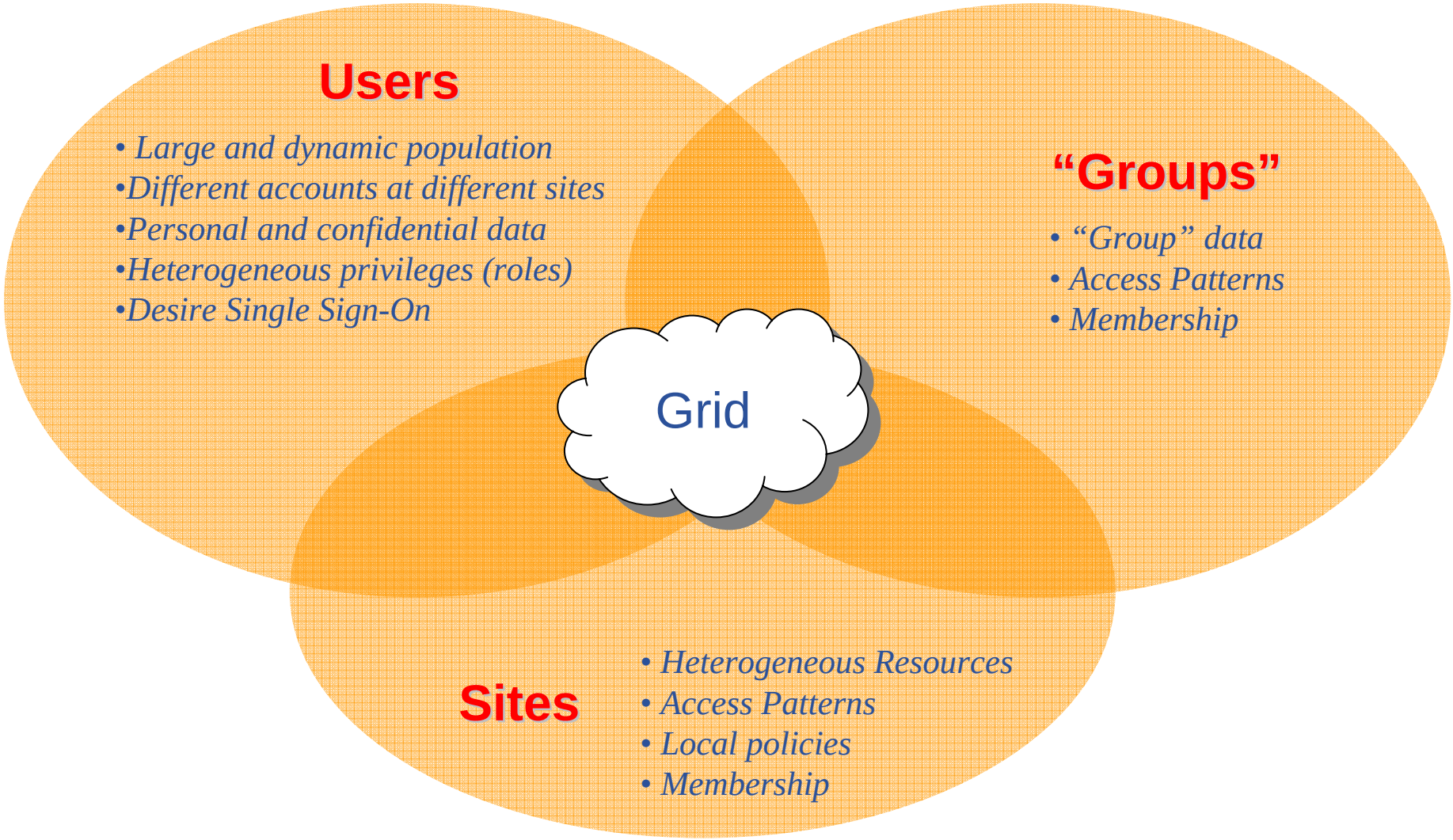
Gilda Practicals

GILDA TUTORS

ISSGC05, Vico Equense 20.07.2005

GRID Security: the players



Digital certificates

The goal of authorization and autentication of users and resources is done through digital certificates, in x509 format

Certification Authority **(CA)**

- **Issue Digital Certificates for users and machines**
- **Check the identity and the personal data of the requestor**
  - Registration Authorities (RAs) do the actual validation
- **CA's periodically publish a list of compromised certificates**
  - **Certificate Revocation Lists** (CRL): contain all the revoked certificates yet to expire
- **CA certificates are self-signed**

For each player, CA guarantees its autenticity with a certificate

Certificate Use

- Digital certificates are split in public/private keys
- Public key is spread along the net, while the private stays encripted on the disk
- Default location for public/private keys is `$HOME/.globus` (attention to file permissions)

```
[glite-tutor] /home/giorgio > ll .globus
-rw-r-----    1 giorgio  users        1613 Jul 16 16:48
  usercert.pem
-r--------    1 giorgio  users        1914 Jul 16 16:48
  userkey.pem
```

Verify your certificate

To get information on your certificate, run

```
openssl x509 -in .globus/usercert.pem –noout\ -text
```

```
[glite-tutor] /home/giorgio > openssl x509 -in
   .globus/usercert.pem  -noout  -text
Certificate:
    Data:
        Version: 3 (0x2)
        .....
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=IT, O=GILDA, CN=GILDA Certification
  Authority
        Validity
            Not Before: Apr 13 08:15:36 2005 GMT
            Not After : Apr 13 08:15:36 2006 GMT
        Subject: C=IT, O=GILDA, OU=Personal Certificate,
  L=INFN, CN=Emidio Giorgio/Email=emidio.giorgio@ct.infn.it
 .....
```

X.509 proxy certificates

- **GSI extension to X.509 Identity Certificates**
  - signed by the normal end entity cert (or by another proxy)
- **Support some important features**
  - Delegation
  - Mutual authentication
- **Has a limited lifetime (minimized risk of "compromised credentials")**
- **It is created by the** grid-proxy-init **command:**

```
%grid-proxy-init
Your identity: /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase for this identity:
Creating proxy ..................................... Done
Your proxy is valid until: Mon Jul 18 00:04:12 2005
```

Inspecting your proxy

- By `grid-proxy-info` you can inspect info on your proxy

```
%grid-proxy-info -all
subject  : /C=IT/O=GILDA/OU=Personal
  Certificate/L=INFN/CN=Emidio
  Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy
issuer   : /C=IT/O=GILDA/OU=Personal
  Certificate/L=INFN/CN=Emidio
  Giorgio/Email=emidio.giorgio@ct.infn.it
identity : /C=IT/O=GILDA/OU=Personal
  Certificate/L=INFN/CN=Emidio
  Giorgio/Email=emidio.giorgio@ct.infn.it
type     : full legacy globus proxy
strength : 512 bits
path     : /tmp/x509up_u513
timeleft : 11:56:48
```

Long term proxy

- **Proxy has limited lifetime (default is 12 h)**
  - Bad idea to have longer proxy
- **However, a grid task might need to use a proxy for a much longer time**
  - Grid jobs in HEP Data Challenges on LCG last up to 2 days
- **myproxy server:**
  - Allows to create and store a long term proxy certificate:
  - myproxy-init -s <host_name>
    - -s: <host_name> specifies the hostname of the myproxy server
  - myproxy-info -s <host_name>
    - Get information about stored long living proxy
  - myproxy-get-delegation -s <host_name>
    - Get a new proxy from the MyProxy server
  - myproxy-destroy -s <host_name>
    - Destroy the credential into the server
  - Check out the myproxy-xxx - - help option
- **A dedicated service on the RB can renew automatically the proxy**
  - contacts the myproxy server

Installing MyProxy Server

- **MyProxy is not gLite/lcg native (*external dependencies*)**
- **It is distributed with the most of gLite services (UI,WMS..)**
- **So MyProxy server can run where one of these run**
- **Before configuration**
  - Check that $LD_LIBRARY_PATH exports *globus* and *myproxy* lib

```
%echo $LD_LIBRARY_PATH
/usr/lib:/opt/glite/lib:/opt/glite/externals/lib:/opt/globus/lib:/opt/glite/externals/myproxy-1.14/lib
```

  - Ckeck that *globus* bin directory is into $PATH
  - Edit `/etc/myproxy.config`, defining policy access for repository

myproxy-server.config

- `tail /etc/myproxy-server.config`

```
accepted_credentials "/C=BE/O=BEGRID/*"
accepted_credentials "/C=AT/O=AustrianGrid/*"
accepted_credentials "/C=TW/*"
accepted_credentials "/C=CN/O=IHEP/OU=CC/*"
accepted_credentials "/C=AM/O=ArmeSFo/*"
accepted_credentials "/C=it/O=GILDA/*"
accepted_credentials "/C=IT/O=GILDA/*" certificate accepted to store
authorized_retrievers "*" certificate allowed to retrieve
```

Myproxy server start script

```
rpm -ivh http://grid-deployment.web.cern.ch/grid-deployment/download/RpmDir i386-rh73-manual/external/myproxy-config-1.1.8-13.edg1.noarch.rpm
```

- Adds start/script for myproxy-server
- It's packaged for lcg → some adjusts are needed
- Open /etc/init.d/myproxy (vi,emacs….)

comment

```
. ${GLOBUS_LOCATION}/libexec/globus-script-initializer
. ${libexecdir}/globus-sh-tools.sh
```

Replace

```
MYPROXY=/opt/glite/externals/myproxy-1.14/sbin/myproxy-server
```

Store credentials on MyProxy Server

```
%grid-proxy-destroy (remove local credentials)
%myproxy-init -s grid001.ct.infn.it
...
Enter GRID pass phrase for this identity:
...
Enter MyProxy pass phrase:
...
A proxy valid for 168 hours (7.0 days) for
  user giorgio now exists on
  grid001.ct.infn.it.
```

Now your credentials are stored on MyProxy server, and are available for delegation or renewal by RB

Get delegation

```
%myproxy-get-delegation -s grid001.ct.infn.it
Enter MyProxy pass phrase:
A proxy has been received for user giorgio in
   /tmp/x509up_u513

%grid-proxy-info -all
subject  : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=
   proxy/CN=proxy
issuer   : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it/CN=proxy/CN=
   proxy
identity : /C=IT/O=GILDA/OU=Personal
   Certificate/L=INFN/CN=Emidio
   Giorgio/Email=emidio.giorgio@ct.infn.it
```

THE END