

8 - Digital Personal Certificates and Proxies management



Requesting a digital personal certificate (INFN users only)

Using Tier1 computing and storage resources by means of the Grid tools requires a personal (digital) X509 certificate, which is not needed when using resources locally. A personal certificate can be obtained following these instructions [11]:

- Go to your own Web Browser and open the URL <https://cert-manager.com/customer/GARR/idp/clientgeant>.
- Choose your institution (i.e. INFN)


Choose Your Institution

Recent institutions


 **INFN - National Institute for Nuclear Physics** 
inf.n.it

[+ Add another institution](#) [Edit](#)


- log in IdP of AAI



IT | EN



Username o e-mail



Password

ACCEDI

REGISTRATI

[Cambio o Rigenerazione Password - Recupero Username](#)

- You will be faced with a screen of this type:



Digital Certificate Enrollment

This is your certificate enrollment form. Once you submit, your certificate will be generated and downloaded to your computer.

Name Vincenzo Rega
Organization Istituto Nazionale di Fisica Nucleare - INFN
Email vincenzo.rega@cnaif.infn.it

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*

- The own email address attribute is automatically inherited from the IdP INFN.
- Choose your certificate profile
- Select **GEANT Personal Authentication**, which provides a grid certificate

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*

GEANT Personal Authentication



Personal GRID

GEANT Personal Automated Authentication

GEANT Personal email signing and encryption

Personal GRID certificate with default term for 395 days

Select your Certificate Profile to enable your enrollment options.

Certificate Profile*

GEANT Personal Authentication



Personal Authentication Certificate - provides client authentication, enables you to authenticate you to e-Infrastructure services.

Term*

395 days

- Select RSA as private key (Generate RSA)

Enrollment Method

- ☒ Key Generation
- ☐ CSR

Key Type*
RSA - 2048

Password is required to unlock the certificate file download to protect private key.

Password*



Password Confirmation*



- Choose **secure** key protection algorithm , read and agree term and conditions

Choose key protection algorithm.

Algorithm
Secure AES256-SHA256

☒ [I have read and agree to the terms of the EULA](#)

- Waiting for generating certificate



Generating Certificate

This may take a few moments.

Once your Certificate is generated you will be redirected to a page where it will be automatically downloaded.

Do not close this tab or your browser.

- Insert the password to generate and download the certificate.



Digital Certificate Enrollment



Your certificate has been successfully generated.

- Then import the certificate in your own browser and check it in the user certificate manager of your browser

Certificate Installation on a user interface

Once obtained the pk12 certificate (certs.p12), it is necessary to split it in public and private keys and put them in the `.g1obus/` folder in side your home directory in the UI.

Commands to be issued:

```
$ cd $HOME
$ mkdir .globus
$ cd .globus
$ openssl pkcs12 -clcerts -nokeys -in certs.pl2 -out usercert.pem
$ openssl pkcs12 -nocerts -in certs.pl2 -out userkey.pem
$ chmod 600 usercert.pem
$ chmod 400 userkey.pem
```

The files must have the following permissions:

```
-rw----- 1 arendina user-support 3257 Jul 1 17:02 usercert.pem
-r----- 1 arendina user-support 2661 Jul 1 17:03 userkey.pem
```

Interacting with the VOMS server

To transfer files or submit jobs using VO-based authentication (need registration on an experiment VOMS server), first the user have to generate a proxy with VOMS extensions using the command:

```
$ voms-proxy-init --voms <vo name>
```

To check the proxy:

```
$ voms-proxy-info --all
```

The output should be something like:

```
subject : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.it/CN=1964287159
issuer  : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.it
identity : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.it
type    : RFC3820 compliant impersonation proxy
strength : 1024
path    : /tmp/x509up_u10162
timeleft : 11:47:50
key usage : Digital Signature, Key Encipherment
=== VO juno extension information ===
VO      : juno
subject : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.it
issuer  : /C=CN/O=HEP/OU=CC/O=IHEP/CN=voms.ihep.ac.cn
attribute : /juno/Role=NULL/Capability=NULL
timeleft : 11:47:50
uri     : voms.ihep.ac.cn:15008
```

If the "VO extension information" is not present or any of the timeleft field is zero, the proxy has no VOMS extensions and it has to be regenerated.

Long lived proxies: manual proxy extension

Proxies created as described above naturally pose a problem: if a job does not finish before the expiration time of the proxy, it is aborted. The easiest solution to the problem would be to use very long-lived proxies, but at the expense of an increased security risk.

Also, the duration of a VOMS proxy is limited by the VOMS server and cannot be made arbitrarily long.

To overcome this limitation, a proxy credential repository system is used, which allows the user to create and store a long-term proxy in a dedicated server (a "MyProxy" server).

The maximum lifetime of long-lived proxy on a MyProxy server is (by default) one week, and it can be prolonged with 48 hour steps, to achieve this it's necessary, after using:

```
myproxy-init --voms virgo:/virgo/virgo -s myproxy.cnaf.infn.it -d
```

the user will be asked to set a password for the token retrieval.

To recreate the proxy before expiration:

```
myproxy-logon --proxy_lifetime 48 -d -S < password
```

Where "password" is the text file with the MyProxy passphrase.

Please note that the proxy is regenerated locally, all this procedure does not affect all the delegated proxies created by services eventually accessed by the user with the expired proxy, i.e. CEs, FTS, etc.. To renew the delegated proxies the user should consult the documentation of the accessed services.

Since the maximum lifetime is one week, `myproxy-init` needs to be issued at least once a week.

A full set of commands can be found here:

```
-bash-4.2$ voms-proxy-destroy
-bash-4.2$ voms-proxy-info --all
Proxy not found: /tmp/x509up_u10162 (No such file or directory)
-bash-4.2$ myproxy-init -t 200 --voms virgo:/virgo/virgo -s myproxy.cnaf.infn.it -d
Enter GRID pass phrase for this identity:
Contacting voms-01.pd.infn.it:15009 [/DC=org/DC=terena/DC=tcs/C=IT/L=Frascati/O=Istituto Nazionale di Fisica
Nucleare/CN=voms-01.pd.infn.it] "virgo"...
Remote VOMS server contacted succesfully.

voms-01.pd.infn.it:15009: The validity of this VOMS AC in your proxy is shortened to 518400 seconds!

Created proxy in /tmp/myproxy-proxy.10162.8697.

Your proxy is valid until Thu Aug 06 10:44:38 CEST 2020
Enter MyProxy pass phrase:
Verifying - Enter MyProxy pass phrase:
A proxy valid for 168 hours (7.0 days) for user /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica
Nucleare/CN=Andrea Rendina arendina@infn.it now exists on myproxy.cnaf.infn.it.
-bash-4.2$ myproxy-logon --proxy_lifetime 48 -d -S < pass
A credential has been received for user /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare
/CN=Andrea Rendina arendina@infn.it in /tmp/x509up_u10162.
-bash-4.2$ voms-proxy-info --all
subject : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.
it/CN=1158094269/CN=1184384110/CN=1415320726
issuer : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.
it/CN=1158094269/CN=1184384110
identity : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina
arendina@infn.it
type : RFC3820 compliant impersonation proxy
strength : 2048
path : /tmp/x509up_u10162
timeleft : 47:59:51
key usage : Digital Signature, Key Encipherment
=== VO virgo extension information ===
VO : virgo
subject : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Andrea Rendina arendina@infn.
it
issuer : /DC=org/DC=terena/DC=tcs/C=IT/L=Frascati/O=Istituto Nazionale di Fisica Nucleare/CN=voms-01.pd.infn.it
attribute : /virgo/virgo/Role=NULL/Capability=NULL
attribute : /virgo/Role=NULL/Capability=NULL
timeleft : 143:59:20
uri : voms-01.pd.infn.it:15009
```

