GRID Certificates & VOMS

Agnese Martini

GRID

- GRID is a distributed pool of resources
- The users must be recognized by the distributed systems
- The users must be authorized to use the resources
- The users must authenticate themselves so the system can give permissions about different operations

Authorization/Authentication

- Authorization (AUTHZ) describe what the user can do
- Authentication (AUTHN) recognize if the user can or cannot access the resource

The service in charge of this task is the **VOMS** **V**irtual **O**rganisation **M**anagement **S**ervice

AUTHN/AUTHZ

- The resources belong to the organizations, called VO (Virtual Organizations) that have joined the GRID and have funded these resources
- VOs allow users different types of access depending on their role and membership of a given group

Digital Certificate (X509)

- The certificate is the way to make the authentication/authorization in the GRID
- Composed by 2 elements
  - Public key
  - Private key
- Different formats
  - pem : 2 files
  - Pk12 : bundle in 1 file

Digital Certificate (X509)

- Every user, server or service operating in the GRID is identified by means of its digital certificate certifying its identity (AUTHN)
- The VOs give the resource access rights to user groups or roles (AUTHZ)
- Through the digital certificate the access to resources takes place in safe way and with a granularity that go at the single user level

VOMS Virtual Organization Membership Service

- VOs own resources and need service to apply their access policy
- Authorization services of GRID must guarantee the correct user access rights
- The GRID users must be mapped to local “pool accounts” configured to guarantee them the correct access rights
- Most GRID infrastructures use Virtual Organization Management Service (VOMS)
- An other service called Identity and Access Management (IAM) with the same scope but based on token, in the near future will be used in JUNO

VOMS Virtual Organization Membership Service

- The administrators of the VO use VOMS for:
  - The creation of user group
  - The creation of different role within existing group
  - Accepting users making membership request to a VO

VOMS Virtual Organization Membership Service

The first step for a new grid user is to request the membership to a VO

To do that the user must:

- Have an X509 certificate imported in a browser
- Visit the VOMS web page from that browser
- Must request membership and roles
- Agree the Acceptable Use Policy (AUP)

For JUNO:

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

Get your Digital Certificate

- In most countries there is at least one CA (Certification Authority). The CA is a certificate fabric trusted by organizations in 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/

gridpma

uctures
bership
act us

GTF
ridPMA
PMA
EDS

cuments
ter
elines
Statement Policies

PS-WG

hnical Info
istribution download
ect Locator
your local CA
t your certificate

sletter issues
scribe
ice notices

s download and fetch-crl
nical documentation
OID Registry
-2 timeline

etings
hing bei München, May 23-25,
al, January 25-27, 2022

view
das
net 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 availa as the 1.116 release with updated trust anchor information and new meta-data from the distribution w 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 documentati and download it today. This release is also available f the Fedora Extras, EPEL, and Debian repositories. **Version 3.0.22** addresses high-frequency (minute-sc update scenarios

Find your CA

Find your national or regional issuing authority with th 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 or exceed the relevant guidelines.

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

About Certificate

- Generally the certificate is automatically stored into the browser used for the request
- It is in format p12 (file with extention .p12 or .pk12) that include both private and public key
- Public key is currently called certificate
- Private key is called key

About Certificate

For GRID use the certificate must be in pem format : 2 separate files for private and public key

To do that use the openssl command under linux OS

- *openssl pkcs12 -in certificate.p12 -out userkey.pem -nocerts*
- *openssl pkcs12 -in certificate.p12 -out usercert.pem –clcerts -nokeys*

DIRAC environment implement a script to do this conversion:

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

About Certificate

- The GRID user has his certificate in format pem (2files)
- He can use an user interface
- To access the GRID resource he needs a PROXY
- The proxy is a temporary certificate that is exposed by the user job

About Certificate

- Installing the certificate in the home of UI
- Create a directory called ./globus
  - cd ~
  - mkdir .globus
- Copy the public key with name usercert.pem
  - cp certificate.pem ./globus/usercert.pem
- Copy private key with name userkey.pem
  - cp key.pem ./globus/userkey.pem

About Certificate

- The permissions of the certificate must be compliant with the request of security required by the GRID

-bash-4.2 chmod 644 .globus/usercert.pem

-bash-4.2 chmod 400 .globus/userkey.pem

-bash-4.2$ ls -l .globus

Totale 2

-rw-r--r--. 1 amartinijuno juno 3354 3 mag 15.01 usercert.pem

-r--------. 1 amartinijuno juno 1958 3 mag 15.01 userkey.pem

- Your are now ready to become a GRID user

Thank for your attention