Security Mechanisms

The European DataGrid Project Team

http://www.eu-datagrid.org

Overview

- User side
  - Getting a certificate
  - Becoming a member of the VO
- Server side
  - Authentication / CA
  - Authorization / VO

(with some examples)

Authentication

- Authentication (CA Working Group)
  - Policies & Procedures ➔ mutual trust
  - Currently the EDG CA group has approved
    - 15 EDG CAs
    - 5 CrossGrid CAs
  - France-CNRS acted as catchall CA to accept sites not covered by accepted CAs
  - Users identified by their personal certificate

DataGrid Certification Authorities
CERN
Czech Republic
Canada
France CNRS
Germany
Ireland
Netherlands
Nordic Countries
Portugal
Russia
Spain
United Kingdom
US – DOE
CrossGrid CAs

CrossGrid Certification Authorities
Slovakia
Cyprus
Poland
Greece

Authorization

- Authorization (Authorization Working Group)
  - Based on Virtual Organizations (VO)
  - Authorizations by experiment
  - 12 + 1 Virtual Organizations
  - Each VO has his own manager

DataGrid Virtual Organizations
WP6
ITEAM
TSTG
ALICE
ATLAS
LHCb
CMS
BABAR
D0
EARTHOB
GENOMIC
MEDICAL IMAGING
Guidelines

Authentication Overview

- Method to request certificate depending of the CA
- A certificate is valid 1 year

- Grid-cert-request
  - Canada
  - CERN
  - Germany
  - Nordic Countries
  - Portugal
  - Russia
  - Spain
- Web request
  - France CNRS
  - Ireland
  - Italy
  - Netherlands
  - United Kingdom
  - US DOE
- Openssl request
  - Czech Republic

CNRS Personal Certificate Request

- http://igc.services.cnrs.fr/Datagrid-fr/
  - *See demo*

Certificate Convertion

- Convert your certificate from PKCS12 format in PEM format
  - /opt/edg/bin/pkcs12-extract

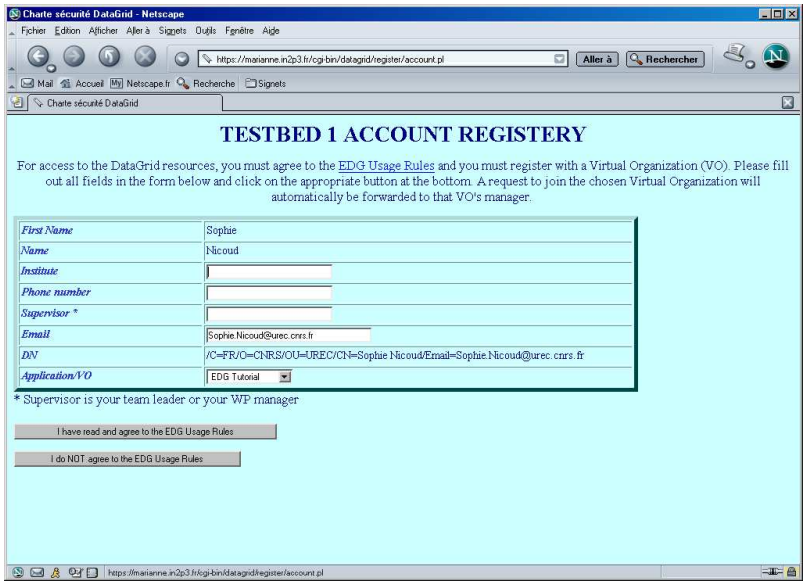
  Or
  - openssl pkcs12 -nocerts \
    -in cert.p12 \
    -out ~user/.globus/userkey.pem
  - openssl pkcs12 -clcerts -nokeys \
    -in cert.p12 \
    -out ~user/.globus/usercert.pem

Authorization

User registration in an EDG Virtual Organisation

- Sign the usage guidelines:
  https://marianne.in2p3.fr/cgi-bin/datagrid/register/account.pl
- In case of problem, contact your VO Manager

->You are registered in the VO server and have a user account.



Usage

You must have a valid certificate from a trusted CA!

- „login": **grid-proxy-init**

  short lifetime certificate: 24 hours

```
Enter PEM pass phrase:
.........................+++++
.....................................+++++
```

- checking the proxy: **grid-proxy-info -subject**

```
/O=Grid/O=CERN/OU=cern.ch/CN=Akos Frohner/CN=proxy
```

- „logout": **grid-proxy-destroy**

-> use the grid services

CNRS Host Certificate Request

- http://igc.services.cnrs.fr/Datagrid-fr/
  - *See demo*
- You receive by crypted and signed email the host certificate

Configuration on the Server

- All RPMs are here:
  - http://datagrid.in2p3.fr/autobuild/rh6.2/rpmlist/
- Certificate and CRL URLs of the CAs: Authentication
  - http://datagrid.in2p3.fr/autobuild/rh6.2/rpmlist/CE-ca-v1_4_3.html
- Creation of the gridmapfile: Authorization
  - http://datagrid.in2p3.fr/distribution/datagrid/wp6/RPMS/edg-mkgridmap-1.0.9-2.i386.rpm
- Scripts to update gridmapfile and CRLs: Authentication/Authorization
  - http://datagrid.in2p3.fr/distribution/datagrid/wp6/RPMS/edg-utils-system-1.3.2-1.noarch.rpm

Summary

- Authentification
  - http://marianne.in2p3.fr/datagrid/ca/ca-table-ca.html
  - http://marianne.in2p3.fr/datagrid/ca/ca-help.html
  - http://igc.services.cnrs.fr/Datagrid-fr/
- Authorization
  - https://marianne.in2p3.fr/cgi-bin/datagrid/register/account.pl
  - http://marianne.in2p3.fr/datagrid/vo/vo-table.html

Further Information

Grid

- EDG CAs: http://marianne.in2p3.fr/datagrid/ca
- Globus Security: http://www.globus.org/security/
- EDG WP2: http://grid-data-management.web.cern.ch/grid-data-management/security/
- EDG D7.5: http://edms.cern.ch/document/340234

Background

- GGF Security: http://www.gridforum.org/security/
- GSS-API: http://www.faqs.org/faqs/kerberos-faq/general/section-84.html
- IETF PKIX charter: http://www.ietf.org/html.charters/pkix-charter.html
- PKCS: http://www.rsasecurity.com/rsalabs/pkcs/index.html