ENTERING IN DCI

AUTHENTICATION AND CERTIFICATES

CERTIFICATE

- What is a certificate?
- Why I get a certificate?
- Where I get it?
- What I do with?

What is a CERTIFICATE

Composed by 2 elements

- Public key
- Private key

Different formats

- pem 2 files
- Pk12 1 file

GRID authentication requires pem format

Why I get a certificate?

VOs (virtual organizations) are the group that own the physical resources

Into the GRID each user or resource or server must be recognized has belonging to VO.

VO users will be able to perform actions according to they role

To do that each user must have a digital certificate (X509) certifying its identity

Why I get a certificate?

- The authorization service guarantees the use of resources according to membership in a VO and a role. The GRID infrastructures use VOMS Virtual Organization Membership Service or IAM Identity and Access Management
- So after the users have get their certificate they must request the membership and agree the AUP Acceptable Use Policy with the VO

How To get a Personal Certificate

- In most countries there is at least one CA (Certification Authority). The CA is a fabric of certificate trusted by GRID
- There is a web page where to find instructions and form to require a Personal Certificate
  1. Contact the CA web page and access the request form
  2. Follow instructions
  3. Upon submission you should receive your **personal certificate** in **p12** file format, usually inside the browser
  4. Export the personal certificate **from your browser** (see specific OS and browser instructions)
  5. Sometimes you need to convert a certificate from p12 to pem format or viceversa

https://www.eugridpma.org/

eugridpma

Structures
Membership
Contact us

IGTF
APGridPMA
TAGPMA
REFEDS
SCI
WISE

Documents
Charter
Guidelines
One Statement Policies

CAOPS-WG
Wiki

Technical Info
CA Distribution download
Subject Locator
Find your local CA
About your certificate

Newsletter issues
Subscribe
Service notices

Tools download and fetch-crl
Technical documentation
IGTF OID Registry
SHA-2 timeline

Meetings
Garching bei Müchen, May 23-25, 2022
Virtual, January 25-27, 2022

Overview
Agendas
Intranet and Reviews

EUGridPMA - Building Trust for Distributed IT Infrastructures for Research

The EUGridPMA is the international organisation to coordinate the trust fabric for e-Infrastructure for research in Europe, the Middle-East, and Africa. It collaborates with the regional peers APGridPMA for the Asia-Pacific and The Americas Grid PMA in the Interoperable Global Trust Federation. The charter document defines the group's objective, scope and operation. It is the basis for the guidelines documents on the accreditation procedure, such as the Authentication profile for secured "classic" authorities and other IGTF recognised profiles supporting federated identity, as well as the dvelopment of guidelines and best practices fostering trust for authorization, attribute management and credential management.

News and Quick Links

Important messages and announcements (such as new distributions of the list of accredited authorities) are carried over the EUGridPMA Announce news service. Every relying party (that means: you) is strongly encouraged to subscribe. Subscription can be via e-mail or the Mailman web interface. You may also be interested in the following direct links:

- Current distribution of IGTF accredited authorities
- Getting your own certificate: find your national or regional authority
- Locate issuing authorities by certificate subject name
- Authentication Profiles managed by this PMA

Getting the Roots of Trust

An installable form of the IGTF trust anchor repository is provided in a variety of forms, such as RPM, deb's, tar-balls and Java Key Stores on the IGTF Distribution site. The latest version is currently **1.116** .

PMA Spotlight

Update to 1.116 available
An update to the trust anchor repository is now available as the 1.116 release with updated trust anchor information and new meta-data from the distribution web site. The April 25th newsletter contains the full announcement of the 1.116 distribution.

Fetch-CRL3.0.22: for high volume environments
The fetch-crl3 series utility facilitates downloading of timely revocation data for IGTF and other PKI infrastructures. Read the feature list and documentation and download it today. This release is also available from the Fedora Extras, EPEL, and Debian repositories. **Version 3.0.22** addresses high-frequency (minute-scale) update scenarios

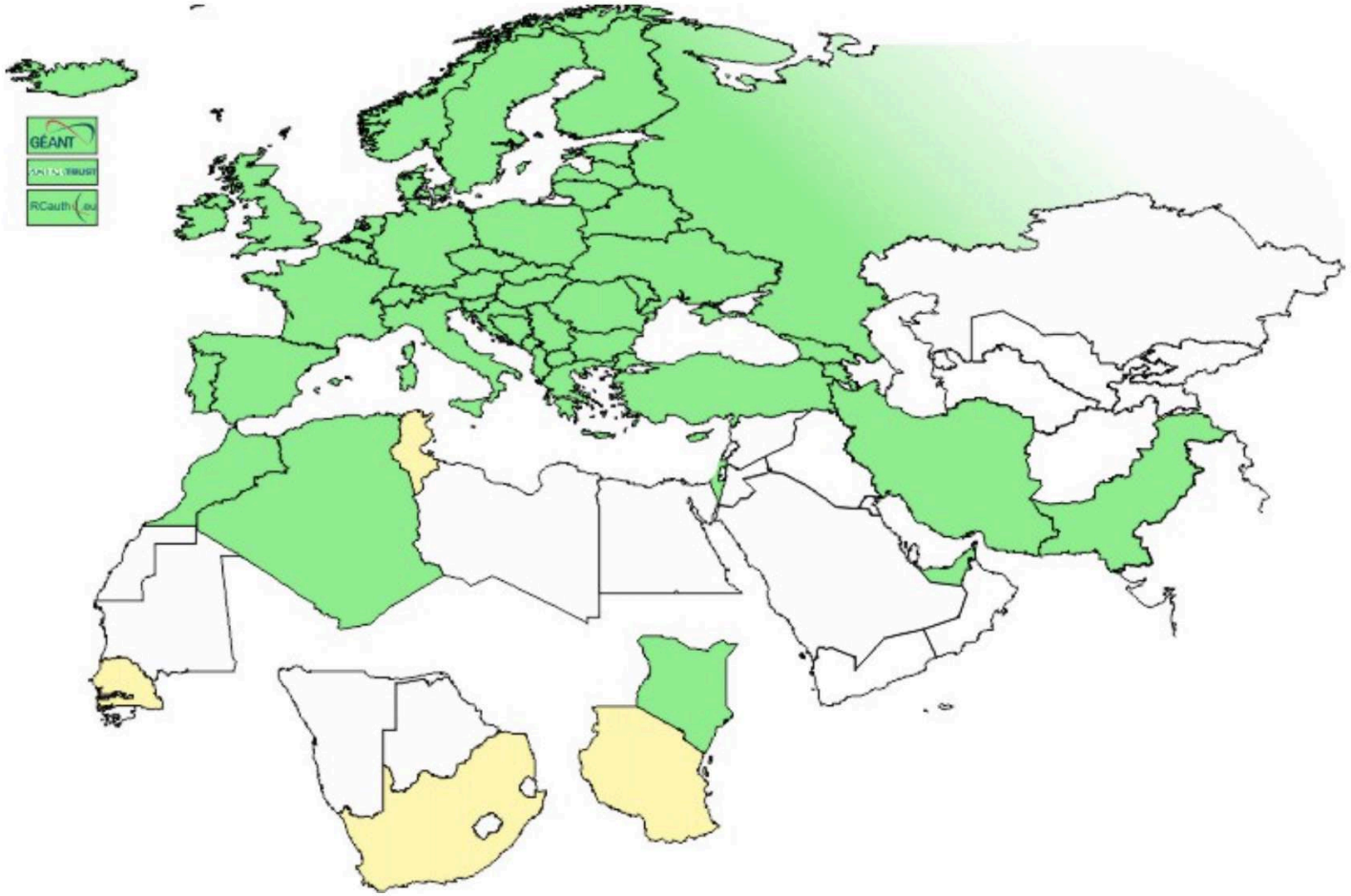
Find your CA

Find your national or regional issuing authority with the new clickable membership map. Read more...

The European Policy Management Authority for Grid Authentication in e-Science is a body to establish requirements and best practices for grid identity providers to enable a common trust domain applicable to authentication of end-entities in inter-organisational access to distributed resources. As its main activity the EUGridPMA coordinates a Public Key Infrastructure (PKI) for use with Grid authentication middleware. The EUGridPMA itself does not provide identity assertions, but instead asserts that - within the scope of the charter - the certificates issued by the Accredited Authorities meet or exceed the relevant guidelines.

Comments to David Groep. *This site is hosted at Nikhef, subject to the privacy policy.*

https://www.eugridpma.org/members/worldmap/



How to convert certificate

The certificate can be downloaded from CA site as a file with .pk12 or .p12 extension

This file are both public and private key

To transform them in 2 files .pem

- openssl pkcs12 -in *certificate.p12* -out *key.pem* -nocerts
- openssl pkcs12 -in *certificate.p12* -out *cert.pem* –clcerts -nokeys

Or with DIRAC environment

- dirac-cert-convert.sh *certificate.p12*

Access to GRID as JUNO member

- Install your certificate into your browser (if not yet)
- Submit the membership to JUNO VO administrator adnd accept the AUP at:

https://voms.ihep.ac.cn:8443/voms/juno/

Follow the indications on the page

DIRAC in JUNO

DIRAC environment allows to access the JUNO GRID resources.

To enable :

- it login in a user interface configured to access to JUNO VO ex: ui-juno.cr.cnaf.infn.it
- source /cvmfs/dcomputing.ihep.ac.cn/dirac/DIRAC_Client/v0r18/bashrc

Now you have access to the DIRAC command line and you can grant the access to GRID

Use the GRID

Install your certificate

```
$ mkdir .globus
$ cp mycertificate/usercert.pem .globus/
$ cp mycertificate/userkey.pem .globus/
$
$ ls -l .globus
totale 8
-rw-r--r--. 1 martini atlas 3374 12 mag 11.45 usercert.pem
-rw-r--r--. 1 martini atlas 1985 12 mag 11.45 userkey.pem

$ chmod 400 .globus/userkey.pem
$
$ ls -l .globus
totale 8
-rw-r--r--. 1 martini atlas 3374 12 mag 11.45 usercert.pem
-r--------. 1 martini atlas 1985 12 mag 11.45 userkey.pem
```

Create a PROXY

- The PROXY is a temporary new certificate file (24 hours by default) signed with your private key so you have to give the password that was required during the creation of the PEM key
- It is stored in a file named /tmp/x509up_u$(id –u)

Proxy command lines

Now you have to generate your proxy

- Create a proxy

  dirac-proxy-init juno [-g xxx] [-v 24:00]

- Get info about proxy

  voms-proxy-info [--all]

- Destroy proxy

  voms-proxy-destroy

- For more info type: voms-proxy-xxxx --help

Proxy command lines

-bash-4.2$ dirac-proxy-init JUNO

```
Generating proxy...
Enter Certificate password:
Added VOMS attribute /juno
Uploading proxy for juno_user...
Proxy generated:
subject      : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it/CN=4043796477/CN=986107055
issuer       : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it/CN=4043796477
identity     : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it
timeleft     : 23:53:56
DIRAC group  : juno_user
rfc          : True
path         : /tmp/x509up_u46631
username     : amartini
properties   : NormalUser, JobMonitor
VOMS         : True
VOMS fqan    : ['/juno']

Proxies uploaded:
 DN                                                                                                | Group        | Until (GMT)
 /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it | juno_user | 2023/04/14 23:54
```

Proxy command lines

-bash-4.2$ dirac-proxy-info

subject : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it/CN=482311095

issuer : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it

identity : /DC=org/DC=terena/DC=tcs/C=IT/O=Istituto Nazionale di Fisica Nucleare/CN=Agnese Martini amartini@infn.it

timeleft : 23:51:43

DIRAC group : juno_user

rfc : True

path : /tmp/x509up_u46631

username : amartini

properties : NormalUser, JobMonitor

-bash-4.2$ dirac-proxy-destroy

Local proxy deleted.

-bash-4.2$ dirac-proxy-info

No proxy found

Cannot contact CS to get user list

Can't find proxy (1101 :)

CVMFS

We have used CVMFS to define the DIRAC environment but with CVMFS is the way to distribute the software.

2 trees are availables:

- /cvmfs/dcomputing.ihep.ac.cn
  where are available the variables and scripts to use the DCI
- /cvmfs/juno.ihep.ac.cn
  where are available the experiment software