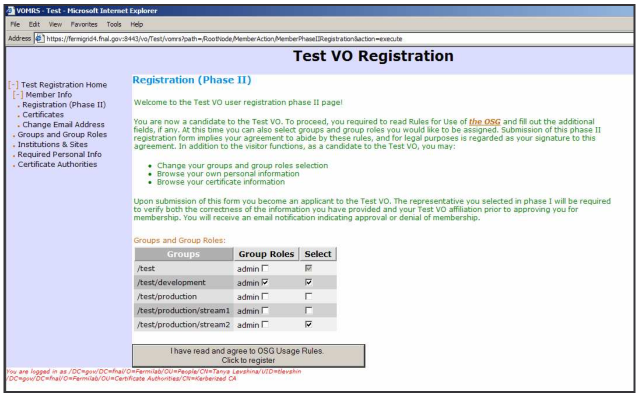
You are logged in as /DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Tanya Levshina/UID=tlevshin /DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Kerberized CA

Figure 2 Phase I of registration procedure

After receiving email notification, a user proceeds to Phase II by accessing the url in the email notice.

Phase II

In Phase II, the applicant provides any personal information required, selects the group(s) and group role(s) desired and signs the Usage Rules document for the VO.



https://fermigrid4.fnal.gov:8443/vo/Test/vomrs?path=/RootNode/MemberAction/MemberPhaseIIRegistration&action=execute

Test VO Registration

Registration (Phase II)

Welcome to the Test VO user registration phase II page!

You are now a candidate to the Test VO. To proceed, you required to read Rules for Use of *the OSG* and fill out the additional fields, if any. At this time you can also select groups and group roles you would like to be assigned. Submission of this phase II registration form implies your agreement to abide by these rules, and for legal purposes is regarded as your signature to this agreement. In addition to the visitor functions, as a candidate to the Test VO, you may:

- Change your groups and group roles selection
- Browse your own personal information
- Browse your certificate information

Upon submission of this form you become an applicant to the Test VO. The representative you selected in phase I will be required to verify both the correctness of the information you have provided and your Test VO affiliation prior to approving you for membership. You will receive an email notification indicating approval or denial of membership.

Groups and Group Roles:

Groups	Group Roles	Select
/test	admin ☐	☑
/test/development	admin ☑	☑
/test/production	admin ☐	☐
/test/production/stream1	admin ☐	☐
/test/production/stream2	admin ☐	☑

I have read and agree to OSG Usage Rules.
Click to register

You are logged in as /DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Tanya Levshina/UID=tlevshin /DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Kerberized CA

Figure 3 Phase II of registration procedure

In order to become a VO member with grid resource privileges, the user's registration must be approved by user's Representative or VO Admin.

Notification Events

An event in the VOMRS constitutes any changes to member's status or privileges. For example, an event is generated each time a new administrative role is assigned, a member’s certificate is suspended or a member is assigned to group. Events are also created when the structure of the VO has been altered. For example, an event is generated when a new group is inserted, the expiration of a CA certificate is changed, or an institution is added.

Events can trigger a call to an external system via a registered interface. Some events can require action to be taken by a VO member. For example, a Representative is asked to approve/deny a registration or a member is asked to sign a new Usage Rules document.

The events to which the member can subscribe depend upon the member’s roles and membership status.

Membership and Certificate Statuses

VOMRS maintains a membership status. The following membership status can be assign to a user:

- New
- Approved
- Denied
- Suspended: member is currently not in good standing in the VO
- Expired: occurs when a new Usage Rules document must be signed; member's validity period has expired; member's institutional affiliation has expired

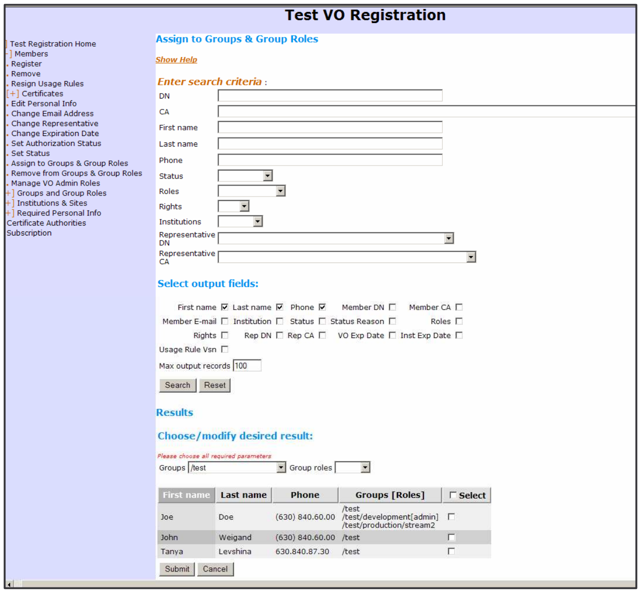
A Member can possess multiple certificates. Each certificate has its own status. The following certificate statuses are recognized:

- New
- Approved
- Denied
- Suspended: the certificate has been somehow compromised
- Expired: indicates that the certificate issuer does not currently have a valid certificate

Each VO member has at least one registered certificate. Only a valid member (with approved membership status) can request additional certificates. Each such request must be approved by VO Admin. A member can access VOMRS using any approved certificates.

Group and Group Roles

A VO Applicant or Member can select the group and group role association desired. VO Administrators such as Group Owner, Manager or VO Admin can assign group and group roles to any member as well. They can also block a member’s association with any group or group role. Once a member’s association with group or group role within group is blocked, a member can not choose it again until an administrator re-assigns her/him to this group.



Assign to Groups & Group Roles

Enter search criteria :

DN

CA

First name

Last name

Phone

Status

Roles

Rights

Institutions

Representative DN

Representative CA

Select output fields:

First name ☑ Last name ☑ Phone ☑ Member DN □ Member CA □
Member E-mail □ Institution □ Status □ Status Reason □ Roles □
Rights □ Rep DN □ Rep CA □ VO Exp Date □ Inst Exp Date □
Usage Rule Vsn □

Max output records 100

Results

Choose/modify desired result:

Please choose all required parameters

Groups /test Group roles

First name	Last name	Phone	Groups [Roles]	□ Select
Joe	Doe	(630) 840.60.00	/test /test/development[admin] /test/production/stream2	□
John	Weigand	(630) 840.60.00	/test	□
Tanya	Levshina	630.840.87.30	/test	□

Figure 5 Group and Group Role assignment page for VO Admin

Interfacing Third Party Software

Interfaces can be registered with VOMRS and can be subscribed to receive event notification. Currently there are three interfaces:

- “LCG” Registration Type. For this type a user's registration in the CERN HR DB is verified via a query during Phase I of the VOMRS registration. No data is downloaded from CERN DB to VOMRS. A VOMRS instance can be configured such that whenever an administrator queries a member's personal data, the CERN HR DB is queried and both the VOMRS and CERN DB data displayed together.
- “SAM” [6] Registration Type. This type mandates VOMRS to query the SAM DB to obtain list of SAM’s group. The SAM DB is updated by using sam-admin commands when a member’s status/privileges are changed.
- EGEE VOMS. VOMS is updated by using the VOMS Admin API when a member’s status/privileges are changed, and group/role added or removed. Only the valid certificates of the valid members are propagated to VOMS.

Since Last CHEP

The following major features are added to VOMRS since last CHEP:

- Implemented “LCG” Registration type using LCG Registration API (developed by K.Lorentey) to verify member standing with CERN HR DB
- Integrated with SAM by using VOMRS-SAM API
- Implemented Oracle support

- Implemented two phases of registration that include email verification
- Introduced VO and institutional membership expiration
- Introduced VO-level management of CAs
- Implemented selection of groups and group roles by member
- Added multipart messaging, improved message format
- Implemented customizable on-line help

Implementation and Distribution Details

VOMRS is Java based. It requires java version 1.4.1 or higher. WEB UI uses JavaScript. All configuration scripts are written in python (version 1.5 and higher) and configuration files are in xml format. VOMRS supports both Oracle and Mysql dbms.

The current distribution of VOMRS software is built with EGGE trustmanager package (gLite 1.4 [7]) and can be synchronized with EGGE VOMS by using VOMS Admin API (gLite 1.4). VOMRS components are distributed using Pacman[8] and are available from the cache:
http://www.uscms.org/SoftwareComputing/Grid/VO/VOMRS
RPMs are available from:
http://www.uscms.org/SoftwareComputing/Grid/VO/downloads.html

Current Deployment

Currently VOMRS is deployed on the several sites:

- Fermilab: 14 instances with total number of registered users > 5,000
- CERN: 4 instances are using "LCG Registration Type" and connect to CERN HR DB. 5 instances are using "General Registration Type". Total number of registered users > 190.
- BNL: 2 instances (all are synchronized with corresponding installation of VOMS).
- Test installations:
    - 2 instances in Texas Tech University
    - 1 instance in University of Melbourne

All instances are synchronized with corresponding installation of VOMS.

Dependencies and Issues

VOMRS uses internally EGEE trustmanager and VOMS Admin API to push relevant information to VOMS. That is why the support of these packages is crucial for VOMRS. There are several issues that have to be addressed in order to improve VOMRS/VOMS reliability. For the time being the bug fixing is slow, the fixes releases are depended on gLite releases and their integration in VDT.

We are working very closely with LCG VO Management Registration Task Force. LCG VO Managers submitted many constructive requests for improvements and new features. Most have been implemented in previous releases. New requests included:

- implement a hierarchy of representative associates with country, region and institution
- allow customizable description of roles and group roles
- improve VOMRS performance
- add configurable subject in notification emails

We are planning to transfer some of the responsibilities for VOMRS support to a yet to be chosen person at CERN. VOMRS/VOMS workshop is planned in March.

Summary

VOMRS is a successfully implemented VO registration service providing the means to better identify and communicate with VO members, and to assign grid privileges to them. Through the use of its multiple administrative roles, VOMRS allows for delegation of responsibilities within the VO while still providing a high level of control over privileges granted. As a highly configurable service, it can meet the needs of a wide variety of VOs , both in terms of membership size and complexity of privileges required. Its installation at numerous sites has resulted in increased requests for additional features to improve management and control of VO membership.

Fermilab is committed to future support of this product for the LCG and OSG.

ACKNOWLEDGEMENTS

We greatly appreciate discussions, support and software contributions provided by our collaborators at BNL, TTU, CERN, and INFN as well as OSG and VDT.

REFERENCES

[1] http://www.uscms.org/SoftwareComputing/Grid/VO/
[2] http://glite.web.cern.ch/glite/security/
[3] http://www.fnal.gov/docs/products/voprivilege/.
[4] http://grid.racf.bnl.gov/GUMS/.
[5] http://computing.fnal.gov/docs/products/saz/SAZ.htm
[6] http://projects.fnal.gov/samgrid/WhatisSAM.html
[7] http://glite.web.cern.ch/glite/
[8] http://physics.bu.edu/pacman/