



Enabling Grids for E-scienceE

AAI and Grids

Andrea Ceccanti

*Workshop sul Calcolo e Reti dell'INFN
Rimini, Maggio 2007*

www.eu-egee.org



Information Society
and Media



- **AAI in current production Grid**
- **VOMS**
 - Architecture
 - Administrative services
- **VOMS in practice**

Security infrastructure based on X.509 certificates (PKI)

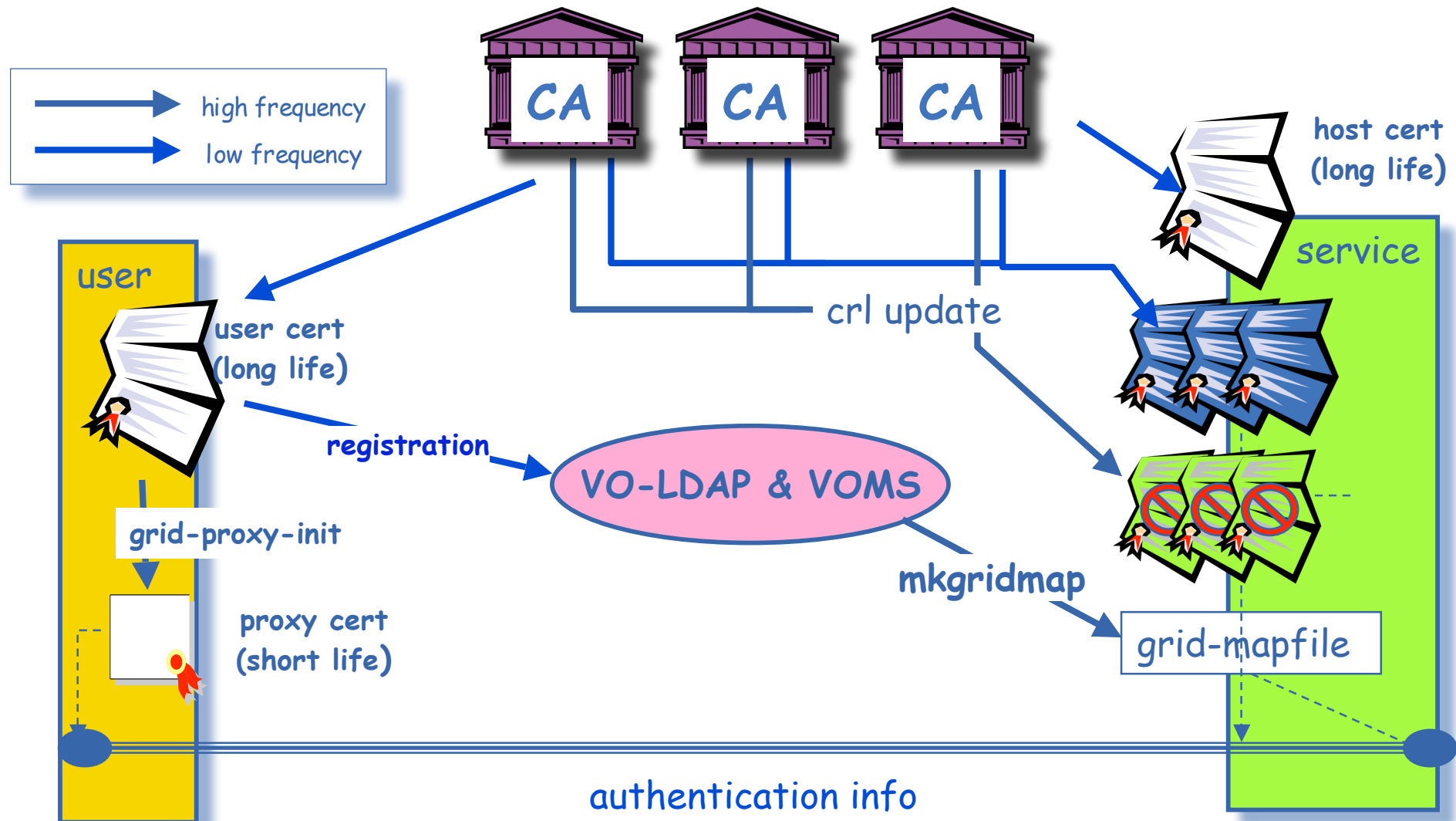
Authentication

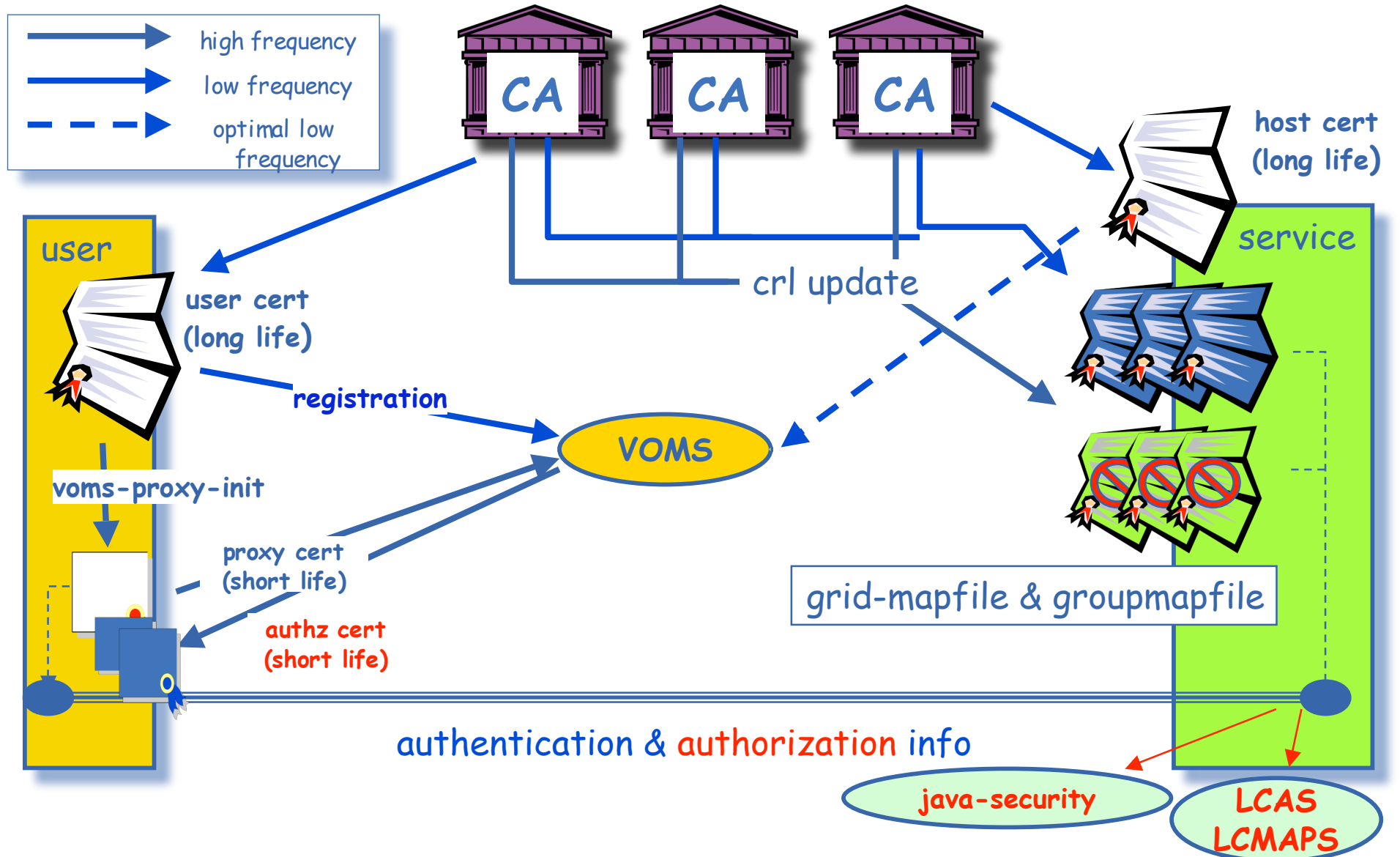
- Needs “trusted third parties”, i.e. Certificate authorities (CAs)
- Users identified with “identity” certificates signed by CAs
- Delegation & single sign-on via proxy certificates

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

Traditional grid-mapfile

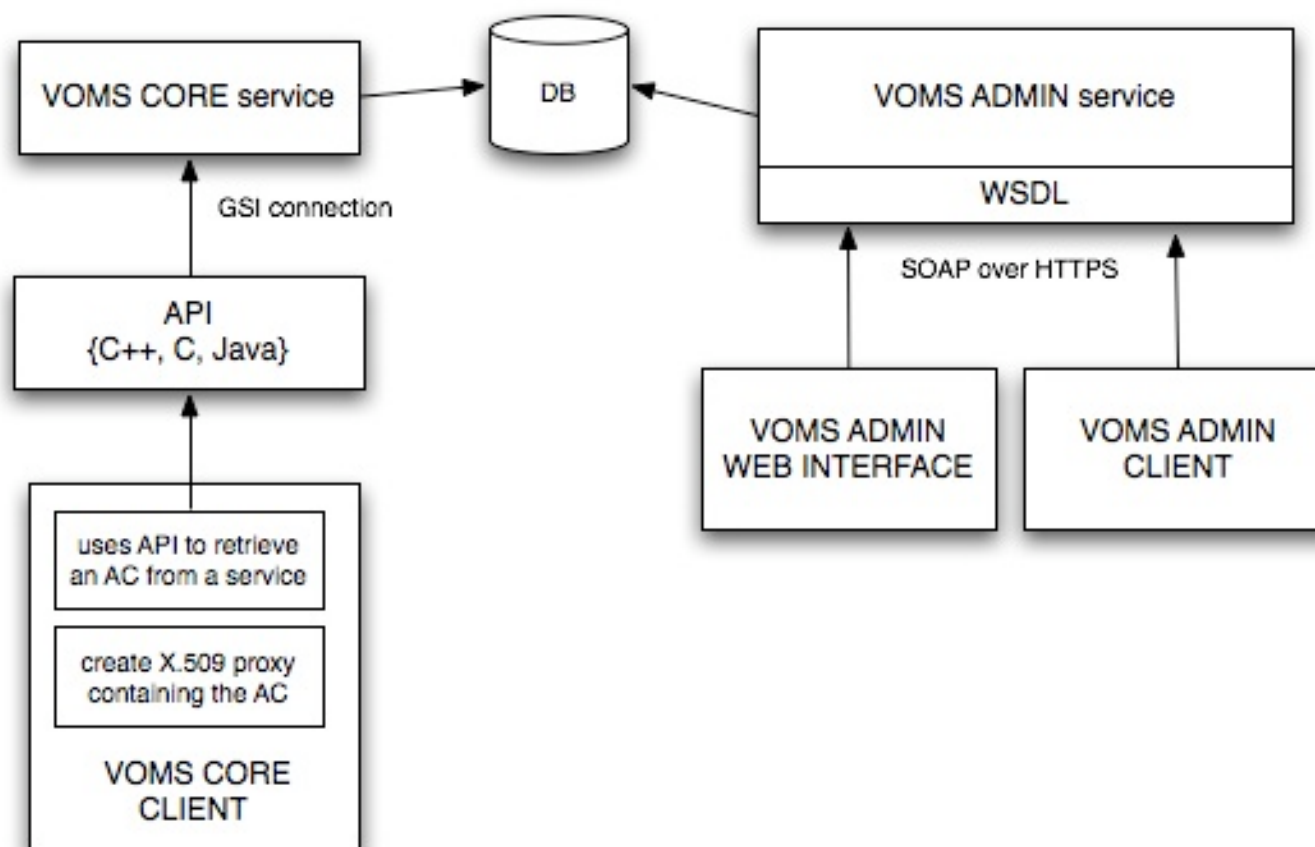




- When you create a proxy certificate via `voms-proxy-init`, you contact a VOMS server, which contains informations about the user.
- This information is then added in the proxy certificate, which is then used to authenticate and authorize the user.
 - Implies that the user should be registered in a voms server before submitting a job
 - The information consists of organizational info
 - Group/Roles
 - Plus Freeform Attributes
 - Name = Value

- **VOMS**
 - In a grid environment, VOs tend to be extremely large and change frequently.
 - Thousands of users.
 - Sites need to know the users because of the need to prepare local accounts
 - It is not scalable to manage them by hand

- **VOMS is...**
 - An Attribute Authority.
 - Provides membership information regarding a VO user (e.g., groups, roles,...) in the form of Attribute Certificates (ACs)
 - A VO Management System
 - A VO Registration service.
 - A source of trust for authorization.
 - Used via voms-proxy-init command.
 - Compatible with grid-proxy-init
 - Adds Attribute Certificates (ACs) directly in the user proxy.



VOMS Attribute Authority

- **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
 - Nothing prevents the use of a service certificate or user certificates instead of host certs in this signing process
- **The Authorization tokens are listed as *FQANs* in the AC**
 - FQAN: Fully Qualified Attribute Name
 - Example:
 - /cms/Higgs/Role=cmsprod/Capability=NULL

- **The Attribute signing certificate *MUST** be installed on each infrastructural machine that needs to verify VOMS Attributes**
 - This means that all entry-point middleware *MUST** verify the VOMS Attributes
 - Installed in \$VOMSDIR (default: “/etc/grid-security/vomsdir/”)
 - Though it seems similar to the CA RPMs distribution and installation, the amount of VOs on planet Earth will exceed the amount of CAs
 - VOMS certificates are normal {host|service|user} X.509 certificates
 - Usually expire each year
 - Will need timely renewal and redistribution
- **New mechanism in VOMS >1.7.0 makes the installation of the VOMS Issuer Certificates optional**
 - *More about this in more detail later in the slides*

***: these *MUST* are specific to EGEE/LCG/INFNGRID as deployed today**

- **Group structuring is expressed in the FQAN**
 - /<root group>/<subgroup>/.../<subgroup>
- **<root group> MUST be the name of the Virtual Organization**
- **Amount of subgroups is unlimited in a FQAN**
- **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 not organized in a hierarchical structure
- Roles are optional
- Ownership of a role is always associated to membership in a group
- If no specific role is held, the <role name> is NULL
- The member **MUST** be also a member of the group in which the Role is associated
- **FQAN:**
 - <group name>/Role=<role name>/Capability=<capability name>

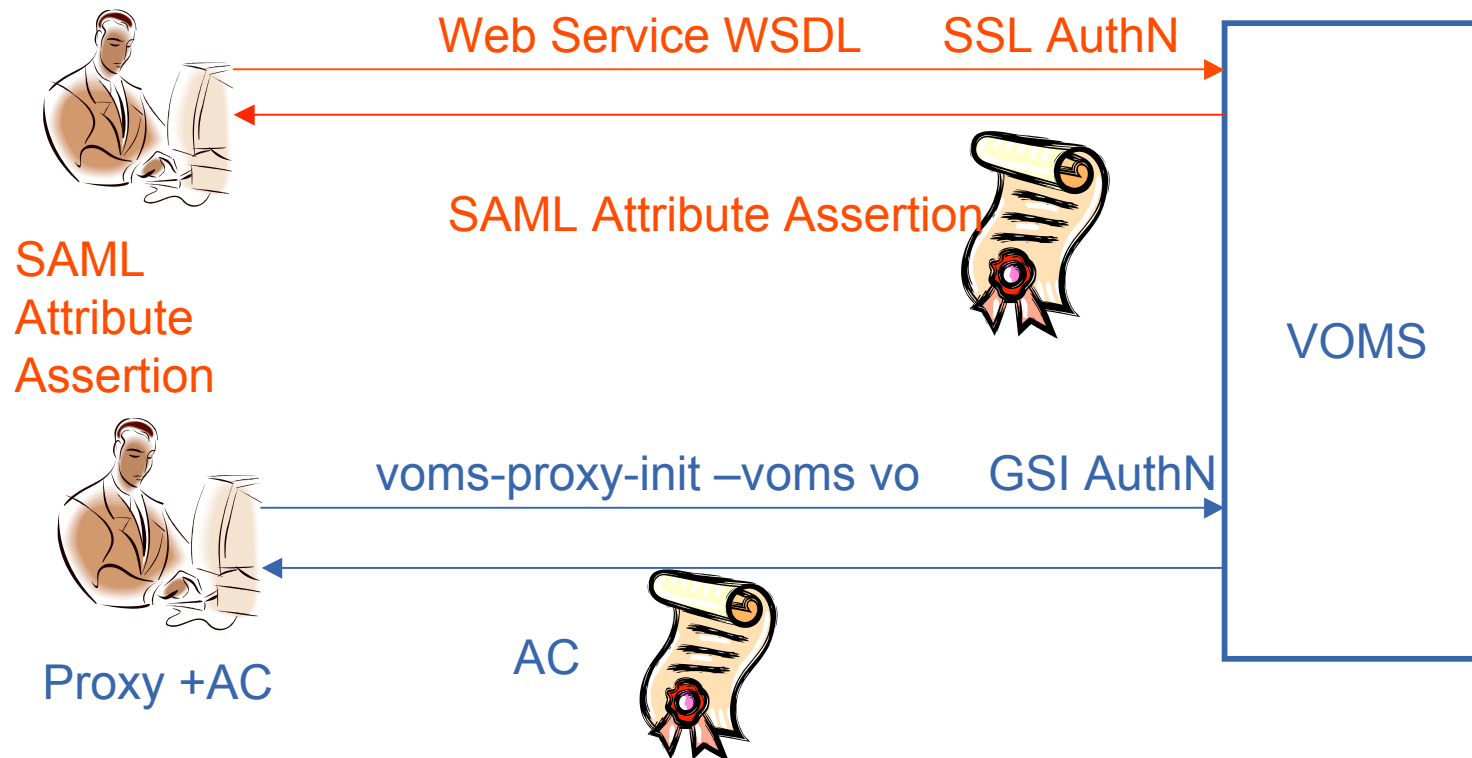
/infngrid

/infngrid/TEST/Role=SoftwareManager/Capability=NULL

/infngrid/CNAF/developers

- **VOMS version > 1.7.0 allow for extensions to the existing fields in the AC**
 - **Issuer Certificate:**
 - This extension is meant to include the AA's public key certificate and the whole certificate chain leading to it, up to and excluding the CA certificate that is expected to be on the evaluator's machine (typically, the root CA)
 - If this extension is present, the evaluator MAY choose to use this certificate to verify the AC
 - **Tags: (*VOMS version > 1.7.10*)**
 - 'name' = 'value' pair plus 'qualifier' are linked to a policyAuthority
 - *The policyAuthority specifies which authority is the source of the enclosed tags*
 - Intended to provide a way to specify (arbitrary) attributes

- **SAML (Security Assertion Markup Language) support**
 - VOMS will generate standard SAML Attribute Assertions
 - Useful to make VOMS contactable by Web Services
 - Attribute Assertions will be usable independently from the user's credentials.



VOMS Management and Registration services (Voms Admin)

- **A web application that manages the contents of the VOMS database and 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...
- **Provides a WSDL interface to its functions**
 - that is mainly used by VOMRS
 - and mkgridmap
- **Has a command line client**
- **Has a web-based user interface**

Voms-Admin 2.0

https://omii001.cnaf.infn.it:8443/voms/omiieurope/ ccr 2007 workshop

Come iniziare Ultime notizie news Slashdot: News for ... DEAD AIR SPACE docs Morfemix

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize To

WorkShop 2007 sul Calcolo e ... Voms-Admin 2.0

voms admin

for VO: omiieurope

Current user: Andrea Ceccanti

VO management Subscriptions Other VO's on this server

Manage

- Users
- Groups
- Roles
- Attributes

User details

[Delete this user](#)

User's DN & CA: /C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Andrea Ceccanti/Email=andrea.ceccanti@cnaf.infn.it
/C=IT/O=INFN/CN=INFN CA

User's common name:

User's email address:

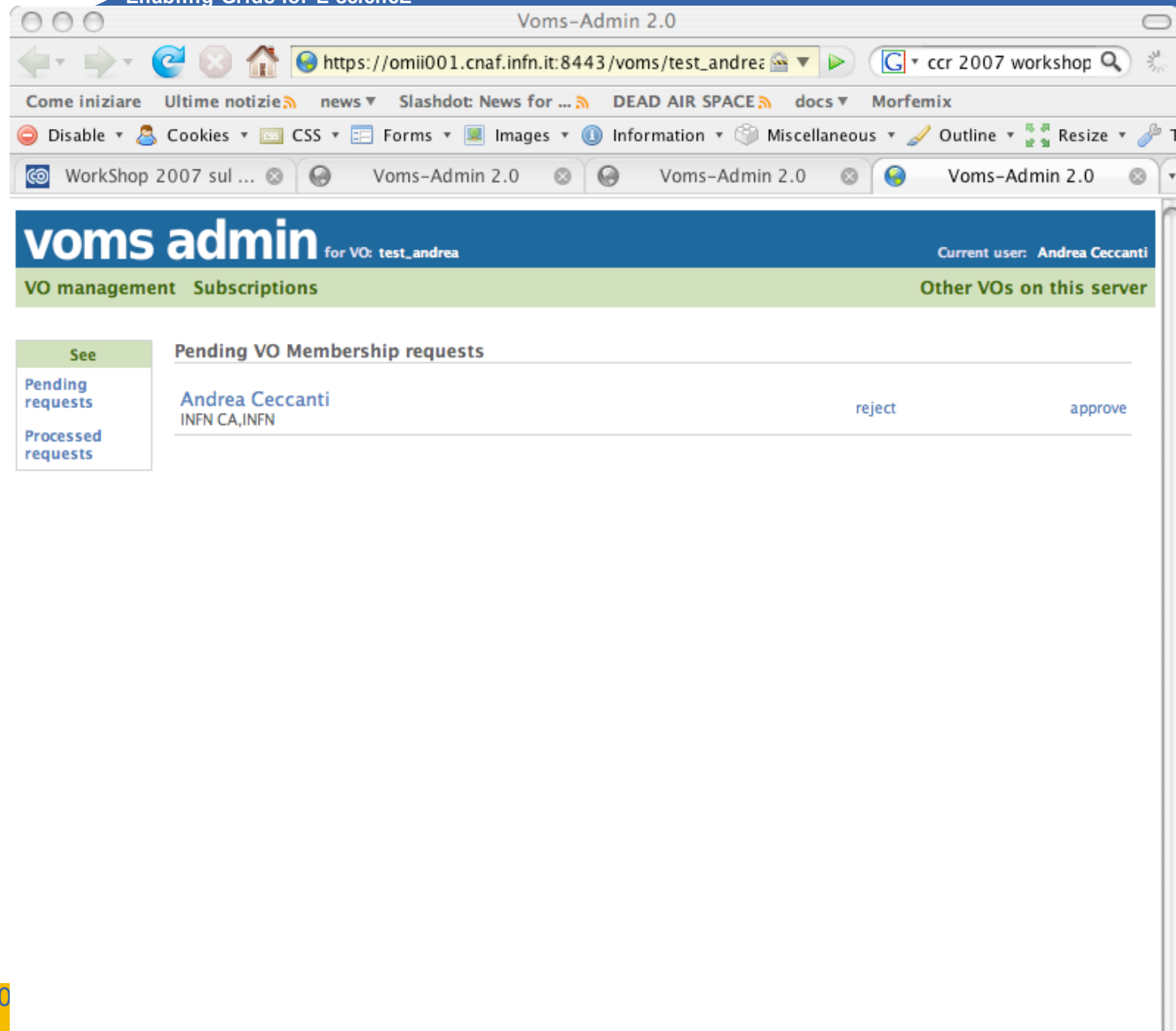
User's CRL url:

Membership details

Group name	Roles	
/omiieurope/INFN/Padova		<input type="button" value="Add to group"/>
/omiieurope	VO-Admin	<input type="button" value="dismiss role"/>
	SoftwareManager	<input type="button" value="Assign role"/>
/omiieurope/INFN	SoftwareManager	<input type="button" value="Assign role"/> <input type="button" value="remove"/>

Generic attributes management

No attribute classes defined for this vo.



The screenshot shows a web browser window titled "Voms-Admin 2.0" with the URL https://omii001.cnaf.infn.it:8443/voms/test_andrea. The browser's address bar shows "ccr 2007 workshop". The page has a blue header with "voms admin" and "for VO: test_andrea". The current user is "Andrea Ceccanti". The page is divided into two main sections: "VO management" and "Subscriptions". Under "Subscriptions", there is a table titled "Pending VO Membership requests". The table has one row with the name "Andrea Ceccanti" and the email "INFN CA,INFN". There are two buttons, "reject" and "approve", next to the email. On the left side of the page, there is a sidebar with a "See" button and two links: "Pending requests" and "Processed requests".

Pending VO Membership requests	
See Pending requests Processed requests	<div> Andrea Ceccanti INFN CA,INFN </div> <div> reject approve </div>

VOMS in practice

To use the currently deployed production Grid, you need

- Access to an host with User Interface (UI) software installed
- Valid X.509 credentials issued by a trusted CA
- To be member of a VO

- **.globus directory contains your personal public / private keys**

```
[glite-tutor] /home/giorgio > ls -l .globus
total 8
-rw-r----- 1 giorgio users 1613 Oct  4 19:30 usercert.pem
-r----- 1 giorgio users 1914 Oct  4 19:30 userkey.pem
```

Pay attention to permissions !

- **Main options**

-voms <vo-name>:[command]>

- **command** syntax is :/<vname>/group for group specify (default none)
- **command** syntax is :/<vname>/Role=<role name> for Role choice (default none)

```
voms-proxy-init --voms gildav:/gildav/Role=VO-Admin
voms-proxy-init --voms gildav:/gildav/tutors
```

-valid **x:y**, create a proxy valid for **x** hours and **y** minutes

-vomslife **x**, create a proxy with AC valid for **x** hours (max 24 h)

-cert <certfile> Non-standard location of user certificate

-key<keyfile> Non-standard location of user key

-out <proxyfile> Non-standard location of new proxy cert

-userconf <file> Non-standard location for user-defined voms server addresses

- **Default** location for voms server address file is /opt/glite/etc/vomses or ~/.glite/vomses. **Syntax**

```
"vo-nickname" "voms server FQDN" "port" \ "voms server
certificate subject" "vo name"
```

Vomses parameters are usually provided by VOs manager

```
voms-proxy-init --voms gildav
Your identity: /C=IT/O=GILDA/OU=Personal
Certificate/L=INFN/CN=Emidio
Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase for this identity:
[insert your certificate passphrase]
Creating temporary proxy
..... Done
/C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-01.cnaf.infn.it
/C=IT/O=INFN/CN=INFN Certification Authority
Creating proxy
..... Done
Your proxy is valid until Mon Jun 13 09:06:00 2005
```


Verify obtained credentials

```
[giorgio@glite-tutor:~]$ voms-proxy-info --all
subject      : /C=IT/O=GILDA/OU=Personal
               Certificate/L=INFN/CN=Emidio
               Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy
issuer       : /C=IT/O=GILDA/OU=Personal
               Certificate/L=INFN/CN=Emidio
               Giorgio/Email=emidio.giorgio@ct.infn.it
identity     : /C=IT/O=GILDA/OU=Personal
               Certificate/L=INFN/CN=Emidio
               Giorgio/Email=emidio.giorgio@ct.infn.it
type         : proxy
strength     : 512 bits
path         : /tmp/x509up_u513
timeleft     : 20:59:53
VO           : gildav
subject      : /C=IT/O=GILDA/OU=Personal
               Certificate/L=INFN/CN=Emidio
               Giorgio/Email=emidio.giorgio@ct.infn.it
issuer       : /C=IT/O=INFN/OU=Host/L=CNAF/CN=cert-voms-
               01.cnaf.infn.it
attribute    : /gildav/Role=NULL/Capability=NULL
timeleft     : 20:58:28
```

- Using glite-job-submit command

```
$ glite-job-submit [options] <jdl_file>
```

- where <jdl file> is a file containing the job description, usually with extension .jdl.
- vo** <vo name> : perform submission with a different VO than the UI default one.
- output, -o** <output file> save jobId on a file.
- resource, -r** <resource value> specify the resource for execution.
- nomsgi** neither message nor errors on the stdout will be displayed.



- **This presentation includes slides gathered from presentations made by the following people:**
 - Vincenzo Ciaschini
 - Antonia Ghiselli
 - Emidio Giorgio
 - David Groep
 - Oskar Koeroo
- **Thank you!**