



Enabling Grids for E-scienceE

# GILDA Practicals : Security systems

## GILDA Tutors

*Bari, BIOINFOGRID Initial training course*

*8-10 March 2006*

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



Information Society



# How access the Gilda User Interface

**Login :** **bariXX@glite-tutor.ct.infn.it**  
where **XX=01,..40**

**Passwd :** **GridBARXX XX=01,..,40**

**PEM PASSPHRASE : BARI**



Enabling Grids for E-scienceE

# Practicals on VOMS and MyProxy

*Diego Scardaci*

*INFN*

*Bari, BIOINFOGRID Initial training course*

*8-10 March 2006*

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



Information Society



- **VOMS proxy usage**
- **MyProxy Usage**

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

```
[glite-tutor] /home/giorgio > ls -l .globus
total 8
-rw-r--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**
  - `userkey.pem` contains your private key, and must be readable just by yourself (400)
  - `usercert.pem` contains your public key, which should be readable also from outside (644)

- **Main options**

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

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

```
voms-proxy-init --voms gilda:/gilda/Role=VO-Admin
voms-proxy-init --voms gilda:/gilda/generic-users
```

-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 \$HOME/.glite/vomses.

**Syntax** : "vo-nickname" "voms server FQDN" "port" "voms server \ certificate subject" "vo name"

Parameters for vomses are usually provided by VOs manager

**Exercise 1** : **create** a voms proxy requesting your group membership (all of you belong to `generic-users` group); **then** verify obtained credentials with

```
voms-proxy-info
```

- **voms-proxy-info**
  - Main options :
    - all** prints all proxy options
    - file** specifies a different location of proxy file

```

/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_u513
timeleft    : 11:59:52
=== 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/tutors/Role=NULL/Capability=NULL
attribute   : /gilda/Role=NULL/Capability=NULL
timeleft    : 11:59:45
    
```

Standard globus attributes

Voms extensions

- **myproxy server:**
  - myproxy-init
    - Allows to create and store a long term proxy certificate:
  - myproxy-info
    - Get information about stored long living proxy
  - myproxy-get-delegation
    - Get a new proxy from the MyProxy server
  - myproxy-destroy
  - Check out them with myproxy-xxx --help option
- **A dedicated service on the RB can renew automatically the proxy**
  - contacting the myproxy server

```
[giorgio@glite-tutor:~]$ myproxy-init -s grid001.ct.infn.it
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:
Creating proxy .....
Done
Proxy Verify OK
Your proxy is valid until: Sun Jun 19 21:18:27 2005
Enter MyProxy pass phrase:
Verifying password - Enter MyProxy pass phrase:
A proxy valid for 168 hours (7.0 days) for user giorgio now exists
on grid001.ct.infn.it.
```

- **Principal options**
- **-c** hours specifies lifetime of stored credentials
- **-t** hours specifies the maximum lifetime of credentials when retrieved
- **-s** <hostname> specifies the myproxy server where to store credentials
- **-d** stores credential with the distinguished name in proxy, instead of user name (mandatory for some data management services and proxy renewal)
- For proxy renewal it's also mandatory **-n** (no passphrase). You've to specify also subject of principals that can renew a delegation (**-R** subject, or **-A** for any principal)

- Useful to retrieve info on stored credentials
- Need local credentials to be performed
- If credentials have been initialized with `-d` switch, you have also to specify it there

```
[giorgio@glite-tutor:~]$ myproxy-info -s grid001.ct.infn.it
username: giorgio
owner: /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
Giorgio/Email=emidio.giorgio@ct.infn.it
timeleft: 167:55:34 (7.0 days)
```

- This command is used to retrieve a delegation from a long lived proxy stored on myproxy server
- It is independent by the machine ! You don't need to have your certificate on board
- If credentials have been initialized with `-d` switch, you have to specify it also in myproxy-get-delegation request

```
[giorgio@glite-tutor:~]$ myproxy-get-delegation \
-s grid001.ct.infn.it
Enter MyProxy pass phrase:
A proxy has been received for user giorgio in /tmp/x509up_u513
```

- Delete, if existing, the long lived credentials on the specified myproxy server

```
[glite-tutor] /home/giorgio > myproxy-destroy \  
-s grid001.ct.infn.it
```

```
Default MyProxy credential for user giorgio was successfully  
removed.
```

- **Exercise 2**
  - Create a myproxy on the server `grid001.ct.infn.it`
  - Visualize information on that
  - Create a myproxy with `-d` option
  - Which differences you note ?
  - Destroy both

- myproxy doesn't support natively VOMS
- To allow storing of voms ext., myproxy client has been modified,
- The faculty of choosing VO and group/roles has been added, while the previous options have all been kept

```
myproxy-init --voms gilda
```

- Proxies then retrieved with `myproxy-get-delegation` will have the requested voms extension but...
- There's a limitation, due to voms extensions lifetime: typically it's limited, and it's not renewed when performing `myproxy-get-delegation`



Studying solutions to extend voms extension renew in get-delegation

- The “modified” client is available only on GILDA UI's
- Will be largely deployed when the above issues will be solved

```
[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    : 23:59:57
```

Voms extension  
lifetime



# THE END