

Brief notes on gridftp transfers using proxy certificates from the ELIXIR CILogon service.

Mikael Borg
Feb 2016

Background

I have set up a gridftp endpoint for testing purposes. So far, test transfers have been authenticated using a Terena e-science certificate obtained from my university. Here is a brief description of data transfers authenticated with a proxy certificate obtained from the CILogon demo portal.

Client-server transfer

In this test, a file is transferred to and from my workstation and a gridftp endpoint. The user is authenticated with an ELIXIR proxy certificate.

On gridftp server

Obtain CA certificate:

```
$ wget --no-check-certificate -O \  
/etc/grid-security/certificates/ELIXIR-demo.pem \  
https://snf-676811.vm.oceanos.grnet.gr/ca/demoroot.html
```

Specify certificate signing policy file /etc/grid-security/certificates/ELIXIR-demo.signing_policy with the content (this was just an educated guess):

```
#  
access_id_CA    X509      '/O=Grid/OU=GlobusTest/CN=Globus Simple CA for Demo  
Portal'  
pos_rights      globus    CA:sign  
cond_subjects   globus    '/O=Grid/OU=GlobusTest/*''
```

Create symbolic links based on certificate hash:

```
$ export HASH=`openssl x509 -in
/etc/grid-security/certificates/ELIXIR-demo.pem -noout -hash`
$ cd /etc/grid-security/certificates
$ ln -s ELIXIR-demo.pem $HASH.0
$ ln -s ELIXIR-demo.signing_policy $HASH.signing_policy
```

Add proxy certificate subject and username to /etc/grid-security/grid-mapfile.

Restart gridftp server.

On workstation:

Obtain proxy certificate from <https://elixir-cilogon-mp.grid.cesnet.cz/vo-portal/> by pressing “Get Proxy” button. You need to have an ELIXIR account which you can create by registering to Intranet (<https://www.elixir-europe.org/intranet>).

Copy certificate file to /tmp/x509up_u1000 and change permissions to 600 (1000 is my numerical uid).

Check certificate:

```
$ grid-proxy-info
subject :
/O=Grid/OU=GlobusTest/CN=932d5e00216556be236eff3fb858b9b9297b9a02@elixir-euro
pe.org/CN=1272315132/CN=1222112553
issuer  :
/O=Grid/OU=GlobusTest/CN=932d5e00216556be236eff3fb858b9b9297b9a02@elixir-euro
pe.org/CN=1272315132
identity :
/O=Grid/OU=GlobusTest/CN=932d5e00216556be236eff3fb858b9b9297b9a02@elixir-euro
pe.org
type   : RFC 3820 compliant impersonation proxy
strength : 2048 bits
path   : /tmp/x509up_u1000
timeleft : 8:30:09
```

Copy file from workstation to gridftp server:

```
$ globus-url-copy -v -vb -nodcau tmp.txt
gsiftp://gridftp.bils.se/home/borg/tmp/tmp.txt
Source: file:///home/borg/tmp/
Dest:   gsiftp://gridftp.bils.se/home/borg/tmp/
        tmp.txt
```

Copy file from gridftp server back to workstation:

```
$ globus-url-copy -v -vb -nodcau  
gsiftp://gridftp.bils.se/home/borg/tmp/tmp.txt tmp2.txt
```

Check that the files are identical:

```
$ diff tmp.txt tmp2.txt
```

Third-party transfer

Here, a data transfer between two gridftp endpoints is initiated from my workstation. It is demonstrated that the transfer is not possible without first

- installing the trust anchor of the CILogon certificate authority
- adding the users identity (i.e. certificate subject) to the grid-mapfile that maps certificates to use accounts.

Set up additional gridftp endpoint. Obtain ELIXIR proxy certificate.

1 Test without installing CA on new endpoint (should not work):

```
$ globus-url-copy -v -vb -nodcau  
gsiftp://gridftp.bils.se/home/borg/tmp/nt.00.tar.gz  
gsiftp://gridftp.borg.hk/home/borg/tmp/nt.00.tar.gz  
Source: gsiftp://gridftp.bils.se/home/borg/tmp/  
Dest:   gsiftp://gridftp.borg.hk/home/borg/tmp/  
        nt.00.tar.gz
```

```
error: globus_ftp_client: the server responded with an error  
530 530-globus_xio: Authentication Error  
530-OpenSSL Error: s3_srvr.c:3297: in library: SSL routines, function  
SSL3_GET_CLIENT_CERTIFICATE: no certificate returned  
530-globus_gsi_callback_module: Could not verify credential  
530-globus_gsi_callback_module: Can't get the local trusted CA certificate:  
Cannot find trusted CA certificate with hash 93df451c in  
/etc/grid-security/certificates  
530 End.
```

2 Install CA certificate and try again (should still not work)

```
$ globus-url-copy -v -vb -nodcau  
gsiftp://gridftp.bils.se/home/borg/tmp/nt.00.tar.gz  
gsiftp://gridftp.borg.hk/home/borg/tmp/nt.00.tar.gz
```

```
Source: gsiftp://gridftp.bils.se/home/borg/tmp/  
Dest:   gsiftp://gridftp.borg.hk/home/borg/tmp/  
       nt.00.tar.gz
```

```
error: globus_ftp_client: the server responded with an error  
530 530-Login incorrect. : globus_gss_assist: Gridmap lookup failure: Could  
not map  
/O=Grid/OU=GlobusTest/CN=932d5e00216556be236eff3fb858b9b9297b9a02@elixir-euro  
pe.org  
530-  
530 End.
```

3 Add entry to gridmap-file and retry (should work!):

```
$ globus-url-copy -v -vb -nodcau  
gsiftp://gridftp.bils.se/home/borg/tmp/nt.00.tar.gz  
gsiftp://gridftp.borg.hk/home/borg/tmp/nt.00.tar.gz  
Source: gsiftp://gridftp.bils.se/home/borg/tmp/  
Dest:   gsiftp://gridftp.borg.hk/home/borg/tmp/  
       nt.00.tar.gz
```

836184904 bytes

78.18 MB/sec avg

80.99 MB/sec inst