Training event:
Application development course
10.March 2005, IISAS Bratislava

Certificate management

Miroslav Dobrucký
Institute of Informatics SAS

Information Society

EGEE is a project funded by the European Union under contract INFSO-RI-508833

Contents

- How do I login on the Grid?
- Grid certificates
- Creating the key/request pair
- Obtaining the certificate
- Installing the certificate
- Creating the proxy

How do I login on the Grid?

- **Distribution of resources: secure access is a basic requirement**
  - Secure communication (SSL)
  - Security across organisational boundaries (PKI, X.509)
  - Single “sign-on” for users of the Grid (proxy certificates)
- **Two basic concepts:**
- **Authentication: Who am I?**
  - Equivalent to ID card, passport, ...
  - Certificates
- **Authorisation: What can I do?**
  - Certain permissions, duties, etc.
  - Virtual organizations

Grid certificates

- Each user must have a valid X.509 certificate issued by a recognized Certification Authority (CA)
- Before doing any Grid operation, user must log in User Interface (UI) machine and create a proxy certificate
- A proxy certificate is a delegated user credential that authenticates the user in every secure interaction, and has a limited lifetime (security reasons)

Creating the key/request pair

grid-cert-request command

```
[miro@cluster2 miro]$ grid-cert-request
Enter your name, e.g., John Smith: Miroslav Dobrucky
A certificate request and private key is being created.
You will be asked to enter a PEM pass phrase.
This pass phrase is akin to your account password,
and is used to protect your key file.
If you forget your pass phrase, you will need to
obtain a new certificate.

Using configuration from /etc/grid-security/globus-user-ssl.conf
Generating a 1024 bit RSA private key
.....................++++++
.............................++++++
writing new private key to '/home/miro/.globus/userkey.pem'
Enter PEM pass phrase:************
```

Obtaining the certificate

Mail the request to the relevant CA

```
[miro@cluster2 miro]$ cat
  home/miro/.globus/usercert_request.pem | mail
  ca.ui@savba.sk
```

User should deliver his/her request to the relevant **Registration** or **Certification Authority** (RA or CA) and personally authenticate by his/her ID card, passport or similar official document with his/her photo included.

The RA will deliver his/her request to the CA. The CA will sign the request and send back the certificate. Usually it is valid for 1 year, before that period finishes, the user can create a rekey request using his valid certificate. It means no further personal travel is needed.

Relevant trusted CAs

- C=CZ, O=CESNET, CN=CESNET CA
- C=ES, O=DATAGRID-ES, CN=DATAGRID-ES CA
- C=FR, O=CNRS, CN=CNRS
- C=GR, O=HellasGrid, CN=HellasGrid CA
- C=PT, O=LIPCA, CN=LIP Certification Authority
- C=SK, O=SlovakGrid, CN=SlovakGrid CA
- C=UK, O=eScience, OU=Authority, CN=CA/Email=ca-operator@grid-support.ac.uk
- ...

They are accredited by "The European Policy Management Authority for Grid Authentication in e-Science"
www.eugridpma.org

Installing the certificate

Install the certificate to the UI machine into the ~/.globus directory:

```
[miro@cluster2 .globus]$ ls -l
-r--r--r-- 1 miro  miro 4774 Oct  8 13:11 usercert.pem
-r--r--r-- 1 miro  miro 1270 Oct  8 10:51 usercert_request.pem
-r-------- 1 miro  miro  963 Oct  8 10:51 userkey.pem
```

Creating the proxy

grid-proxy-init command

```
[miro@cluster2 miro]$ grid-proxy-init
 Your identity: /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
 Enter GRID pass phrase for this identity:
 Creating proxy ..................................... Done
 Your proxy is valid until: Fri Nov 12 12:37:05 2004
```

grid-proxy-info

grid-proxy-destroy

Thank you.

http://public.eu-egee.org

http://ups.savba.sk/ca/