Hands-on session

http://grid.ucy.ac.cy/egee

Grid certification and VO registration

Kyriacos Neocleous
Cyprus Grid Certification Authority
http://cygrid.org.cy/CyGridCA/

High Performance Computing systems Laboratory
Department of Computer Science
University of Cyprus

EGEE-II is a project funded by the European Union under contract INFSO-RI-031688

Digital Certificates (1)

- A **digital certificate** is your **electronic identity** to access the Grid.
- Digital certificates are used for
  - **Authentication**
  - **Authorization**
  - **Data confidentiality** (by encryption mechanisms)
  - **Data integrity** (by cryptographic checksum mechanisms)
- Every user has his/her own personal digital certificate
  - Do not share or expose your private key file
  - Keep your private key file offline except when necessary
  - Do not reveal your private key password

Digital Certificates (2)

- Digital Certificates are issued by accredited **Certification Authorities (CAs)** with the help of Registration Authorities (RAs)**.**
- There exists a CA in every EGEE-participating country, and usually an RA operating at each Resource Centre.
- In Cyprus, the responsible party for issuing certificates is the Cyprus Grid Certification Authority (CyGridCA)
  - http://cygrid.org.cy/CyGridCA/

How to get a grid certificate

Process overview

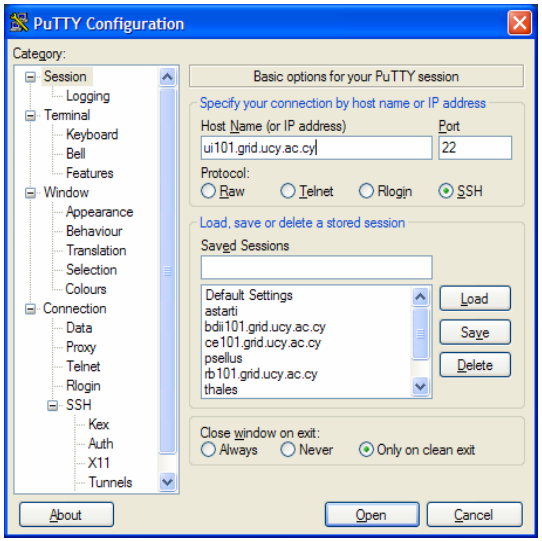
1. obtain a User Interface (UI) account (ui101.grid.ucy.ac.cy)
2. generate a private key on the UI
3. generate a certificate request
4. turn in the completed new user application form, with your ID / passport / driver's license

Details will follow for each step (slides 5-11)

Accessing your UI account

- Use Putty
  - Putty is a secure terminal for windows
  - Access from Start → All Programs → X-Win32 6.1 → PuTTy
- Login to the User Interface
  - Configure for Host **ui101.grid.ucy.ac.cy**, Port **22**, Protocol **SSH**
  - *see screenshot next slide*
  - Press button **Open** to open the terminal
  - You may be prompted with a **PuTTy Security Alert** window:
    - Check if the rsa2 key fingerprint matches the following:
    - **ee:d0:93:41:fd:6c:3c:47:58:6c:30:f5:d6:40:6a:2d**
    - *Only if it matches* you should press **Yes**, otherwise **Cancel**
  - **Username**: your email login (the part before the @)
  - **Password**: the phone number you provided during pre-registration
- You can (and should) change your password when you gain access, with the following command:
  - `$ passwd`

PuTTy configuration window



Private key generation

Login to your UI account (puTTy) and do the following:

Create the directory for storing private and public keys:

```
$ mkdir ~/.globus/
$ cd ~/.globus/
```

Output some random data in a file, wait a few seconds and press Ctrl-C:

```
$ cat /dev/random > random_data
```

Create your private key file:

```
$ openssl genrsa –rand random_data –des3 –out userkey.pem 1024
```

- You will be asked to give a password (PEM pass phrase) that will protect your private key. Choose a strong password, at least 15 characters long, containing numbers, small and capital letters, and special characters. This can be a (long!) phrase you easily remember, but not easy for someone else to guess.

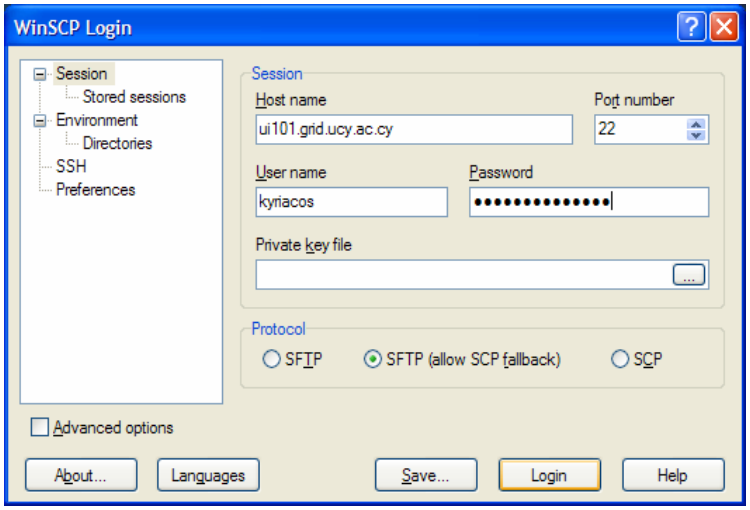
Change the permissions on this file so it's readable only by yourself

```
$ chmod 400 userkey.pem
```


Private key storage

- Transfer your private key to the floppy provided (using WinSCP)
  - WinSCP (Secure CoPy for Windows)
  - Download from **http://winscp.net/download/winscp376.exe**
- Start WinSCP with these parameters (see screenshot in next slide)
  - Host name: ui101.grid.ucy.ac.cy, Port number: 22
  - Username/password: the same you used from putty
  - Press button **Login** to start the session
  - You may be prompted with a **Warning** window:
    - Check if the rsa2 key fingerprint matches the following:
    - **ee:d0:93:41:fd:6c:3c:47:58:6c:30:f5:d6:40:6a:2d**
    - *Only if it matches* you should press **Yes**, otherwise **Cancel**
  - Select floppy drive A: on the left half of the screen (drop-down menu)
  - Drag and drop the userkey.pem file from .globus to the floppy
  - Remove the floppy and close WinSCP
- Make 2-3 backups when you have the chance (floppies often become unusable), and store offline (preferably on a USB stick).
- In general, load your private key file into the UI (using WinSCP or scp from Linux machines) only when necessary, delete it after use and keep the offline copies only

WinSCP Login window



Certificate Request (1)

Get the CyGridCA configuration file:

```
$ wget http://cygrid.org.cy/CyGridCA/ra-hpcl.cnf
```

Generate the certificate request file:

- The following is one command to be given in a single line
- Replace <username> with your e-mail login, *e.g.* kneocleous

```
$ openssl req –new -days 365 -key userkey.pem -out <username>.csr -
   config ra-hpcl.cnf
```

Then you are prompted to enter the private key password to sign this request, and then complete the following information. The first two fields must be exactly **CY** and **CyGrid**, and the rest of the fields are given as examples (those values underlined), use your own:

- **Country Name** (2 letter code) = **CY**
- **National Grid Initiative Name** = **CyGrid**
- **Organization name** (your company or institute name) = **UCY**
- **Your name** (firstName lastName) = **Kyriacos Neocleous**
- **Email Address** = **kyriacos@cs.ucy.ac.cy**

Certificate Request (2)

Change permissions to read-only and copy the request file to a common directory. Replace <username> with your real username (email login):

```
$ chmod 400 <username>.csr
$ cp <username>.csr /cert_req/
```

- Bring your **ID** (or passport or Cypriot driver's license) and the **completed application form**
  - Form is at http://cygrid.org.cy/join.html
  - You **don't** need to complete the section "Software Application Information" at this time
- **STOP HERE, wait for your certificate to be created before proceeding with the instructions in the next slide**

Grid certificate issued by CA

CONTINUE FROM HERE when you receive notification that your certificate has been created. Your grid certificate, i.e. CA-signed request file, should be under .globus/ directory, file name **<username>.crt**

- Login to the UI using PuTTy
- Check the certificate file exists by listing contents of .globus
  - `$ ls ~/.globus`
- Rename the file to usercert.pem
  - `$ mv ~/.globus/<username>.crt  ~/.globus/usercert.pem`
- Change permissions to read-only by all
  - `$ chmod 444 ~/.globus/usercert.pem`

SEE-VO registration (1)

- Registration to the South East Europe Virtual Organization will follow (final step, be patient)
- First a P12 bundle needs to be created (a single file containing your private and public [certificate] keys):
  - From .globus directory, issue the following command (single line):
  - The following is one command to be given in a single line
  - Replace <username> with your e-mail login, *e.g.* kneocleous
  - Replace First Last with your first and last name (include the quotes)
  - `$ openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -name "First Last" -out <username>.p12`
- You will be asked your PEM passphrase (that's the private key password you created before), and then you will be asked to define an export password. You can use the same as your PEM passphrase.

SEE-VO registration (2)

- Use WinSCP to transfer this file to the Windows machine you use
  - Hostname: ui101.grid.ucy.ac.cy, same username/password
  - Select **Desktop** on the left half
  - Drag and drop the <username>.p12 file from .globus to the desktop
- Next, load the P12 bundle into the FireFox web browser:
  - Start FireFox browser
  - Go to menu Tools → Options
  - Click on **Advanced** on the bottom left
  - Scroll down to **Certificates** and click to expand
  - Click on button **Manage Certificates**
  - Click on button **Import** and locate your P12 file, click **Open**
  - Define a new password for the Software Security device
  - Input the P12 *export password* at the prompt (see previous slide)
  - Click **OK** twice to close all dialogs

SEE-VO Registration (3)

- Point FireFox to URL:
  - http://www.grid.auth.gr/pki/hellasgrid-ca-2002/cacert/hellasgrid-ca-cert.crt
- You will be asked to confirm:
  - Click on button **View** and verify that the sha1 fingerprint is **36:12:69:64:31:35:FD:E1:FA:9B:6B:9C:4F:31:32:B5:B3:20:13:B5**
  - Click on **Close** to return to the confirmation dialog
  - Check all three purposes boxes and click on **OK**
- **FINALLY ☺**
  - You must visit the following site to register to the SEE-VO
  - https://www.grid.auth.gr/services/voms/SEE/request.php

SEE-VO Registration (4)

- After registering, check your e-mail for the confirmation message (you need to follow the link to confirm)
  - Please confirm only once!
- Normally within 6 hours from confirmation you can use the SEE-VO to submit jobs on the grid

Acceptance of CP/CPS

- The Certification Policy and Certification Practice Statement (CP/CPS) of CyGridCA has to be read by all new users
  - http://cygrid.org.cy/CyGridCA/docs/CyGrid-CPS-v1.0.4.pdf
- The CP/CPS has to be signed by all new users within the following two weeks, for signifying acceptance to the terms of the Certification Authority
- Specific instructions on how to setup your e-mail application to digitally sign messages in order to do this will be sent via e-mail shortly after you obtain your certificate

Questions/Problems?

Thanks for your attention
(and your patience!)

Sources for more information

- Cyprus Grid Certification Authority
  - http://cygrid.org.cy/CyGridCA/
- Cyprus Grid initiative
  - http://cygrid.org.cy/
- EGEE project website for Cyprus
  - http://grid.ucy.ac.cy/egee/
- EGEE project website for South East Europe
  - http://www.egee-see.org/
- South East Europe Virtual Organisation
  - https://www.grid.auth.gr/services/voms/SEE/

Contact information

CyGrid Certification Authority
High Performance Computing systems Lab
Department of Computer Science
University of Cyprus
P.O.Box 20537
CY-1678 Nicosia
CYPRUS

Phone: +357-22.89.26.63
Fax: +357-22.89.27.01

WWW: http://cygrid.org.cy/CyGridCA
E-mail: cygrid-ca@cs.ucy.ac.cy