Introduction to VOMS (and VOMS-Admin)

Vincenzo Ciaschini, Andrea Ceccanti
(Francesco Giacomini)

CCR & INFNGrid Workshop
Santa Tecla, 19th May 2010

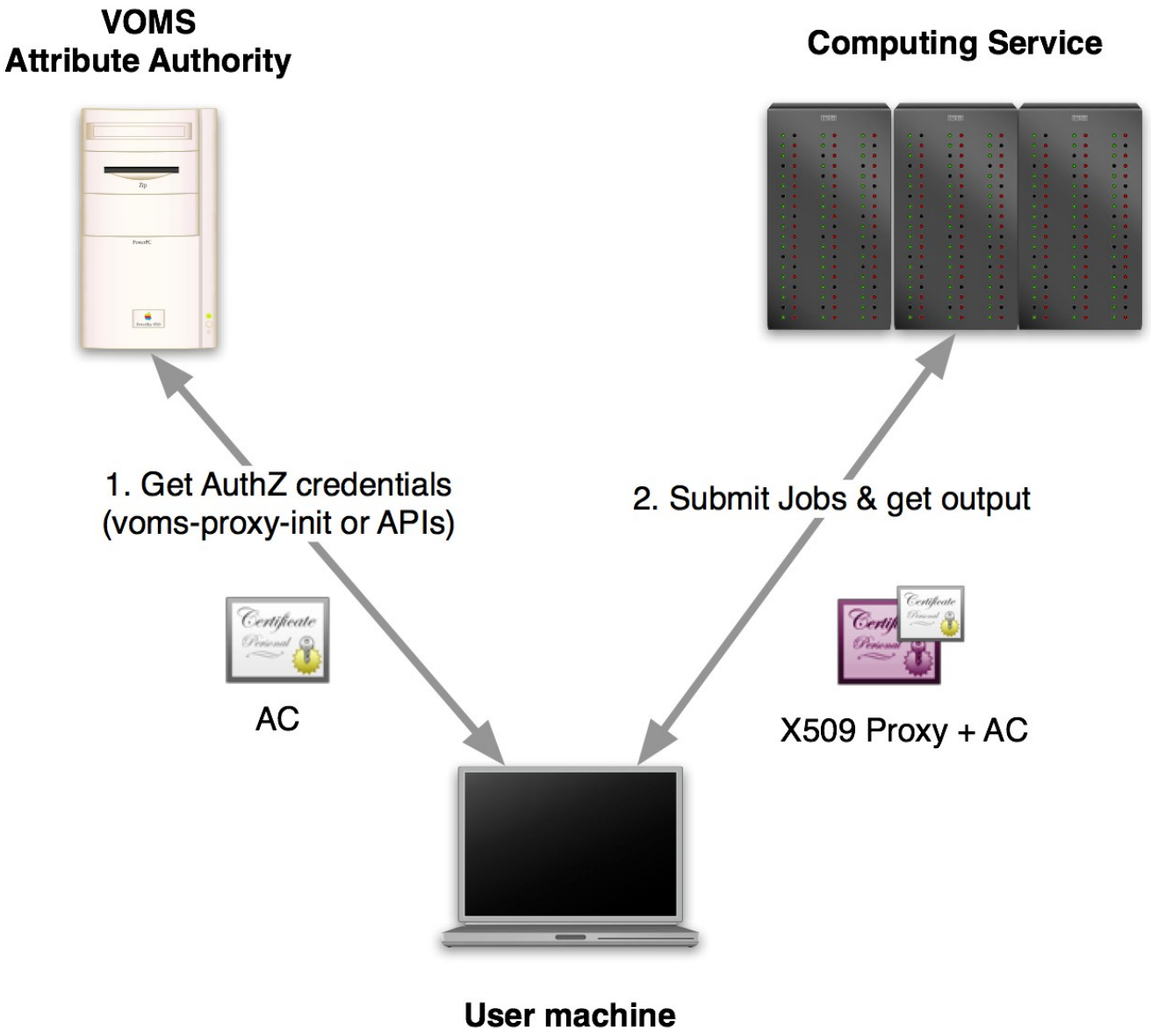
www.eu-egee.org

Information Society and Media

What is VOMS?

- **Virtual Organization Membership Service**
- **VOMS is an X.509 Attribute Authority**
  - Issues X.509 Attribute Certificates
  - Original motivation: support for Grid and VOs
  - De-facto standard, stable and mature, in production since 2003
- **VOMS is a tool to manage membership**
- **VOMS is a SAML Attribute Authority**
  - Issues SAML Assertions
- **VOMS is integrated with Shibboleth through VASH (VOMS Attributes from Shibboleth)**
- **VOMS has native support for replication**

Typical Usage Scenario



Types of Attribute

- **Organizational**
  - Groups/subgroups
  - Roles within those groups
  - e.g. /cms/prod/Role=scg
- **Generic**
  - name = value
  - e.g. login = vciaschi

Management Interface

- **A J2EE Web application that**
  - manages the contents of the VOMS database
  - provides a registration service for VO users
  - can talk with external databases (e.g. the CERN orgdb) to synchronize/validate membership information
- **Used by VO Administrators mainly to**
  - approve membership requests
  - add/remove users to the VO
  - put them in VOMS groups
  - assign VOMS roles to them
  - manage generic attributes
- **Implements a flexible AuthZ framework on top of HTTPS**

Management Interface /2

- **Moreover:**
  - Multiple certificates per user support
  - VO membership suspension/expiration/renewal
  - AUP management
  - VO member's ability to request group/role membership
  - Availability of Web Service interface and command-line

voms admin for VO: test_vo

Current user: Andrea Ceccanti

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@cnaf.infn.it

Your CA:

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

Your email address:

andrea.ceccanti@cnaf.infn.it

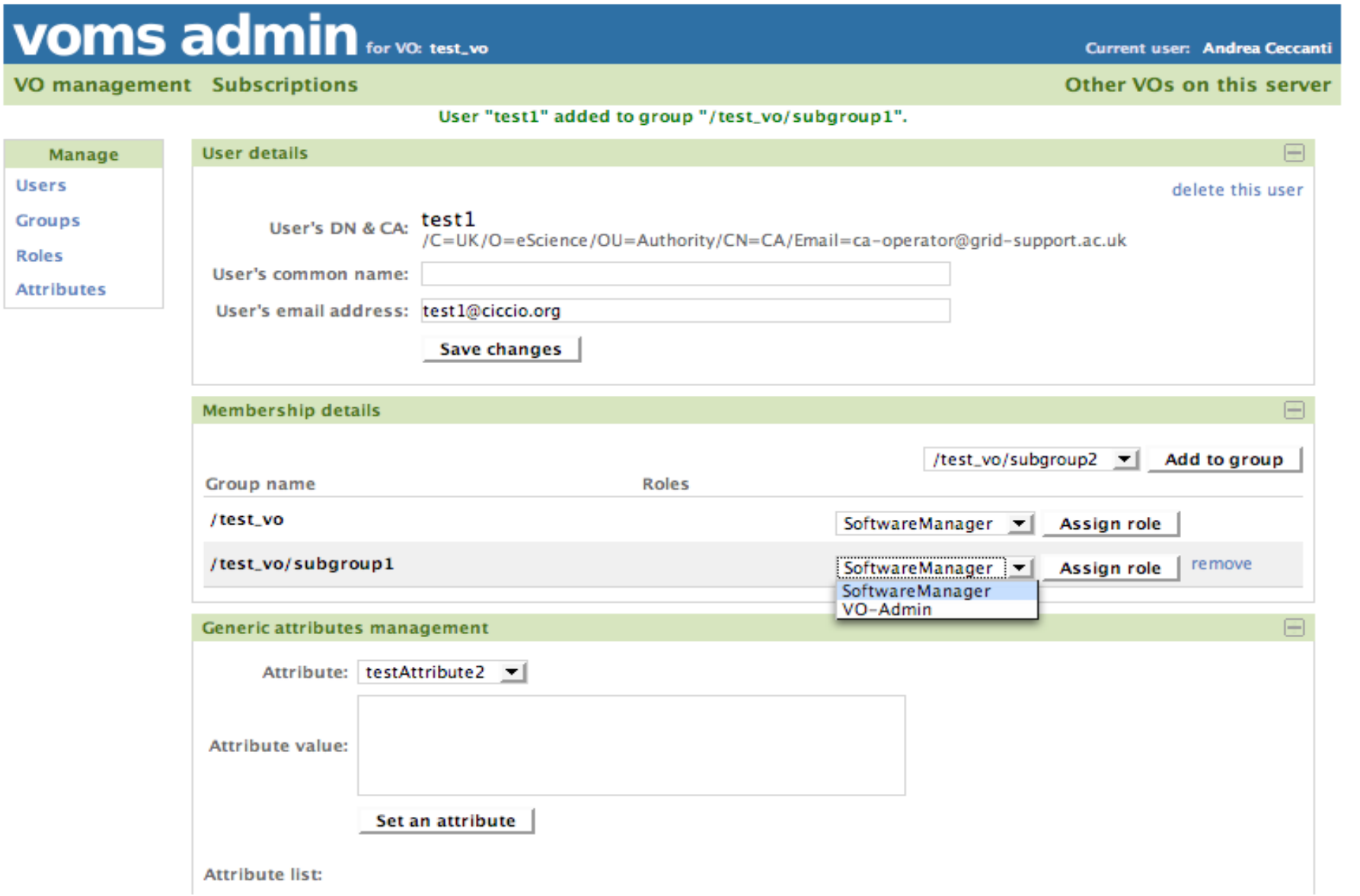
Your institute:

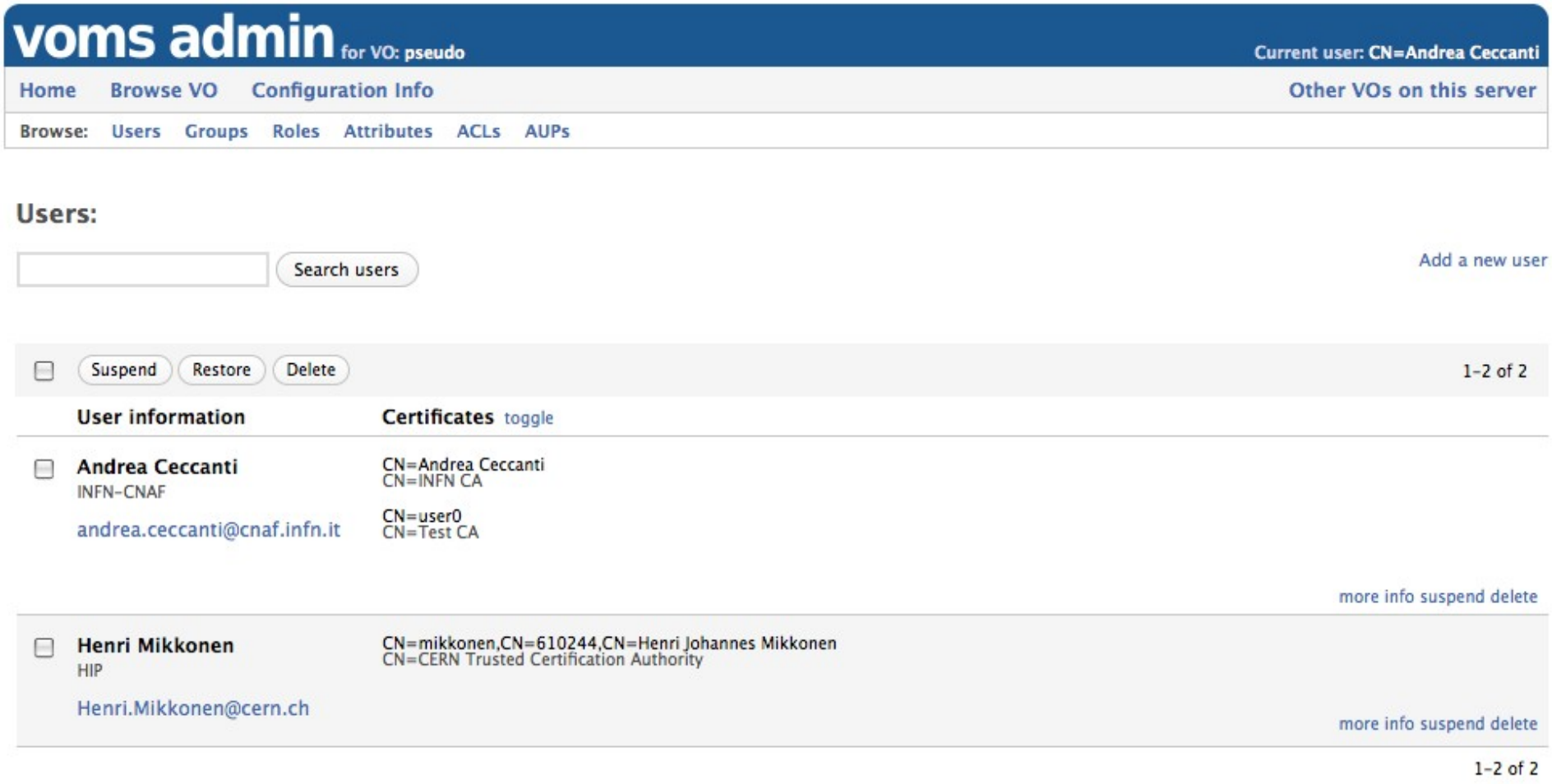
Your phone number:

Comments for the VO admin:

☐ You agree on the VO's usage rules.

Register!


voms admin for VO: test_vo
Current user: Andrea Ceccanti
VO management
Subscriptions
Other VOs on this server
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:
test1@ciccio.org
Save changes
Membership details
/test_vo/subgroup2
Add to group
Group name
Roles
/test_vo
SoftwareManager
Assign role
/test_vo/subgroup1
SoftwareManager
Assign role
remove
SoftwareManager
VO-Admin
Generic attributes management
Attribute:
testAttribute2
Attribute value:
Set an attribute
Attribute list:


voms admin for VO: pseudo
Current user: CN=Andrea Ceccanti
Home
Browse VO
Configuration Info
Other VOs on this server
Browse: Users Groups Roles Attributes ACLs AUPs
Users:
Search users
Add a new user
Suspend
Restore
Delete
1-2 of 2
User information
Certificates toggle
Andrea Ceccanti
INFN-CNAF
andrea.ceccanti@cnaf.infn.it
CN=Andrea Ceccanti
CN=INFN CA
CN=user0
CN=Test CA
more info suspend delete
Henri Mikkonen
HIP
Henri.Mikkonen@cern.ch
CN=mikkonen,CN=610244,CN=Henri Johannes Mikkonen
CN=CERN Trusted Certification Authority
more info suspend delete
1-2 of 2

Manage the Access Control List for

Group: /pseudo **Role:** -- **Show default ACL:**

ACL for context /pseudo

Add entry

Admin DN & CA	Container	Membership	ACL	Attributes	Requests	Personal info	Suspend	
CN=mikkonen,CN=610244,CN=Henri Johannes Mikkonen CN=CERN Trusted Certification Authority	rw	rw		rw		rw		edit delete
/pseudo/Role=VO-Admin CN=VOMS Role	rw	rw	rwd	rw	rw	rw	yes	edit delete
CN=Any Authenticated User CN=Dummy Certificate Authority	r	r						edit delete
CN=devel13.cnaf.infn.it CN=INFN CA	rw	rw	rwd	rw	rw	rw	yes	edit delete

Current deployment

- 172 VOs on 42 servers
- Max n. of attribute requests (Jan 2010):
  938753 (ALICE), i.e. 30 Kreq/day (on two hosts)