VOMS

Vincenzo Ciaschini

EGEE/OSG Workshop

Boston, 24/6/08

What is VOMS, in short

- **VOMS is a X.509 compliant Attribute Authority**
  - See RFC 3281
- **VOMS is a SAML Attribute Authority**
  - See
    - SAML V2.0 Deployment Profile for X.509 Subjects
    - OGF document currently in public comments

The Problem:

- **In a Virtual Organization World, resource utilization is authorized on a VO basis**
  - Not all users are alike!
  - Membership in a VO is large and subject to change
  - Resources are many and subject to change
  - *Authorizing every single user on every single resource does not scale!*
- **So, why not authorize user on the basis of a set of attributes?**
  - Many, many less attributes that users
  - Much less frequent changes

What is VOMS

- **VOMS is a X509 Attribute Authority with special support for Grids and VOs**
  - Adds direct support to represent organizational data
    - Workgroups
      - *Subgroups of workgroups, subgroups of subgroups, etc…*
    - Provisions for special roles inside groups
  - Also keeps support for more “standard” attributes
    - Name = value
    - And allows them to be associated not only to users, but also to subgroups and roles

Examples

- **Examples of Attributes:**

/vo1 **workgroup**

/vo1/group1 **subgroup**

/vo1/group1/Role=TestRole **role in subgroup**

login = marotta

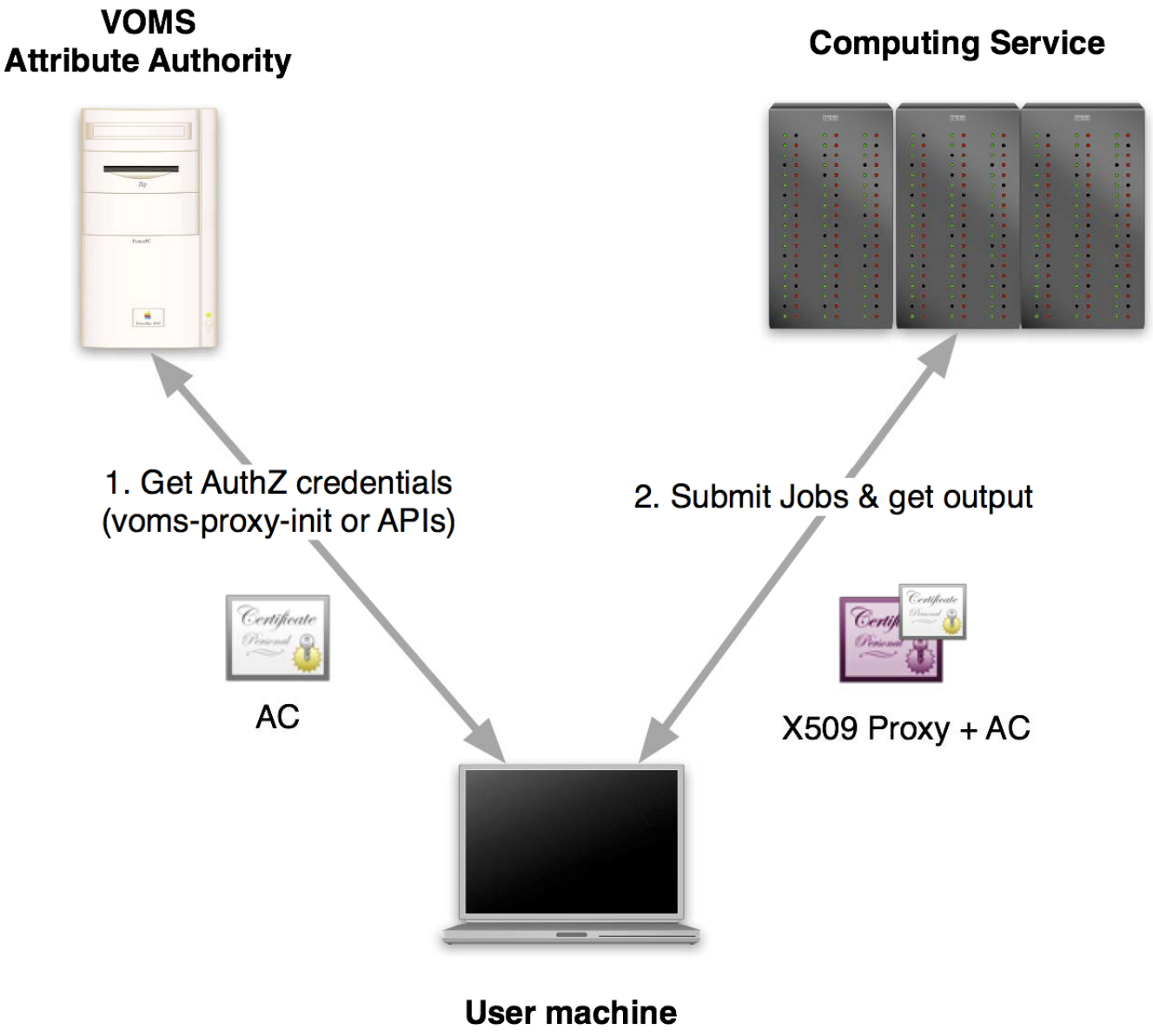
guarantor = Vincenzo C. (/vo1/group1/Role=TestRole)

location = Bologna (/vo1/group1)

Usage of attributes

- **Attributes are useless if resources and applications could not access them.**
- **Both push and pull are supported:**
  - Pull:
    - Resources and applications can directly contact VOMS on behalf of users to obtain their attributes.
  - Push:
    - A voms-proxy-init command is provided to contact VOMS and put the attributes in the user's proxy, which is subsequently delegated to applications.
- **Grid software almost completely uses push.**
- **The protocol to contact the server is proprietary but documented.**
  - No update will ever break forward and backward compatibility

VOMS Interaction



VOMS Formats and Standards

- VOMS inserts its attributes into Attribute Certificates conforming to RFC 3281
- Proxies generated by voms-proxy-init conform to RFC 3820
- VOMS uses X509 certificates and proxies (both RFC 3820 and old-style) to authenticate

What is VOMS?

- **VOMS is a X509 Attribute Authority with special support for Grids and VOs**
- **VOMS is a Membership management tool**
  - Membership in VO <=> Membership in a VOMS
  - Membership in a VOMS implies a lot of things
    - A user may be a member of many groups
    - A user may hold multiple roles
    - A user may have many attributes
  - A tool is needed to manage this: VOMS-Admin

VOMS-Admin

- **VOMS-Admin is a tool used to manage user membership data in a VOMS**
  - A separate process from VOMS
  - Comprised by both a Web Application and a Web Service

VOMS-Admin user registration

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:

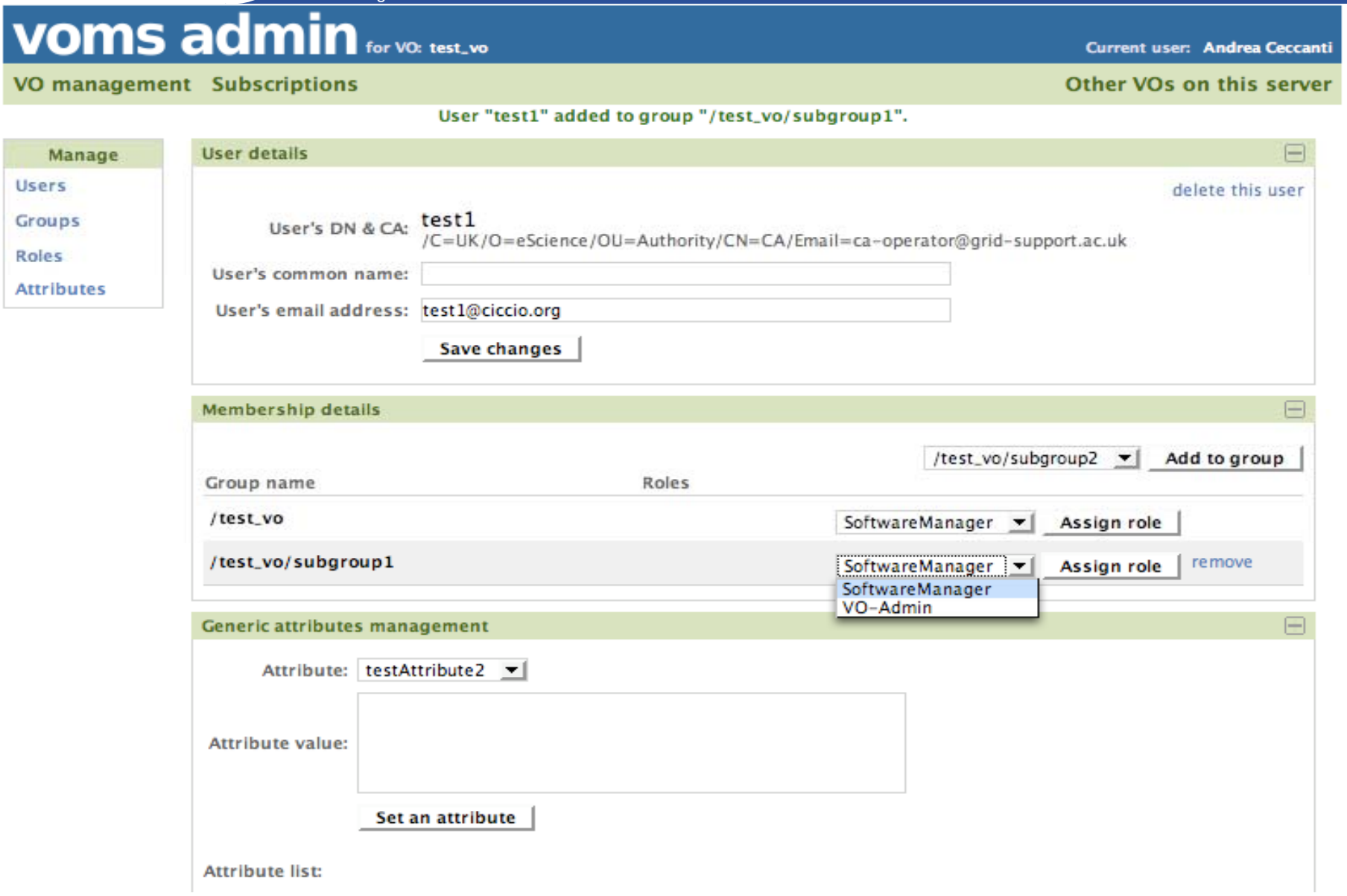
Comments for the VO admin:

☐ You agree on the VO's usage rules.

Register!

VOMS-Admin Group Management

Enabling Grids for E-sciencE

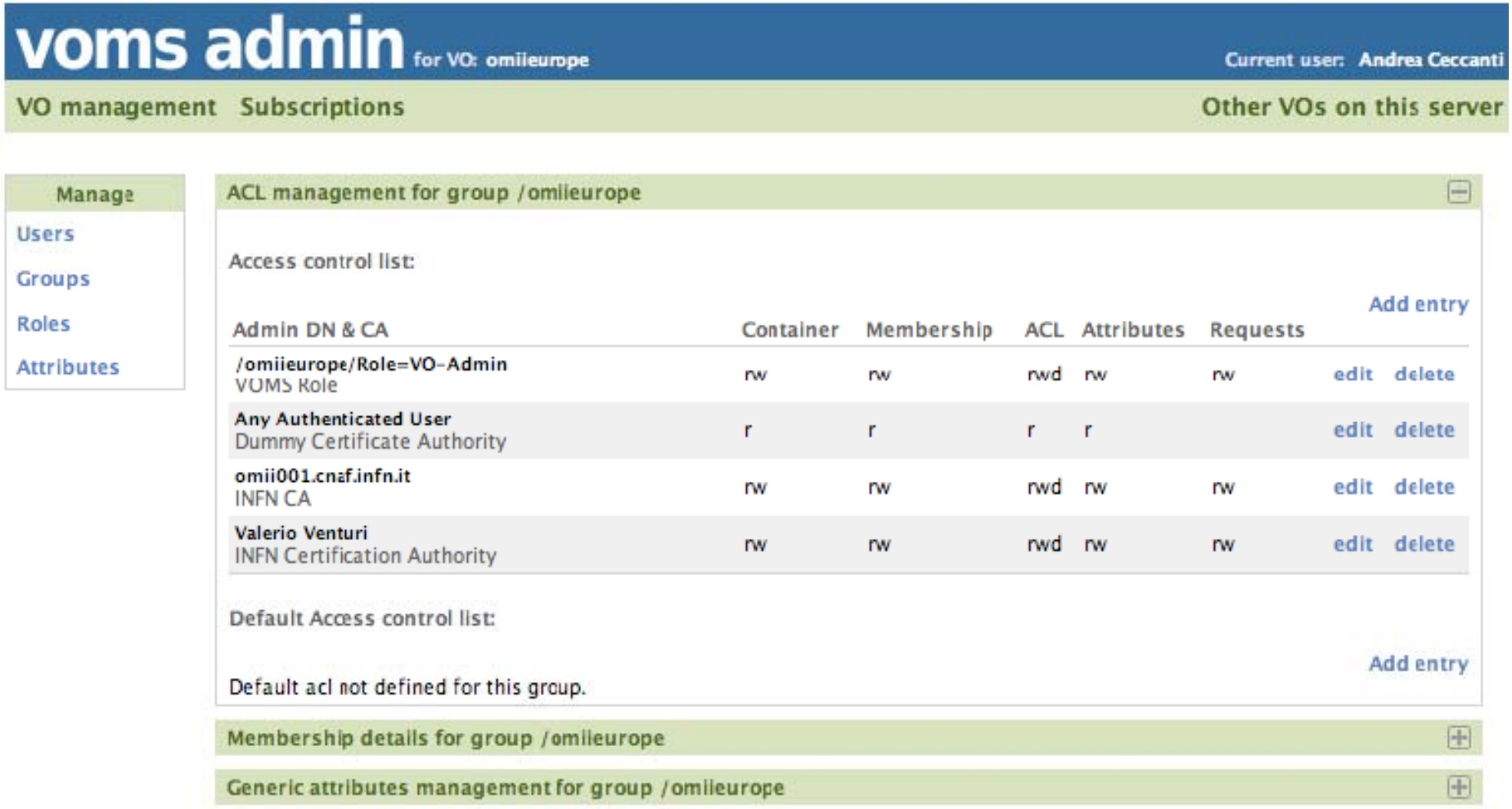


VOMS-Admin AuthZ framework

- **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 ACLs



What is VOMS

- **VOMS is a X509 Attribute Authority with special support for Grids and VOs**
- **VOMS is a Membership management tool**
- **VOMS is a SAML Attribute Authority**
  - The world is not a X509-monoculture!
  - The exact same data from X509 can be expressed in SAML

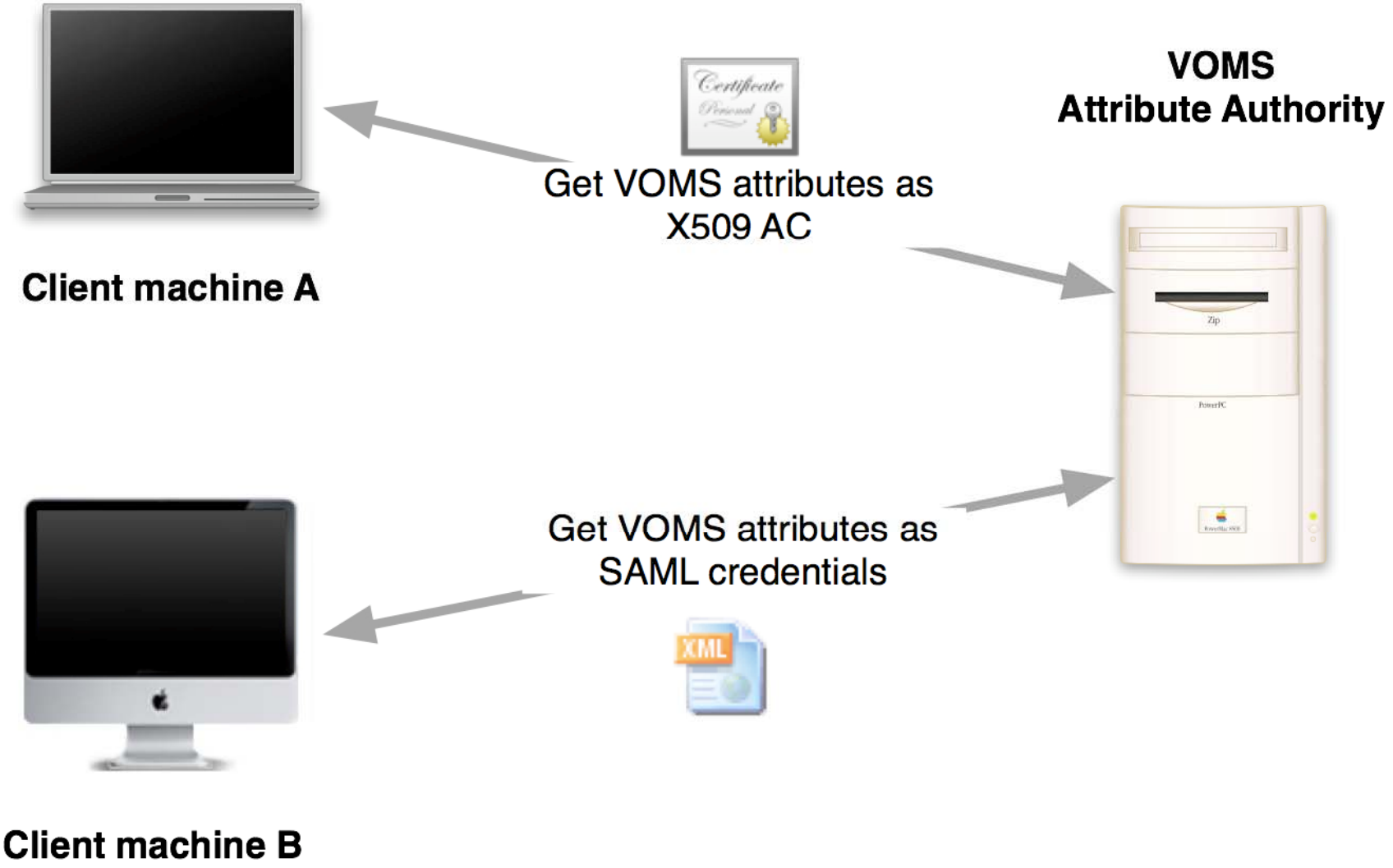
VOMS & SAML

- **Outside from hardcore grid applications, many services rely on a SAML AttributeAssertion**
- **VOMS can generate an AttributeAssertion containing the exact same data as the AC.**
- **VOMS exposes an interface compliant to the SAML Query/Request Profile and the SAML SOAP Binding**
  - Temporary independent package
    - From the same developers
    - Integration in the main packages ongoing

SAML AttributeAssertion Ex.

```
<saml:Assertion ID="_ebff47fb-21a4-4f3d-bf7d-6b2a12b3b81b"
  IssueInstant="2008-04-21T09:56:20.020Z" Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <saml:Issuer>
    CN=omii002.cnaf.infn.it,L=CNAF,OU=Host,O=INFN,C=IT
  </saml:Issuer>

  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    .. signature here
  </ds:Signature>

  <saml:Subject>
    <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
      CN=Valerio Venturi,L=CNAF,OU=Personal Certificate,O=INFN,C=IT
    </saml:NameID>
    <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
      ... says the subject was authenticated using a X.509 certificate
    </saml:SubjectConfirmation>
  </saml:Subject>

  <saml:Conditions NotBefore="2008-04-21T09:56:20.020Z" NotOnOrAfter="2008-04-21T21:56:20.020Z" />

  <saml:AttributeStatement>
    <saml:Attribute Name="http://voms.forge.cnaf.infn.it/group"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema">
        /omiieurope/INFN
      </saml:AttributeValue>
      <saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema">
        /omiieurope
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>

</saml:Assertion>
```

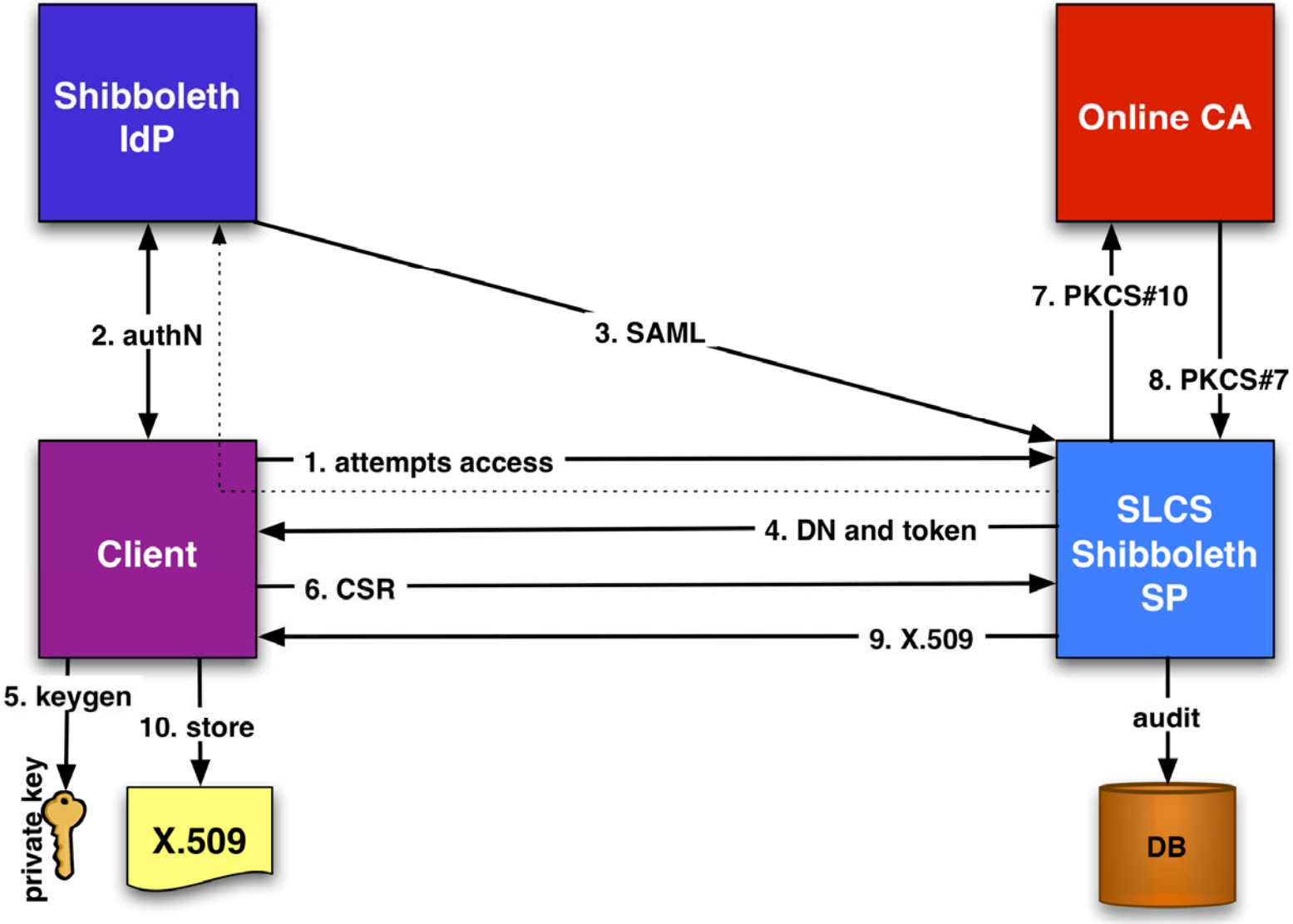
How SAML Credentials work



What is VOMS

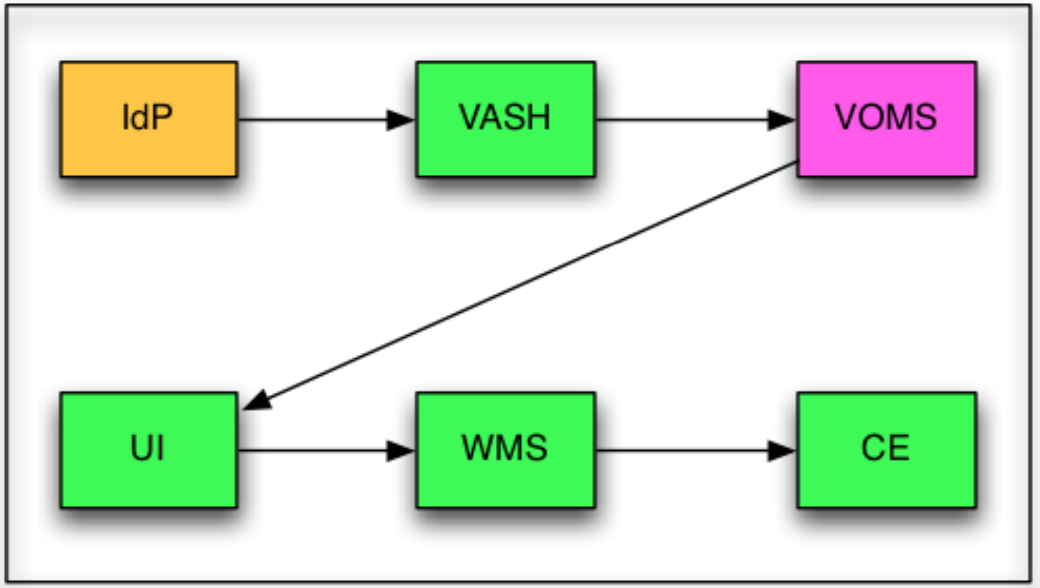
- **VOMS is a X509 Attribute Authority with special support for Grids and VOs**
- **VOMS is a Membership management tool**
- **VOMS is a SAML Attribute Authority**
- **VOMS integrates with Shibboleth**
  - In the sense that VOMS makes Shibboleth attributes available to Grid services
    - Or to X509 based services in general

SLCS (Certificates from Shibboleth)

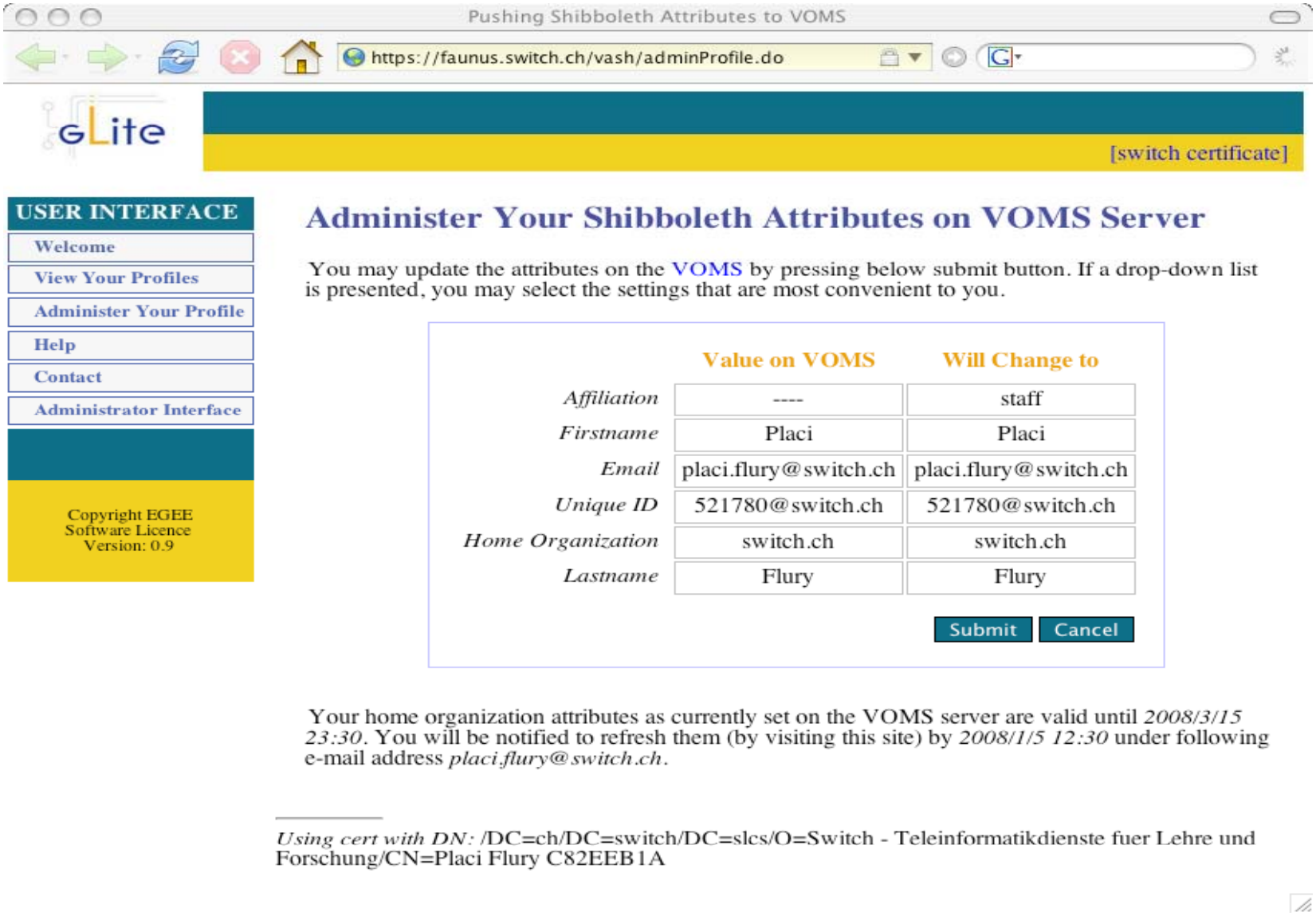


VASH

- **VOMS Attributes from Shibboleth (VASH)**
  - Collaboration between SWITCH and INFN



VASH UI


Pushing Shibboleth Attributes to VOMS
https://faunus.switch.ch/vash/adminProfile.do
gLite
[switch certificate]
USER INTERFACE
Welcome
View Your Profiles
Administer Your Profile
Help
Contact
Administrator Interface
Copyright EGEE
Software Licence
Version: 0.9
Administer Your Shibboleth Attributes on VOMS Server
You may update the attributes on the VOMS by pressing below submit button. If a drop-down list is presented, you may select the settings that are most convenient to you.
Value on VOMS
Will Change to
Affiliation
----
staff
Firstname
Placi
Placi
Email
placi.flury@switch.ch
placi.flury@switch.ch
Unique ID
521780@switch.ch
521780@switch.ch
Home Organization
switch.ch
switch.ch
Lastname
Flury
Flury
Submit
Cancel
Your home organization attributes as currently set on the VOMS server are valid until 2008/3/15 23:30. You will be notified to refresh them (by visiting this site) by 2008/1/5 12:30 under following e-mail address placi.flury@switch.ch.
Using cert with DN: /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A

Shib in VOMS - Full list

How to use the voms with Shibboleth Attributes

```
[flury@aurora flury]$ slcs-init -i switch.ch
Shibboleth Password:
New Key Password:
Key password is empty, using Shibboleth password.
[flury@aurora flury]$ voms-proxy-init -voms switch
Enter GRID pass phrase:
Your identity: /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
Creating temporary proxy ..................................................... Done
Contacting  egeria.switch.ch:15015 [/O=GRID-FR/C=CH/O=SWITCH/OU=MIDDLEWARE/CN=egeria.switch.ch] "switch" Done
Creating proxy ..................................... Done
Your proxy is valid until Fri Jun 15 05:17:32 2007
[flury@aurora flury]$ voms-proxy-info -all
subject   : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A/CN=proxy
issuer    : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
identity  : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u965
timeleft  : 11:59:46
=== VO switch extension information ===
VO        : switch
subject   : /DC=ch/DC=switch/DC=slcs/O=Switch - Teleinformatikdienste fuer Lehre und Forschung/CN=Placi Flury C82EEB1A
issuer    : /O=GRID-FR/C=CH/O=SWITCH/OU=MIDDLEWARE/CN=egeria.switch.ch
attribute : /switch/Role=NULL/Capability=NULL
attribute : urn:mace:switch.ch:attribute-def:swissEduPersonUniqueID = 521780@switch.ch (switch)
attribute : urn:mace:dir:attribute-def:sn = Flury (switch)
attribute : urn:mace:dir:attribute-def:givenName = Placi (switch)
attribute : urn:mace:dir:attribute-def:mail = placi.flury@switch.ch (switch)
attribute : urn:mace:dir:attribute-def:eduPersonAffiliation = staff (switch)
attribute : urn:mace:switch.ch:attribute-def:swissEduPersonHomeOrganization = switch.ch (switch)
timeleft  : 11:59:46
```

What is VOMS

- **VOMS is a X509 Attribute Authority with special support for Grids and VOs**
- **VOMS is a Membership management tool**
- **VOMS is a SAML Attribute Authority**
- **VOMS integrates with Shibboleth**
- **VOMS has native support for replication**
  - Only one server is a single point of failure

VOMS and Replication

- **A VOMS server is stateless.**
- **VOMS uses a DB to keep track of users and administrators.**

- **Replicating a VOMS is simple:**
  - Replicate the DB somewhere else
  - Run a new instance of VOMS insisting on the replicated DB

- **Support is native**
  - APIs allow to discover replicas
  - CLI tools switch between replicas automatically

VOMS Advanced features

- **Multiple Certificates**
  - A user may have more than one certificate
  - It is possible to register them as synonymous with each other

The Team

- Vincenzo Ciaschini
- Valerio Venturi
- Andrea Ceccanti

Questions?