

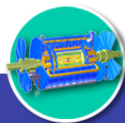
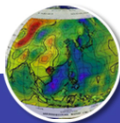
gLite Security

Dr. Marco Fargetta

Marco.Fargetta@ct.infn.it

INFN, Italy

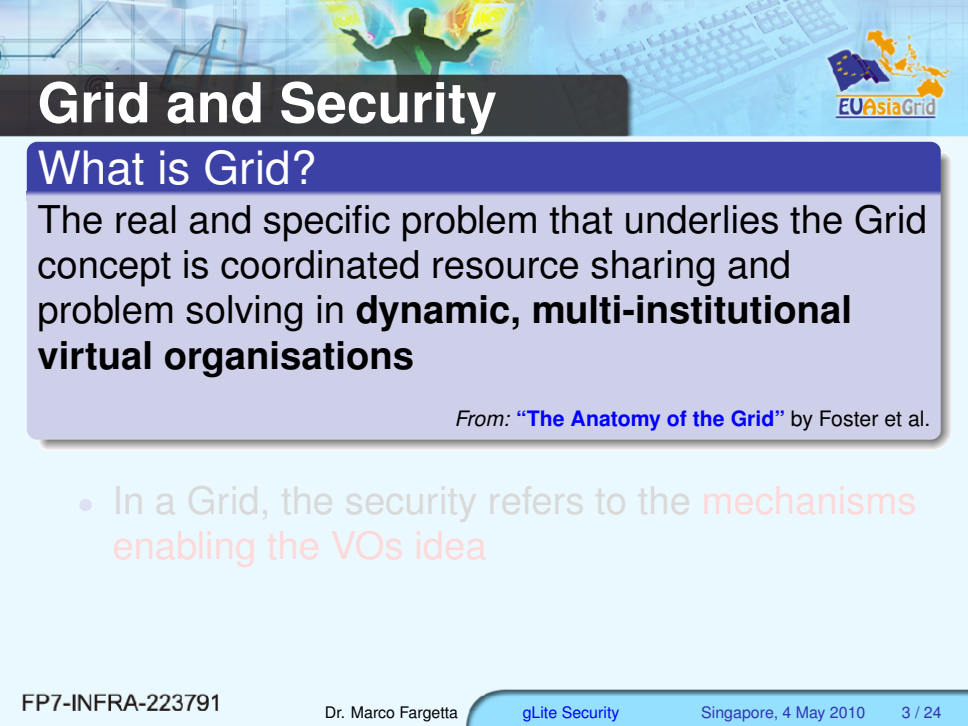
***EUAsiaGrid BioWorkshop
NUS, Singapore 2010***



Outline



- 1 Grid and Security
- 2 Security at Network Level: PKI
- 3 Security at VO level: VOMS
- 4 gLite Security Commands Interface
- 5 Conclusion



Grid and Security

What is Grid?

The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in **dynamic, multi-institutional virtual organisations**

From: "The Anatomy of the Grid" by Foster et al.

- In a Grid, the security refers to the **mechanisms enabling the VOs idea**

Grid and Security



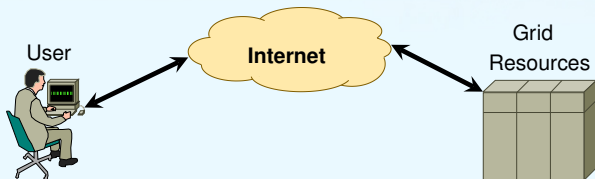
What is Grid?

The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in **dynamic, multi-institutional virtual organisations**

From: "The Anatomy of the Grid" by Foster et al.

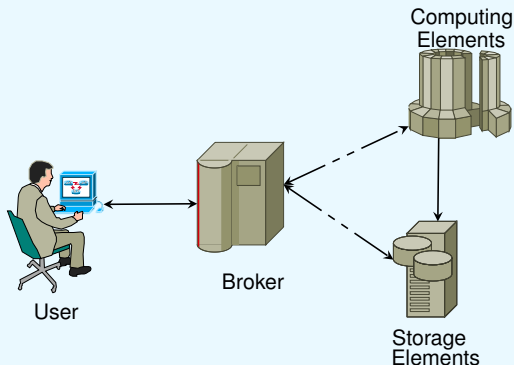
- In a Grid, the security refers to the **mechanisms enabling the VOs idea**

Network Security




- How can communication endpoints be identified?
 - Authentication
- How can a secure channel be established between two partners?
 - Encryption
 - Non-repudiation
 - Integrity

VO Security



- Which entities belong to a VO?
- What are VO members allowed to do?
 - **Authorisation**
- How can services act on behalf of a user?
 - **Delegation**



Grid Security issues



- Illegal actions deflating other sites
 - Large distributed farms of machines, perfect for launching a **Distributed Denial of Service attack**
- Illegal or inappropriate data distribution and access of sensitive information
 - Growing number of users have **data that must be private**, e.g. biomedical imaging
 - Massive distributed storage capacity ideal for **illegal sharing**, e.g. movies sharing
- Damage caused by viruses, worms etc.
 - In highly connected infrastructure **worms could spread faster** than on the Internet in general

Grid Security issues



- Illegal actions deflating other sites
 - Large distributed farms of machines, perfect for launching a **Distributed Denial of Service attack**
- Illegal or inappropriate data distribution and access of sensitive information
 - Growing number of users have **data that must be private**, e.g. biomedical imaging
 - Massive distributed storage capacity ideal for **illegal sharing**, e.g. movies sharing
- Damage caused by viruses, worms etc.
 - In highly connected infrastructure **worms could spread faster** than on the Internet in general

Grid Security issues



- Illegal actions deflating other sites
 - Large distributed farms of machines, perfect for launching a **Distributed Denial of Service attack**
- Illegal or inappropriate data distribution and access of sensitive information
 - Growing number of users have **data that must be private**, e.g. biomedical imaging
 - Massive distributed storage capacity ideal for **illegal sharing**, e.g. movies sharing
- Damage caused by viruses, worms etc.
 - In highly connected infrastructure **worms could spread faster** than on the Internet in general

Public Key Infrastructure



- The Grid authentication is based on **X.509 PKI infrastructure**
 - Certificate Authorities (CA) issue certificates identifying individuals
 - Trust between CAs and sites is established off-line
- Grid users identification is done by (short lived) **proxies** of their certificates
 - Be delegated to a service
 - Include additional attributes
 - Be stored in an external proxy store (MyProxy)
 - Be renewed (in case they are about to expire)

Public Key Infrastructure



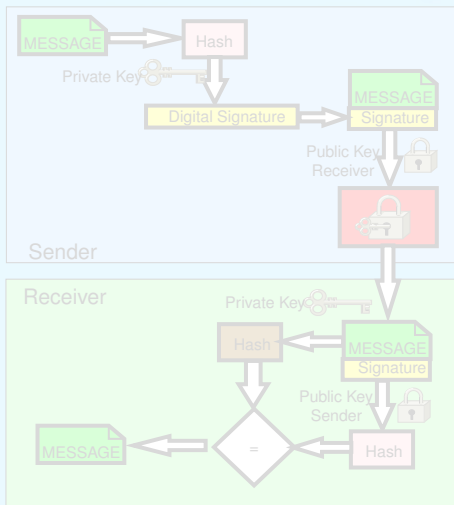
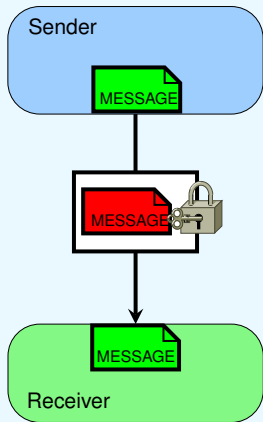
- The Grid authentication is based on **X.509 PKI infrastructure**
 - Certificate Authorities (CA) issue certificates identifying individuals
 - Trust between CAs and sites is established off-line
- Grid users identification is done by (short lived) **proxies** of their certificates
 - Be delegated to a service
 - Include additional attributes
 - Be stored in an external proxy store (MyProxy)
 - Be renewed (in case they are about to expire)

PKI in brief

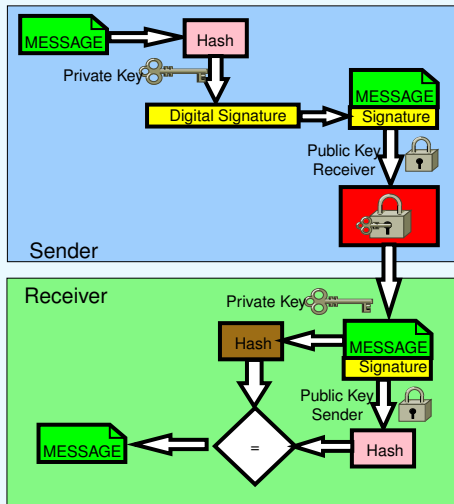
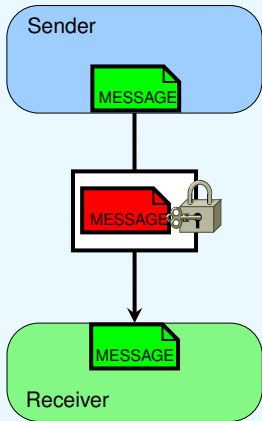


- Every networked entity (user|machine|software) is assigned with **two keys: one private key and one public key**
 - It is impossible to derive the private key from the public one
 - A message encrypted by one key can be decrypted only by the other one
- Security mechanism:
 - Public keys are exchanged
 - The sender encrypts using receiver's public key and sign with his/her private key
 - The receiver decrypts using his/her private key and verify the signature using the sender's public key

PKI in action

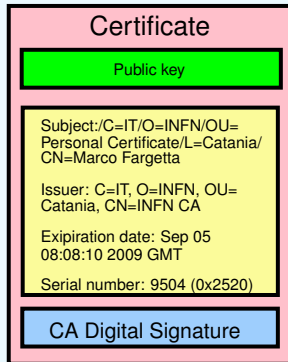


PKI in action



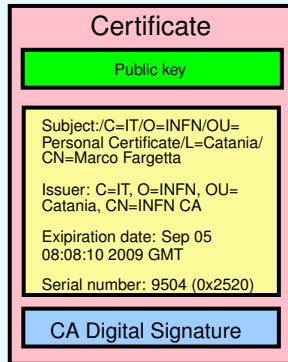
Public and Private keys

- Public key is wrapped into a “certificate file”
- Certificate file are created by trusted third parties:
Certification Authority (CA)
- Private key is stored in encrypted file
 - Protected by a pass-phrase
- Private key is created by the user



Public and Private keys

- Public key is wrapped into a “certificate file”
- Certificate file are created by trusted third parties:
Certification Authority (CA)
- Private key is stored in encrypted file
 - **Protected by a pass-phrase**
- Private key is created by the user

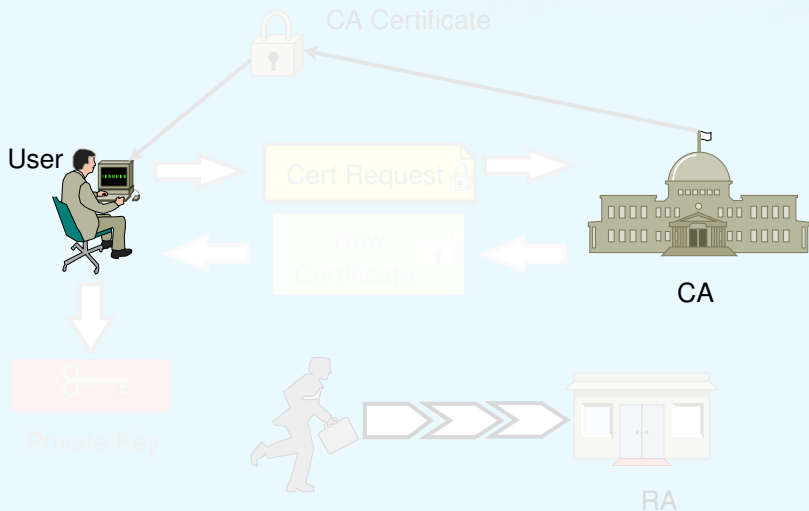


Certification Authorities

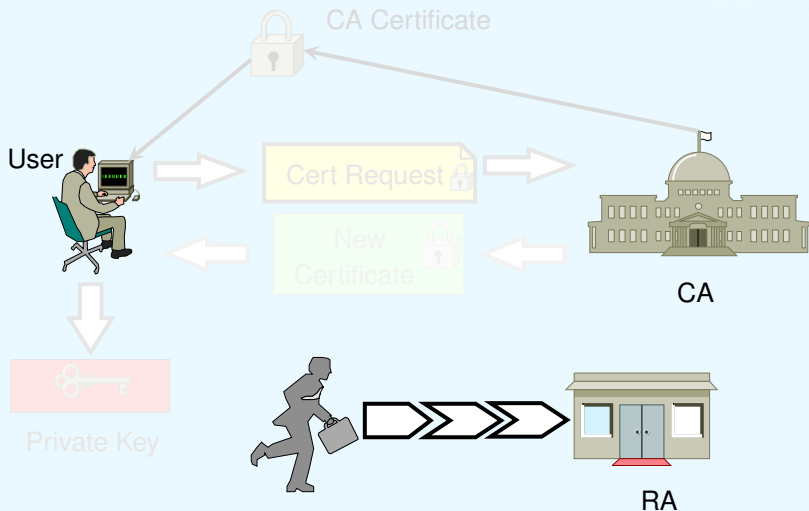


- Grid users must generate private and public key
- Public key must be **signed by a recognised CA**
 - CAs can establish a number of people Registration Authorities (RAs): Personal visit to the nearest RA instead of the national CA
- CAs recognised by EGEE:
<http://www.gridpma.org>

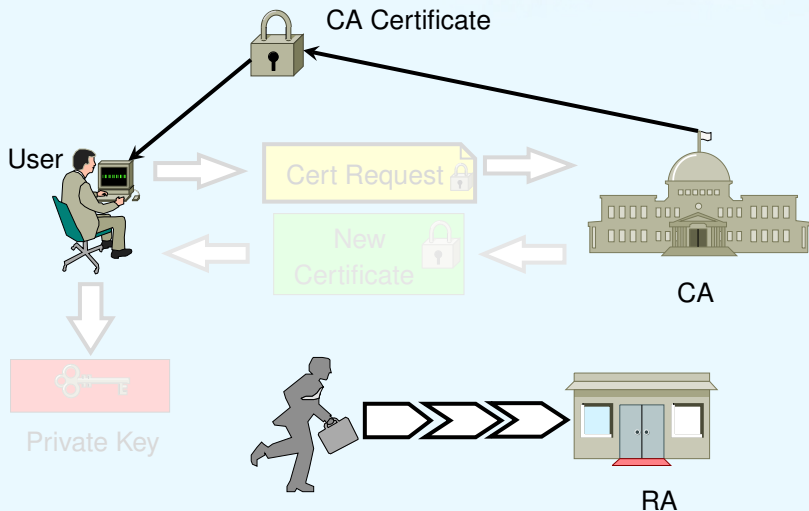
Issuing a Certificate



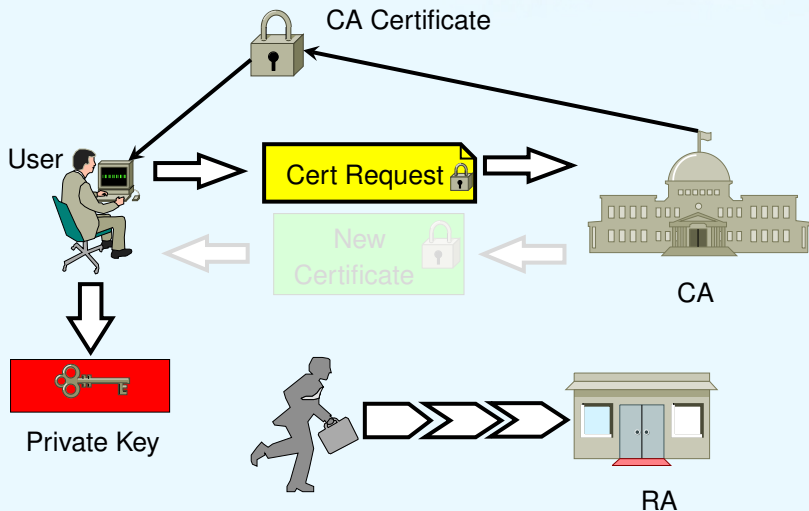
Issuing a Certificate



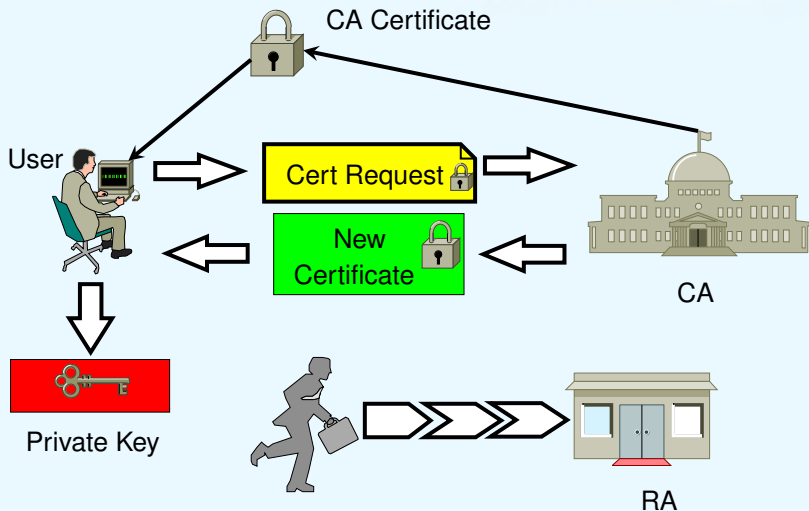
Issuing a Certificate



Issuing a Certificate



Issuing a Certificate



Private key and certificate



- Keep your private key secure
 - If your certificate is used by another user, you cannot demonstrate that was not you
- Do not loan your certificate to anyone
- Report any problem to your CA

Location in gLite and other middleware

```
$ ls -l .globus
total 24
-rw-r--r--  1 marco  users 1806 Mar  3  2008 usercert.pem
-r-----  1 marco  users 1910 Mar  3  2008 userkey.pem
```

Private key and certificate



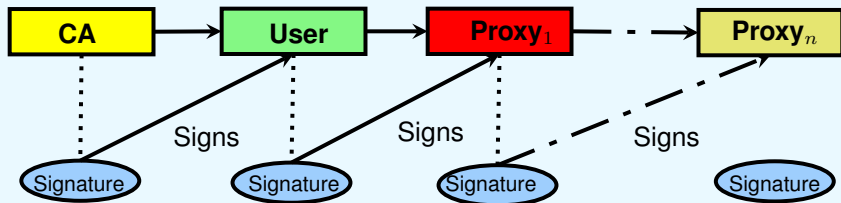
- Keep your private key secure
 - If your certificate is used by another user, you cannot demonstrate that was not you
- Do not loan your certificate to anyone
- Report any problem to your CA

Location in gLite and other middleware

```
$ ls -l .globus
total 24
-rw-r--r--  1 marco users 1806 Mar  3  2008 usercert.pem
-r-----  1 marco users 1910 Mar  3  2008 userkey.pem
```

Identity Delegation

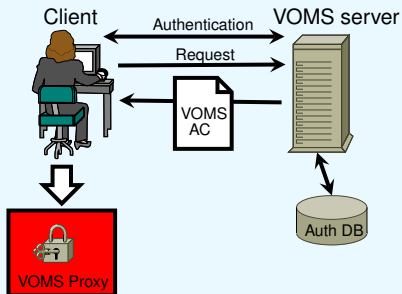
- Delegation allows remote process and services to **authenticate on behalf of the user**
- Achieved by the creation of a new private key - certificate pair signed by the user
 - New key-pair is a single file: **Proxy credential**
 - Proxy private key is not protected by password
 - Proxy has limited lifetime



VO manager: VOMS

Virtual Organisation Membership Service (VOMS)

- Extends the proxy with info on **VO membership, group, roles**
- Fully compatible with GSI
- Each VO has a database containing group membership, roles and capabilities informations for each user
- User contacts VOMS server requesting his authorisation info
- Server sends authorisation info to the client, which includes it in a proxy certificate



FQAN and AC

- VOMS uses the **Fully Qualified Attribute Name (FQAN)** to express membership and other authorisation info
- Groups membership, roles and capabilities may be expressed in a format that bounds them together
 - `<group>/Role=[<role>] [/Capability=<capability>]`
- **Attribute Certificates** are used to bind a set of attributes (like membership, roles, authorisation info etc) with an identity
- ACs are digitally signed
- VOMS uses AC to include the attributes of a user in a proxy certificate

gLite Security Commands



- **voms-proxy-init**
 - Create the proxy (i.e. login to the Grid)
 - Require the passphrase protecting the private key
 - Common Options:
 - `-voms <vo_name>`
 - `-hours <credential lifetime>`
 - `-vomslife <VOMS attribute lifetime>`
- **voms-proxy-destroy**
 - Destroy the existing proxy (i.e. logout from the Grid)
- **voms-proxy-info**
 - Provide proxy related information

Proxy with GENIUS



- Using GENIUS web portal it is possible to create a proxy
- If the proxy exists in the UI it will be used
 - For the hands-on proxy will be available in the UI
- After the log-out proxies are destroyed

Proxy with GENIUS



File Edit View History Bookmarks Tools Help

https://glite-tutor.ct.infn.it/ Google

Welcome to the GENIUS Grid Portal

INFN Enabling Grids for E-science
genius
enginframe
NICE

Grid Enabled web + Network for
Independent User job Submission

Job Data Interactive Preferences VO Services

*.p12 or *.pfx file
infn/Certificate/infn/MyPrFN2010.p12 Select

Insert the certificate's export password
***** Check

Proxy lifetime (seconds): 12000

Back Clean Create

Proxy with VOMS Extension

Group name: /giida/

Role name: Role=

Capability name: Capability=

Applet Time Life
Available time: 00:09:00

Copyright © 1998 - 2010 Nice S.r.l. All trademarks and logos on this page are owned by NICE S.r.l. or by their respective owners.

Long term proxy: MyProxy

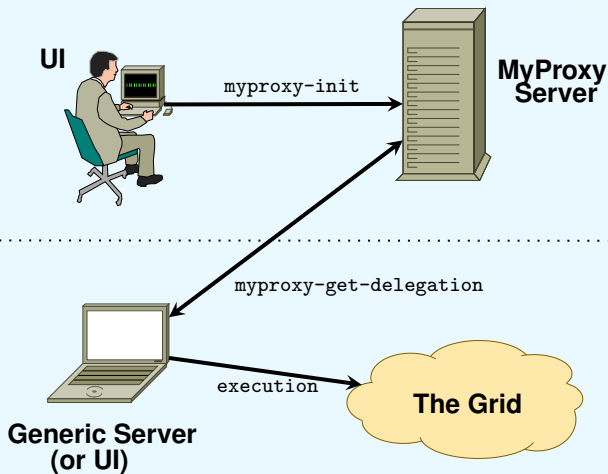


- Proxy has limited lifetime (default is 12 h)
 - **Bad idea to have longer proxy**
 - A grid Job can need a longer time to complete
- **MyProxy** server allows to use long term proxy
 - `myproxy-init` stores a proxy on MyProxy server
 - `myproxy-info` get information about stored proxy
 - `myproxy-get-delegation` get a new proxy from the server
- A service on the **WMS** can renew automatically the proxy
- The **File transfer services** in gLite uses MyProxy to validates user request and eventually **renew proxies**

Long term proxy: MyProxy

- Proxy has limited lifetime (default is 12 h)
 - **Bad idea to have longer proxy**
 - A grid Job can need a longer time to complete
- **MyProxy** server allows to use long term proxy
 - `myproxy-init` stores a proxy on MyProxy server
 - `myproxy-info` get information about stored proxy
 - `myproxy-get-delegation` get a new proxy from the server
- A service on the **WMS** can **renew automatically the proxy**
- The **File transfer services** in gLite uses MyProxy to validates user request and eventually **renew proxies**

Authentication with MyProxy



Summary



- The security system of gLite is **based on PKI**
 - Users are identified by certificates
- Activities delegation performed by means of proxy certificate
- **VOMS server connects user to VOs**, groups and roles adding attributes to the proxy certificate
- Long term **proxy can be stored on MyProxy server** for later retrieval

References



- GGF Security Group
http://www.ogf.org/gf/group_info/areasgroups.php?area_id=7
- VOMS Core User and Reference Guide
<https://edms.cern.ch/file/973684/1/voms-guide.pdf>
- MyProxy Server
<http://grid.ncsa.illinois.edu/myproxy/>



Questions?