

Manipulating certificates and proxies

D. Weissenbach

- CA certificates: located in `$X509_CERT_DIR`, defaults to `/etc/grid-security/certificates`. Uses following naming conventions:
 - file name without extension: Hash of CA's name (DN)
 - f.0: CA certificate;
 - f.crl_url: URL to get the CA's CRL;
 - f.r0: last CRL.
- VOMS server certificates: located in `$X509_VOMS_DIR`, defaults to `/etc/grid-security/vomsdir`;
- User certificate:
 - In web browser (*mozilla: Edit* → *Preferences*, then *Privacy&Security* → *Certificates* → Manage Certificates...)
 - On the UI. Default location in `$HOME/.globus`

```
ls -l $HOME/.globus
-rw----- 1 esrsgm esr 5930 Jan  4 2008 cert.p12
-rw-r--r-- 1 esrsgm esr 1941 Jan  4 2008 usercert.pem
-rw----- 1 esrsgm esr 1916 Jan  4 2008 userkey.pem
```

Info about (display) a certificate:

```
grid-cert-info [-file cert.pem]
```

Exporting a certificate from web browser (*mozilla*):

Manage Certificates... → *select cert.* → Backup

Will ask for filename & "Backup Password".

Watch file mode!!

Converting a certificate:

```
openssl pkcs12 -in cert.p12 -nokeys -clcerts \  
    -out usercert.pem    Will ask for "Import Password"  
openssl pkcs12 -in cert.p12 -nocerts -out userkey.pem  
Will ask for "Import Password", then key (GRID) pass phrase (twice).
```

Watch file mode for private key!!

Proxy creation (asks for private key (GRID) pass phrase):

```
voms-proxy-init --voms vo_alias
voms-proxy-init \
  --voms alias[:/vo_fullname/group/[Role=Master]]
  [-out filename] # better use $X509_USER_PROXY
  [--valid HH:MM] [--pwstdin < pass_file]
```

Default proxy location: /tmp/x509up_u\$(id -u)

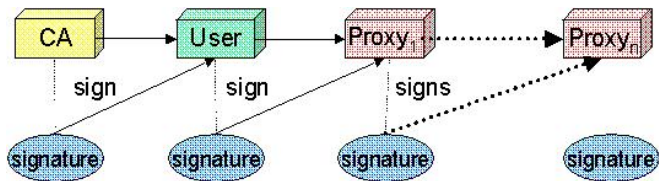
Proxy file mode is and must always remain 0600.

Must have access to voms server certificate (see Slide 1)

Configuration file: vo_name-server_name in
 \$GLITE_LOCATION/etc/vomses or \$HOME/.vomses,
 or file as --vomses option to voms-proxy-init

```
$ cat /opt/glite/etc/vomses/astro.vo.eu-egee.org-grid12.lal.in2p3.fr
"astro" "grid12.lal.in2p3.fr" "20012" \
"/O=GRID-FR/C=FR/O=CNRS/OU=LAL/CN=grid12.lal.in2p3.fr" "astro.vo.eu-egee.org"
```

Proxy contents: `voms-proxy-info -all [-file pxfile]`



- A proxy is a complete certificate (public + unencrypted private keys) issued and signed by the user;
- two kind of proxies: full and limited (which prevent job submission). The full proxy is kept by the WMS and only limited proxies are issued afterwards;
- a job must have a valid proxy during its execution;
- a different proxy (but from the same user) can be used for job status queries output retrieval.

Environment variable: `$MYPROXY_SERVER`

Proxy creation:

```
myproxy-init [-s server] [-c lifetime] -d -n
```

Notes:

- doesn't create a proxy on the client side;
- can be created during job execution.

```
myproxy-info [-s server] -d
```

```
myproxy-destroy [-s server] -d
```

Difficulties:

1. myproxy itself is not voms enabled.
2. WMS used for submitting jobs should be explicitly allowed by myproxy server to get the delegations.