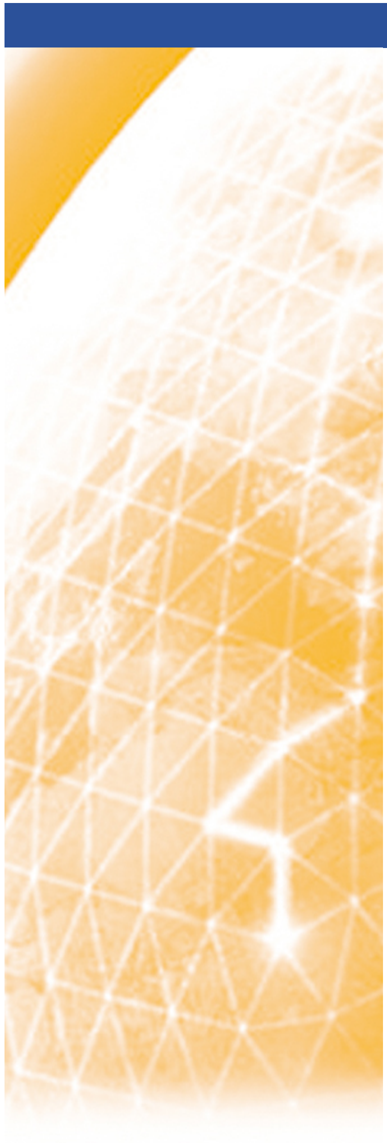


VOMS & MyProxy interaction

Emidio Giorgio

INFN

NA4 Generic Applications Meeting

10 January 2006

www.eu-egee.org

Overview

- Introduction to VOMS
  - Features
  - Groups & Roles
  - Advanced Usage
- Introduction to MyProxy
  - Features
  - Use
- Interaction of VOMS with MyProxy
  - Problems
  - Solution
  - Restrictions

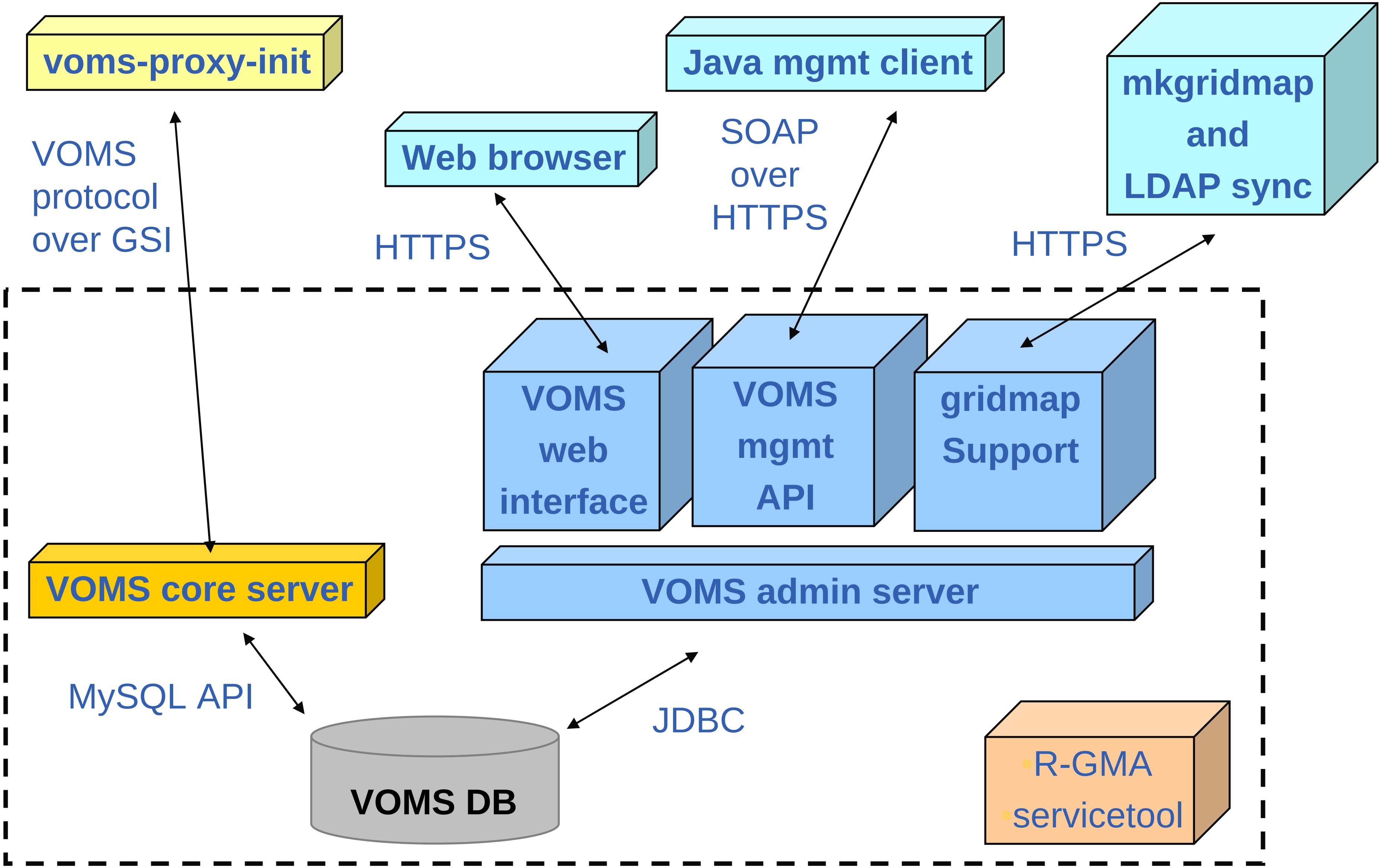
Introduction to VOMS

- Virtual Organization Membership Service (VOMS)
  - Account Database
    - Serving information in a special format (VOMS credentials)
    - Can be administered via command line & via web interface
  - Provides information on the user's relationship with his/her Virtual Organization (VO)
    - Membership
    - Group membership
    - Roles of user

Introduction to VOMS

- VOMS Features
  - Single login using (proxy-init) only at the beginning of a session
    - VOMS extesions are attached to user proxy
  - Expiration time
    - The authorization information is only valid for a limited period of the time as the proxy certificate itself
  - Multiple VO
    - User may log-in into multiple VOs and create an aggregate proxy certificate, which enables him/her to access resources in any one of them
  - Support for Group and Roles
    - Group membership is automatically inserted when requesting voms proxy
    - Role has to be requested explicitly
  - Backward compatibility
    - The extra VO related information is in the user's proxy certificate
    - User's proxy certificate can be still used with non VOMS-aware service
  - Security
    - All client-server communications are secured and authenticated

VOMS architecture



voms-proxy-init

VOMS protocol over GSI

Web browser

HTTPS

Java mgmt client

SOAP over HTTPS

mkgridmap and LDAP sync

HTTPS

VOMS web interface

VOMS mgmt API

gridmap Support

VOMS core server

VOMS admin server

MySQL API

VOMS DB

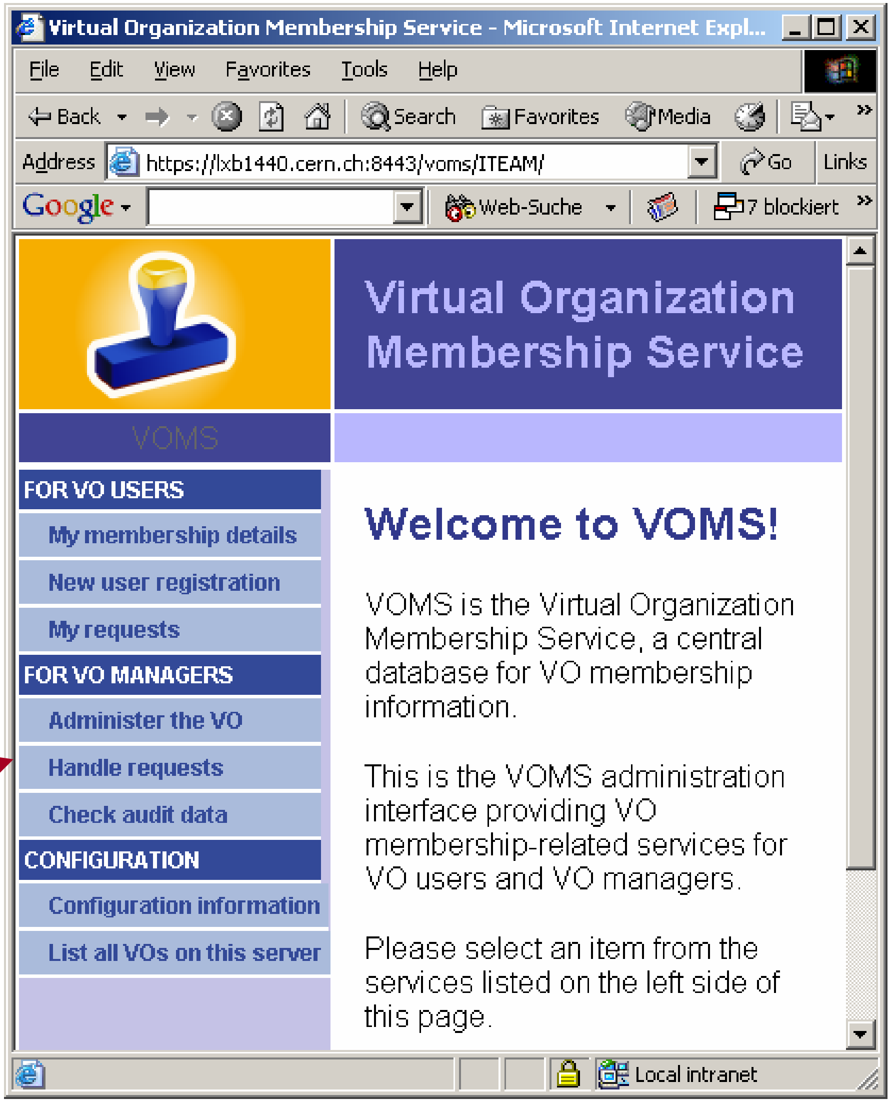
JDBC

- R-GMA
- servicetool

VOMS Web interface

- VO user can
  - Query membership details
  - Register himself in the VO
    - You will need a valid certificate
  - Track his requests

- VO manager can
  - Handle request from users
  - Administer the VO


Virtual Organization Membership Service - Microsoft Internet Expl...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://lxb1440.cern.ch:8443/voms/ITEAM/
Go Links
Google Web-Suche 7 blockiert
Local intranet

Virtual Organization Membership Service

VOMS

FOR VO USERS
- My membership details
- New user registration
- My requests

FOR VO MANAGERS
- Administer the VO
- Handle requests
- Check audit data

CONFIGURATION
- Configuration information
- List all VOs on this server

Welcome to VOMS!

VOMS is the Virtual Organization Membership Service, a central database for VO membership information.

This is the VOMS administration interface providing VO membership-related services for VO users and VO managers.

Please select an item from the services listed on the left side of this page.

Groups

- The number of users of a VO can be very high:
  - E.g. the experiment ATLAS has 2000 member

- Make VO manageable by organizing users in groups:

  Examples:
  - VO GILDA
    - Group Catania
      - *INFN*
        - Group Barbera
      - *University*
    - Group Padua
  - VO GILDA
    - /GILDA/TUTORS `can write to normal storage`
    - /GILDA/STUDENT `only write to volatile space`

- Groups can have a hierarchical structure, undefinitely deep

Roles

- **Roles are specific roles a user has and that distinguishes him from others in his group:**
  - Software manager
  - VO-Administrator

- **Difference between roles and groups:**
  - Roles have no hierarchical structure – there is no sub-role
  - Roles are not used in ‘normal operation’
    - They are not added to the proxy by default when running *voms-proxy-init*
    - But they can be added to the proxy for special purposes when running *voms-proxy-init*

- **Example:**
  - User Emidio has the following membership
    - VO=gilda, Group=tutors, Role=SoftwareManager
  - During normal operation the role is not taken into account, e.g. Emidio can work as a normal user
  - For special things he can obtain the role “Software Manager”

Requesting group/role membership

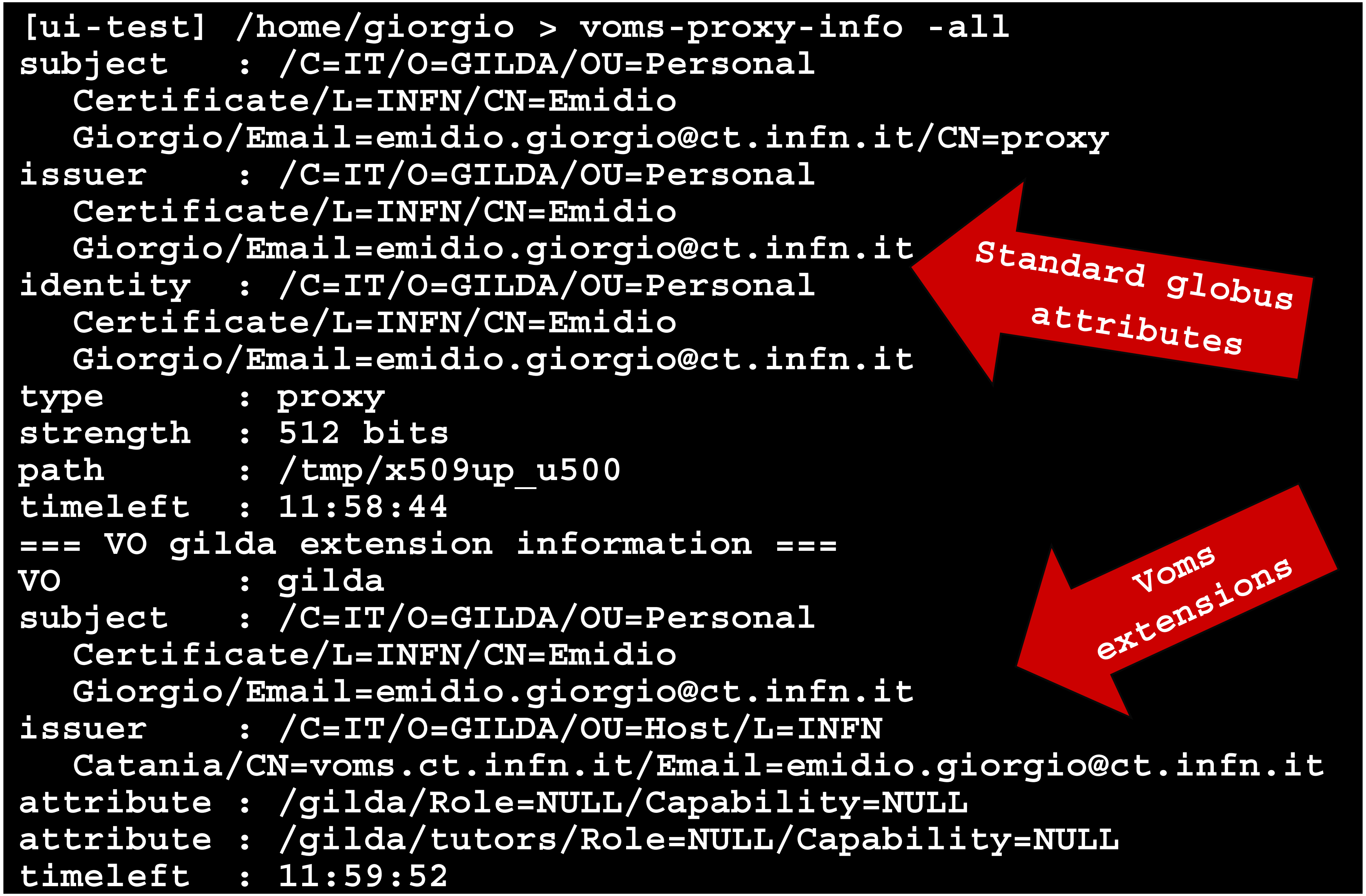
- Any group membership is automatically added when performing `voms-proxy-init`
- Default group is /<`vo-name`>, if not differently specified it's the 1st group inserted in attributes.
- All groups in which
- User can specify a different order for groups

```
voms-proxy-init –voms gilda:/gilda/tutors
```

- Role membership has to be requested explicitly

```
voms-proxy-init --voms gilda:/Role=Vo-Admin
```

voms extensions in proxy



```
[ui-test] /home/giorgio > 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_u500
timeleft  : 11:58:44
=== VO gilda extension information ===
VO        : gilda
subject   : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
issuer    : /C=IT/O=GILDA/OU=Host/L=INFN
   Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it
attribute : /gilda/Role=NULL/Capability=NULL
attribute : /gilda/tutors/Role=NULL/Capability=NULL
timeleft  : 11:59:52
```

Standard globus attributes

Voms extensions

Groups / Role mapping on resources

- gLite services offers native support to Group / Role
- Grouping can also be performed acting on gridmap file configuration

```
group vomss://voms.ct.infn.it:8443 /voms/gilda?/gilda .gilda
group vomss://voms.ct.infn.it:8443 /voms/gilda?/gilda/\
Role=SoftwareManager  gildasgm
```

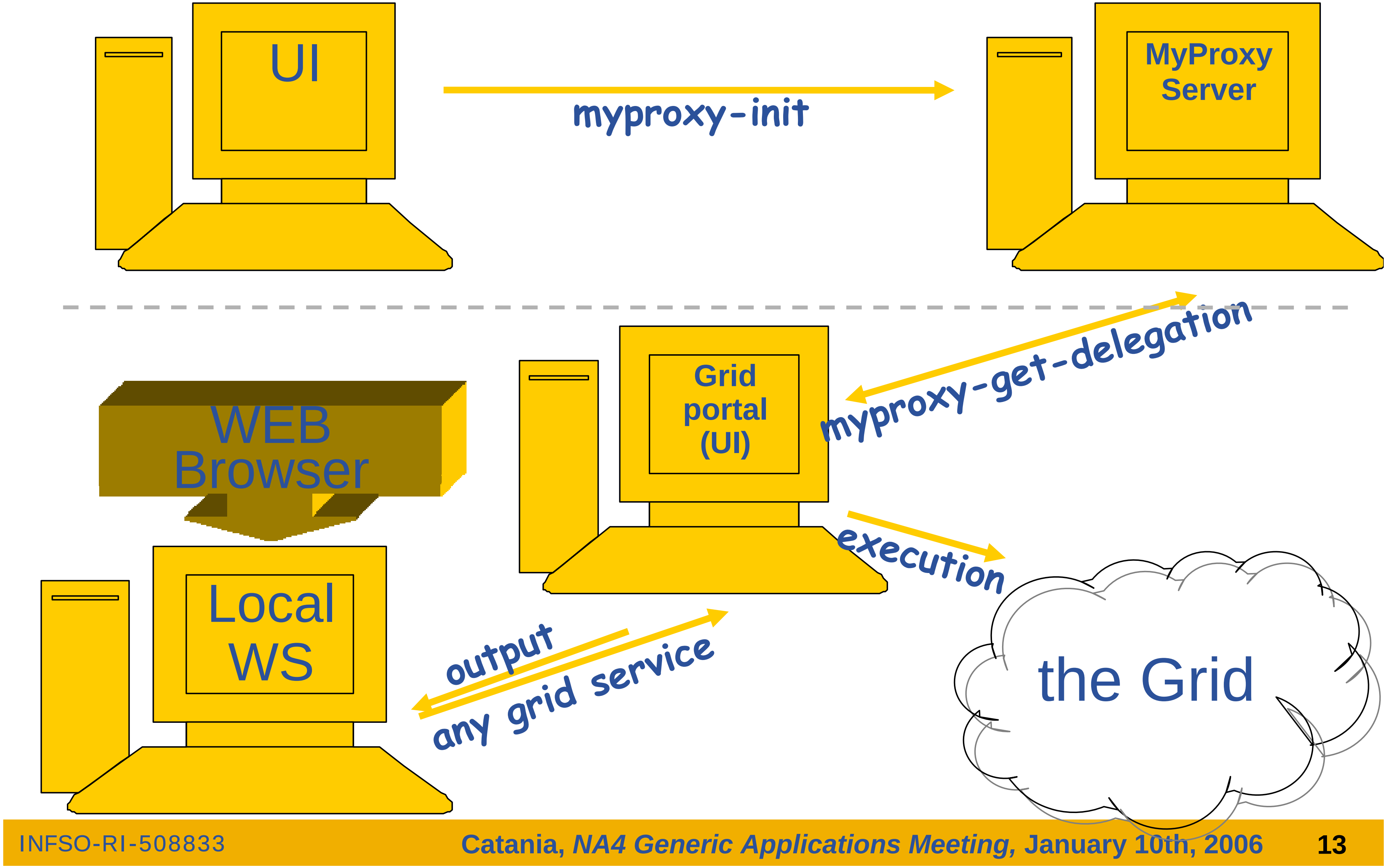
On glite-mkgridmap.conf

- `.gilda` is the prefix of (local) set of pool users where normally memberes of VO gilda are mapped to
- `gildasgm` is a (local) privileged user, for example it could have the rights to install software under a dedicated directory

Long term proxy

- **Proxy has limited lifetime (default is 12 h)**
  - Bad idea to have longer proxy
- **However, a grid task might need to use a proxy for a much longer time**
  - Grid jobs in HEP Data Challenges on LCG last up to 2 days
- **myproxy server:**
  - Allows to create and store a long term proxy certificate:
  - myproxy-init -s <host_name>
    - -s: <host_name> specifies the hostname of the myproxy server
  - myproxy-info
    - Get information about stored long living proxy
  - myproxy-get-delegation
    - Get a new proxy from the MyProxy server
  - myproxy-destroy
  - Chech out the myproxy-xxx - - help option
- **A dedicated service on the RB can renew automatically the proxy**
- **File transfer services in gLite validates user request and eventually renew proxies**
  - contacting myproxy server

Grid authentication with MyProxy



VOMS and MyProxy

- **Problem :** MyProxy support natively just plain proxies**,** **without** voms extension
- User can just store plain proxies on MyProxy servers
- For WMS issues it's faced by **ProxyRenewal**
- For remote authentication purposes there are two approaches
  1. **Retrieve from server a proxy-delegation, using it to sign the request for a voms-proxy**
  2. **Store on the server proxies with voms extension**
- With **1. ,** length of certificates chain on proxy is very long (5 cert nested !), and will likely produce authentication errors

Storing long lived voms proxies

- To allow storing of voms ext., myproxy client has been modified,
- The faculty of choosing the VO and group/roles has been added, while the previous options have all been kept

```
myproxy-init --voms gilda:/Role=VO-Admin
```

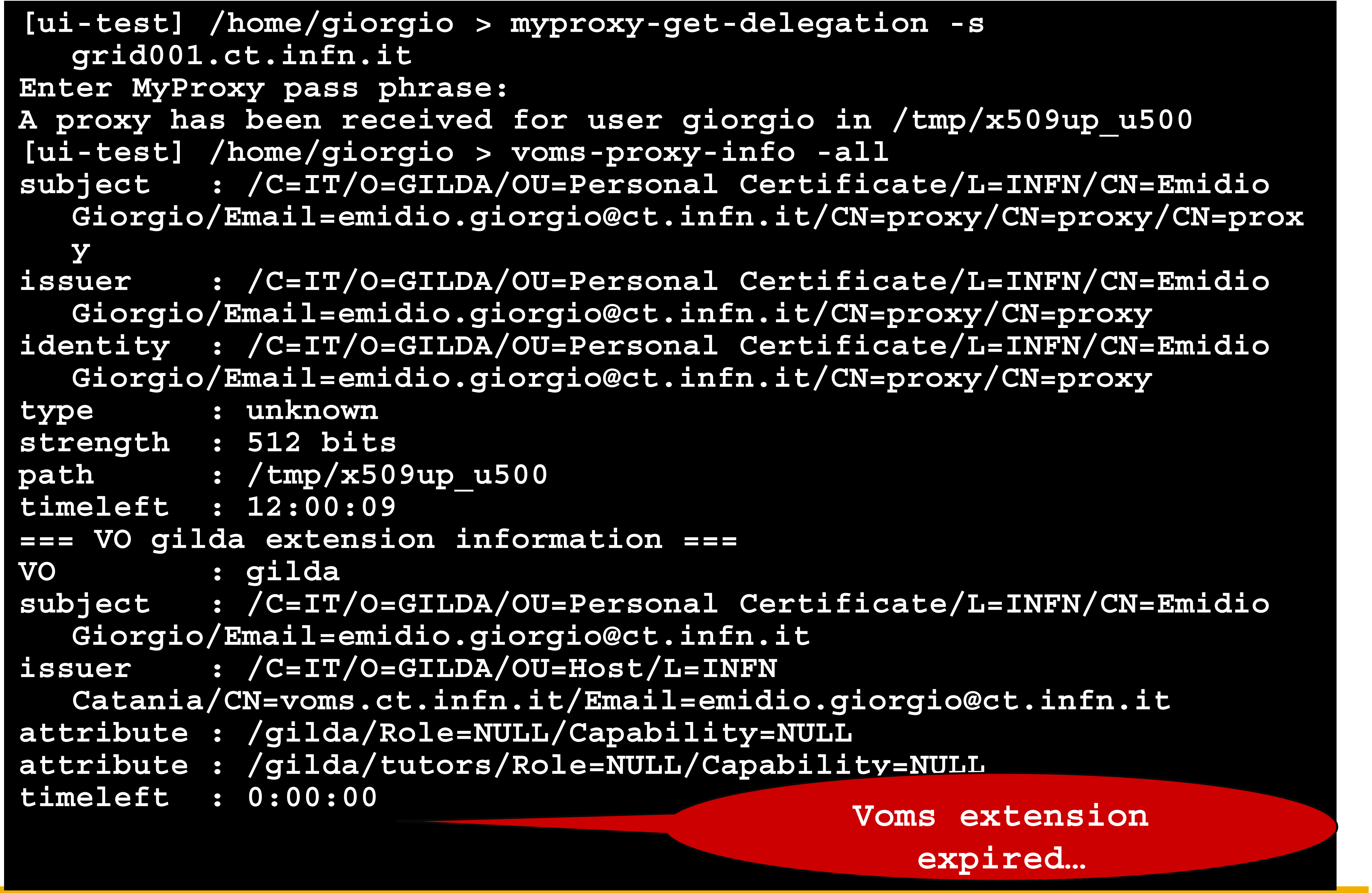
- Proxies then retrieved with `myproxy-get-delegation`

  will have the requested voms extension but…
- There's a limitation, due to voms extensions lifetime: tipically it's limited, and they are not renewed when performing `myproxy-get-delegation`

Studying solutions to extend renew of voms extension in delegation

- The "modified" is available on all of GILDA UI's
- Will be largely deployed when the above issues will be solved

voms extension on a delegated proxy



```
[ui-test] /home/giorgio > myproxy-get-delegation -s
   grid001.ct.infn.it
Enter MyProxy pass phrase:
A proxy has been received for user giorgio in /tmp/x509up_u500
[ui-test] /home/giorgio > 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/CN=proxy/CN=prox
   y
issuer    : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=proxy
identity  : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=proxy
type      : unknown
strength  : 512 bits
path      : /tmp/x509up_u500
timeleft  : 12:00:09
=== VO gilda extension information ===
VO        : gilda
subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
issuer    : /C=IT/O=GILDA/OU=Host/L=INFN
   Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it
attribute : /gilda/Role=NULL/Capability=NULL
attribute : /gilda/tutors/Role=NULL/Capability=NULL
timeleft  : 0:00:00
```

Voms extension expired…

References

- **VOMS suite : user and installation guide**
  - http://infnforge.cnaf.infn.it/voms/software.pdf
- **MyProxy user's guide**
  - http://grid.ncsa.uiuc.edu/myproxy/credmgmt.html
- **VOMS with MyProxy, how to**
  - http://egee-na4.ct.infn.it/genapps/wiki/index.php/VomsMyProxy

Questions…

?