

Virtual Organisations and the NGS

Mike Jones

Research Computing Services

e-Science & “The Grid” for Bio/Health Informaticians, IT407

18 January 2008

Virtual Organisations

What is a Virtual Organisation

- Is it like an organisation, only virtual?
 - Does it need to be a *legal entity*?
 - *not always but to function fully will probably need at least one legal representative*
- Is it a group of people?
 - Does it need to be more than one person?
- An inter-organisation entity
 - Does it need to involve more than one *organisation*?
 - *Does it need to involve any organisation?*
- Is it only about people?
 - Organisations have buildings, computers, data, ...

Defining A VO As A Grid Entity

- Lists
 - of Members
 - *of Distinguished Names*
 - *of Certificates*
 - *of DNs + the DN of the issuer*
- Lists express
 - VO Memberships
 - Role Memberships
 - Group Memberships
 - ...
- Regulations/T&Cs
 - Acceptable Use Policy

Granting A VO Access to the Grid

- Copying the lists
 - of DNs, of Certificates, or of subject and issuer DNs
 - *'Poll' Model*
- Defining Rules
 - e.g. Everyone from Manchester and Edinburgh
 - *O=Edinburgh, C=UK || O=Manchester, C=UK*
 - *(NB this doesn't work well in grids)*
- Ask someone else
 - Call out to some on-line service, e.g. SAML Requests
 - *Pull Model*
- User Provided Credentials
 - e.g. Attribute Certificates or SAML Assertions,
 - *Push model*

How Do VOs help – List Maintenance

- Grid resources grant access based on local policy
 - Attribute matching
 - *against a list, e.g. a bunch of named individuals*
 - *against a rule e.g. a time constraint*
- Maintaining lists can be cumbersome
 - especially if they're dynamic
 - especially if they need to be in many locations
- Delegate list maintenance
 - Maintain lists of VOs not users
 - *Reduces overheads on resources*
 - *Empowers Project Managers*

How Do VOs help - Accounting

- How to get charging right for resource usage
 - Possibility of using a resource for more than one purpose
 - (but) DN list based authorisation
 - *First “mapping” = Project to charge to*
- How to assert to which account to charge my usage.
 - Supply VO membership details or attributes
 - *i.e. authorise me to use resource as NNNN from VO MMMM*
- VO -> Project Mapping?

VOs and Network Entities

■ Resources used by the VO

– Easiest case:

- *VO = Project,*
- *Project requires resources: CPU / Disk / Bandwidth / Detector ...*
- *Project maintains list of people, their roles and groups*
- *Project applies for resources on behalf of its people*

■ Resources provided by the VO

– Harder case:

- *VO = Project / Organisation, People and Resource*
- *Project requires occasional extra resources / different resources*
- *Project can trade their resources*

MANCHESTER
1824

The University
of Manchester

The Virtual Organisation Membership Service

What is VOMS

- **The Virtual Organisation Membership Service**
 - One or more databases of users, groups and roles
 - A set of Web Services
 - *to query and administer the these databases*
 - A portal to interface to these Web Services
 - A GSI service for obtaining “Attribute Certificates”
 - A bundle of client and administration tools

- VO Names
 - usually DNS based names
 - *(to avoid name-space conflicts)*
 - e.g. ngs.ac.uk

VOMS Database

- Each VO on a VOMS server has a database
 - DN
 - Issuer DN
 - Groups
 - Roles
 - ..., email, CN, Institute, Phone Number, ...

- Each VOMS has a Web Service interface
 - Allowing script based access
 - *For VO Administration*
 - *List retrieval (polling)*
- Each VOMS has a Web Portal interface
 - Allowing non-technical VO administration
 - *Users can request to join a VO*
 - *VO Managers may add users and change users' roles*
- Each VO will have a URI:
 - NGS VO's is <https://voms.ngs.ac.uk:8443/voms/ngs.ac.uk/>
 - *pointing a browser at this will reveal the Portal interface*

- VOMS works with the Grid Security Infrastructure
 - A Proxy certificate may contain a VOMS extension
 - extensions may contain 1 or more “Attribute Certificates”
 - Resources may extract and use these ACs
 - *instead of polling VOMS servers*

- Each VO on a VOMS server has a VOMS daemon
 - This is what *voms-proxy-init* will talk to
 - *Clients need configuring*
 - It is used mainly to obtain Attribute Certificates
 - It is a mutually authenticated connection
 - *you and it need to have grid (GSI) credentials*

VOMS and Attribute Certificates

- ACs tie a Grid Certificate to Attributes
- Attributes are called:
 - Fully Qualified Attribute Names (FQAN)
- FQANs may look like these:
 - “/ngs.ac.uk/Role=NULL”
 - “/ngs.ac.uk/SomeGroup/Role=Some Role”
- ACs may contain multiple FQANs
 - The first one is usually taken for authorisation purposes
- ACs are signed by the VOMS server
 - *(NB to validate the AC one needs the VOMS server certificate)*

VOs VOMS and the NGS


VOs on the NGS

- NGS provides a VOMS server
 - Hosting a VO is separate to an NGS project application
 - *may have a VO without any NGS resource allocation*
 - *Useful not only for NGS but also other grids*

VOMS on the NGS

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/> Google Search

 **NGS**
National Grid Service

Welcome to the manchester.ac.uk VO

The manchester.ac.uk VO

For VO users

- [My membership details](#)
- [New user registration](#)
- [My requests](#)

For VO managers

- [Administer the VO](#)
- [Handle requests](#)
- [Check audit data](#)

Configuration

- [Configuration information](#)
- [List all VOs on this server](#)

VOMS Admin 1.2.19
Release 1
Copyright © 2005 CERN, ELTE
on behalf of the EU EGEE Project

Welcome to VOMS!

VOMS is the Virtual Organization Membership Service, a central database for VO membership information.

This is the web user interface of the VOMS Admin service for the manchester.ac.uk VO. It provides services relating to VO membership for VO users and VO managers.

Please select an item from the services listed on the left side of this page.

You are logged in as "/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones" certified by "/C=UK/O=eScienceCA/OU=Authority/CN=CA".

VOMS on the NGS – List My Details

The screenshot shows a web browser window with the address bar containing the URL: `https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/info`. The browser's menu bar includes Location, Edit, View, Go, Bookmarks, Tools, Settings, Window, and Help. The page content is as follows:

NGS National Grid Service logo is displayed on the left. The main heading reads: **Your membership information in the manchester.ac.uk VO**.

The page is titled **The manchester.ac.uk VO** and **Membership details**.

MEMBERSHIP DETAILS

Here is what the VOMS service knows about you:

- Certificate name (DN): `/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones`
- Issuer authority (CA): `/C=UK/O=eScienceCA/OU=Authority/CN=CA`
- Common Name (CN): michael jones
- Email address: mike.jones@manchester.ac.uk

Here is a list of your VOMS attributes. The type of each attribute is shown in the second column for your convenience.

Attribute	Type
<code>/manchester.ac.uk</code>	Group
<code>/manchester.ac.uk/Role=VO-Admin</code>	Role

VOMS Admin 1.2.19
Release 1
Copyright © 2005 CERN, ELTE
on behalf of the EU EGEE Project

You are logged in as `"/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones"`
certified by `"/C=UK/O=eScienceCA/OU=Authority/CN=CA"`.

Page loaded.

VOMS on the NGS – Apply for Membership

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/request/user/create> Google Search

accounting, monitoring and security purposes only. This information may be disclosed to other organizations anywhere in the world for these purposes. Although efforts are made to maintain confidentiality, no guarantees are given.

6. The Resource Providers, the VO and the GRID operators are entitled to regulate and terminate access for administrative, operational and security purposes and you shall immediately comply with their instructions.
7. You are liable for the consequences of any violation by you of these conditions of use.

DN: /C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones
CA: /C=UK/O=eScienceCA/OU=Authority/CN=CA
CA URI: <http://ca.grid-support.ac.uk/pub/crl/escience-ca-crl.crl>

Family Name:

Given Name:

Institute:

Phone Number:

Email:

comment:

VOMS Admin 1.2.19
Release 1

You are loaded in as "/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones"

VOMS on the NGS – List All Members

The screenshot shows a web browser window with the URL `https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/admin/users/list`. The page header features the NGS National Grid Service logo and the title "Virtual Organization Membership Service". The main content area displays the "List of users" for the "The manchester.ac.uk VO". It lists two users with their DNs and associated actions:

DN	edit	remove	manage attributes
<code>/C=UK/O=eScience/OU=Manchester/L=MC/CN=robin pinning</code>	edit	remove	manage attributes
<code>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</code>	edit	remove	manage attributes

Below the user list, there is a note: "You can click on the DN for more details." The footer of the page includes the version "VOMS Admin 1.2.19 Release 1", copyright information "Copyright © 2005 CERN, ELTE", and the user's current session information: "You are logged in as "/code>C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones" certified by "/code>C=UK/O=eScienceCA/OU=Authority/CN=CA".

VOMS on the NGS – List All Roles

The screenshot shows a web browser window with the following elements:

- Browser Menu:** Location, Edit, View, Go, Bookmarks, Tools, Settings, Window, Help.
- Browser Address Bar:** Location: <https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/admin/roles/list>
- Page Header:**
 - Logo:** NGS National Grid Service (with a map of the UK).
 - Title:** Virtual Organization Membership Service
- Breadcrumbs:** Administration » Roles » list the roles
- Left Navigation Menu:**
 - ADMINISTRATION
 - Users
 - List of users
 - Search for users
 - Create a new VO user
 - Groups
 - List of groups
 - Search for groups
 - Create a new group
 - Roles
 - list the roles (selected)
 - search for roles
 - add a new role
 - Global ACL
- Main Content Area:**
 - Text: "The roles in this VO :
 - Text: "Role=VO-Admin" followed by buttons: [list ACL](#), [delete](#), [add users](#)
 - Text: "You can display the ACL, or *delete* the role with the corresponding button."
- Footer:**
 - Left: VOMS Admin 1.2.19, Release 1, Copyright © 2005 CERN, ELTE
 - Right: "You are logged in as "/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones" certified by "/C=UK/O=eScienceCA/OU=Authority/CN=CA".

VOMS on the NGS – Add New Members

The screenshot shows a web browser window with the following elements:

- Browser Address Bar:** Location: <https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/admin/users/create>
- Page Header:** NGS Virtual Organization Membership Service National Grid Service
- Navigation Menu (Left):**
 - The manchester.ac.uk VO
 - ADMINISTRATION
 - Users
 - List of users
 - Search for users
 - Create a new VO user
 - Groups
 - List of groups
 - Search for groups
 - Create a new group
 - Roles
 - list the roles
 - search for roles
 - add a new role
 - Global ACL

- Main Content Area:**
- Administration » Users » Create a new VO user
- Form fields:
 - DN:
 - CA:
 - CA:
 - URI:
 - CN:
 - Email:
- Submit button: Add the user to the VO
- Footer:**
- VOMS Admin 1.2.19 Release 1
- You are logged in as "/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones"

VOMS on the NGS – Configure Access Control

The screenshot shows a web browser window displaying the VOMS Global Access Control List (ACL) configuration page. The browser's address bar shows the URL: `https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/admin/global-acl`. The page header includes the NGS logo and the text "The Global Access Control List".

The left sidebar contains a navigation menu with the following items:

- The manchester.ac.uk VO
- ADMINISTRATION
 - Users
 - List of users
 - Search for users
 - Create a new VO user
 - Groups
 - List of groups
 - Search for groups
 - Create a new group
 - Roles
 - list the roles
 - search for roles
 - add a new role
 - Global ACL

The main content area displays the title "The Global Access Control List" and a brief description: "The following ACL entries are consulted for each VOMS operation, in addition to". Below this is a table of ACL entries:

Allow	Operation	Admin DN
Allow	all	<i>The Local Database Administrator</i>
Allow	all	<i>Anyone with role /manchester.ac.uk/Role=VO-Admin</i>
Allow	all	<i>/C=UK/O=eScience/OU=Manchester/L=MC/CN=voms.ngs.ac.uk/Email=supp</i>
Allow	all	<i>/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones</i>
Allow	all	<i>/C=UK/O=eScience/OU=Manchester/L=MC/CN=voms05.ngs.ac.uk/Email=su</i>
Allow	all	<i>/C=UK/O=eScience/OU=Manchester/L=MC/CN=robert frank</i>
Allow	all	<i>/C=UK/O=eScience/OU=Manchester/L=MC/CN=voms04.ngs.ac.uk/Email=su</i>
Allow	list	Anyone who presents a certificate issued by a known CA

Below the table is a button labeled "Edit this ACL".

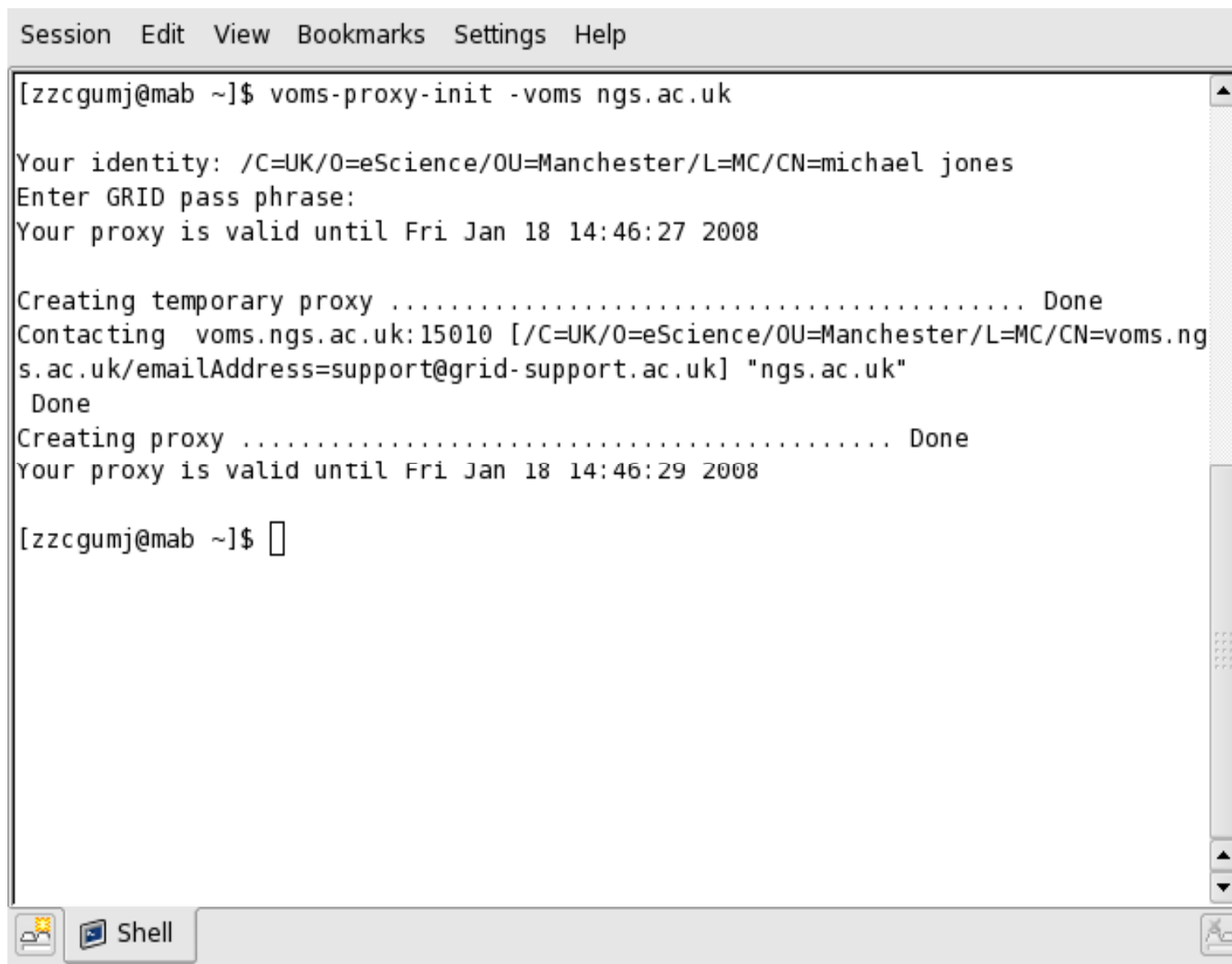
The footer of the page displays the version information "VOMS Admin 1.2.19 Release 1" and the login status: "You are logged in as "/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones"".

VOMS on the NGS – Client/Server Config

The screenshot shows a web browser window with the following elements:

- Browser Menu:** Location, Edit, View, Go, Bookmarks, Tools, Settings, Window, Help
- Address Bar:** Location: <https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk/webui/config>
- Page Header:**
 - NGS National Grid Service** logo (green map of the UK)
 - Configuration data for using the manchester.ac.uk**
- Main Content Area:**
 - The manchester.ac.uk VO** (Section Header)
 - VO configuration files** (Section Header)
 - VO CONFIGURATION FILES** (Section Header)
 - Base URL of the administration interface:**
`https://voms.ngs.ac.uk:8443/voms/manchester.ac.uk`
 - Content for the "vomsses" file: (/opt/glite/etc/vomsses/manchester.ac.uk-voms.ngs.a**
`"manchester.ac.uk" "voms.ngs.ac.uk" "15017" "/C=UK/O=eScience/OU=Manchester/L=M`
 - Example configuration line for mkgridmap:**
`group vomss://voms.ngs.ac.uk:8443/voms/manchester.ac.uk .manchester.ac.uk`
- Footer:**
 - VOMS Admin 1.2.19 Release 1
 - Copyright © 2005 CERN, ELTE on behalf of the EU EGEE Project
 - You are logged in as "/C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones" certified by "/C=UK/O=eScienceCA/OU=Authority/CN=CA".

VOMS on the NGS – Getting a VOMS Proxy



```
Session Edit View Bookmarks Settings Help
[zzcgumj@mab ~]$ voms-proxy-init -voms ngs.ac.uk

Your identity: /C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones
Enter GRID pass phrase:
Your proxy is valid until Fri Jan 18 14:46:27 2008

Creating temporary proxy ..... Done
Contacting voms.ngs.ac.uk:15010 [/C=UK/O=eScience/OU=Manchester/L=MC/CN=voms.ngs.ac.uk/emailAddress=support@grid-support.ac.uk] "ngs.ac.uk"
Done
Creating proxy ..... Done
Your proxy is valid until Fri Jan 18 14:46:29 2008

[zzcgumj@mab ~]$
```

VOMS on the NGS – examining a VOMS Proxy

```
Session Edit View Bookmarks Settings Help
[zzcgumj@mab ~]$ voms-proxy-info -all
WARNING: Unable to verify signature!
Error: Cannot find certificate of AC issuer for vo ngs.ac.uk
subject   : /C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones/CN=proxy
issuer    : /C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones
identity  : /C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u6360
timeleft  : 11:59:26
=== VO ngs.ac.uk extension information ===
VO        : ngs.ac.uk
subject   : /C=UK/O=eScience/OU=Manchester/L=MC/CN=michael jones
issuer    : /C=UK/O=eScience/OU=Manchester/L=MC/CN=voms.ngs.ac.uk/Email=support@
grid-support.ac.uk
attribute : /ngs.ac.uk/Role=NULL/Capability=NULL
timeleft  : 11:59:25
[zzcgumj@mab ~]$
```

VOs on the NGS future

- NGS currently associates VOs with projects *but*
 - project application mechanisms not quite in place today
 - support of VOs is in development and available only for testing/training purposes, *but* watch this space!
- The NGS is working towards VOs with resources
 - i.e. to enable NGS Associate and Partner sites resource to trade with each other and with core sites

MANCHESTER
1824

The University
of Manchester



Research Computing Services
University of Manchester