Installing Certificates Tutorial

NGS Induction Event, Guy Warner, NeSC Training Team

This tutorial will take you through the stages needed to convert your certificate from the format it is sent from the UK CA into the format needed to run your first job on the NGS. All of the commands in this tutorial should be run on the server training-ui.nesc.ed.ac.uk which may be connected to using the "Putty" ssh client which may be found from the "Start Menu" under "All Programs" then "CC Open Access Labs Menu", "Network" and finally "Putty Access to UNIX " (enable X11 forwarding).

Note: text in marked in **`bold red`** represents commands to be typed whilst text between < and > should be replaced as appropriate.

1. Ensure you are at the top level of your account

   ```
   cd
   ```

2. Next you need to create and change to the default directory that Globus commands expect to find your certificate in.

   ```
   mkdir .globus
   cd .globus
   ```

3. The next stage is to generate your private key from your certificate.

   ```
   openssl pkcs12 -nocerts -in ~/nescuserXX.pfx -out userkey.pem
   ```

   where the ***XX should be replaced with the number in your user name***. You will firstly be asked to enter the Import Password. This is the password that has been used to protect your Certificate. When you are first sent your Certificate it will be stored in your web browser. You have to then export the Certificate to a file and you will prompted to protect the Certificate with a password. This is the password that the openssl command refers to as the Import Password. For this tutorial this stage has already been done for you. After that you will be asked to enter (and verify) a new PEM Password. This is the password that will be used to protect your private key. Your private key is stored in the file userkey.pem. This is the file name expected by Globus commands.
4. Now we generate your public key from your certificate.

   ```
   openssl pkcs12 -clcerts -nokeys -in ~/nescuserXX.pfx -out
   usercert.pem
   ```

   Again you are asked for the password used to protect your Certificate. Note that this time you are not asked for a passphrase to protect the resulting file. This is because your public key needs to be readable by anyone or any service needing to verify/decrypt data sent by you and signed with your private key.
5. It is now necessary to set the permissions on the files to set their correct levels of access. Important - This is the most likely source of errors with authentication not working. If you have problems with authentication this is the first place you should look. Your private key must be only readable by you and for extra safety it should not be writable by you. If when you are later using a full UK non-

training Certificate you have reason to believe anyone other than yourself has seen this file then you must report it immediately to the UK CA. This will allow the certificate to be revoked (the process of making the certificate unusable) and a new certificate issued.

```
chmod 400 userkey.pem
```

Your public key as already stated needs to be world readable and so a more open set of permissions may be used.

```
chmod 644 usercert.pem
```

6. At this it is worth just inspecting what your public key contains.

   ```
   grid-cert-info
   ```

   Note in particular that the certificate contains who issued it and when it is valid for as well as the Distinguished Name (DN) of the person the certificate was issued for (the Subject). This command only accesses your public key.
7. The final stage is to test that you have installed your certificates correctly. This is best done by creating a grid proxy.

   ```
   grid-proxy-init
   ```

   The password you are asked for is the password you created in Step 3 (in openssl terminology your PEM passphrase). If all has gone well you will see a message about creating a proxy. This proxy will by default be valid for 12 hours, it is not recommended that you would ever need to change this. This proxy is storred in a file under the /tmp folder and is therefore independent of your current session.
8. It is possible to inspect the details of your current proxy.

   ```
   grid-proxy-info
   ```

   Note in particular the issuer. Compare this to the issuer of your certificate you saw in step 6.
9. To finish the tutorial explicitly destroy your proxy.

   ```
   grid-proxy-destroy
   ```

   You can check that your proxy has been destroyed by running the grid-proxy-info command again.

For comparison a run-through of the commands is shown below.

```
[gcw@lab-07 gcw]$ cd
[gcw@lab-07 gcw]$ mkdir .globus
[gcw@lab-07 gcw]$ ls
UK_CERT.pfx
[gcw@lab-07 gcw]$ ls -l
total 4
-rw-r--r-- 1 gcw users 2590 Feb 11 16:47 UK_CERT.pfx
[gcw@lab-07 gcw]$ cd .globus
[gcw@lab-07 .globus]$ ls
[gcw@lab-07 .globus]$ openssl pkcs12 -nocerts -in ~/UK_CERT.pfx -out userkey.pem
Enter Import Password:
MAC verified OK
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
[gcw@lab-07 .globus]$ openssl pkcs12 -clcerts -nokeys -in ~/UK_CERT.pfx -out usercert.pem
Enter Import Password:
MAC verified OK
```

```
[gcw@lab-07 .globus]$ chmod 400 userkey.pem
[gcw@lab-07 .globus]$ chmod 644 usercert.pem
[gcw@lab-07 .globus]$ ls -l
total 8
-rw-r--r-- 1 gcw users 2026 Feb 17 11:04 usercert.pem
-r-------- 1 gcw users 1202 Feb 17 10:53 userkey.pem
[gcw@lab-07 .globus]$ grid-cert-info
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 3451 (0xd7b)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=UK, O=eScience, OU=Authority, CN=CA/Email=ca-operator@grid-support.ac.uk
Validity
Not Before: Feb 11 16:28:21 2005 GMT
Not After : Feb 11 16:28:21 2006 GMT
Subject: C=UK, O=eScience, OU=Edinburgh, L=NeSC, CN=guy warner
Subject Public Key Info:
.....
[gcw@lab-07 .globus]$ grid-proxy-init
Your identity: /C=UK/O=eScience/OU=Edinburgh/L=NeSC/CN=guy warner
Enter GRID pass phrase for this identity:
Creating proxy ........................................................................ Done
Your proxy is valid until: Thu Feb 17 23:52:20 2005
[gcw@lab-07 .globus]$ grid-proxy-info
subject : /C=UK/O=eScience/OU=Edinburgh/L=NeSC/CN=guy warner/CN=proxy
issuer : /C=UK/O=eScience/OU=Edinburgh/L=NeSC/CN=guy warner
identity : /C=UK/O=eScience/OU=Edinburgh/L=NeSC/CN=guy warner
type : full legacy globus proxy
strength : 512 bits
path : /tmp/x509up_u501
timeleft : 11:51:22
[gcw@lab-07 .globus]$ grid-proxy-destroy
[gcw@lab-07 .globus]$ grid-proxy-info


ERROR: Couldn't find a valid proxy.
Use -debug for further information.
```