

# ca.html

## *E-grid live-CD*

# Certification Authorities

## Install your certificate on the UI

Log in into the UserInterface, copy there the file you exported, and create a directory where your certificate + private key will be stored:

```
mkdir ~/.globus
```

It is likely that you have got from the browser a PKCS12 file (\*.p12). Unfortunately this format is not accepted by Globus security infrastructure, but you can easily convert it into the supported standard (PEM). This operation will split your \*.p12 file in two files: the certificate (usercert.pem) and the private key (userkey.pem). The conversion can be performed with openssl tool:

```
openssl pkcs12 -nocerts -in mycert.p12 -out ~/.globus/userkey.pem
openssl pkcs12 -clcerts -nokeys -in mycert.p12 -out ~/.globus/usercert.pem
chmod 0400 ~/.globus/userkey.pem
chmod 0600 ~/.globus/usercert.pem
```

Of course replace mycert.p12 with the right filename. At end you should have something like:

```
[localuser@userinterface .globus]$ pwd
/home/localuser/.globus
[localuser@userinterface .globus]$ ll total 8
-rw----- 1 localuser localuser 2008 Nov 13 16:50 usercert.pem
-r----- 1 localuser localuser 963 Nov 13 16:50 userkey.pem
```

If you received the files usercert.pem and userkey.pem directly from CA, then copy these files into directory

/.globus. Remember, you should check the permissions of these files.

Permissions are vital not only for security: `grid-proxy-init` command will fail if your private key is not protected as listed.

More information about how to create your own certificate, please go to:  
<http://sial.org/howto/openssl/ca/>

Some related sites:

<http://grid-it.cnaf.infn.it/>

<http://www.egrid.it/gridats/tutorial>

## Host Certificates

CE, LFC, MON, PROXY, RB, SE and VOBOX nodes require the host certificate/key files before you start their installation.

Contact your national Certification Authority (CA) to understand how to obtain a host certificate if you do not have one already.

Instruction to obtain a CA list can be found in:

<http://grid-deployment.web.cern.ch/grid-deployment/lcg2CAlist.html>

From the CA list so obtained you should choose a CA close to you.

Once you have obtained a valid certificate, i.e. a file

\* `hostcert.pem`

containing the machine public key and a file

\* `hostkey.pem`

containing the machine private key

Make sure that you have a root privileges and place the two files in the target node into the directory `/etc/grid-security`, later check the access right `hostkey.pem` only readable by root and the certificate readable by everybody.

# CA Certificates

The public key of the Certification Authority (CA) used to sign the certificates for both the hosts and the users must be available on each grid node. The default path for the public key is `/etc/grid-security/certificates/`. All the Certification Authority certificates involved in the grid which you are using MUST be present on each grid node. The default CA certificates path is `/etc/grid-security/certificate`

## More Information

<http://grid.infn.it/fileadmin/users/certmgr/certmgr.html>

Section "Certificates, Accounts, Proxy and Renewal" at <http://www.bo.infn.it/alice/introgrid/edg2/node3.html>