MANCHESTER 1824

The University of Manchester

Virtual Organisations and the NGS

Mike Jones
Research Computing Services

e-Science & “The Grid” for Bio/Health Informaticians, IT407
18 January 2008

MANCHESTER
1824

The University of Manchester

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 o*rganisation?*
  - *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

VOMS VO

- 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, ...

VOMS Web

- 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 and GSI

- 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)*

MANCHESTER 1824

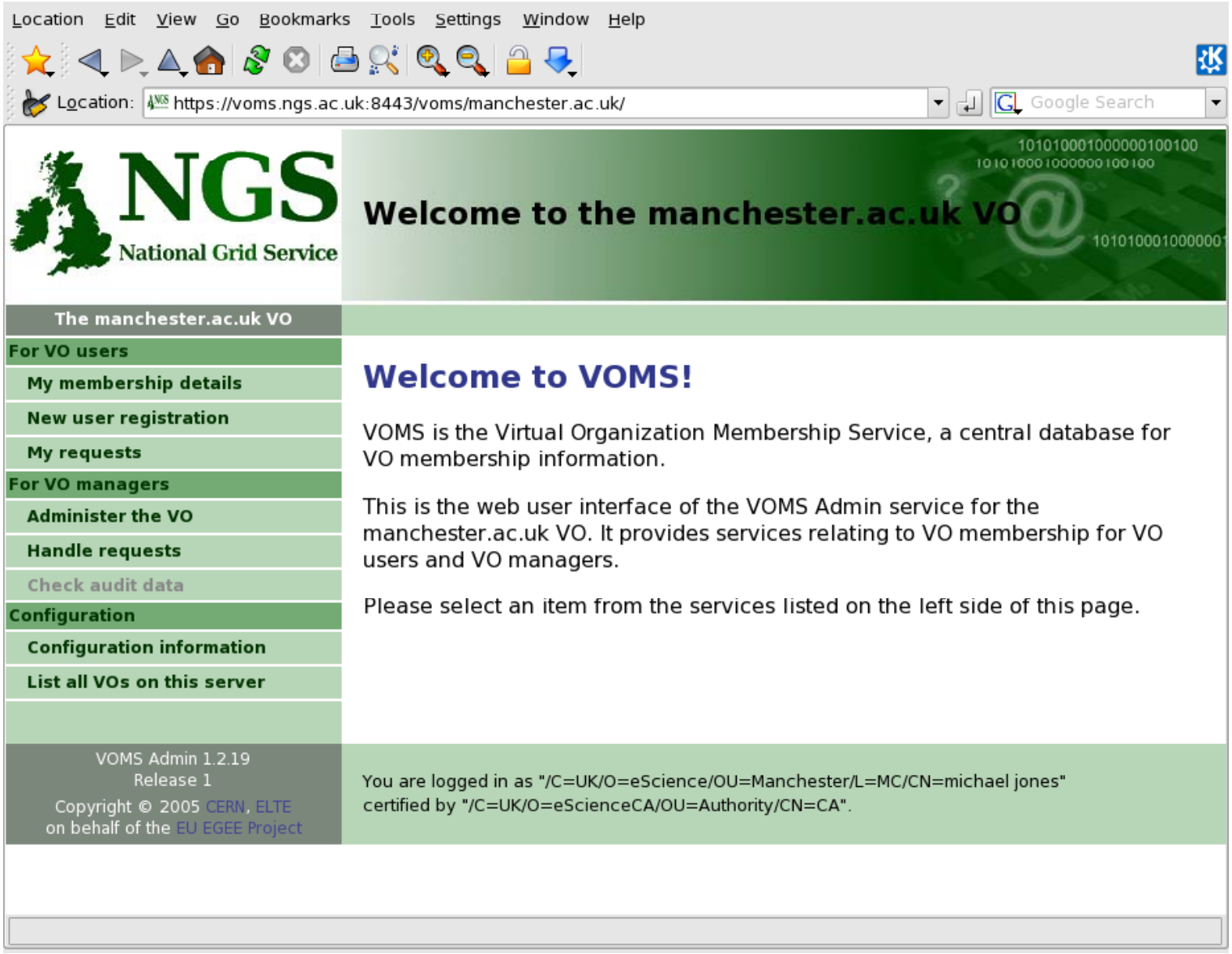
The University of Manchester

VOs VOMS and the NGS

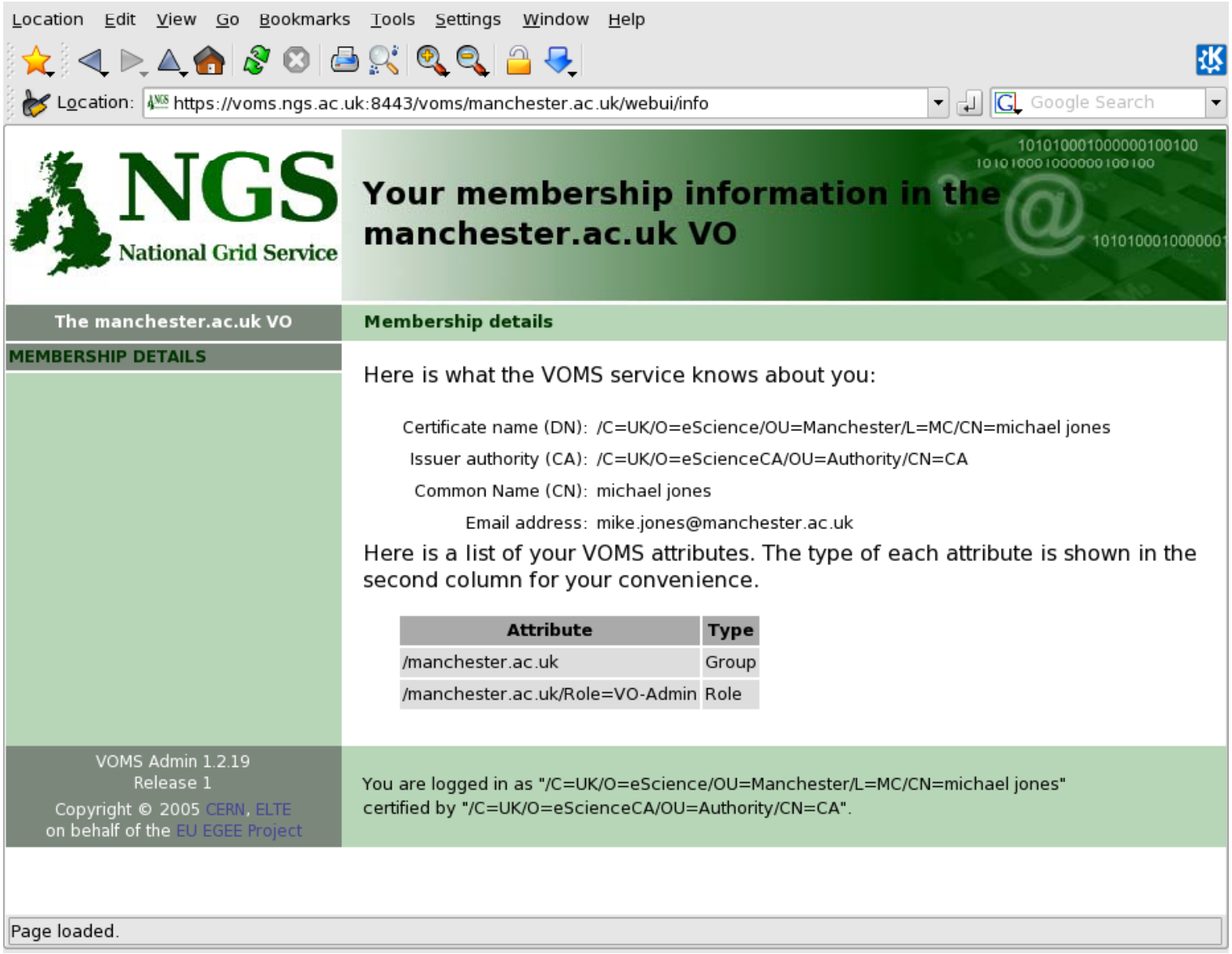
VOs on the NGS

- 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*

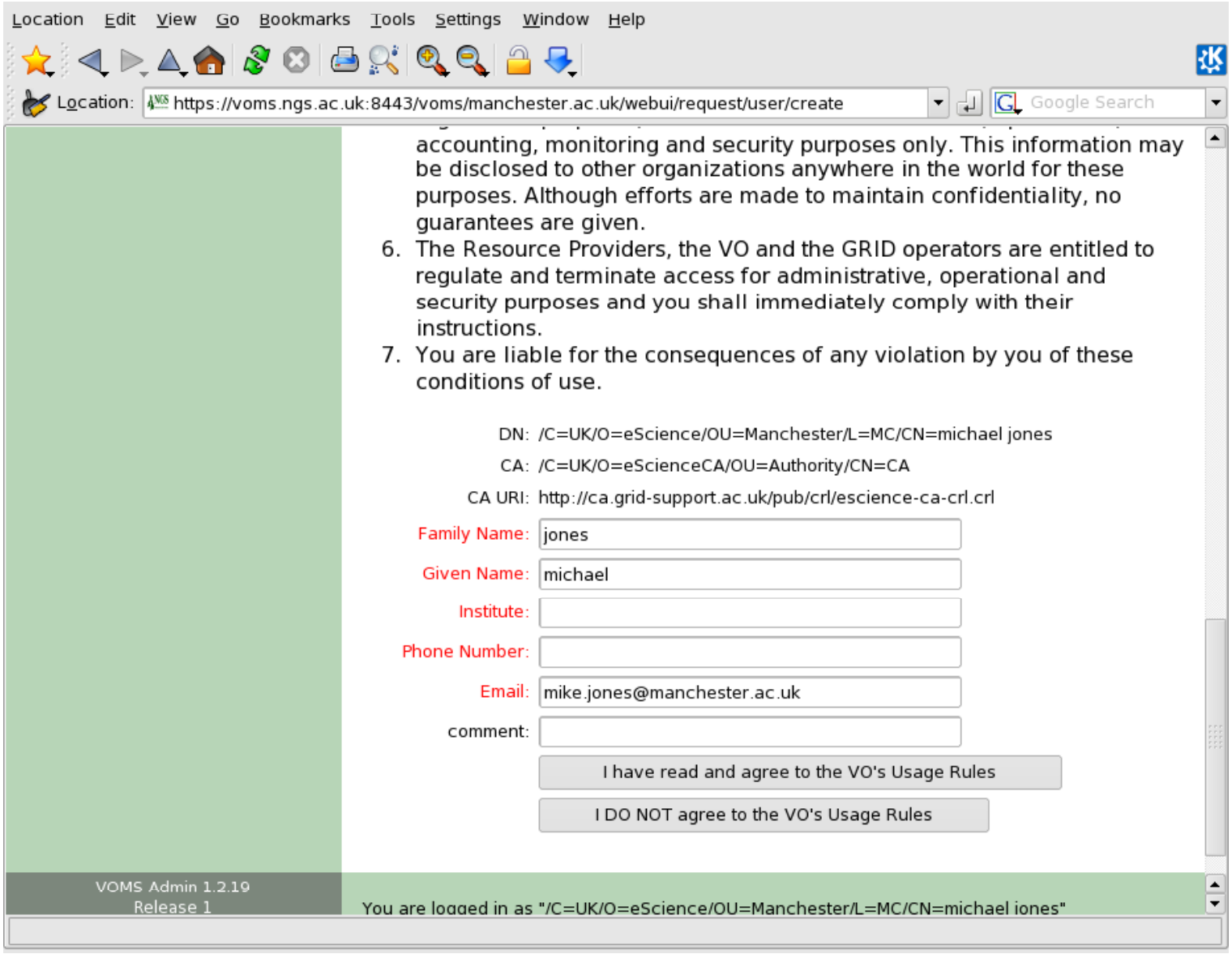
VOMS on the NGS



VOMS on the NGS – List My Details



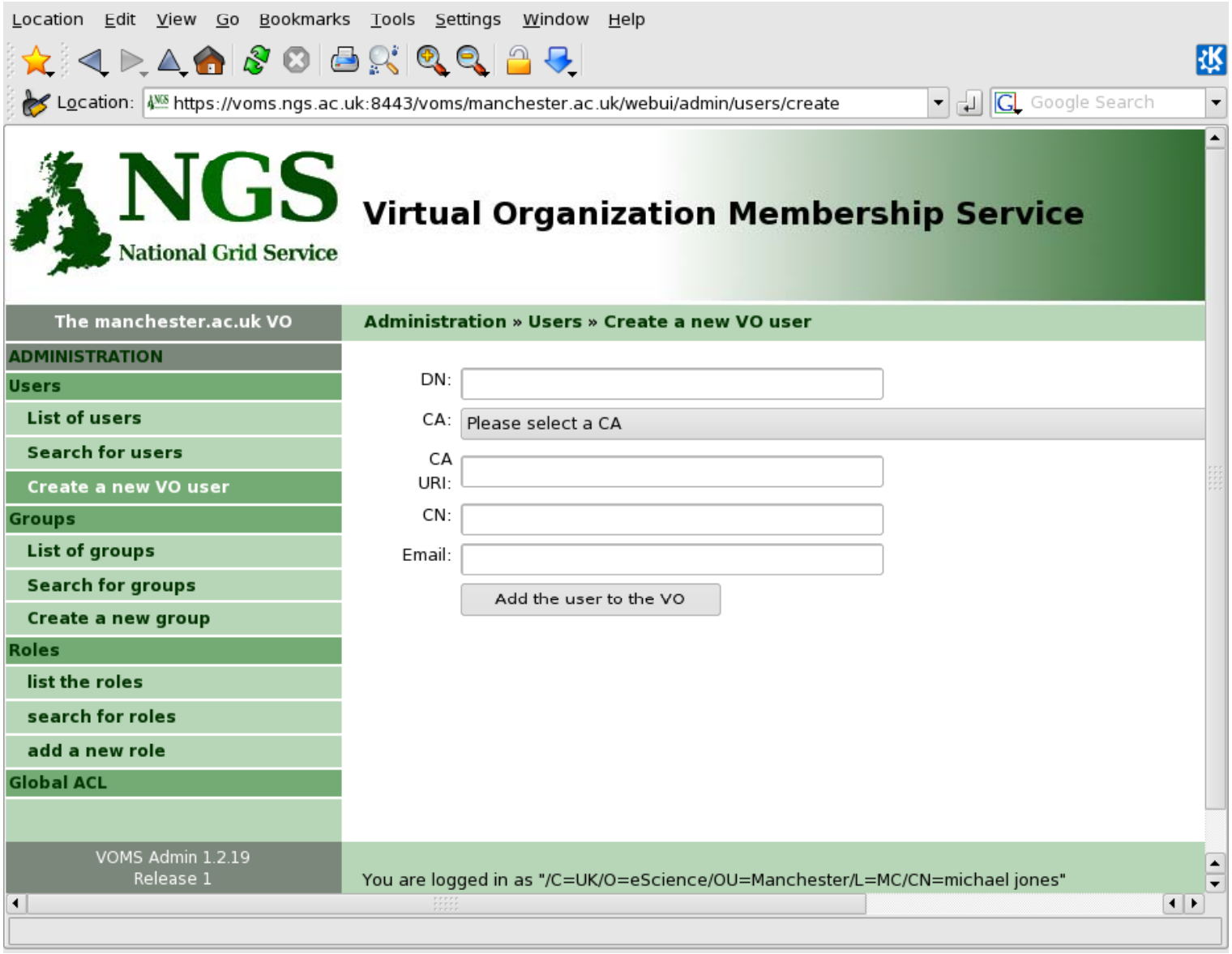
VOMS on the NGS – Apply for Membership



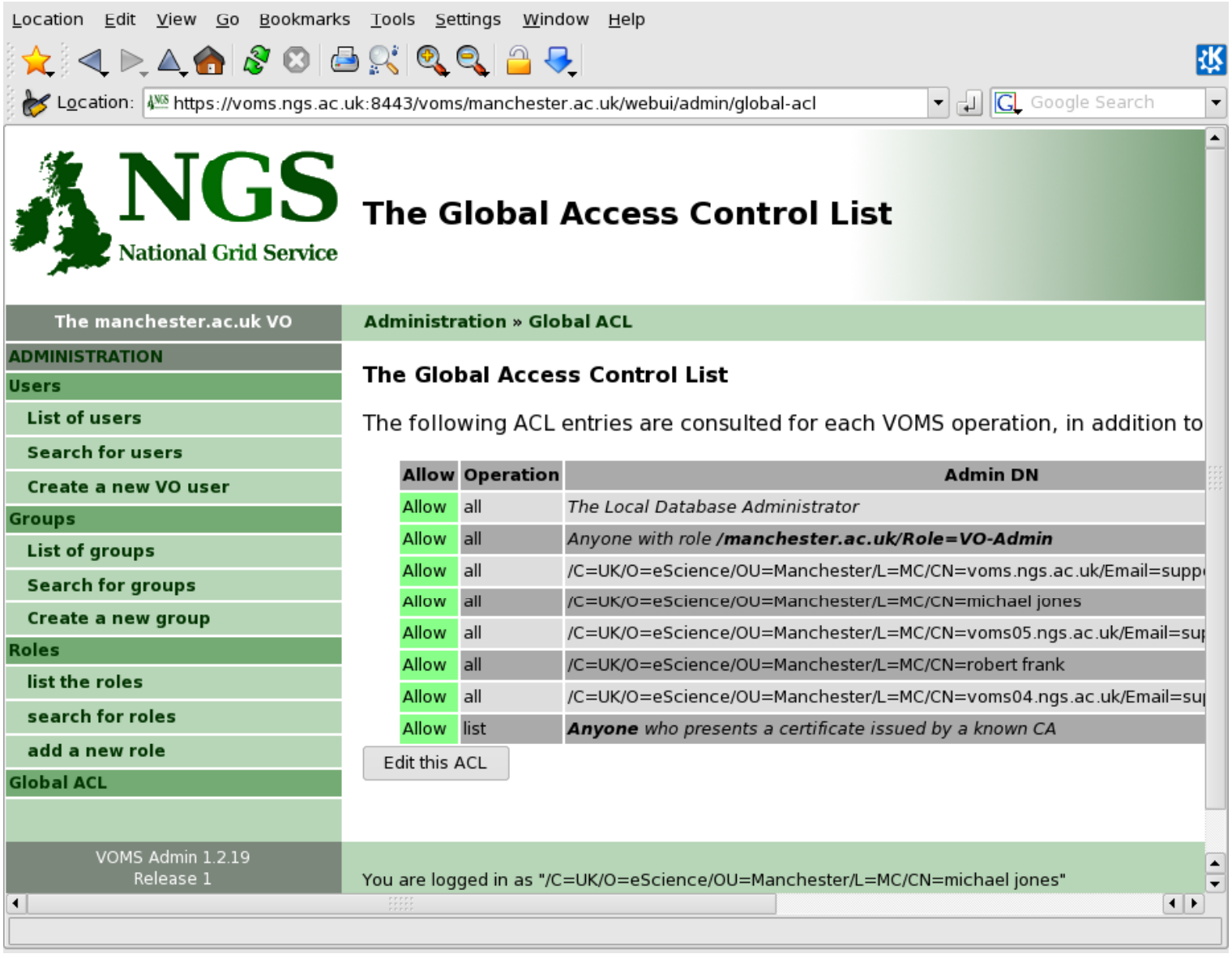
VOMS on the NGS – List All Members

VOMS on the NGS – List All Roles

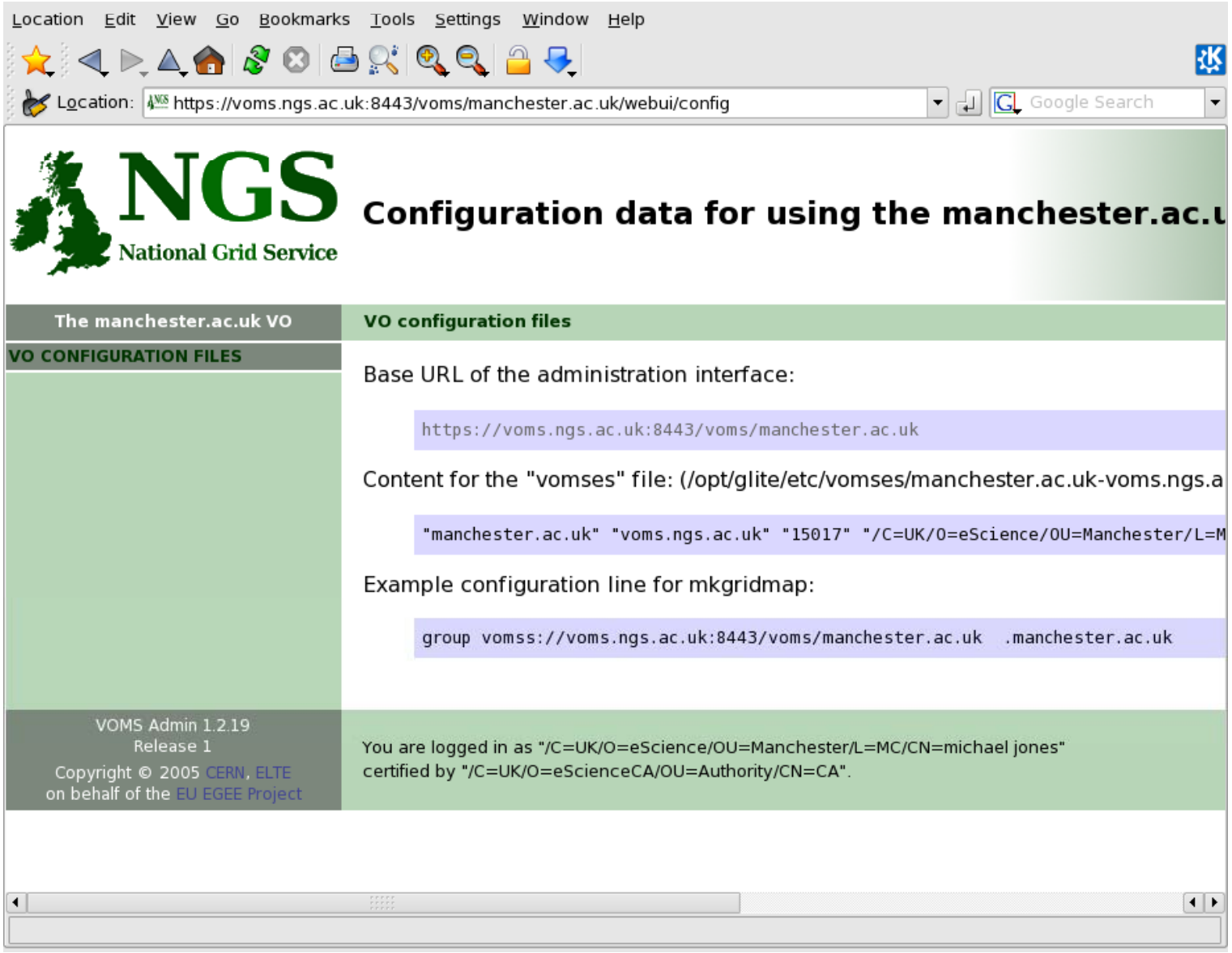
VOMS on the NGS – Add New Members



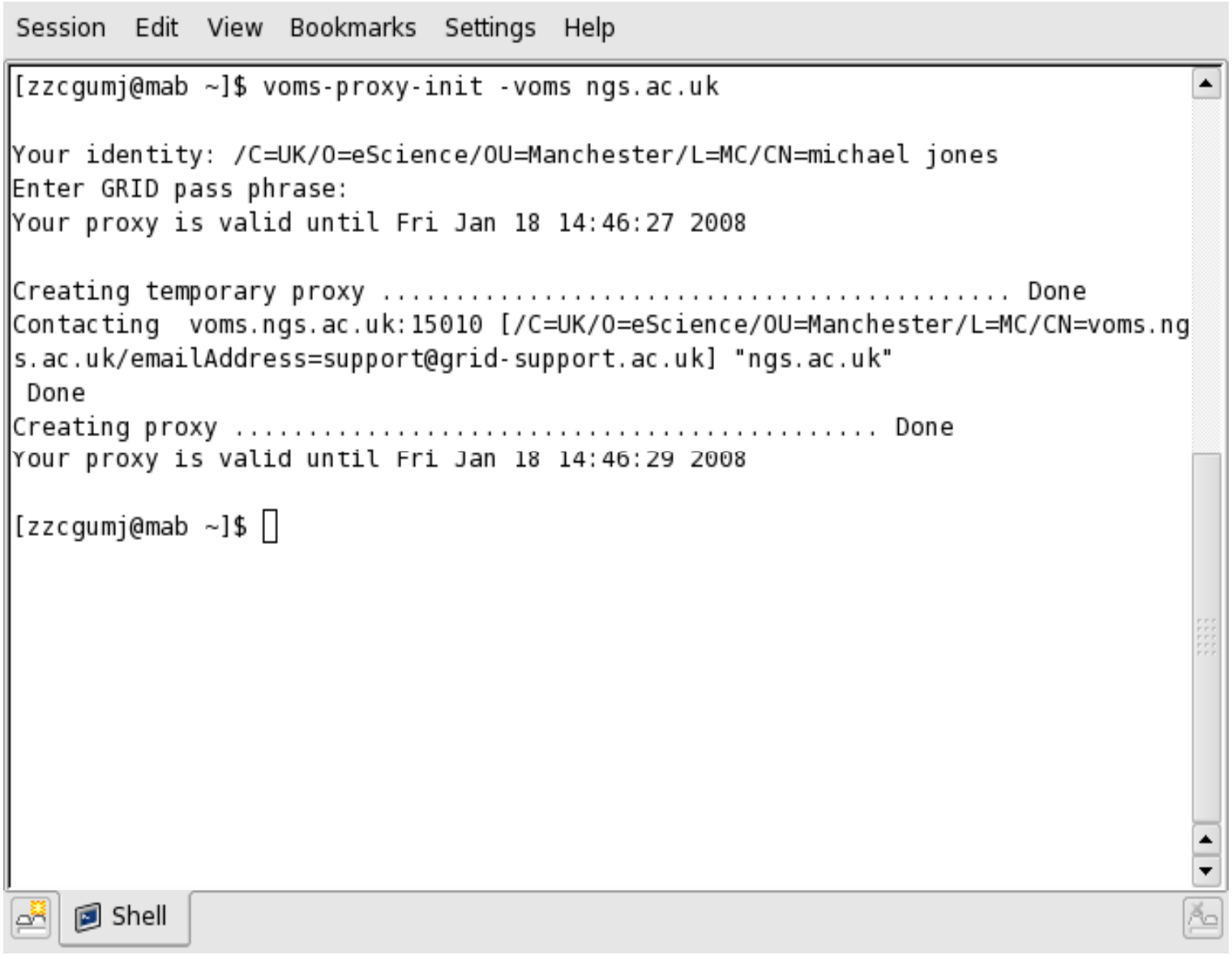
VOMS on the NGS – Configure Access Control



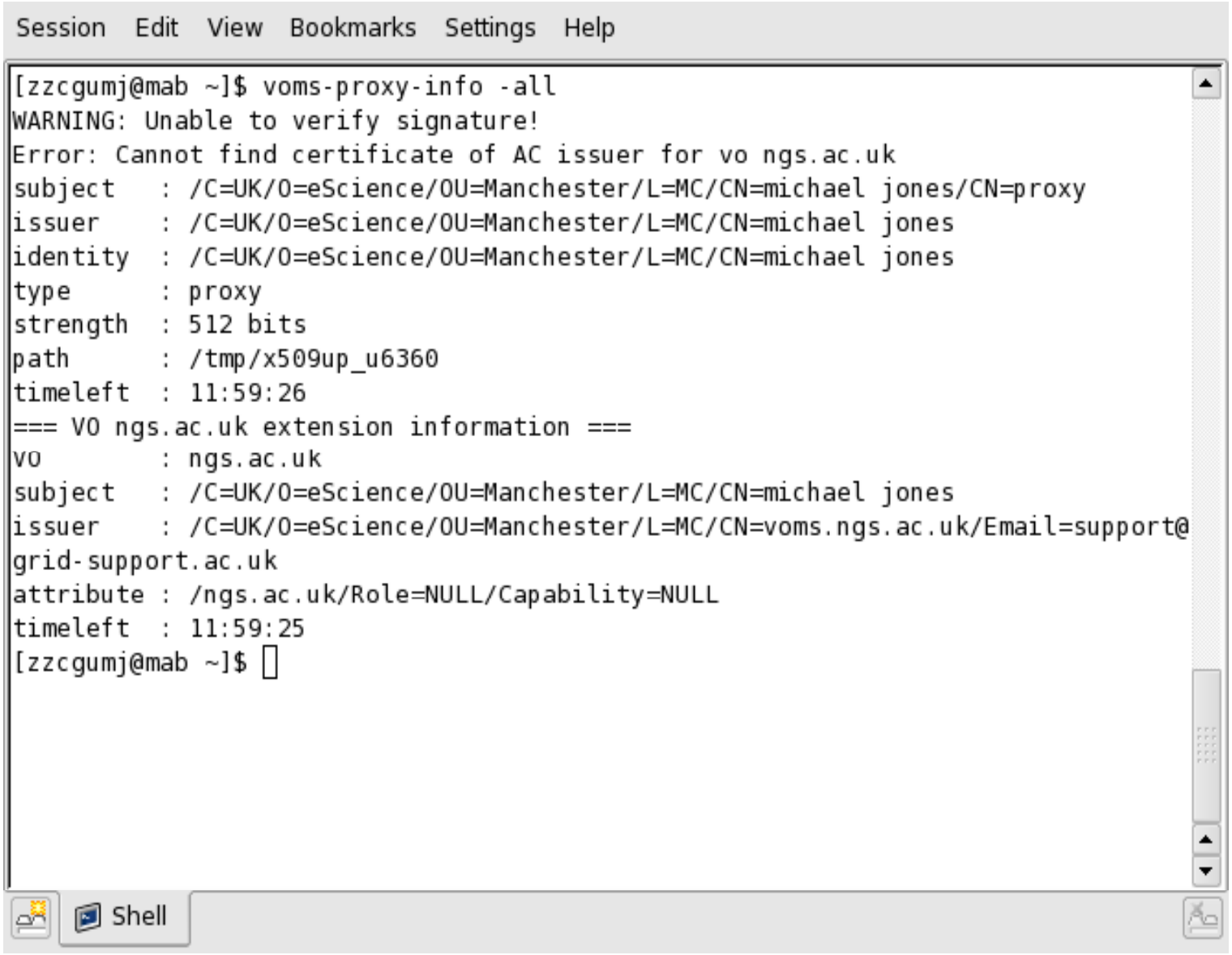
VOMS on the NGS – Client/Server Config



VOMS on the NGS – Getting a VOMS Proxy



VOMS on the NGS – examining a VOMS Proxy



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

Research Computing Services
University of Manchester