VOMS/AMI Integration

Implementation of Java Based Solution

ATLAS-LCG-EGEE Task Force

Thomas Doherty

GridPP Physicist Programmer

UNIVERSITY
of
GLASGOW

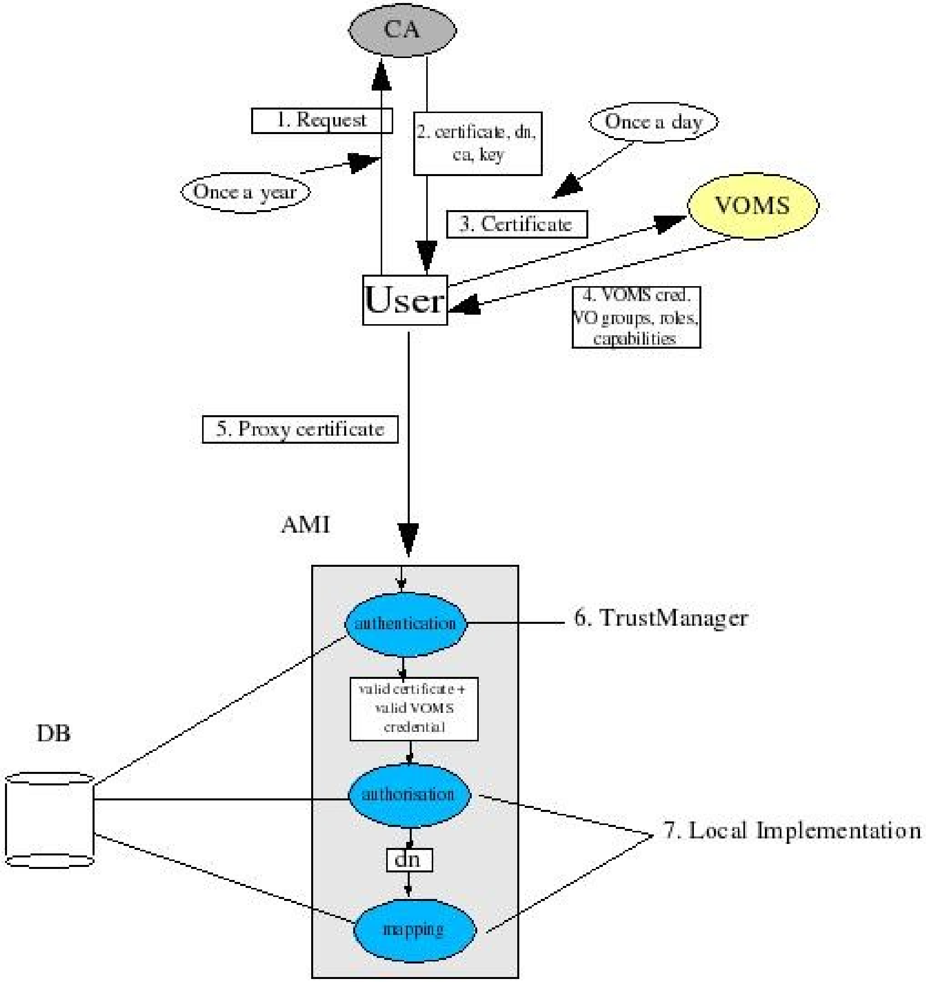
Introduction

- Introduction
  - VOMS and Authorisation
  - Problem with AMI integration
  - Java VOMS Solution
    - AMI's local authorisation mechanism
  - Demonstration
  - Conclusion

VOMS and Authorisation

- Obtain grid-certificate from CA
- Request VOMs proxy certificate
- Access AMI using this certifcate
- User authenticated using TrustManager
- Authorisation achieved depending on user task mapping correctly from their VOMS group/role to their registered user role within AMI

- This poses a problem for AMI



Problems with VOMS and possible solutions

- The main search interface for AMI is browser based
- Browsers at the moment cannot handle proxy certificates
- There are many possible solutions:
  - Mod_gridsite – this method fetches lists of DNs from the VOMS system per group/role
  - MyProxy – this method allows for the storing of proxy-certificates on a remote server
- A purely Java/Tomcat prototype has been developed

Java VOMS solution

- The Java VOMS solution briefly consists of the following steps:

1) The grid user authenticates themselves to AMI (web app.) using a grid certificate

2) AMI allows the user to launch a Java web start application to create a VOMS proxy

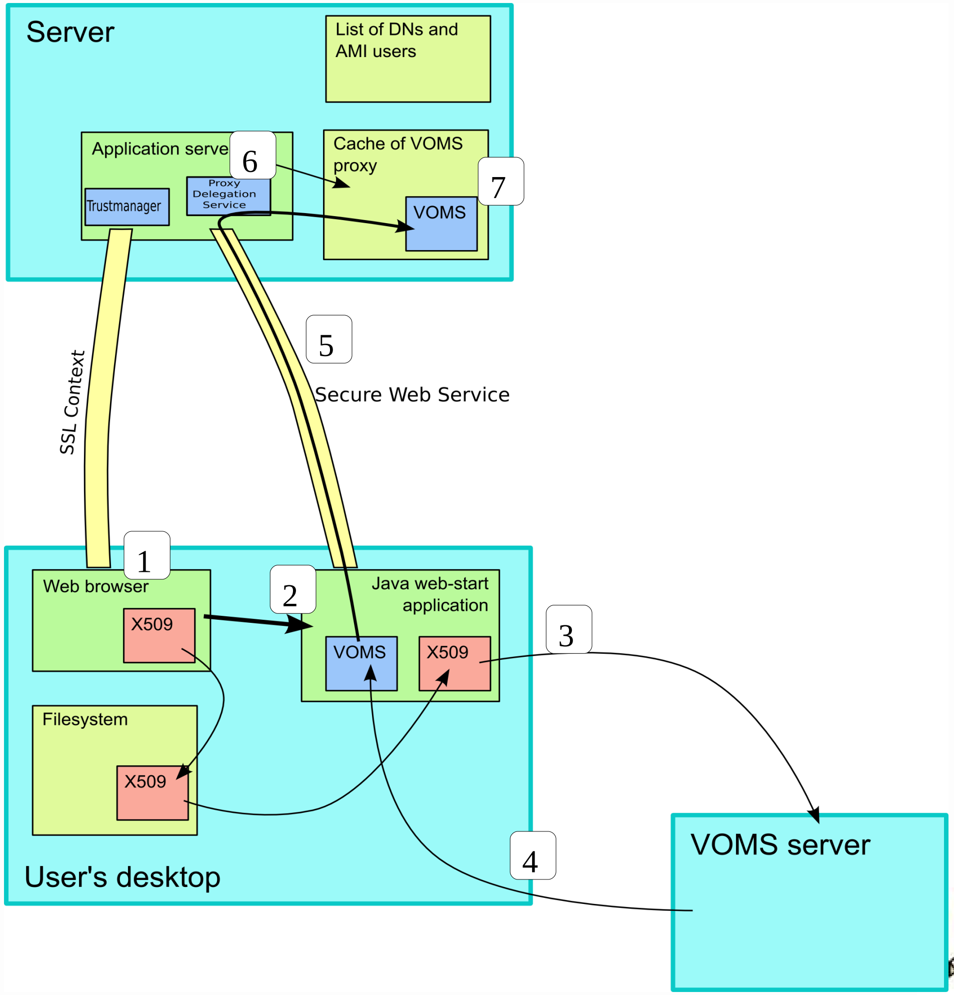
3) The user chooses the x509 certificate to be sent to the VOMS server

4) The VOMS server sends back a VOMS proxy certificate to the W.S application

5) Using Axis set up in Tomcat the VOMS proxy file is uploaded to the server via a secure web service attachment

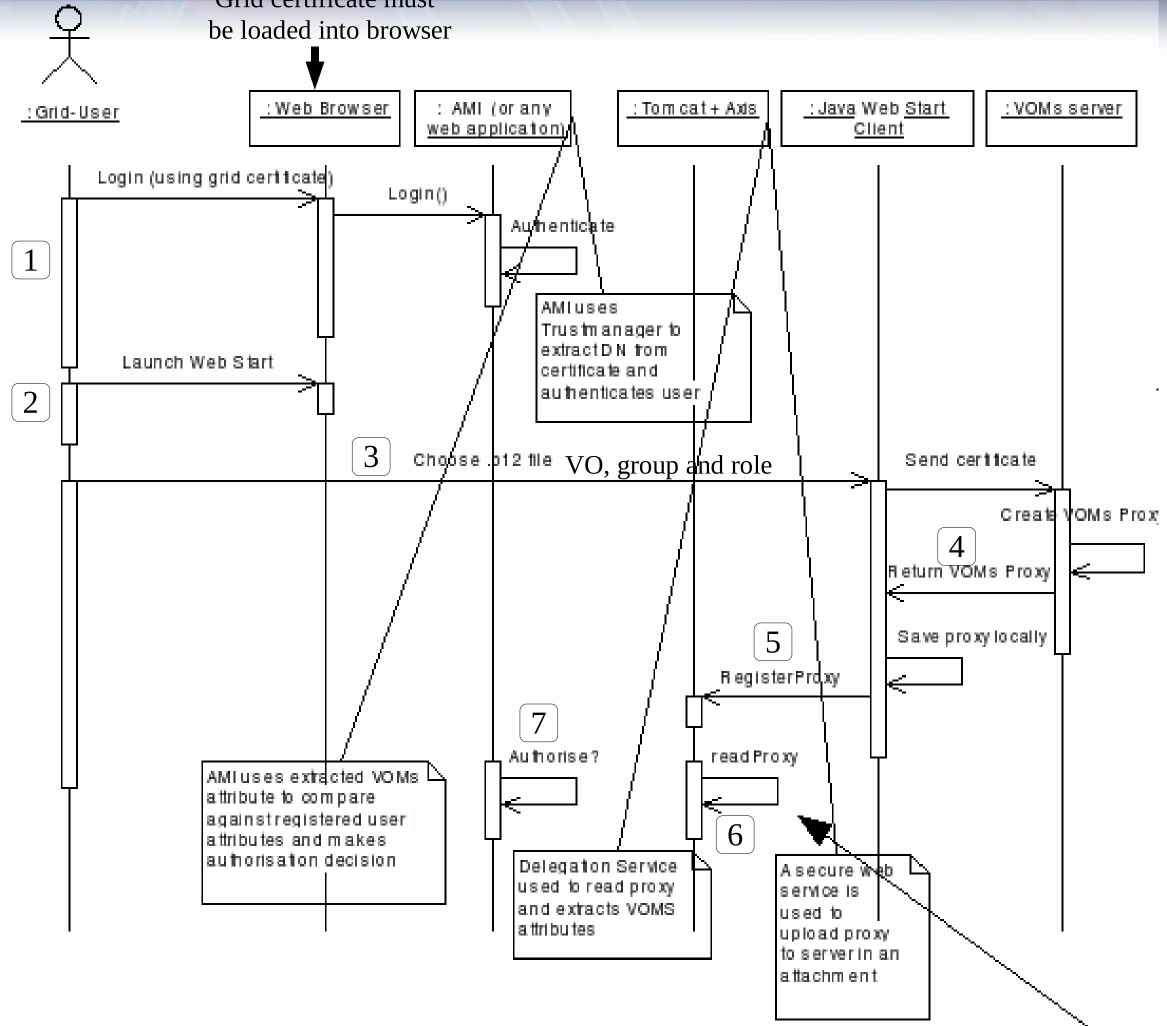
6) A proxy delegation service is available on the server

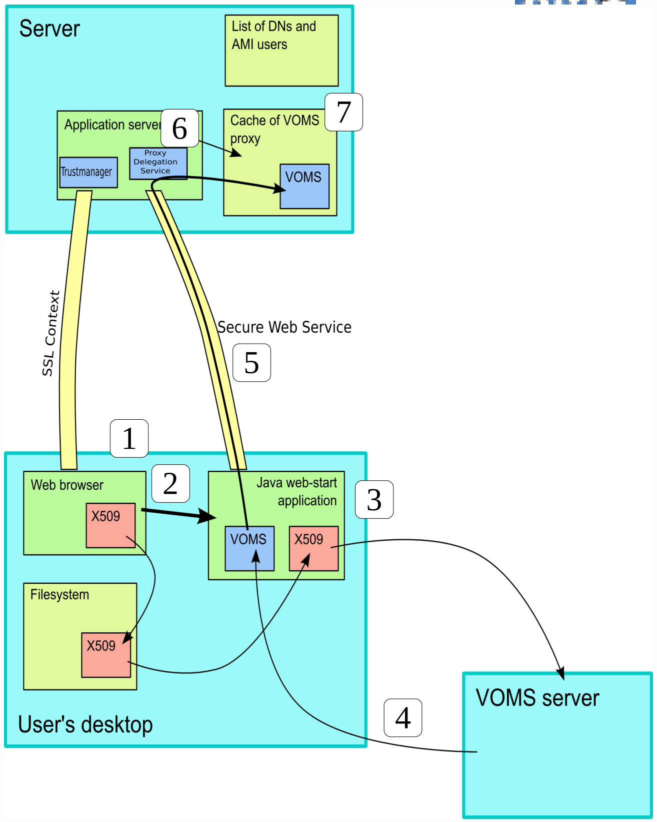
7) The users VO, group and role can be extracted from the proxy and used for authorisation purposes



VOMS Authorisation

Grid certificate must be loaded into browser


: Grid-User
: Web Browser
: AMI (or any web application)
: Tomcat + Axis
: Java Web Start Client
: VOMS server
1
Login (using grid certificate)
Login()
Authenticate
AMI uses Trustmanager to extract DN from certificate and authenticates user
2
Launch Web Start
3
Choose .p12 file
VO, group and role
Send certificate
Create VOMs Proxy
4
Return VOMs Proxy
Save proxy locally
5
RegisterProxy
7
Authorise?
read Proxy
6
AMI uses extracted VOMS attribute to compare against registered user attributes and makes authorisation decision
Delegation Service used to read proxy and extracts VOMS attributes
A secure web service is used to upload proxy to server in an attachment



Java servlet created to extract group/role from VOMs proxy

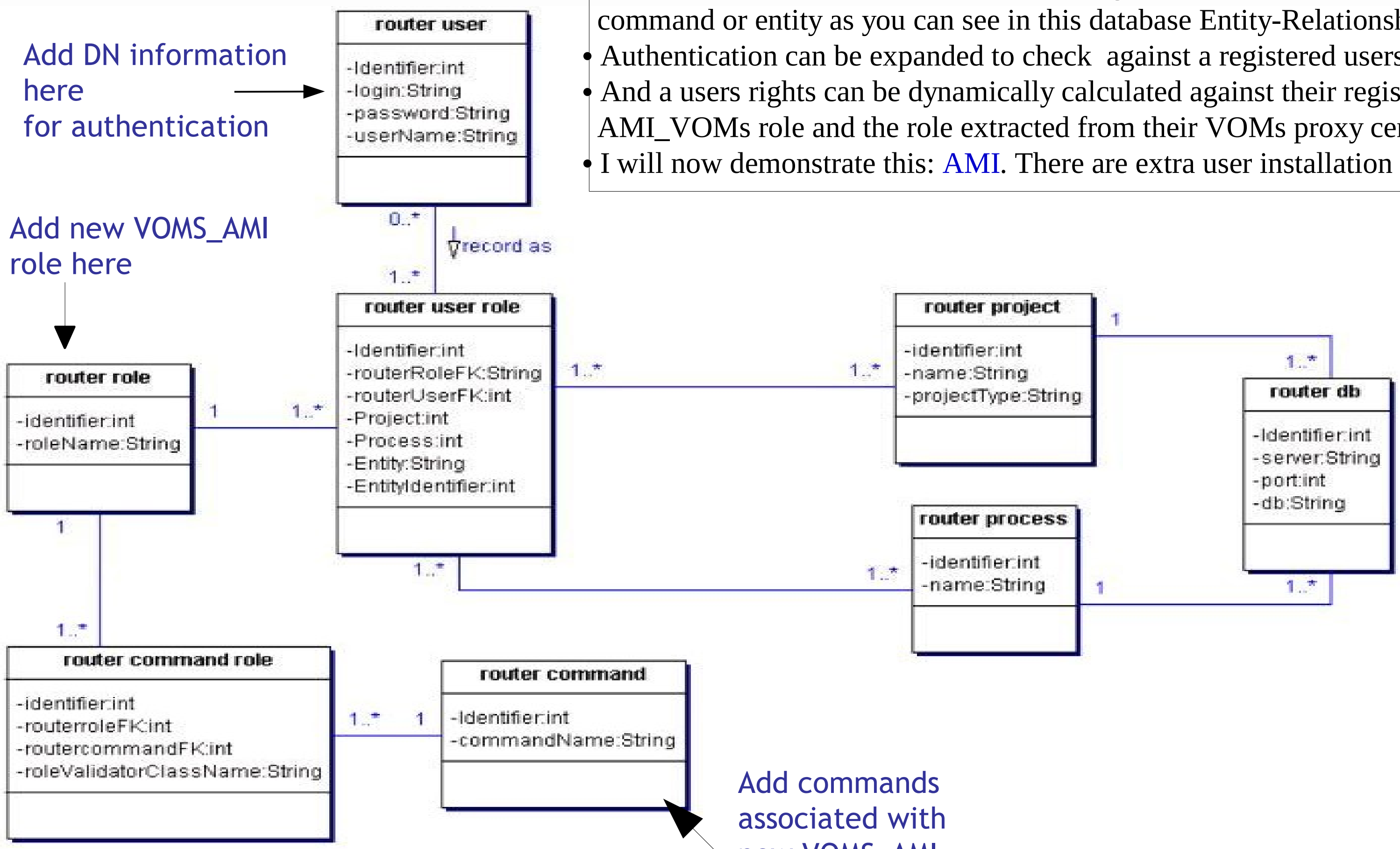
UNIVERSITY of GLASGOW

Authorisation and DNs

- In the local authorisation mechanism the rights of a user can be defined per command or entity as you can see in this database Entity-Relationship diagram
- Authentication can be expanded to check against a registered users DN.
- And a users rights can be dynamically calculated against their registered AMI_VOMs role and the role extracted from their VOMs proxy certificate.
- I will now demonstrate this: AMI. There are extra user installation notes here.

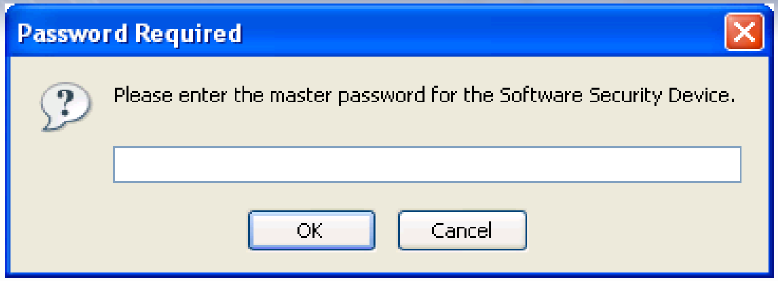
Add DN information here for authentication

Add new VOMS_AMI role here



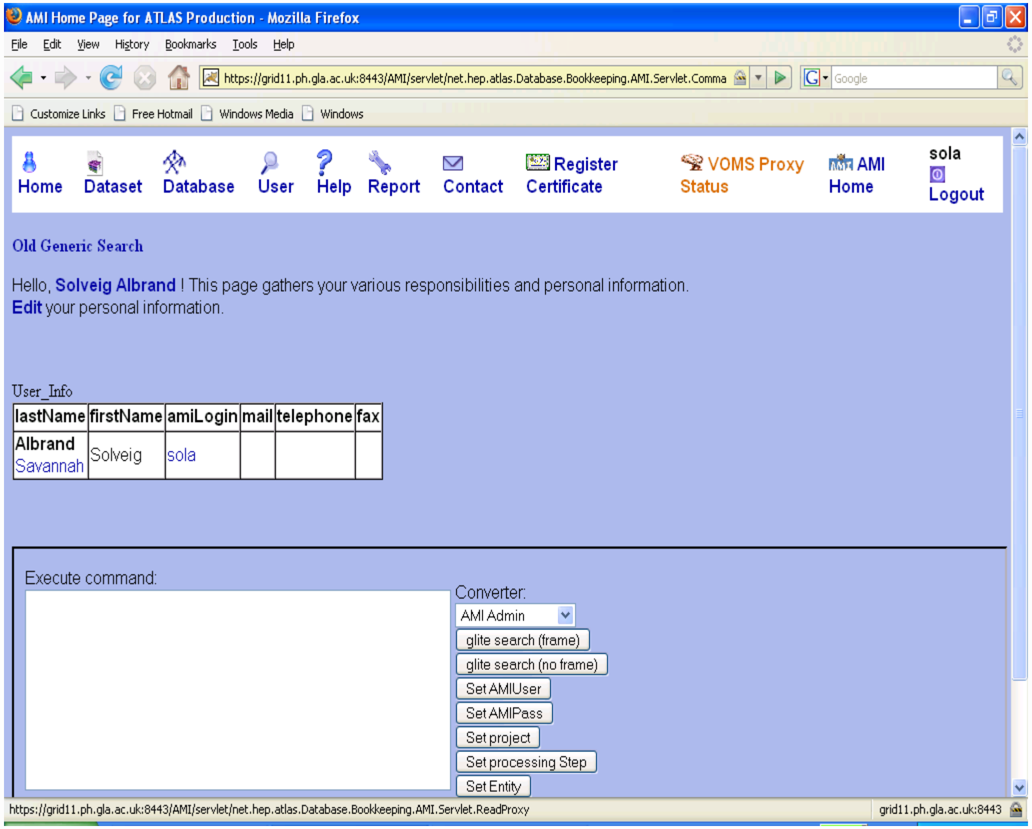
Add commands associated with new VOMS_AMI role here

Demo - Login with user certificate loaded in browser



Password Required

Please enter the master password for the Software Security Device.



AMI Home Page for ATLAS Production - Mozilla Firefox

https://grid11.ph.gla.ac.uk:8443/AMI/servlet/net.hep.atlas.Database.Bookkeeping.AMI.Servlet.Comma

Old Generic Search

Hello, Solveig Albrand ! This page gathers your various responsibilities and personal information.
Edit your personal information.

User_Info

lastName	firstName	amiLogin	mail	telephone	fax
Albrand Savannah	Solveig	sola			

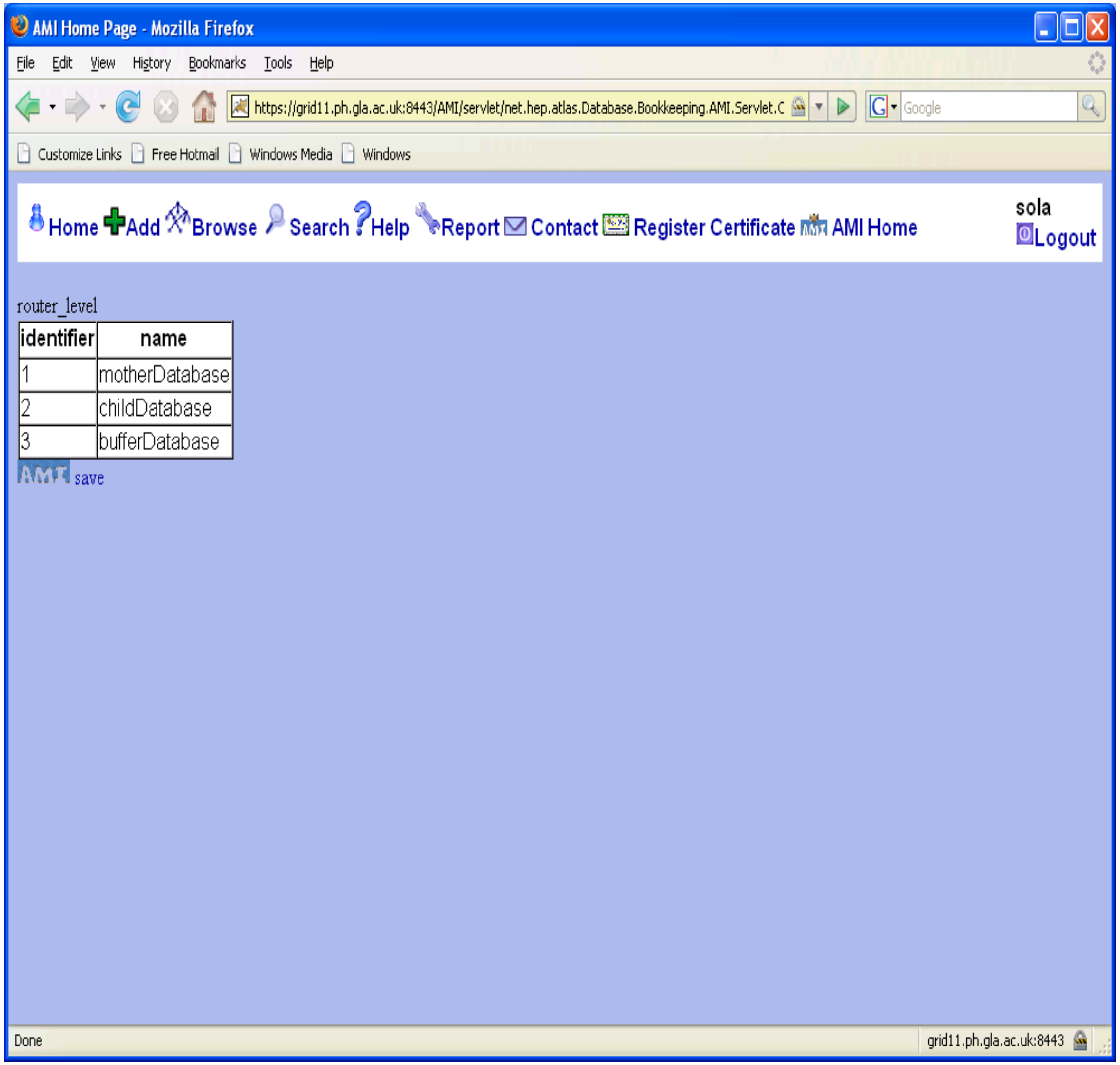
Execute command:

Converter: AMI Admin

https://grid11.ph.gla.ac.uk:8443/AMI/servlet/net.hep.atlas.Database.Bookkeeping.AMI.Servlet.ReadProxy

grid11.ph.gla.ac.uk:8443

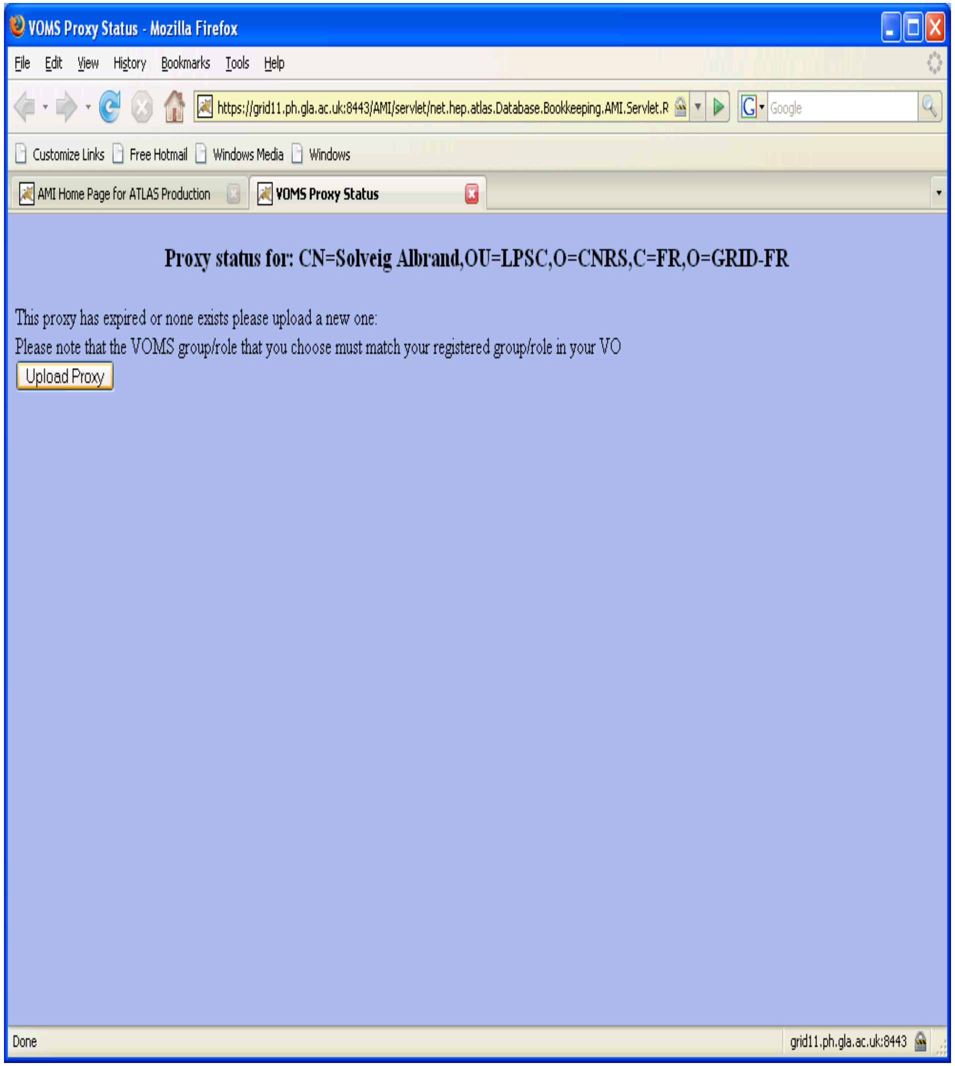
Demo - Choosing AMI command with no proxy loaded


AMI Home Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://grid11.ph.gla.ac.uk:8443/AMI/servlet/net.hep.atlas.Database.Bookkeeping.AMI.Servlet.C
Google
Customize Links
Free Hotmail
Windows Media
Windows
Home
Add
Browse
Search
Help
Report
Contact
Register Certificate
AMI Home
sola
Logout
save
Done
grid11.ph.gla.ac.uk:8443

router_level

identifier	name
1	motherDatabase
2	childDatabase
3	bufferDatabase

Demo – Loading web start application


VOMS Proxy Status - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://grid11.ph.gla.ac.uk:8443/AMI/servlet/net.hep.atlas.Database.Bookkeeping.AMI.Servlet.R
Google
Customize Links
Free Hotmail
Windows Media
Windows
AMI Home Page for ATLAS Production
VOMS Proxy Status
Done
grid11.ph.gla.ac.uk:8443

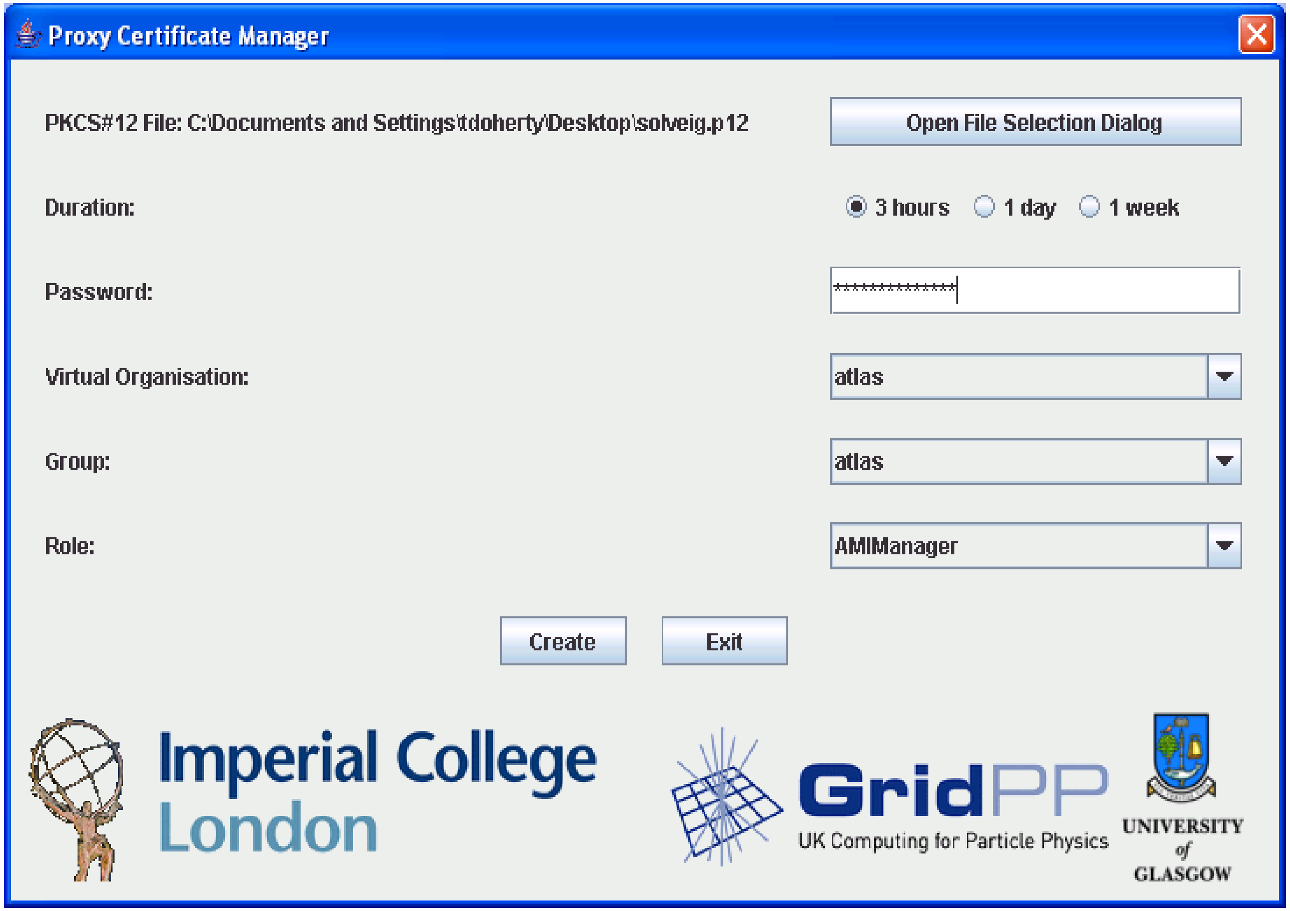
Proxy status for: CN=Solveig Albrand,OU=LPSC,O=CNRS,C=FR,O=GRID-FR

This proxy has expired or none exists please upload a new one:

Please note that the VOMS group/role that you choose must match your registered group/role in your VO

Upload Proxy

Demo - Choosing VO, group and role



Proxy Certificate Manager

PKCS#12 File: C:\Documents and Settings\tdoherty\Desktop\solveig.p12

Duration: ● 3 hours ○ 1 day ○ 1 week

Password: ***************

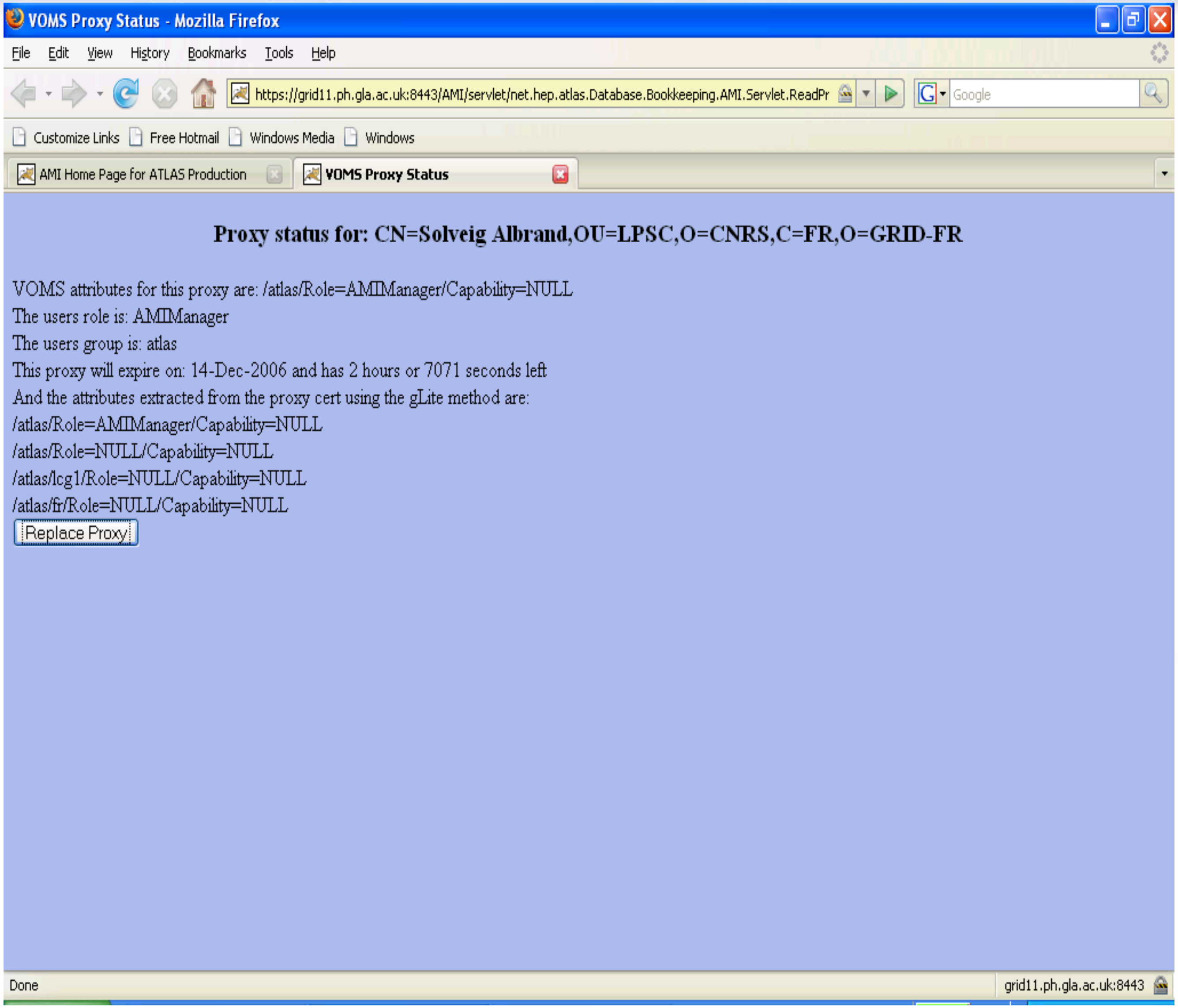
Virtual Organisation: atlas

Group: atlas

Role: AMIManager

GridPP
UK Computing for Particle Physics

Demo - Reading Proxy



VOMS Proxy Status - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://grid11.ph.gla.ac.uk:8443/AMI/servlet/net.hep.atlas.Database.Bookkeeping.AMI.Servlet.ReadPr
Google
Customize Links
Free Hotmail
Windows Media
Windows
AMI Home Page for ATLAS Production
VOMS Proxy Status
Done
grid11.ph.gla.ac.uk:8443

Proxy status for: CN=Solveig Albrand,OU=LPSC,O=CNRS,C=FR,O=GRID-FR

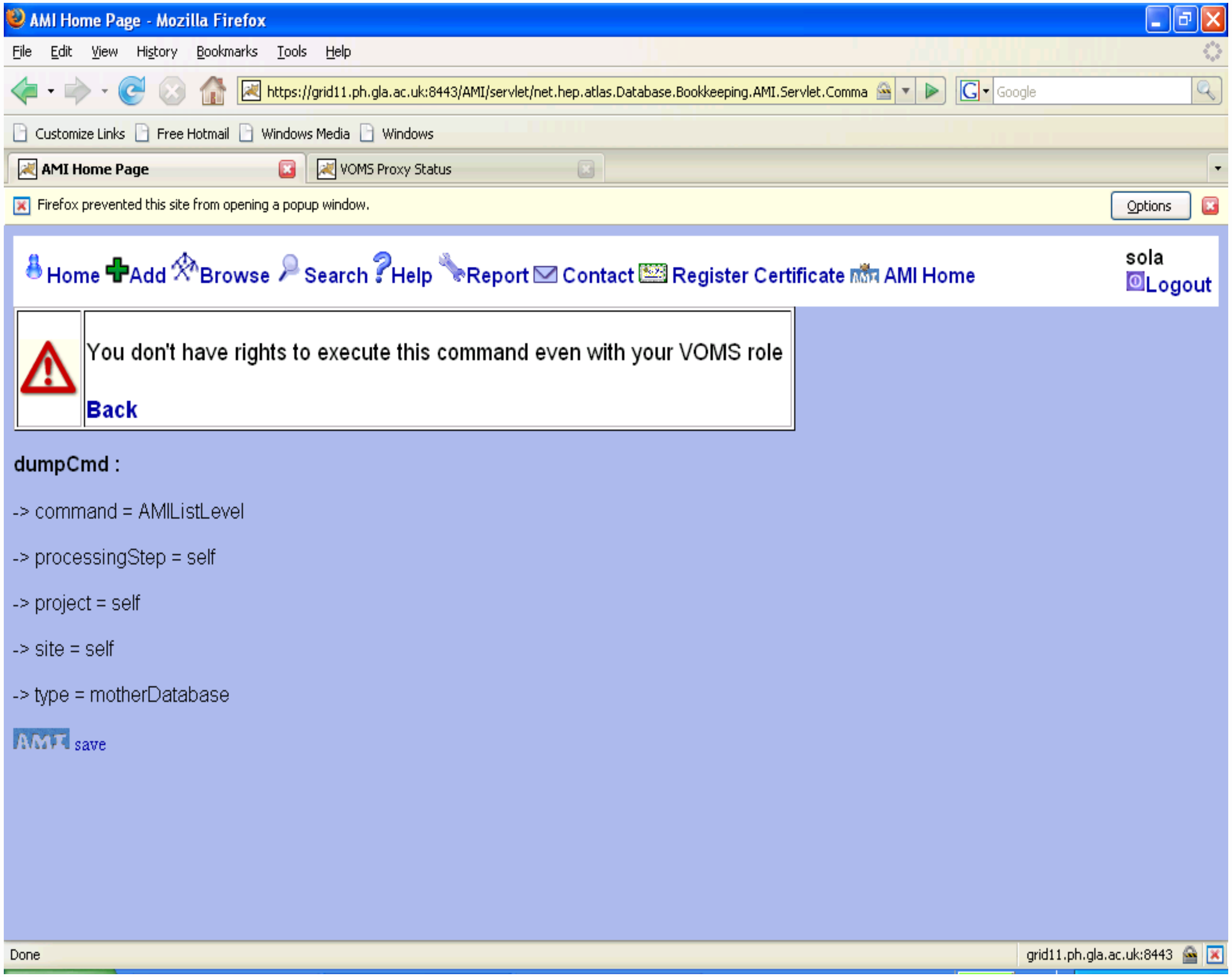
VOMS attributes for this proxy are: /atlas/Role=AMIManager/Capability=NULL
The users role is: AMIManager
The users group is: atlas
This proxy will expire on: 14-Dec-2006 and has 2 hours or 7071 seconds left
And the attributes extracted from the proxy cert using the gLite method are:
/atlas/Role=AMIManager/Capability=NULL
/atlas/Role=NULL/Capability=NULL
/atlas/lcg1/Role=NULL/Capability=NULL
/atlas/fr/Role=NULL/Capability=NULL

Replace Proxy

AMI

UNIVERSITY
of
GLASGOW

Demo – Trying command with proxy uploaded


AMI Home Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://grid11.ph.gla.ac.uk:8443/AMI/servlet/net.hep.atlas.Database.Bookkeeping.AMI.Servlet.Comma
Google
Customize Links
Free Hotmail
Windows Media
Windows
AMI Home Page
VOMS Proxy Status
Firefox prevented this site from opening a popup window.
Options
Home
Add
Browse
Search
Help
Report
Contact
Register Certificate
AMI Home
sola
Logout
Done
grid11.ph.gla.ac.uk:8443

You don't have rights to execute this command even with your VOMS role

Back

dumpCmd :

```
-> command = AMIListLevel

-> processingStep = self

-> project = self

-> site = self

-> type = motherDatabase
```

AMI save

Conclusion

- Illustrated how a tool like AMI fits in to the VOMs mechanism
- Explained what problem that posed for AMI
- Stepped through prototype solution that solves this problem
  - Note: an advantage of this solution is that the proxy is delegated to the server so it can be used to access other external grid applications such as DQ2
- And finally the minimal changes that had to be made for AMI/VOMS integration

Extra slides

VOMS Groups and Roles

The proposed VOMS Groups and Roles that will be used in AMI are as follows:

Groups: det-indet, det-larg, det-muon, det-tile, gen-user, perf -egamma, perf-flavtag, perf-jets, perf-muons, perf-tau
phys-beauty, phys-exotics, phys-gener, phys-hi, phys-higgs
phys-lumin, phys-sm, phys-susy, phys-top, soft-prod
soft-test, soft-valid and trig-pesa

Roles: Editor (write access across group) = AMIManager in VO
Writer (write access to own data only) = AMIWriter in VO
Reader (read access) = Atlas Insider -> Don't need proxy