

**EGI Hands On Training for AEGIS Users
Institute of Physics Belgrade**

Hands-On Session: Setting up the user account

Nikola Grkic

Institute of Physics Belgrade

Serbia

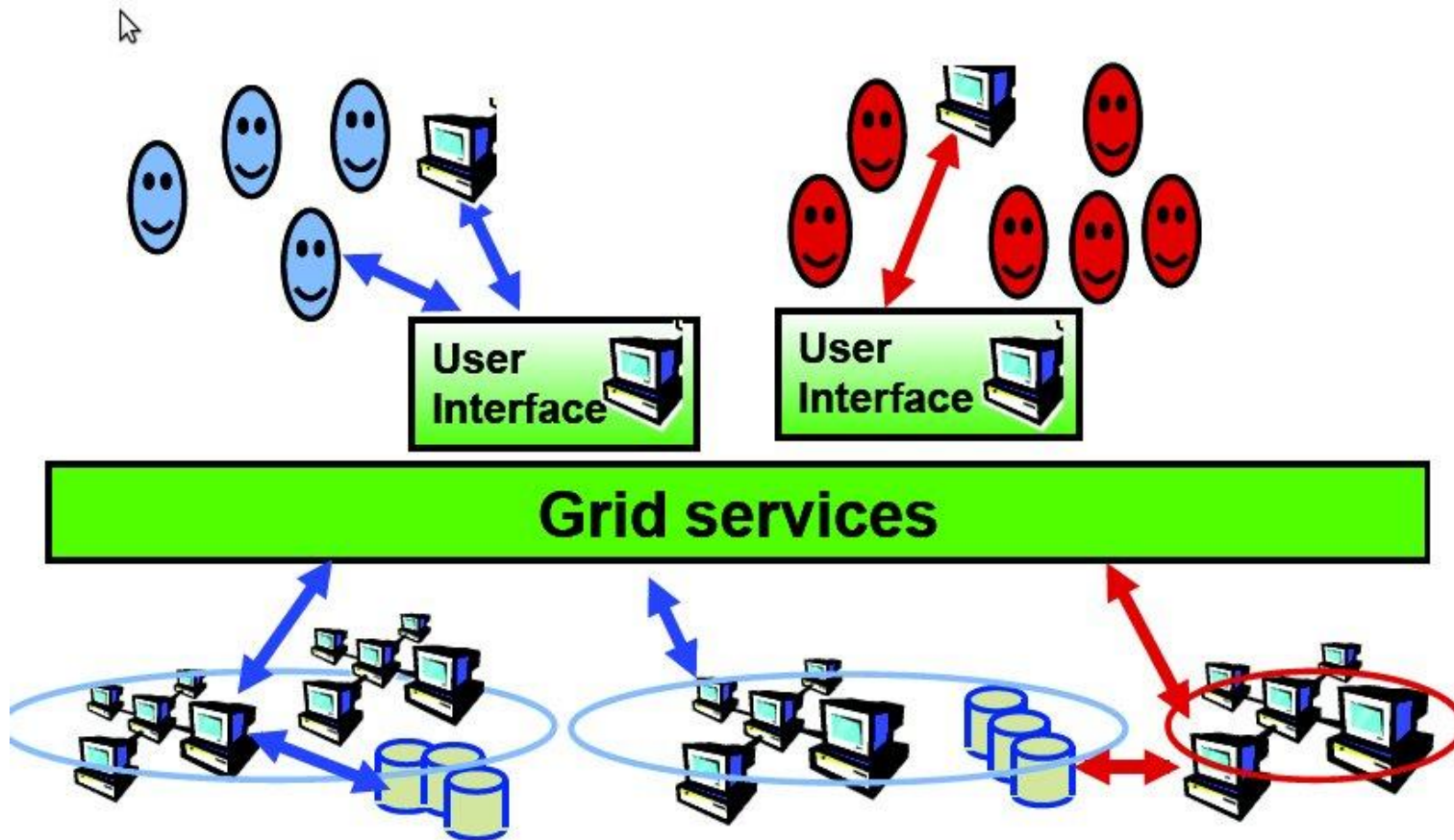
ngrkic@ipb.ac.rs



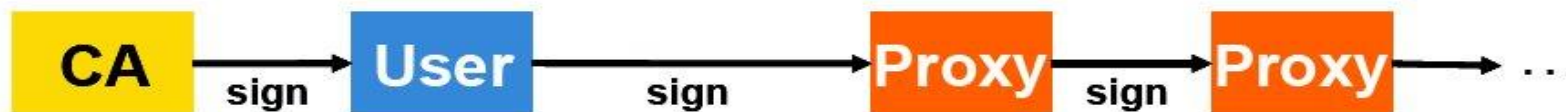
- User Interface (UI)
- Grid Security Infrastructure (GSI)
- Certificate obtaining procedure
- How to use certificate
- Proxies
- My Proxy service
- Certificates renewal

- Access point to Grid
- User must have a local account on the machine
- Perform grid operations:
 - Job operations
 - To submit a job
 - Monitor its status
 - Retrieve output
 - Data operations
 - Upload file to SE
 - Create replica
 - Discover replicas
 - Other grid services

User view of the Grid



- **Grid credentials:** digital certificate and private key
 - Grid passport
 - Based on PKI X.509 standard
 - CA signs certificates. Trust relationship
 - National Certification Authority (CA) – AEGIS CA
- **Proxy certificates:** Temporary self-signed certs, allowing single sign-on: Proxy delegation



- Virtual Organization – VO
 - Entity which typically corresponds to a particular organization or group of people in the real world

- 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 user

- Keep your private key secure
- 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, ...)

- ```
$ grid-cert-info [-subject |-enddate|-issuer]
[ngrkic@ui ~]$ grid-cert-info -subject
/C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola
Grkic
[ngrkic@ui ~]$ grid-cert-info -issuer
/C=RS/O=AEGIS/CN=AEGIS-CA
[ngrkic@ui ~]$ grid-cert-info -enddate
Jul 28 14:14:17 2011 GMT
```
- **Verify a user certificate:**  

```
[ngrkic@ui ~]$ openssl verify -CApath /etc/grid-
security/certificates/ ~/.globus/usercert.pem
/home/ngrkic/.globus/usercert.pem: OK
```
- **Right permissions:**
  - 444 *usercert.pem*
  - 400 *userkey.pem*



- 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
- 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/>

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

```
[ngrkic@!ui ~]$ voms-proxy-init -voms aegis
```

```
Enter GRID pass phrase:
```

```
Your identity: /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola Grkic
```

```
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 Sun Nov 14 08:17:37 2010
```

- **Checking VOMS proxy:**

```
[ngrkic@ui ~]$ voms-proxy-info -all
subject : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola Grkic/CN=proxy
issuer : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola Grkic
identity : /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola Grkic
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=Nikola Grkic
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
```

- 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
```

- Show MyProxy server environment variable:

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

- Creating and storing a long-term proxy:

```
[ngrkic@ui ~]$ myproxy-init -d -n
Your identity: /C=RS/O=AEGIS/OU=Institute of Physics
Belgrade/CN=Nikola Grkic
Enter GRID pass phrase for this identity:
Creating proxy Done
Proxy Verify OK
Your proxy is valid until: Sat Nov 20 20:37:25 2010
A proxy valid for 168 hours (7.0 days) for user
/C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola
Grkic now exists on myproxy.ipb.ac.rs.
```

- Show long-term proxy information:

```
[ngrkic@ui ~]$ myproxy-info -d
```

```
username: /C=RS/O=AEGIS/OU=Institute of Physics
Belgrade/CN=Nikola Grkic
```

```
owner: /C=RS/O=AEGIS/OU=Institute of Physics Belgrade/CN=Nikola
Grkic
```

```
timeleft: 167:59:02 (7.0 days)
```

- 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



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