
VO Management

Tanya Levshina
Computing Division, Fermilab

Talk Outline

- VO and Scope of VO Management
- OSG VO Policy
- VO Management Software in VDT
- Who needs VOMRS and Why?
- VOMRS Main Features Overview
- Member registration and other tasks
- VO Administrators and their responsibilities
- Distribution, deployment and support
- Questions
- Additional slides

What is a Virtual Organization?

- Virtual Organization consists of *“a number of mutually distrustful participants with varying degrees of prior relationship (perhaps none at all) that want to share resources in order to perform some task.”* - Ian Foster
- *“A Virtual Organization (VO) is a collection of people (VO members), computing/storage resources (sites) and services (e.g., databases).”* - from OSG About Page

Scope of VO Management

VO Management:

- seeks to institute and incorporate policies and procedures for working in grid environment
- handles VO membership
- assigns different privileges to members of the VO
- establishes resource-usage agreements with grid resource providers

OSG VO Policy – do not panic yet!

OSG is adopting a VO Policy that the VO Managers will need to adhere to. There are software packages that facilitate all these tasks and they are in VDT!

The VO Managers will:

- maintain a VO membership service to generate authentication/ authorization/id-mapping data for VO services running on the sites
- ensure correct and up-to-date information of the VO members
- apply due diligence in maintaining the confidentiality of such information
- maintain logs of access to and changes to the VO Membership
- use logged and membership information for administrative, operational, accounting, monitoring and security purposes only
- respond promptly to requests or complaints from the Participants in the OSG
- inform the user when access is limited or suspended and restore access as soon as reasonably possible
- provide and maintain accurate contact information on where to report problems with the VO

VO Management Software in VDT

There are two VO Management software packages in VDT:

- Virtual Organization Membership Service (VOMS) developed and supported by EGEE
- Virtual Organization Management Registration Service (VOMRS) developed at Fermilab.
 - built on top of VOMS, has many additional features
 - compliant with OSG VO Policy
 - allows plug-in interfaces to existing HR databases (CERN, Fermilab)

Who needs VOMRS and Why?

- VOs operating across OSG and EGEE need to use VOMRS because it is compliant to OSG VO Policy and requirements for WLCG project and EGEE VOs
- It facilitates management of VOs that need to maintain
 - numerous users
 - hierarchy of administrators
 - delegation of responsibilities
 - persistent membership status
 - VO and institutional membership expiration
 - dynamic set of collected personal information
- and requires notification about
 - changes in VO membership or structure
 - actions required from members or administrators

VOMRS Main Features

VOMRS offers a comprehensive set of services that facilitates secure and authenticated management of VO membership, grid resource authorization and privileges:

- implements a registration workflow providing means for collaborators to register with a Virtual Organization (VO)
- supports management of multiple grid certificates per member
- permits VO-level control of member's privileges
- provides email notifications of selected events
- keeps track of Grid and VO AUPs signed by members
- supports VO-level control over its trusted set of Certificate Authorities (CA)
- permits delegation of responsibilities within the various VO administrators
- manages groups and group roles
- is capable of interfacing to third-party systems and pulling or pushing relevant member information from/to them. Currently there are three known interfaces:
 - “LCG” Registration Type - CERN HR database
 - “SAM” Registration Type – Fermilab CNAS, SAM DB
 - EGEE VOMS for synchronization

What a Member Needs To Know About VOMRS

In order to access VOMRS a user is required to have a valid certificate whose CA is recognized by the VO.

First, a user should register with VOMRS. Registration consists of two steps:

- Phase I - fill out registration form
- After receiving email notification, a user proceeds to Phase II – group selection, AUP signing
- wait for approval for VO membership and group and group role assignment. As soon as membership is approved and groups and group roles are assigned a user becomes a VO member and can use voms-proxy-init to generate an extended proxy certificate and start grid job submission


At any time a member:

- may request a new group and group role assignment
- add an additional certificate to the certificate list. As soon as a new certificate is approved a member could use it to generate a voms proxy
- modify personal information, including email
- re-sign a VO AUP upon request

WEB UI Example (Registration Phase I)

VOMRS - Test - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address  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 :

Select institution :

Select representative :

Grid job submission rights :

Personal Information

First name:

Last name:

Phone:

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

During Phase I a new user:

- fills out personal information
- selects a Representative and an Institution
- provides an email address

WEB UI Example (Registration Phase II)

The screenshot shows a web browser window titled "VOMRS - Test - Microsoft Internet Explorer". The address bar shows the URL: `https://osg-ress-2.fnal.gov:8443/vo/Test/vomrs?path=/RootNode/MemberAction/MemberPhaseIIRegistration&action=execute`. The page has a navigation menu on the left with links like "Test Registration Home", "Member Info", "Registration (Phase II)", "Certificates", "Change Email Address", "Groups and Group Roles", "Institutions & Sites", "Required Personal Info", and "Certificate Authorities". The main content area is titled "Test VO Registration" and "Registration (Phase II)". It includes a welcome message, a paragraph explaining the registration process, a list of actions (Change your groups and group roles selection, Browse your own personal information, Browse your certificate information), and a paragraph about submission. Below this is a table titled "Groups and Group Roles:" with columns: Group, Group Description, Group role, Group Role Description, Status, and Select. The table lists various groups and roles, with the root group "/test" being approved. At the bottom, there is a checkbox for "I have read and agree to the Grid and VO AUPs." and a "Click to register" button. A status bar at the very bottom shows the user is logged in as "/DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Tanya Levshina/UID=tlevshin".

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 the Grid and VO AUPs of [the OSG Grid](#) 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:

Group	Group Description	Group role	Group Role Description	Status	Select
/test	The root group of this VO			Approved	<input checked="" type="checkbox"/>
/test/production	group for grid production				<input type="checkbox"/>
		admin	this is a role for gridadministrators		<input type="checkbox"/>
		operator	this is a role for operators		<input type="checkbox"/>
/test/production/stream1	stream#1 group				<input type="checkbox"/>
		admin	this is a role for gridadministrators		<input type="checkbox"/>
		operator	this is a role for operators		<input type="checkbox"/>
/test/production/stream2	stream#2 group				<input type="checkbox"/>
		admin	this is a role for gridadministrators		<input type="checkbox"/>
		operator	this is a role for operators		<input type="checkbox"/>
/test/test	group for testing				<input type="checkbox"/>
/test/test/test1	group #1 for testing				<input type="checkbox"/>

Please read [the Grid and VO AUPs](#) before you sign it!

☐ I have read and agree to the Grid and VO AUPs.
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=Kerberos CA

After receiving email notification,
a user proceeds to Phase II:

- selects group(s) and group role(s)
- signs the AUP for the VO

What VOMRS Administrators Should Worry About?

- **VO Admin** is responsible for maintaining the VOMRS. A VO admin
 - manages data pertaining to institutions, sites, CAs, group role
 - members' privileges
 - suspends/expires/denies/approves membership's status
 - denies/approves member's group and role affiliation
 - assigns administrative role
 - controls set of personal information required by the VO
 - controls version of AUP and its contents
- **Representative** is responsible for:
 - approving/denying applicants' requests for VO membership based on personal knowledge about each individual applicant's identity and institutional affiliation
 - setting institutional expiration date for member
- **Group Owner** and **Group Manager** are responsible for:
 - managing the group's membership
 - Group Manager can create new subgroups and associate group roles with them
- **Site Admin** and **Local Resource Provider** are responsible:
 - may indicate approval/denying membership access to the site/resource

Watch for Notification Events!

An event in the VOMRS constitutes any changes to:

- member's status/privileges:
 - new administrative role is assigned
 - certificate is suspended
 - member is assigned to group
- structure of the VO:
 - creation of a new group
 - expiration of a CA
 - addition of an institution

Events can trigger a call to external system via registered interface.

Some events can required action to be taken by a VO member:

- a Representative is asked to approve/deny registration
- a member is asked to sign a new AUP

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

Distribution, Current Deployment and Support

■ Product distribution:

- ❑ VOMRS is distributed via VDT (starting with VDT 1.7)
- ❑ rpm is available from:
<http://www.uscms.org/SoftwareComputing/Grid/VO/downloads.html>

■ Deployment

- ❑ Fermilab: 14 instances, number of registered users > 5,000
- ❑ CERN: 9 instances, number of registered users > 3,000
- ❑ BNL: 2 instances; Texas Tech University: 2 instances ; APAC (Australia Grid): 2 instances DESY:2 instances

■ Support

- ❑ More information at
<http://www.uscms.org/SoftwareComputing/Grid/VO/index.html>
- ❑ Email: privilege_project@fnal.gov
- ❑ Report a bug:
<https://savannah.cern.ch/> or <http://cmssrv07.fnal.gov/bugzilla/> (local access only)

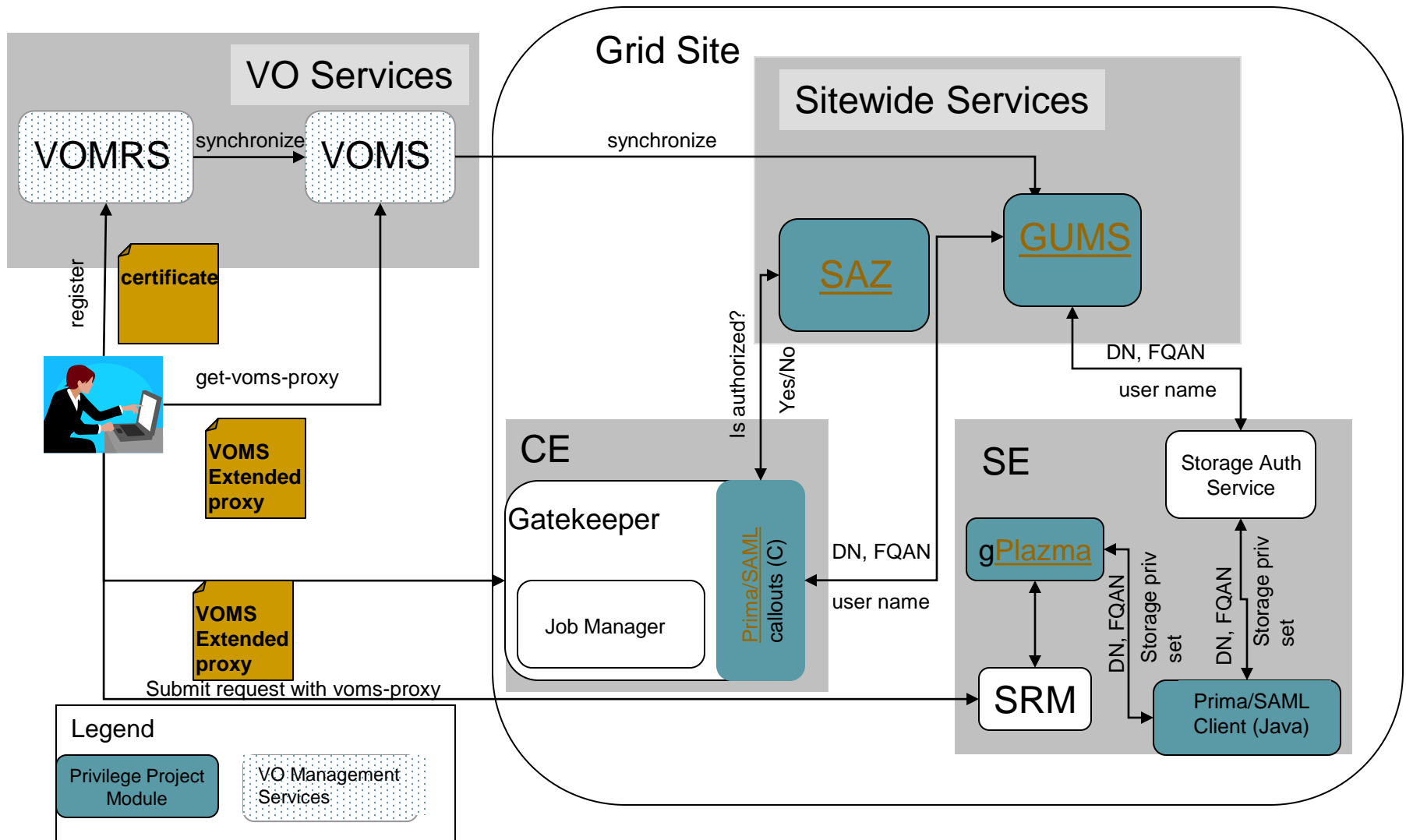
Questions from the Audience?

- What do YOU need as regards Management of your VOs?
- Does VOMRS give you what you need?

Additional Slides

- VO Management Software place in Grid World
- VOMRS Entities
- VOMRS Administrators
- Membership and Certificate Statuses
- Groups and Group Roles
- Group and Group Role Assignment
- Help file tailoring
- Synchronization with VOMS

VO Management Software place in Grid World



VOMRS Entities

Certificate Authorities

- ❑ allows list management of CAs accepted in VO
- ❑ offers a consistent way of managing membership status for members whose certificate CAs become obsolete or invalid

Groups and Group Roles

- ❑ supports hierarchy of groups
- ❑ allows creation/deletion of group roles and their association with group
- ❑ provides interface to manage groups and group roles

Institutions and Sites

- ❑ provides interface to manage Institutions and Sites
- ❑ requires member affiliation with Institution; expiration date imposed

Personal Data Set

- ❑ supports real time editing of data set collected during registration
- ❑ distinguishes between private and public data, persistent and non persistent data, etc

Grid and VO Acceptable Use Policies

- ❑ keeps versioning of the documents
- ❑ allows local or remote access to the documents
- ❑ requires member to re-sign periodically the latest version of AUP, expiration date imposed

Membership and Certificate Statuses

Membership status

- ❑ New
- ❑ Approved
- ❑ Denied: an applicant is not allowed to be a VO member
- ❑ 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

Certificate status

- ❑ New
- ❑ Approved
- ❑ Denied: a certificate could not be added to member's certificate list
- ❑ Suspended: the certificate has been somehow compromised
- ❑ Expired: indicates that certificate issuer does not currently have a valid certificate

Multiple certificates per member

- ❑ Each VO member has at least one registered certificate
- ❑ A valid member can request additional certificates
- ❑ Each such request should be approved by VO Admin
- ❑ Member can access VOMRS by using one of the approved certificates

Groups and Group Roles

- A group is an organizational entity defined by the VO.
- A group has an access type (Open, Restricted), a description and set of group roles associated with it
- Groups may be organized hierarchically such that the ownership attribute of a parent group is automatically inherited by a child group
- The hierarchy starts with a single VO-wide root group, owned by a VO administrator, to which all members get automatically assigned
- A group may have a Group Owner that controls subgroups creation, appoints Group Managers. Each Group Owner is a Group Manager
- A group may have a Group Manager responsible for managing group membership
- A group role is created by a VO Admin
- A group role can be linked by a Group Owner to a particular group and assigned an access to this group role within this group

The screenshot shows a web browser window titled "VOMRS - Test - Microsoft Internet Explorer". The address bar shows a URL from "osg-ress-2.fnal.gov". The page is titled "Test VO Registration" and displays the "Groups and Group Roles" section. On the left is a navigation menu with links like "Test Registration Home", "Members", "Groups and Group Roles", "Institutions & Sites", "Required Personal Info", "Certificate Authorities", and "Subscription". The main content area has a "Show Help" link, a search criteria input field with "/test" entered, and checkboxes for "Group Access", "Group Description", "Group Role Access", "Group Role Description", "Group owners", and "Group managers". Below this is a table listing various groups and their roles.

Group	Group Access	Group Description	Group Role	Group Role Access	Group Role Description	Group owners
/test	Open	The root group of this VO				
/test/production	Restricted	group for grid production				Huckleberry Finn
			admin	Restricted	this is a role for gridadministrators	
			operator	Restricted	this is a role for operators	
/test/production/stream1	Restricted	stream#1 group				
			admin	Restricted	this is a role for gridadministrators	
			operator	Restricted	this is a role for operators	
/test/production/stream2	Restricted	stream#2 group				
			admin	Restricted	this is a role for gridadministrators	
			operator	Restricted	this is a role for operators	
/test/test	Open	group for testing				
/test/test/test1	Open	group #1 for testing				

Group and Group Role Assignment

- A VO Member can request a group and a group role membership.
- A Member needs administrator's approval in order to be assigned to a Restricted group or a group role.
- A Group Manager can approve or deny member's request
- If a Member is assigned to be in a subgroup, he is automatically assigned to all the parent groups
- If a Member is denied access to a group he is automatically denied access to all subgroups if this group

VOHRS - Test - Microsoft Internet Explorer

Address: https://osg-ress-2.fnal.gov:8443/vo/Test/vohrs/path=/RootNode/MemberAction/ManageGroupAssignment&action=execute&do=select

Test VO Registration

Manage Groups & Group Roles

Enter search criteria:

DN:

CA:

First name:

Last name:

Phone:

Position held:

Status:

Roles:

Rights:

Institutions:

Representative DN:

Representative CA:

Groups:

Group Roles:

Group/Group Role Status:

Select output fields:

First name ☒ Last name ☒ Phone ☐ Position held ☐ Member DN ☐
 Member CA ☐ Member E-mail ☐ Institution ☐ Status ☐ Status Reason ☐
 Roles ☐ Rights ☐ Rep DN ☐ Rep CA ☐ VO Exp Date ☐
 Inst Exp Date ☐ AUPs Vsn ☐

Max output records:

Results

Choose/modify desired result:

Please choose all required parameters

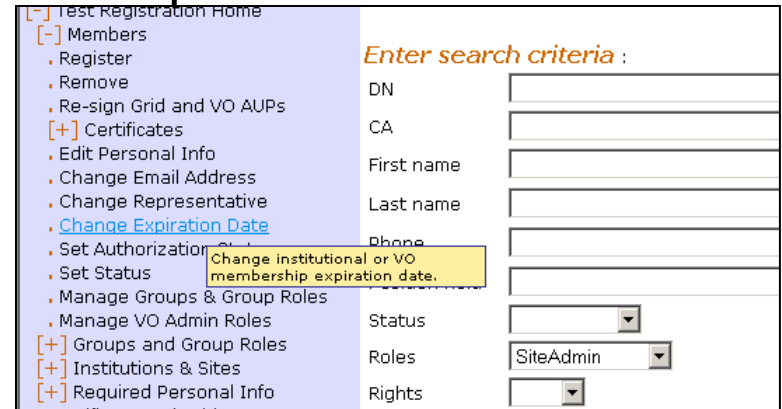
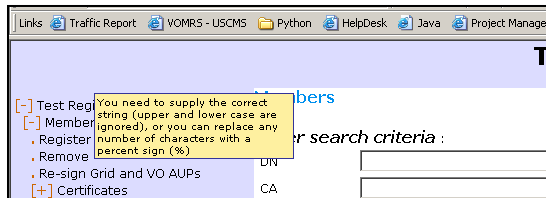
Status:

First name	Last name	Group	Group role	Status	Select
Huckleberry	Finn	/test		Approved	<input type="checkbox"/>
		/test/production		Approved	<input type="checkbox"/>
			admin		<input type="checkbox"/>
			operator		<input type="checkbox"/>
		/test/production/stream1			<input type="checkbox"/>
			admin		<input type="checkbox"/>
			operator		<input type="checkbox"/>
		/test/production/stream2			<input type="checkbox"/>
			admin		<input type="checkbox"/>
			operator		<input type="checkbox"/>
		/test/test			<input type="checkbox"/>
		/test/test/test1			<input type="checkbox"/>

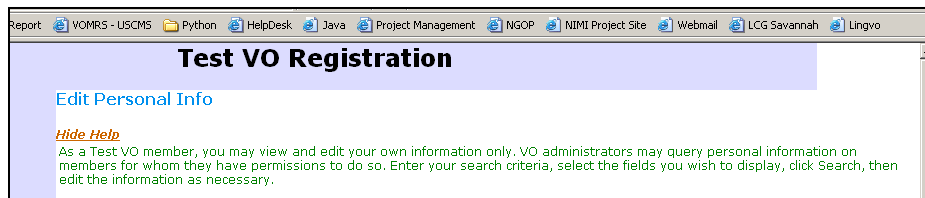
Help file tailoring

■ VOMRS has several kinds of on-line help

□ mouseover help with delay



□ Show/Hide help on the page



■ Help information available in a file in XML format. Administrator could modified any part of this file. Each instance of VOMRS installed on one node could have its own help file.

Synchronization with VOMS

- Member certificate's subject and issuer are
 - added to VOMS when
 - member has an Approved status in VOMRS
 - member's certificate has an Approved status in VOMRS
 - removed from VOMS when
 - Member's certificate is Suspended or Expired in VOMRS
 - Member's status is Suspended or Expired in VOMRS
 - Member is removed from VOMRS
- Member is assigned/dismiss to/from group/role when
 - group/role membership is approved/denied in VOMRS
- Groups and group roles are added to VOMS as soon as they are added to VOMRS
- Groups and group roles are deleted from VOMS as soon as they are deleted from VOMRS
- VO Admin in VOMRS is a VO-Admin in VOMS