Logging into the Grid (certificates)

Grid Security Infrastructure

- The Grid uses public key security infrastructure
  - PKI X.509 infrastructure
  - every user, services, resources must posess a valid certificate on the Grid
  - certificates are the Grid ID-cards
  - Authorities which "issues" certificates are the Certificate Authorities, CAs
  - Establishing the Identity of a Grid entity on the Grid: this is the Authentication process
    - mutual Authentication: both the user & the requested Grid service (or service-service) checks out each-other identity

the Certificate

- **Subject Name (SN, sometimes called DN)**

  /O=Grid/O=NorduGrid/OU=Tutorial/CN=Tore Tutor

  O=Grid, Ou=NorduGrid, Ou=Tutorial, CN=Tore Tutor
- **public key of the User (or Grid service)**
- **some metadata**
  - serial number
  - validity (not before.., not after)
  - signature algorythm
  - possible extension fields
- **the identity of the thrusted third-party (The CA)**

  Issuer: O =Grid, Ou=NorduGrid, CN=NorduGrid Tutorial CA
- **the digital signature of the third-party**

an example certificate

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 29 (0x1d)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: O=Grid, O=NorduGrid, CN=NorduGrid Tutorial CA
    Validity
      Not Before: Oct 18 17:04:16 2002 GMT
      Not After : Nov 18 17:04:16 2002 GMT
    Subject: O=Grid, O=NorduGrid, OU=Tutorial, CN=Tore Tutor
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c2:1f:5c:b6:19:b9:84:f7:ab:91:62:74:9a:a7:
         ....
          e5:7c:c2:09:f3:6a:3d:1c:6f:86:8f:b0:4e:a1:78:
          60:a0:6a:9d:25:27:75:fc:2b
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      Netscape Cert Type:
        SSL Client, SSL Server, S/MIME, Object Signing
  Signature Algorithm: md5WithRSAEncryption
    a3:a3:2b:0d:70:0d:16:c0:22:e0:77:22:5e:4c:52:7d:d2:64:
    ...
    6a:30:00:76:cd:ca:75:b6:11:f2:2e:ef:7b:03:4d:dc:24:60:
    0b:e8
-----BEGIN CERTIFICATE-----
MIICGTCCAYKgAwIBAgIBHTANBgkqhkiG9w0BAQQFADBDMQ0wCwYDVQQKEwRHcmlk
MRIwEAYDVQQKEwlOb3JkdUdyaWQxHjAcBgNVBAMTFU5vcmR1R3JpZCBUdXRvcmlhdqcArGD
hO0tDeXgL6/oZErgKb
...
LzepIMmD7ntLfo/RrY/cPBNqvqxU11qMAB2zcp1
thHyLu97A03cJGAL6A==
-----END CERTIFICATE-----
```

the CA

The Trusted Third Party:

- Binds identities to key pairs
- “issues” 'X.509' certificates
- maintains Certification Policy
- revokes compromised certificates
- extends expired certificates

The NorduGrid Certificate Authority:

- issues certificates for the NorduGrid Testbed
- Trusted/Recognized by several other Grid Projects

obtaining a certificate

- you may request your certificate via the webpage of your CA (not yet supported)
- you need to install the Globus toolkit together with your CA configuration files (CA package, i.e. ca_NorduGrid-local-version.rpm). The NorduGrid standalone client package provides you an out-of-box solution.
  - generate your X509 key pair (public, private) with the appropriate SN name:
    `grid-cert-request`
  - check the generated `usercert_request.pem` file for the correct SN and send the file to the CA for signature
  - within two working days :) you'll get your signed certificate, save it as:
    `$HOME/.globus/usercert.pem`

using your certificate

check the correct file permissions:

```
ls -l .globus/
-r--------    963 Aug 23 13:54 userkey.pem
-rw-r--r--   4020 Aug 23 13:54 usercert.pem
-rw-r--r--   1500 Aug 23 13:54 usercert_request.pem
```

login to the Grid (create your proxy):

- **the proxy is a temporary public-private keypair signed by your certificate, only this temporary file is sent to the Grid services**
- **certificate chains are used for Authentication**
- **type** `grid-proxy-init` **and enter your passphrase**
- **from now on you are on the Grid!**

using your certificates

further hints:

- keep your private key SECURE!!!
- your proxy has a limited lifetime (default 24 hours, use `-valid` for longer proxies)
- check the time settings of your client
- you need the public keys (CA packages) of all the Grid resources that you want to use (in case of the NorduGrid TestBed the `ca_NorduGrid-version-rpm`)
- useful commands:
  - `grid-cert-info`, `grid-change-pass-phrase`, `grid-proxy-info`, `grid-proxy-destroy`
- further information: certificate mini-Howto from

  `www.nordugrid.org/documents/certificate_howto.html`

Authorization

access control to the resources:

- local sites maintains their own policy
- Grid users -> local Unix user mappings, then access control is done with the local Unix accounts
- instead of individual users sites can choose from group of Grid users: Virtual Organization (VO)
- LDAP Grid user database, periodically queried by the sites to update their mappings
- you need to be a member of a VO group if you want to have access to the NorduGrid Testbed.
- further info: `grid.quark.lu.se/NorduGridVO`

exercises:

1, **check out your credentials**

```
ls -l .globus/
```

2, **generate a certificate request**

```
grid-cert-request -dir certdir
```

3, **modify the passphrase of your private key**

```
grid-change-pass-phrase
```

4, **check the content of your credentials**

```
grid-cert-info & grid-proxy-info
```

5, **Log into the Grid: create your proxy**

```
grid-proxy-init
```

6, **destroy your proxy and create a longer one**

```
grid-proxy-destroy; grid-proxy-init -valid 48:0
```