THE VIRTUAL ORGANIZATION MEMBESHIP SERVICE EXTENTION PROJECT (VOX)

T. Levshina[#], L. Bauderick, E. Berman, I. Fisk, G. Graham, A. Heavey, J. Kaiser, R. Pordes, V. Sekhri, D. Skow, J. Weigand, Y. Wu, FNAL, Batavia, IL 60510, USA
R. Baker, G. Carcassi, BNL , Upton, NY 11973-5000
R. Gardner, University of Chicago, Chicago, IL 60637
L.Grundhoefer, University of Indiana, Bloomington, IN 47405-7000

Abstract

Current grid development projects are being designed such that they require end users to be authenticated under the auspices of a "recognized" organization, called a Virtual Organization (VO). A VO must establish resource-usage agreements with grid resource providers. The VO is responsible for authorizing its members for grid computing privileges. The individual sites and resources typically enforce additional layers of authorization.

The VOX project developed at Fermilab is an extension of VOMS, developed jointly for DataTAG by INFN and for DataGrid by CERN. The VOX project provides set of services that facilitate grid users registration with a VO, administration of VO members, as well as control access of grid users to a particular site. The current state of deployment and future steps to improve the prototype and implement some new features will be discussed.

VOX COMPONENTS

The Virtual Organization Membership Registration Service (VOMRS) is a major component of the VOX project. VOMRS is a service that provides the means for registering members of a VO, and coordination of this process among the VO and grid administrators. It consists of a database to maintain user registration and institutional information, a server to handle members' notification and synchronization with various interfaces, web services and a web user interface for the input of data into the database and manipulation of that data.

The VOX project also includes a component for the Site AuthoriZation (SAZ), which allows security authorities at a site to control access to site resources.

VO Management Infrastructure at Fermilab

VO management infrastructure at Fermilab consists of several independent projects that include:

- VOX Project [1]
  - VOMRS
  - SAZ
- VOMS Project [2]
  - EGEE (EDG) VOMS Admin service provides distributed storage of member DN, CA, groups and roles, means to handle this data.
  - DataTag VOMS Core service generates extended proxy upon member's request which include group and role as the attributes.
- Privilege Project [3] automates and facilitates the process of managing fine grain access to a local grid element:
  - PRIMA authorization module at the gatekeeper
    - § elicits information from provided VOMS attributes and other sources
    - § queries a site centralized grid user management server (GUMS) [4]
- GUMS) [4] provides
  - site-consistent user and group assignment
  - interfaces and extensions to the data storage systems

Figure 1 illustrates the connection between these projects.

[#]tlevshin@fnal.gov

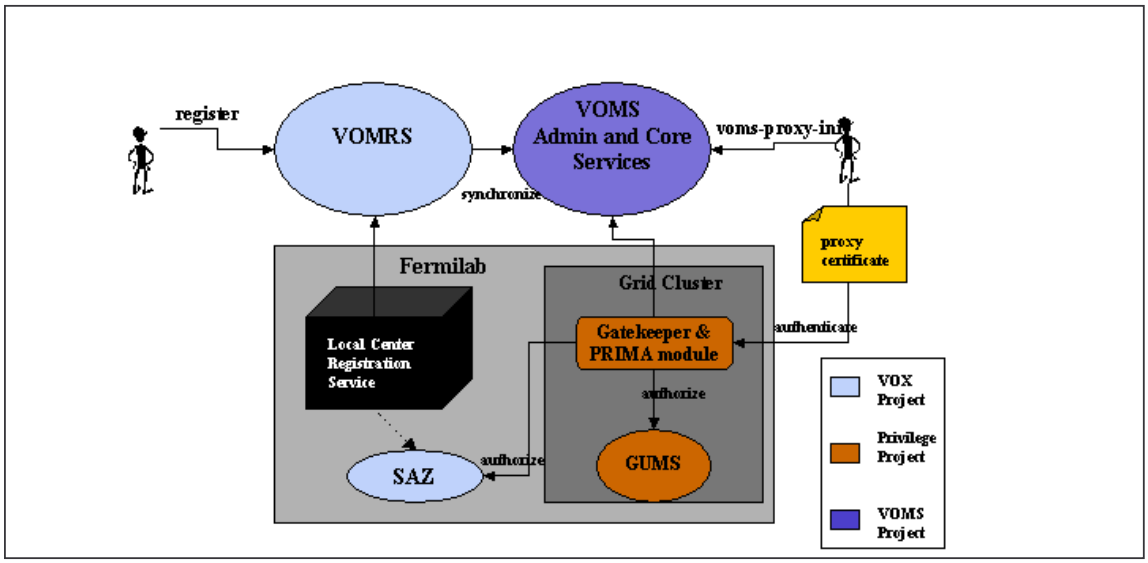

Figure 1: VO Management Infrastructure at Fermilab

VOMRS Glossary [5]

There are several concepts and definitions that are used in VOX project in addition to a standard terminology such as Grid, VO, Certificate, Grid resource, Grid job, etc. The most important ones are defined below:

Experiment: represents research activities that are specific to a particular VO.

Group and group roles: an experiment contains groups. A group may have sub-groups. Group and group roles are included as attributes in a proxy certificate submitted with a grid job.

Institution: is an organization whose members participate in experiments within a particular VO.

Grid site: is an institution that provides grid resources. Each site has policies that require specific personal information.

Personal information: private and public data about an individual that is collected by the VO.

Notification Event: an action taken by the registration software that notifies interested members of a change within the VO and describes any required responses if any.

VOMRS Role: defines actions that a VO Member can perform within the VO and information that a VO Member can access. A VO member can have one or more roles. A VO member event notification depends on member's role.

VOMRS Roles

The VOMRS has adopted a technique of member-to-services mapping in which the permissions for performing particular services in the VOMRS are grouped into a role. An individual who possesses a valid certificate from a trusted CA (a CA trusted by the VO), automatically has the role of "visitor" with respect to the VO. Once a visitor has applied for VO membership but has not yet been approved, he or she is assigned the role of "applicant". Once an applicant has been approved, his or her role is changed to "member".

The state transition diagram of member's registration status is shown in Figure 2.

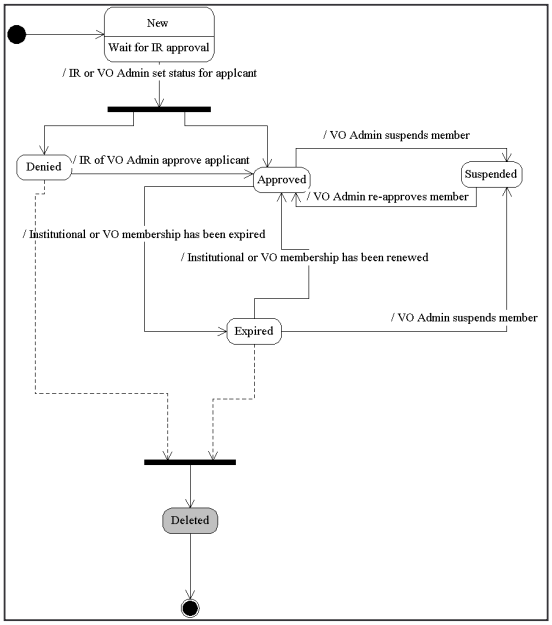

Figure 2:State transition diagram - Member's Registration Status

In addition to the member role, designated VO members may be assigned one or more administrative

roles, granting them greater permissions that go along with greater responsibilities within the VOMRS system.

The most important administrative roles and associated reponsibilities are listed below:

- VO Admin is a designated VO member who is in charge of registration and has access to all information collected by the VO. He is responsible for assigning administrative roles.
- Institutional Representative (IR) vouches for the identity of an applicant when approving applicant's registration request.
- Grid site administrator (SiteAdmin) has access to member personal stored in a VO. He can administer authorization of VO member to the site. The details are site specific and depend on regulations and policies of each particular site.
- Local resource provider (LRP) has access to member's public data stored in a VO. LRP can administer authorization a member to use the grid resource (this could include addition of this member to the gridmapfile, mapping member to local account, etc).

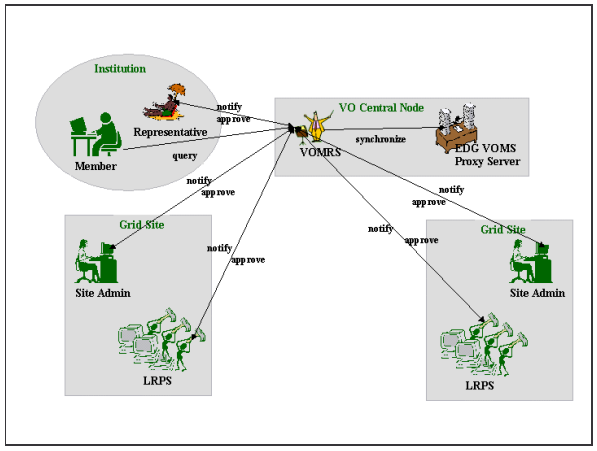

Figure 3: VO Member's Registration flow

VOMRS Architecture

The VOMRS includes the following components:

- A Server (written in Java) is a multithreaded daemon process that is capable of performing the following tasks:
  - Handling remote client request to perform VO membership service
  - Handling event and interface notification
  - Synchronizing VOMRS with VOMS database

  Server behavior is controlled by configuration written in xml
- VOMRS database (MySQL)
- CLI (in Java with GSI authentication (Java Cog Kit [6]) is using proprietary protocol to communicate with a VOMRS server
- Web Services (in Java with SOAP/SSL authentication EDG Trust Manager [7])
- WEB UI (in Java, Java script) with HTTP/SSL authentication EDG Trust Manager). WEB UI behavior is controlled by configuration written in xml

The details of VOMRS architecture is shown on figure 4.

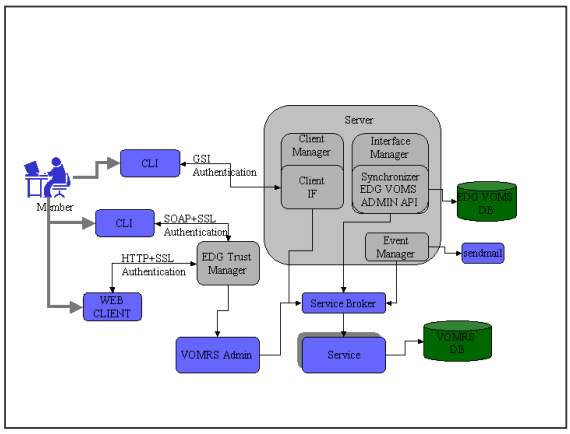

Figure 4: VOMRS Architecture

The VOMRS has a notion of services. Each service is characterized by the action it performs within VOMRS database. Each service is associated with the set of administrative roles and list of input and output arguments. The VOMRS service will failed if the service requester does not have an appropriate role within the VO, or supplies invalid set of arguments.

CLI, WEB services and UI are capable of requesting any available service, the role of requester will be defined by mapping the requester's certificate to his role in VOMRS database.

WEB UI

The majority of WEB UI screens allow to enter query criteria, select output fields and submit a query. After a query is processed, its result is appended to the bottom of the screen. Some of the screens are informational only. Many of the screens include help text. All the terms used to identify database fields and menu options are defined via pop-up help text.

A VO administrator may customize some features of the screens, e.g., VO-specific screen headings, via a configuration file.

There are four basic types of screens in the VOMRS WEB UI:

- informational

- query-only
- query and edit data
- data entry

Some of the screenshots are shown below.

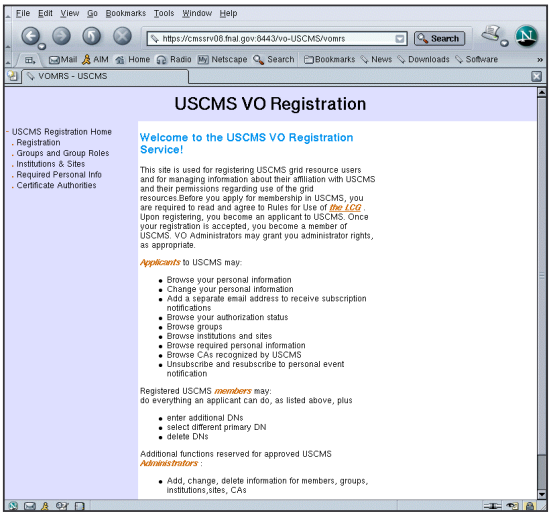

Figure 5: Welcome Page

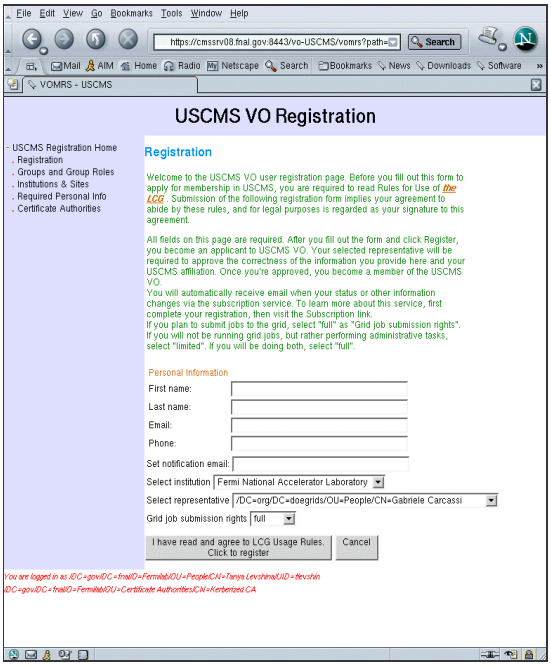

Figure 4:Member Registration Page

Future developments plan

The following improvements and new features will be implemented in the nearest future:

- Continue collaboration with BNL, SDSS, iVDGL, LCG User Registration Task Force etc

- Implement multiple new features requested by collaborators:
  VO membership expiration and renewal processes
  Email verification
  Interface to organizational human resource database (LCG requirement)
- Continue support for VOMRS instances installed at Fermilab and BNL
- Deploy test installation of VOMRS at CERN

ACKNOWLEDGEMENTS

We greatly appreciate discussions, support and software contributions provided by our collaborators at BNL, SDSS, iVDGL, CERN and INFN.

REFERENCES

[1] http://www.uscms.org/s&c/VO/.
[2] http://grid-auth.infn.it/.
[3] http://www.fnal.gov/docs/products/voprivilege/.
[4] http://www.atlasgrid.bnl.gov/testbed/gums/introduction.shtml/.
[5] http://computing.fnal.gov/docs/products/vomrs/wwhelp/wwhimpl/java/html/wwhelp.htm/.
[6] http://www-unix.globus.org/cog/java/.
[7] http://edg-wp2.web.cern.ch/edg-wp2/security/edg-java-security.html/.