**Grid Training for Power Users**
**Institute of Physics Belgrade**

# Hands-On Session: Setting up the user account

Vladimir Slavnic (slavnic@ipb.ac.rs)
Nikola Grkic (ngrkic@ipb.ac.rs)
SCL, Institute of Physics Belgrade
Serbia

28/05/2012

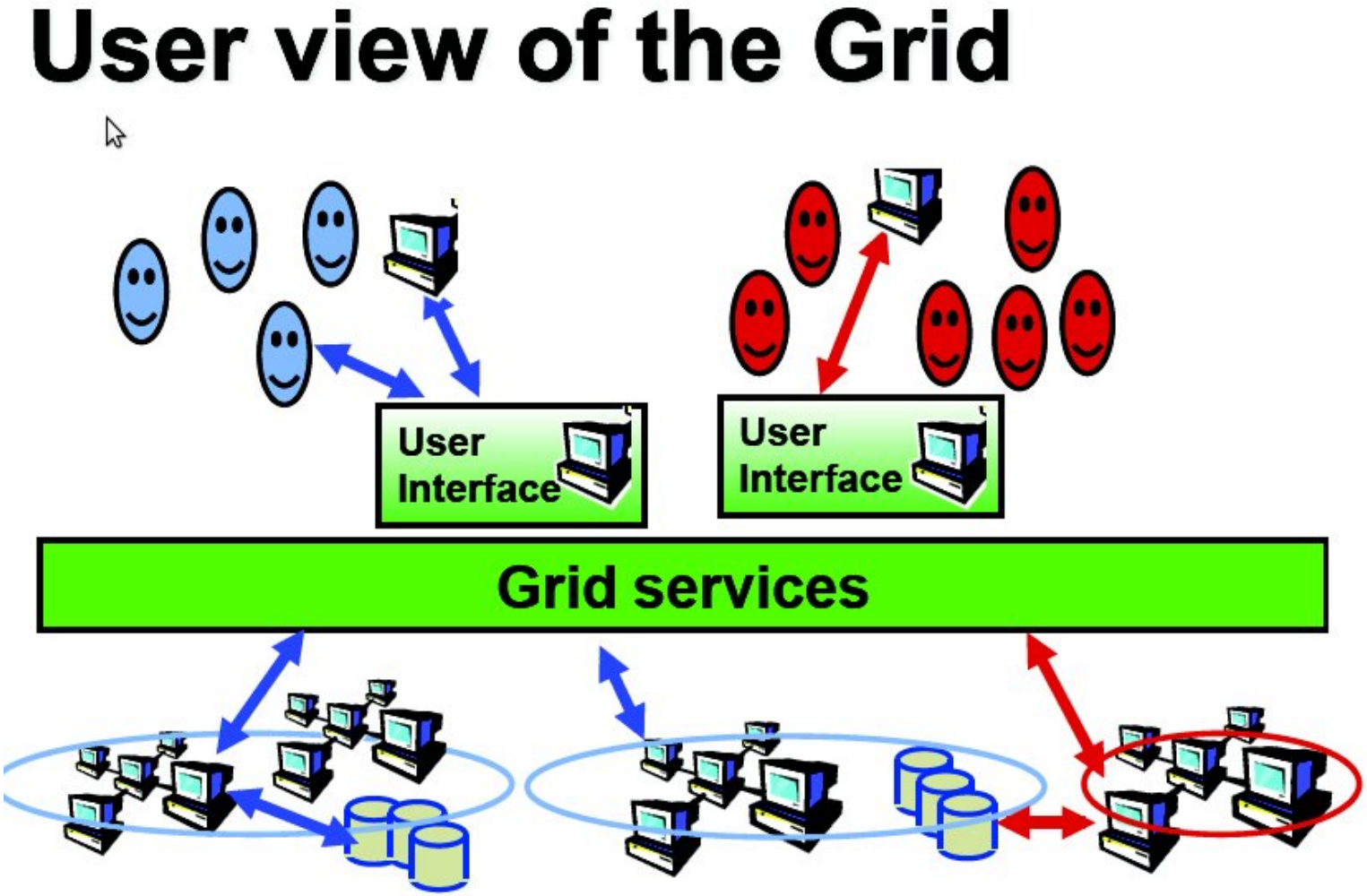
# Overview

- User Interface (UI)
- Grid Security Infrastructure (GSI)
- Certificate obtaining procedure
- How to use certificate
- Proxies
- My Proxy service
- Certificates renewal

# User interface – UI (1)

- Access point to Grid
- User must have a local account on the machine
- It provides CLI tools to perform different Grid operations:
  - list all the resources suitable to execute a given job;
  - submit jobs for execution;
  - cancel jobs;
  - query the status of jobs and retrieve their output;
  - copy, replicate and delete files from the Grid;
  - retrieve the status of different resources from the Information System;

# User interface – UI (2)



# Grid Security Infrastructure (GSI)

- Basic Security Concepts:
  - Private and Public Keys - Encryption
  - Signing
- **Grid credentials**: digital certificate and private key
  - Grid passport
  - Based on PKI X.509 standard
  - A public key connected to some information about who the user (or server) is, signed by the CA
  - CA signs certificates. Trust relationship
    - National Certification Authority (CA) – AEGIS CA
  - The most important thing in the certificate is the Subject Name (SN):

/C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir Slavnic

# Certificate obtaining procedure

- Via browser or from UI
- Command issued on UI:

```
$ grid-cert-request
```

  - PEM pass phrase (do not forget it!!!)
- .globus directory
  - ***userkey.pem***
  - ***usercert_request.pem***
  - ***usercert.pem***
- ***usercert_request.pem*** to be send by RA to CA to be signed
- Signed certificate will be sent back to user
- Confirmation mail signed with new certificate to be send to CA by the user

# Taking care of private keys

- Keep your private key secure
- Right permissions:
  - `444 usercert.pem`
  - `400 userkey.pem`
- Do not loan your certificate to anyone
- Report to your CA if your certificate has been compromised
- Private key and certificate can be stored:
  - In your browser and mail client
  - Stored in files using different file format (PEM, P12, …)

# Checking a certificate

- `$ grid-cert-info [-subject |-enddate|-issuer]`

```
[slavnic@ui ~]$ grid-cert-info -subject
/C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir Slavnic
[slavnic@ui ~]$ grid-cert-info -issuer
/C=RS/O=AEGIS/CN=AEGIS-CA
[slavnic@ui ~]$ grid-cert-info -enddate
Jun 26 08:03:17 2012 GMT
```

- Verify a user certificate:

```
[slavnic@ui ~]$ openssl verify -CApath /etc/grid-security/certificates/ ~/.globus/usercert.pem
/home/slavnic/.globus/usercert.pem: OK
```

# pkcs12 bundle creation and VO registration

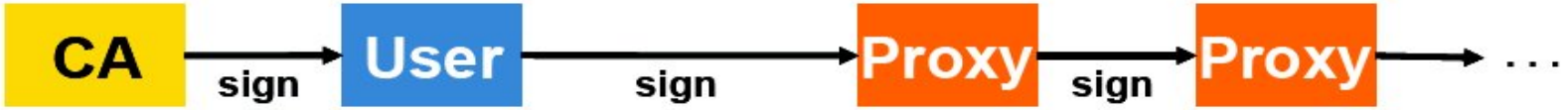
- Creating p12 certificate

```
$ opensslpkcs12 -export -in ~/.globus/usercert.pem -inkey~/.globus/userkey.pem
   -name "My Certificate" -out mycertificate.p12
```

- Importing certificate into the mail client and web browser
- Virtual Organization – VO
  - Entity which typically corresponds to a particular organization or group of people in the real world
- VO membership request (web interface):
  - AEGIS VOMS Web application is located on the following address: https://voms.ipb.ac.rs:8443/voms/aegis/
- AEGIS CA : http://ca.aegis.rs/

# Proxies (1)

- **Proxy certificates**: Temporary self-signed certs




- Types of proxies:
  - Standard proxy
  - VOMS proxy
- VOMS proxies – proxies with VO extensions
  - Group
  - Role

# Proxies (2)

- VOMS proxy UI commands:

```
$ voms-proxy-init -voms<vo>
$ voms-proxy-init -voms<alias>:<group name>:[Role=<role name>]
$ voms-proxy-info (-all)
$ voms-proxy-destroy
```

- Creating VOMS proxy:

```
[slavnic@ui ~]$ voms-proxy-init -voms aegis
Enter GRID pass phrase:
Your identity: /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir
   Slavnic
Creating temporary proxy ............................. Done
Contacting  voms.ipb.ac.rs:15001 [/C=RS/O=AEGIS/OU=Institute of Physics
   Belgrade/CN=host/voms.ipb.ac.rs] "aegis" Done
Creating
   proxy ..................................................................
   Done
Your proxy is valid until Mon May 28 00:34:26 2012
```

# Proxies (3)

- Checking VOMS proxy:

```
slavnic@ui ~]$ voms-proxy-info -all
subject   : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir Slavnic/
   CN=proxy
issuer    : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir Slavnic
identity  : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir Slavnic
type      : proxy
strength  : 1024 bits
path      : /tmp/x509up_u501
timeleft  : 11:50:33
=== VO aegis extension information ===
VO        : aegis
subject   : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir Slavnic
issuer    : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=host/voms.ipb.ac.rs
attribute : /aegis/Role=NULL/Capability=NULL
attribute : /aegis/scl/Role=NULL/Capability=NULL
timeleft  : 11:50:33
uri       : voms.ipb.ac.rs:15001
```

# Proxy renewal – MyProxy (1)

- MyProxy - proxy credential repository system
- User can create and store a long-term proxy in a dedicated server (MyProxy server)
- MyProxy commands on UI:

```
$ myproxy-init -s <myproxy_server> -d -n
$ myproxy-info -s <myproxy_server> -d
$ myproxy-destroy -s <myproxy_server> -d
```

# Proxy renewal – MyProxy (2)

- Show MyProxy server evironment variable:

```
[slavnic@ui ~]$ echo $MYPROXY_SERVER
myproxy.ipb.ac.rs
```

- Creating and storing a long-term proxy:

```
[slavnic@ui ~]$ myproxy-init -d -n
Your identity: /C=RS/O=AEGIS/OU=Institute of Physics
   Belgrade/CN=Vladimir Slavnic
Enter GRID pass phrase for this identity:
Creating proxy ..................................... Done
Proxy Verify OK
Your proxy is valid until: Sun Jun  3 12:37:44 2012
A proxy valid for 168 hours (7.0 days) for user /C=RS/
   O=AEGIS/OU=Institute of Physics Belgrade/CN=Vladimir
   Slavnic now exists on myproxy.ipb.ac.rs.
```

# Proxy renewal – MyProxy (3)

- Show long-term proxy information:

```
[slavnic@ui ~]$ myproxy-info -d
username: /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/
   CN=Vladimir Slavnic
owner: /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/
   CN=Vladimir Slavnic
timeleft: 167:59:02  (7.0 days)
```

# Certificate renewal

- CAs issue certificates with a limited duration (usually one year)
- User needs to send a request for renewal signed with the old certificate to CA before old certificate expires
- Users should try to be aware of the renewal date
- Renewed certificates have the same SN as the old ones

# Links

- AEGIS CA
  - http://ca.aegis.rs
- Glite user guide
  - https://edms.cern.ch/file/722398//gLite-3-UserGuide.pdf