



Enabling Grids for E-science

# A VOMS overview

**Andrea Ceccanti**

(on behalf of the VOMS team)

***NRENS and Grids Workshop  
Malaga, 29-30/11/07***

[www.eu-egee.org](http://www.eu-egee.org)



Information Society  
and Media



- **AAI in Grids**
- **What's VOMS?**
- **What's VOMS-Admin?**

## Security infrastructure based on X.509 certificates (PKI)

### Authentication

- Needs “trusted third parties”, i.e. Certificate authorities (CAs)
- Users identified with “identity” certificates signed by CAs
- Delegation & single sign-on via proxy certificates

### Authorization

- Several entities involved
  - resource providers (e.g., computer centers, storage providers, ...)
  - Virtual organizations (e.g., LHC experiments collaborations)
- Authorization cannot be decided only on local site basis
  - but must reflect the service level agreements settled between VOs and resource providers
- VOs administer user membership (groups, roles, ...)
- RPs evaluate attributes granted by VOs to their users and map them to local credentials used to access resources

- **Virtual Organization Membership Service**
  - an Attribute Authority (AA) that issues attributes (in the form of signed assertions) expressing membership information of a subject in the context of a Virtual Organization (VO)
  - A VO management service
  - A VO registration service
  - A source of trust for authorization
- **Extends the X509 AAI with attributes related to VO structure**
  - so that access to resources can be authorized accordingly!

- **Reflect the structure of a VO**
  - Group membership
    - A VO member may be part of several VO groups
    - Example:
      - */atlas/production, /atlas/analysis*
  - Role assignment
    - A VO member may be assigned roles
    - Example:
      - */atlas/production/Role=SoftwareManager*
  - Generic attributes
    - (Name,Value) pairs that can be associated with a VO membership
    - Example:
      - *cern\_afs\_account = ceccanti*

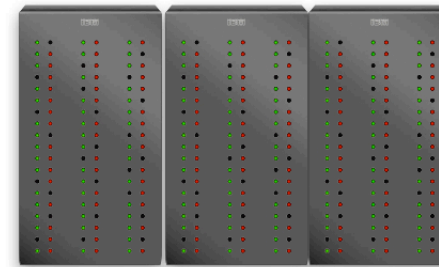
## How does a user get his VOMS attributes?

- **Preconditions:**
  - The user must have an x509 certificate signed by a trusted CA
  - The user must be registered in a VOMS server as a member of a VO
- **The User contacts the VOMS server for his VO using a command line client (voms-proxy-init) or VOMS APIs**
- **A proxy certificate is created containing the user VO membership information**
  - In particular, VOMS creates a signed Attribute Certificate (AC) containing this info that is then packed into a proxy certificate
- **The proxy certificate is used to authenticate and authorize the User at remote services**

## VOMS Attribute Authority



## Computing Service



1. Get AuthZ credentials  
(voms-proxy-init or APIs)



AC

2. Submit Jobs & get output



X509 Proxy + AC



User machine

- **AC as defined by RFC 3281**
  - VOMS OID: 1.3.6.1.4.1.8005.100.100
  - To prevent the stealing of VOMS ACs and other sec. measures:
    - DN of Attribute Holder linked into the ACs
    - Serial Number of User Certificate linked into the ACs
    - ACs have their own Validity period
  - ACs are signed by the private key of the VOMS Server Host certificate
- **VOMS Attributes are listed as *FQANs* in the AC**
  - FQAN: Fully Qualified Attribute Name
  - Example:  
`/cms/Higgs/Role=cmsprod`

- **Group structuring is expressed using this syntax**
  - `/<root group>/<subgroup>/.../<subgroup>`
- **<root group> MUST be the name of the Virtual Organization**
- **Group membership is compulsory and cannot be denied**
- **A member of a subgroup MUST be a member of the parent (sub)group**

`/example_vo/group`

`/example_vo/group/subgroup`

`/example_vo/group/subgroup/subsubgroup`

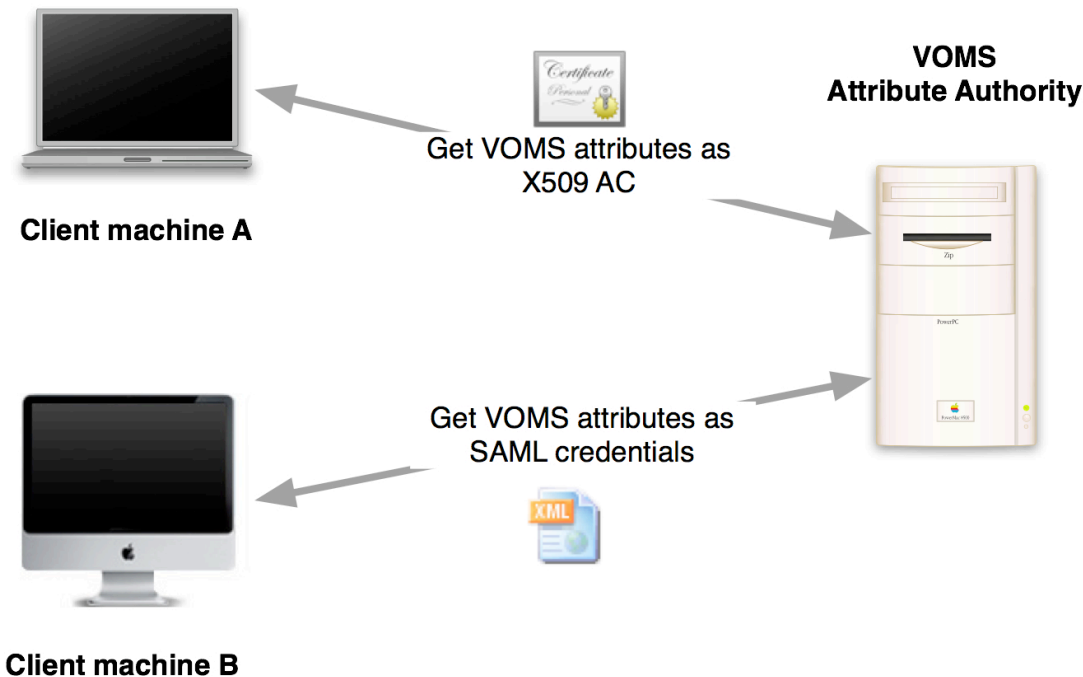
- **Roles are optional**
  - a User request which Roles he wants in his AC at voms-proxy-init time
- **Ownership of a role is always associated to membership in a group**
  - i.e., the User that gets the Role MUST be also a member of the group in which the Role is assigned
- **FQAN syntax:**
  - <group name>/Role=<role name>

/infngid/Role=VO-Admin

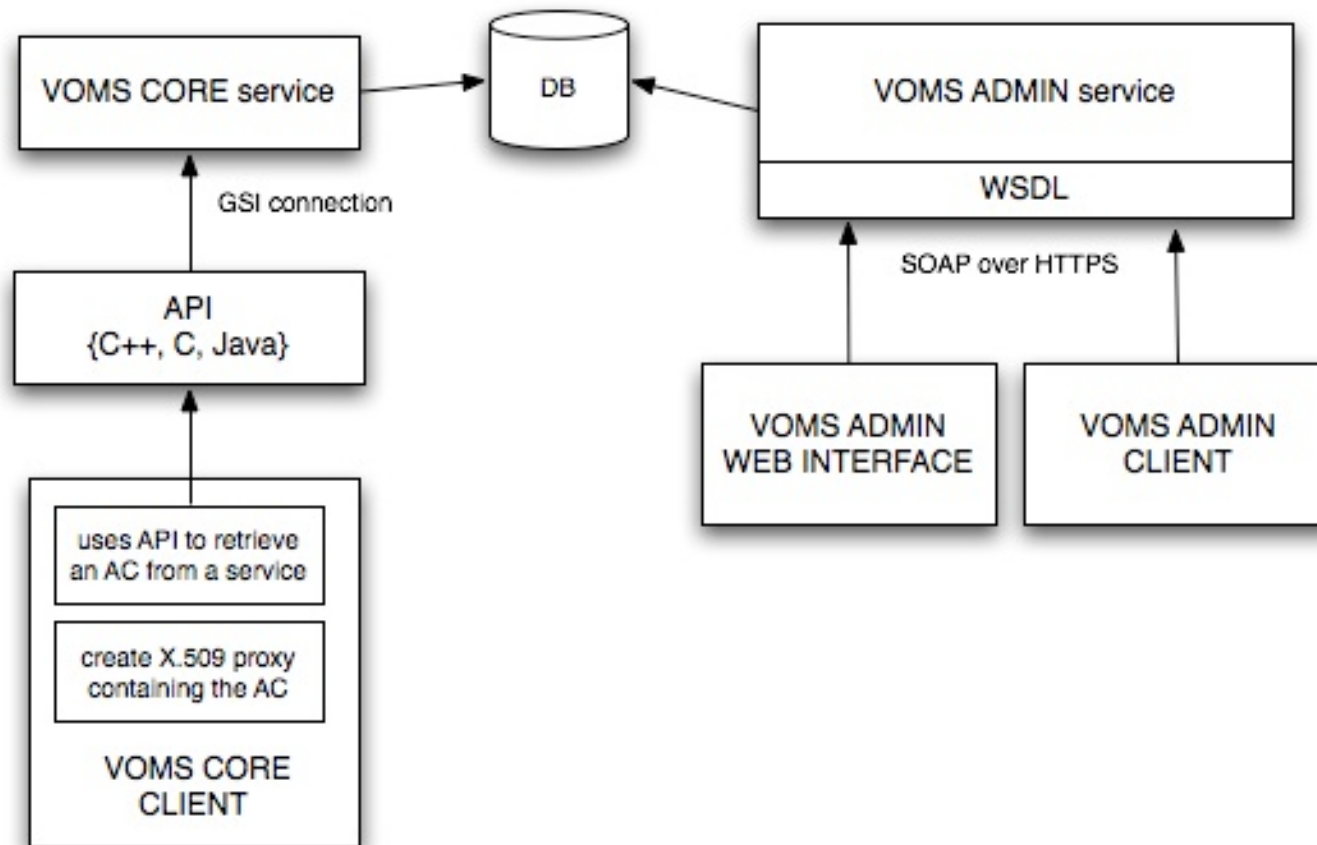
/infngid/TEST/Role=SoftwareManager

- **These are (Name, Value) pairs that can be embedded into the AC**
- **Useful to attach other kind of trusted information to a VO membership**
  - e.g., embed shibboleth attributes inside VOMS ACs

- In order to verify ACs, the certificate that was used to sign them (usually the VOMS server host certificate) must be available where verification takes place
- VOMS currently implements a transparent certificate distribution mechanism
  - AA certificate is embedded in the AC, so that clients can use it to verify the AC itself.
- Historically (i.e., in current production grid :)) VOMS server certificates were distributed as RPMs (like CA RPMs)
  - Difficulties in the management of timely renewal/redistribution of new server certificates



- **Currently VOMS is being extended to encode VOMS attributes using SAML Attribute Assertions**
  - Better interoperability with the Web Services world
- **This is complementary to the “traditional” VOMS service**
  - i.e., the same VOMS server will be able to issue X509 ACs **AND** SAML assertions describing the same VO membership



# VOMS Management and Registration services (Voms Admin)

- **A J2EE Web application that**
  - manages the contents of the VOMS database
  - provides registration services
- **Used by VO Administrators mainly to**
  - add/remove users to the VO,
  - put them in VOMS groups,
  - assign VOMS roles to them
  - manage generic attributes
- **Provides a WSDL interface to its functions**
- **Implements a flexible AuthZ framework**
  - on top of HTTPS

Welcome to voms-admin registration for the **test\_vo** VO.

To access the VO resources, you must agree to the VO's Usage Rules. Please fill out all fields in the form below and click on the submit button at the bottom of the page.

After you submit this request, you will receive an email with instructions on how to proceed. Your request will not be forwarded to the VO managers until you confirm that you have a valid email address by following those instructions.

**IMPORTANT:**

By submitting this information you agree that it may be distributed to and stored by VO and site administrators. You also agree that action may be taken to confirm the information you provide is correct, that it may be used for the purpose of controlling access to VO resources and that it may be used to contact you in relation to this activity.

**Your distinguished name (DN):**

/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti/Email=andrea.ceccanti@cnafe.infn.it

**Your CA:**

/C=IT/O=INFN/CN=INFN CA

**Your email address:**

andrea.ceccanti@cnafe.infn.it

**Your institute:**

**Your phone number:**

**Comments for the VO admin:**

You agree on the VO's usage rules.

**Register!**

- VO-Admins get notified via mail of user's registrations requests and can then approve (or reject) them

voms admin for VO: test\_andrea Current user: Andrea Ceccanti

VO management Subscriptions
Other VOs on this server

See	Pending VO Membership requests			
<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px; text-align: center;">Pending requests</div> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">Processed requests</div>	<hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; padding: 5px;"> <b>Andrea Ceccanti</b>  <small>INFN CA,INFN</small> </td> <td style="width: 20%; text-align: center; padding: 5px;">reject</td> <td style="width: 20%; text-align: right; padding: 5px;">approve</td> </tr> </table> <hr/>	<b>Andrea Ceccanti</b> <small>INFN CA,INFN</small>	reject	approve
<b>Andrea Ceccanti</b> <small>INFN CA,INFN</small>	reject	approve		

## voms admin for VO: test\_vo

Current user: Andrea Ceccanti

[VO management](#) [Subscriptions](#)

[Other VOs on this server](#)

- Manage
- Users
- Groups
- Roles
- Attributes

[Create a new user](#)

### Users:

test1 CA,eScience	delete user
test2 INFN CA,INFN	delete user
test3 GILDA Certification Authority,GILDA	delete user

1-3 of 3

User "test1" added to group "/test\_vo/subgroup1".

- Manage
- Users
- Groups
- Roles
- Attributes

**User details** [-]

[delete this user](#)

User's DN & CA: **test1**  
/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk

User's common name:

User's email address:

**Membership details** [-]

/test\_vo/subgroup2

Group name	Roles
/test_vo	<input type="button" value="SoftwareManager"/> <input type="button" value="Assign role"/>
/test_vo/subgroup1	<input type="button" value="SoftwareManager"/> <input type="button" value="Assign role"/> <input type="button" value="remove"/>

**Generic attributes management** [-]

Attribute:

Attribute value:

Attribute list:

- **All Operations on the VOMS Admin are authorized via ACLs**
- **ACLs are (Context, Principal, Permission) triples**
  - The Context is a FQAN
  - The Principal is either
    - a (DN, CA) couple (i.e., an X509 certificate)
    - a FQAN
    - ANY\_AUTHENTICATED\_USER
  - The Permission states what the principal can do in the Context
    - List/Add members to a Group/Role
    - Create subgroups
    - Manage attributes
    - Manage requests/subscriptions pertaining groups/roles

## voms admin for VO: omiiurope

Current user: **Andrea Ceccanti**

**VO management** Subscriptions

Other VOs on this server

- Manage
- Users
- Groups
- Roles
- Attributes

**ACL management for group /omiiurope** -

Access control list:

Admin DN & CA	Container	Membership	ACL	Attributes	Requests	Add entry
/omiiurope/Role=VO-Admin VOMS Role	rw	rw	rwd	rw	rw	edit delete
<b>Any Authenticated User</b> Dummy Certificate Authority	r	r	r	r		edit delete
omii001.cnaf.infn.it INFN CA	rw	rw	rwd	rw	rw	edit delete
Valerio Venturi INFN Certification Authority	rw	rw	rwd	rw	rw	edit delete

Default Access control list:

Add entry

Default acl not defined for this group.

**Membership details for group /omiiurope** +

**Generic attributes management for group /omiiurope** +

- The web interface is ACL aware
  - only authorized actions are shown and can be executed

**voms admin** for VO: test\_vo Current user: Andrea Ceccanti

VO management Subscriptions Other VOs on this server

**Manage**

- Users
- Groups
- Roles
- Attributes

**User details** ☰

[delete this user](#)

User's DN & CA: **test1**  
/C=UK/O=eScience/OU=Authority/CN=CA/Email=ca-operator@grid-support.ac.uk

User's common name:

User's email address:

**Membership details** ☰

/test\_vo/subgroup2

Group name	Roles	
/test_vo	SoftwareManager	<input type="button" value="Assign role"/>
/test_vo/subgroup1	SoftwareManager	<input type="button" value="Assign role"/> <a href="#">remove</a>

**Generic attributes management** ☰

- **Virtual Organization Membership Service is**
  - an Attribute Authority (AA) that issues attributes (in the form of signed assertions) expressing membership information of a subject in the context of a Virtual Organization (VO)
  - A VO management service
  - A VO registration service
  - A source of trust for authorization
  
  - A robust and widely deployed solution for attribute-based authz in Grid middlewares

