Authorization and Authentication in gLite

Roberto Barbera
Univ. of Catania and INFN

Third EELA Tutorial
Rio de Janeiro, 26-30.06.2006

www.eu-eela.org

Information Society and Media

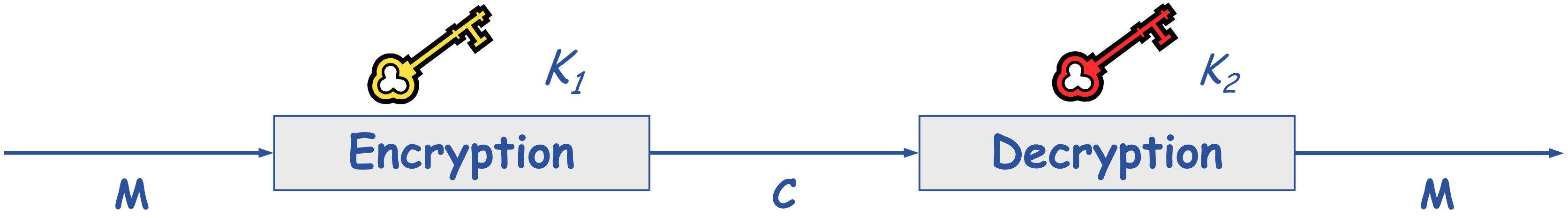
Overview

- **Glossary**
- **Encryption**
  - Symmetric algorithms
  - Asymmetric algorithms: PKI
- **Certificates**
  - Digital Signatures
  - X509 certificates
- **Grid Security**
  - Basic concepts
  - Grid Security Infrastructure
  - Proxy certificates
  - Command line interfaces
- **Virtual Organization**
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS

Glossary

- **Principal**
  - An entity: a user, a program, or a machine
- **Credentials**
  - Some data providing a proof of identity
- **Authentication**
  - Verify the identity of a principal
- **Authorization**
  - Map an entity to some set of privileges
- **Confidentiality**
  - Encrypt the message so that only the recipient can understand it
- **Integrity**
  - Ensure that the message has not been altered in the transmission
- **Non-repudiation**
  - Impossibility of denying the authenticity of a digital signature

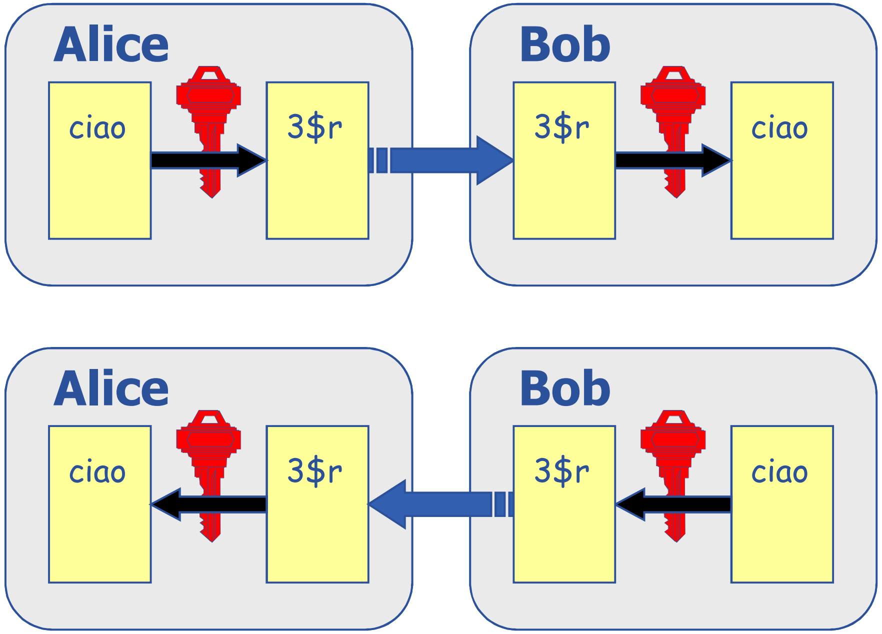
Cryptography



- Mathematical algorithms that provide important building blocks for the implementation of a security infrastructure
- Symbology
  - Plaintext: *M*
  - Cyphertext: *C*
  - Encryption with key K_1 : $E_{K_1}(M) = C$
  - Decryption with key K_2 : $D_{K_2}(C) = M$
- Algorithms
  - Symmetric: $K_1 = K_2$
  - Asymmetric: $K_1 \neq K_2$

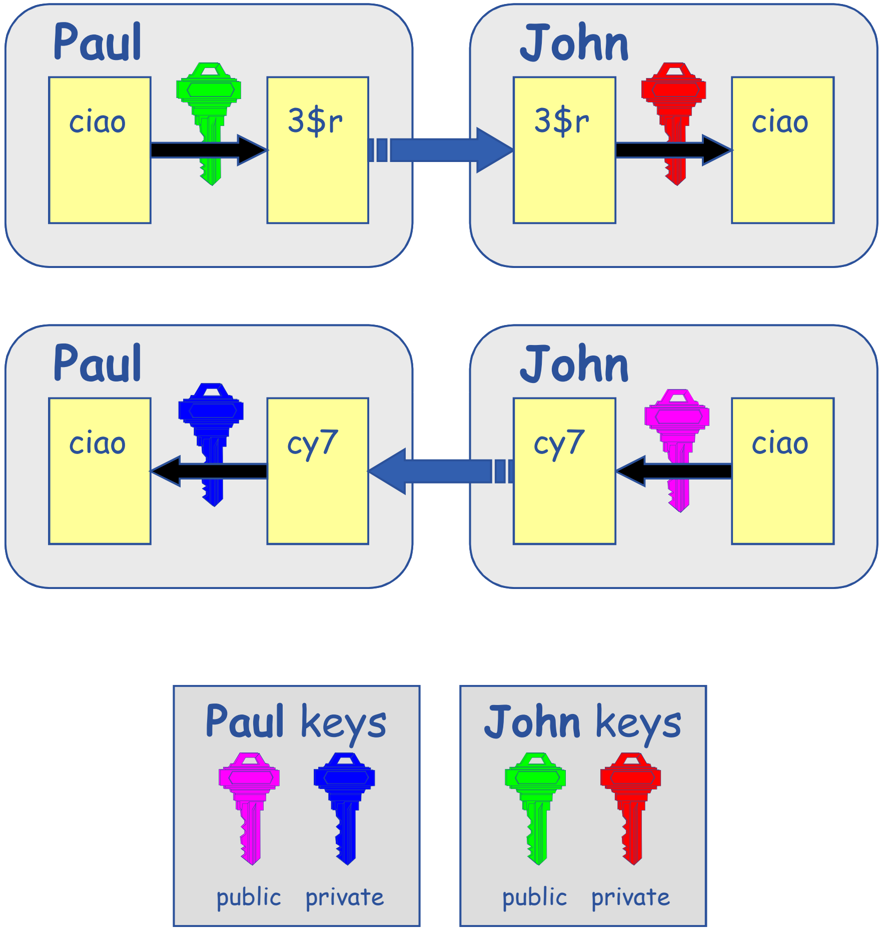
Symmetric Algorithms

- The same key is used for encryption and decryption
- Advantages:
  - Fast
- Disadvantages:
  - how to distribute the keys?
  - the number of keys is O(n^2)
- Examples:
  - **DES**
  - **3DES**
  - **Rijndael** (AES)
  - **Blowfish**
  - **Kerberos**



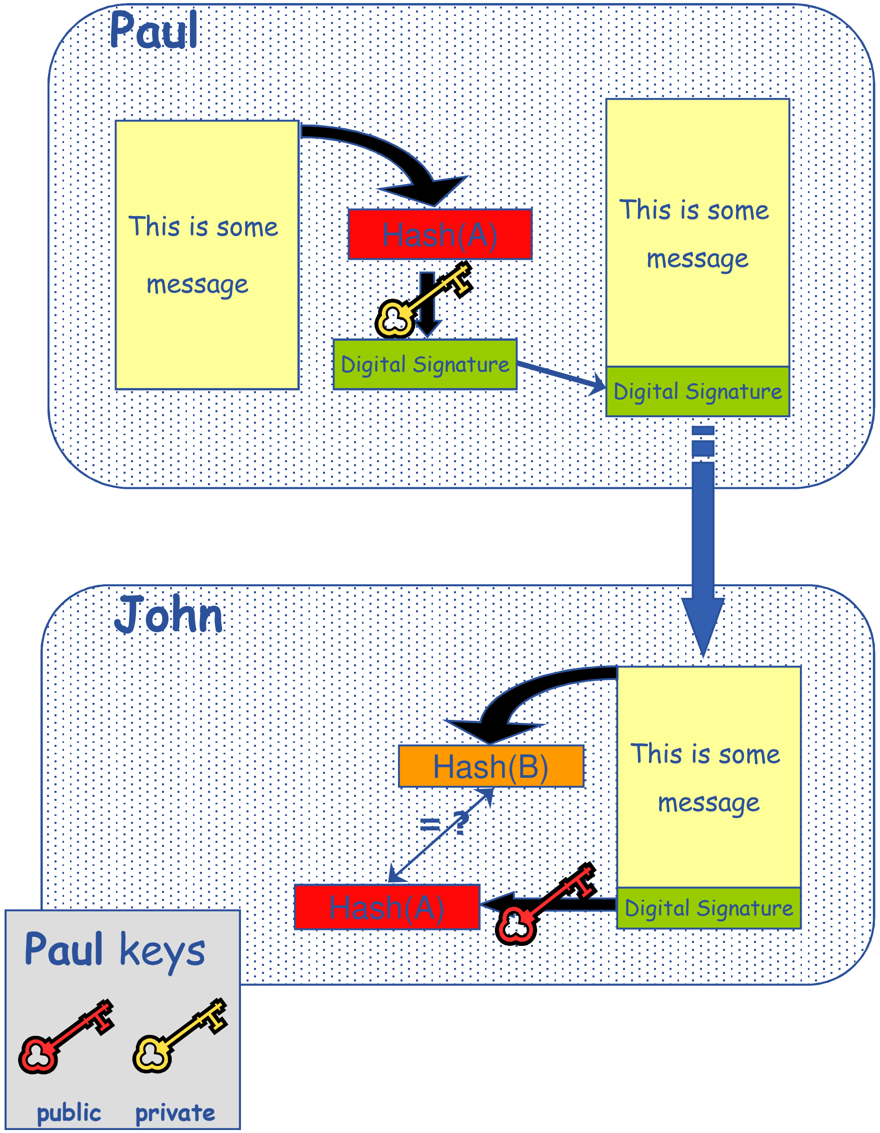
Public Key Algorithms

- **Every user has two keys: one *private* and one *public*:**
  - 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.
- **No exchange of secrets is necessary**
  - the sender cyphers using the *public* key of the receiver;
  - the receiver decrypts using his *private* key;
  - the number of keys is O(n).
- **Examples:**
  - **Diffie-Helmann** (1977)
  - **RSA** (1978)



Digital Signature

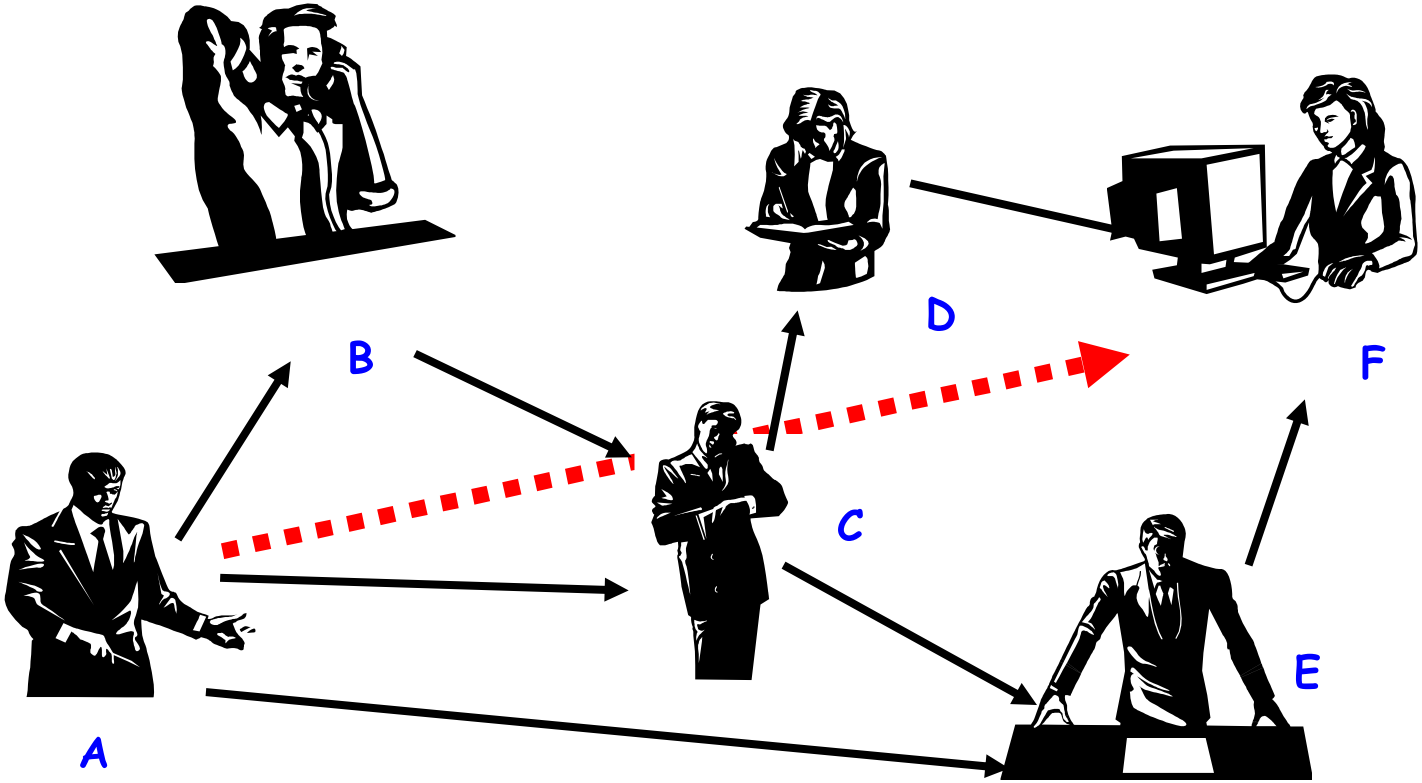
- Paul **calculates the** *hash* **of the message (with a one-way hash function)**
- Paul **encrypts the hash using his** *private* **key: the encrypted hash is the** *digital signature*.
- Paul **sends the signed message to** John.
- John **calculates the hash of the message and** *verifies* **it with A, decyphered with Paul’s** *public* **key.**
- **If hashes equal: message wasn’t modified;** Paul **cannot repudiate it.**



Digital Certificates

- Paul’s digital signature is safe if:
  1. Paul’s private key is not compromised
  2. John knows Paul’s public key
- How can John be sure that Paul’s public key is really Paul’s public key and not someone else’s?
  - A *third party* guarantees the correspondence between public key and owner’s identity.
  - Both A and B must trust this third party
- Two models:
  - X.509: hierarchical organization;
  - PGP: “web of trust”.

PGP “web of trust”



- F knows D and E, who knows A and C, who knows A and B.
- F is reasonably sure that the key from A is really from A.

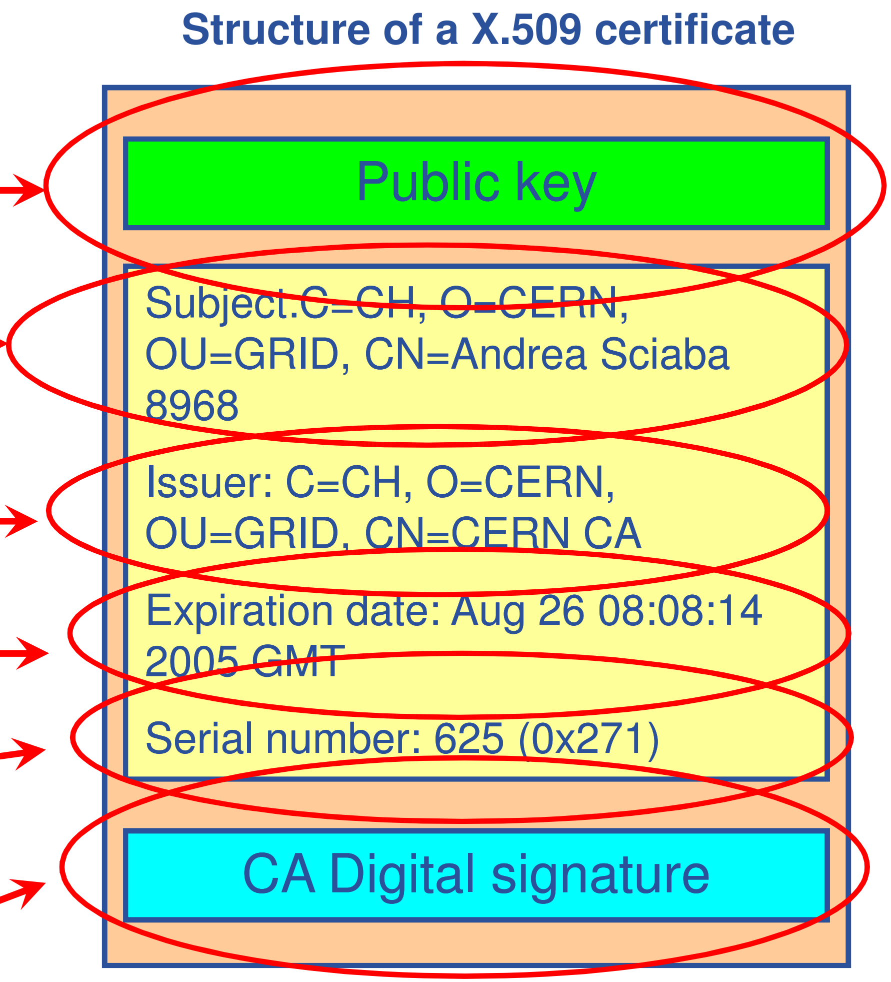
X.509

The "third party" is called *Certification Authority* (CA).

- Issue Digital Certificates (containing public key and owner's identity) for users, programs and machines (signed by the CA)
- Check 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

X.509 Certificates

- An X.509 Certificate contains:
  - owner's public key;
  - identity of the owner;
  - info on the CA;
  - time of validity;
  - Serial number;
  - digital signature of the CA



Structure of a X.509 certificate

Public key

Subject:C=CH, O=CERN, OU=GRID, CN=Andrea Sciaba 8968

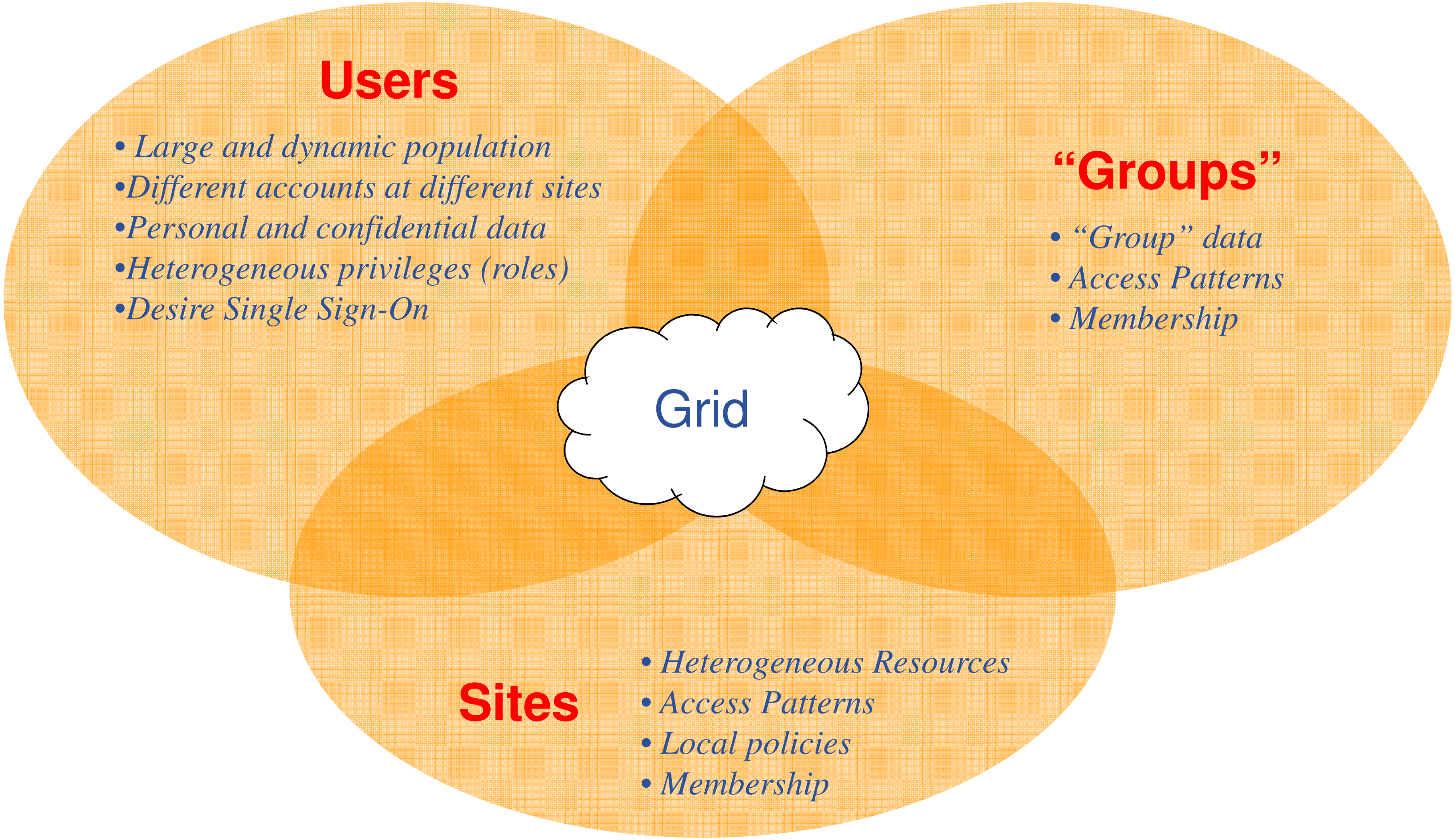
Issuer: C=CH, O=CERN, OU=GRID, CN=CERN CA

Expiration date: Aug 26 08:08:14 2005 GMT

Serial number: 625 (0x271)

CA Digital signature

GRID Security: the players



Users

- Large and dynamic population
- Different accounts at different sites
- Personal and confidential data
- Heterogeneous privileges (roles)
- Desire Single Sign-On

“Groups”

- “Group” data
- Access Patterns
- Membership

Sites

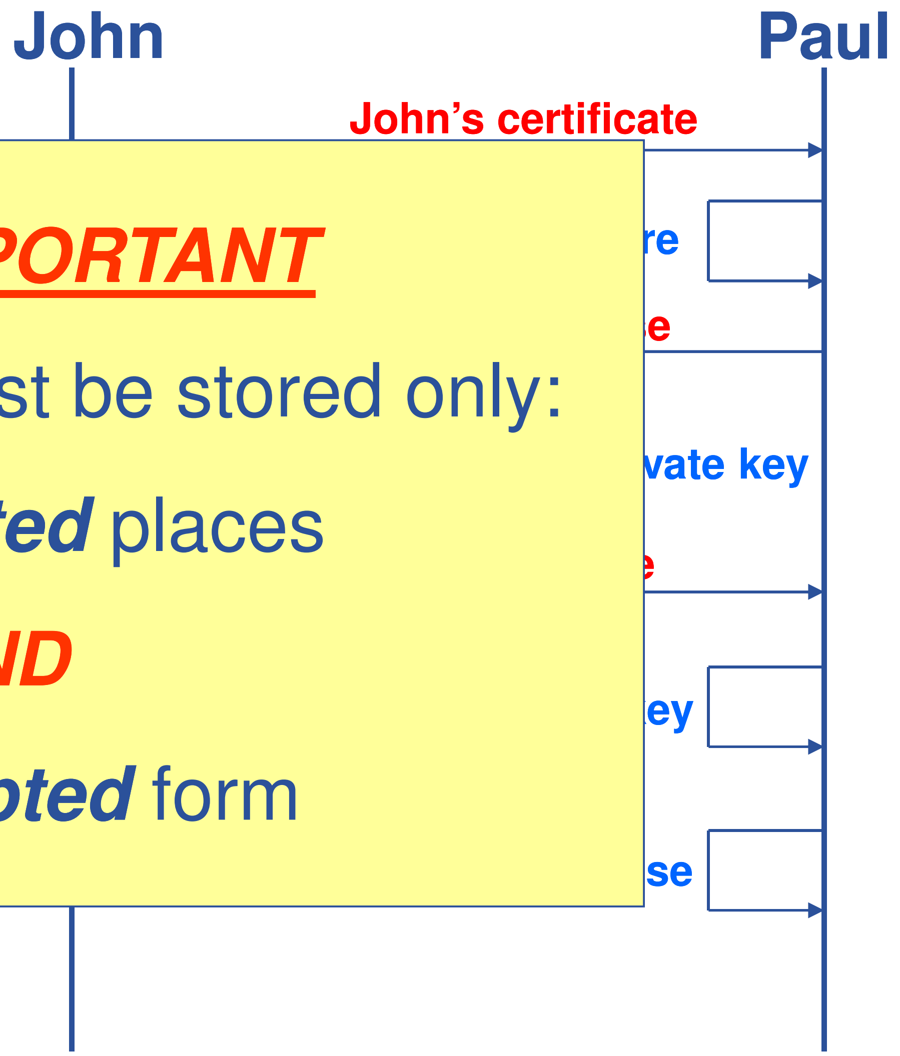
- Heterogeneous Resources
- Access Patterns
- Local policies
- Membership

The Grid Security Infrastructure (GSI)

Based on X.509 PKI:

- every user/host/service has an X.509 certific
- certific local s
- every authen

1. Jo
2. Pa ce
3. Pa
4. Jo his
5. Jo Pa
6. Pa the
7. Paul compares the decrypted string with the original challenge
8. If they match, Paul verified John's identity and John can not repudiate it.



VERY IMPORTANT

Private keys must be stored only:

in ***protected*** places

AND

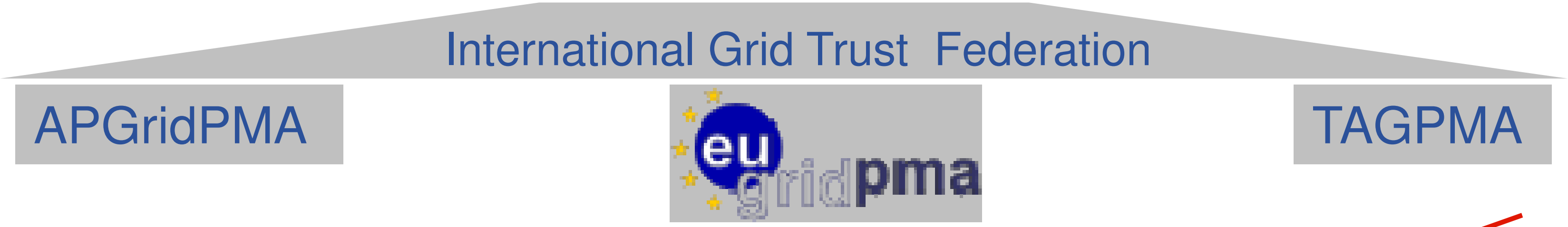
in ***encrypted*** form

More on Authentication

- **In the grid world one single CA usually covers a predefined geographic region or administrative domain:**
  - Organization
  - Country
  - A set of countries
- **A common trust domain for grid computing has been created to join the several existing certification authorities into a single authentication domain and thus enabling sharing of grid resources worldwide.**
  - The International Grid Trust Federation (IGTF) has been created to coordinate and manage this trust domain.
  - IGTF is divided in three Policy Management Authorities (PMAs) covering the Asia Pacific, Europe and Americas.

IGTF

International Grid Trust Federation
(Working to Establish Worldwide Trust for Grids)
www.gridpma.org



International Grid Trust Federation

APGridPMA

eu gridpma

TAGPMA

APGridPMA

- AIST Japan
- APAC Australia
- ASGCC Taiwan
- SDG China
- IHEP China
- KISTI Korea
- Naregi Japan
- BMG Singapore
- CMSD India
- HKU Hong Kong
- NCHC Taiwan
- Osaka U. Japan
- USM Malaysia

eu gridpma

- NorduGrid Nordic countries
- PolishGrid Poland
- Russian Datagrid Russia
- SlovakGrid Slovakia
- DataGrid-ES Spain
- UK e-Science United Kingdom
- BelnetGrid Belgium
- Grid-PK Pakistan
- FNAL Grid USA
- GridCanada Canada
- DOEGrids USA
- ArmeSFo Armenia
- IUCC Israel
- ASCCG Taiwan
- SeeGrid Europe
- RMKI Hungary
- SWITCH Switzerland
- DFN Germany
- RDIG Russia
- LIP CA Portugal
- CERN CA Switzerland
- ArmeSFO Armenia
- CNRS Grid France
- CyGrid Cyprus
- CESNET Czech
- DutchGrid Netherlands
- GermanGrid Germany
- HellasGrid Greece
- GridIreland Ireland
- INFN CA Italy
- Belnet Belgium
- Grid-PK Pakistan
- SIGNET Slovenia
- EstonianGrid Estonia
- AustrianGrid Austria
- NIIF/HungarNet Hungary
- IHEP China
- BalticGrid Europe
- TR-Grid Turkey

TAGPMA

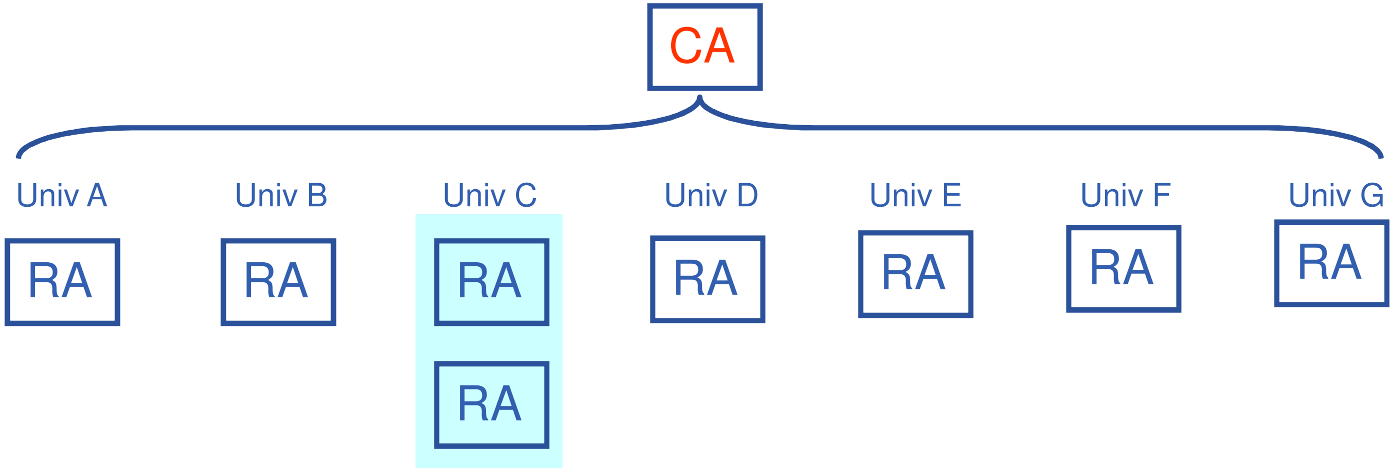
- **EELA** ←
- Dartmouth College
- Texas High Energy Grid
- FNAL USA
- SDSC Centre
- TeraGrid
- Open Science Grid
- DOEGrids
- CANARIE

Classic Profile of CA

- **What is it:**
  - The CA signs and revokes certificates
  - These are long-term certificates (one year)
  - The CA has subordinate RAs that just perform the administrative task of checking the subject identity in different organizations or departments
- **Advantages:**
  - Is the most known CA profile
  - A lot of know-how and solutions do exist
  - Most of the CAs operating today use the classic profile
  - Is the easiest to support across administrative domains
  - The SLCS profile is still under discussion
  - The profile requirements are stable and controlled by EUgridPMA

Classic Profile of a CA

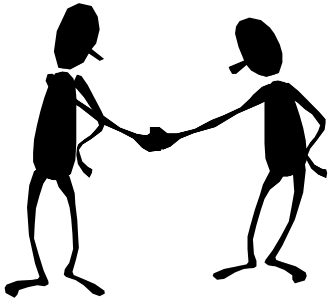
- **A network of subordinated RAs is necessary to perform the identity verification of the subjects**
- **The RAs will be created at the level of the organizations or at the level of departments:**
  - Operating at university or research centre wide level (more difficult)
  - Operating at the level of a department or group
  - The CA can also operate an RA but don't forget that the physical presence of the subject is required for identity verification
  - It is fine to have more than one RA per university or research centre if they are operating for different departments
- **The RAs should be created only upon request, their creation should be user driven.**



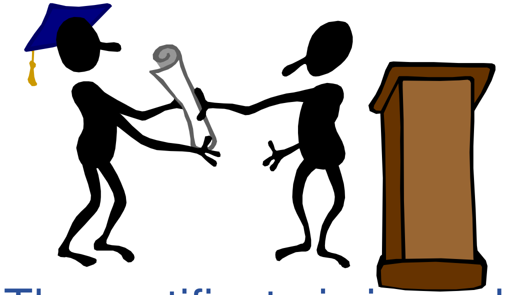
Classic profile of a CA

- **How to obtain a certificate:**

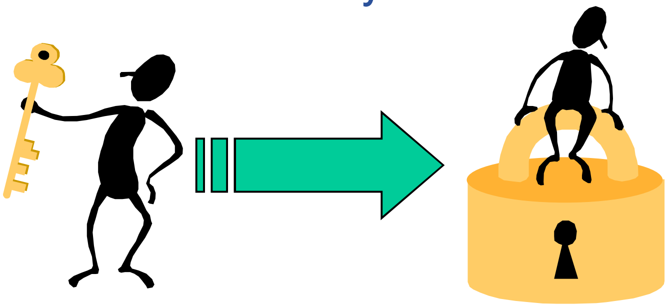
A certificate request is performed



The user identify is confirmed by the RA



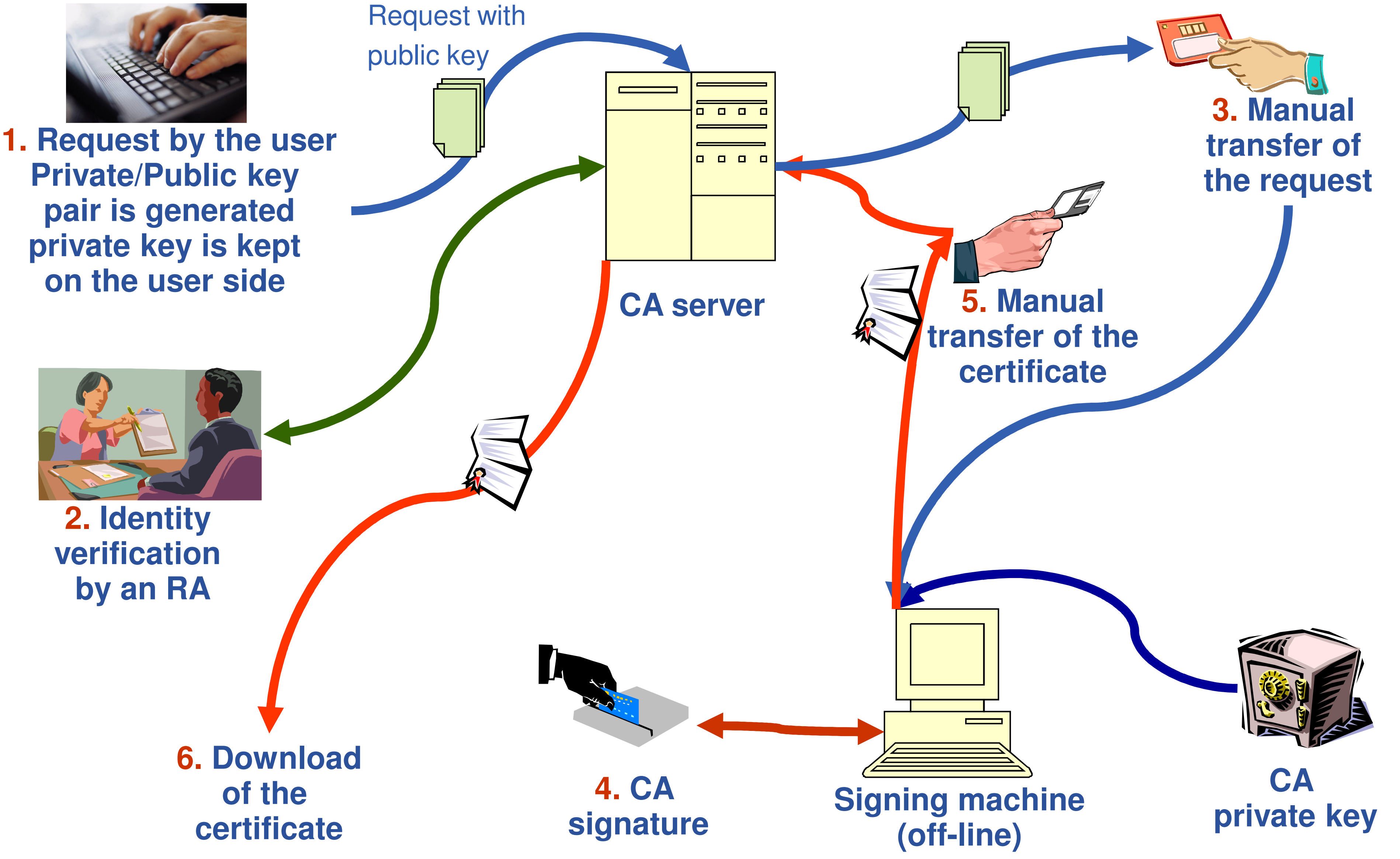
The certificate is issued by the CA



The certificate is used as a key to access the grid

E-infrastructure shared between Europe and Latin America

Certificate issuance in more detail



Request with public key

1. Request by the user Private/Public key pair is generated private key is kept on the user side

CA server

3. Manual transfer of the request

5. Manual transfer of the certificate

2. Identity verification by an RA

6. Download of the certificate

4. CA signature

Signing machine (off-line)

CA private key

Revocation Lists

- **The CAs have the obligation of issue Certificate Revocation Lists (CRL)**
- **The CRLs contain:**
  - a list of the revoked certificates
  - the date when they were issued
  - the end date
- **CRLs are signed with the CA private key**
- **The CRLs must be published so that the relying parties can check the validity of the certificates**
  - Usually available through http://

The Classic CA Profile

- **There should be a single Certification Authority (CA) organisation per country, large region or international organization.**
  - Provide a short number of stable CAs
- **CAs must be operated as a long-term commitment**
  - They should remain operational after the end of the project
- **A network of Registration Authorities (RA) for each CA is responsible for authentication of requests**
- **The CA will handle the task of:**
  - issuing CRLs
  - signing Certificates/CRLs
  - revoking Certificates

CA profile: Identity

- **Any single subject distinguished name (DN) must be linked to one and only one entity**
  - DNs must be unique
- **Over the entire lifetime of the CA a DN must not be linked to any other entity**
- **One entity can have more than one subject name for different key usages**
  - One user can have more than one certificate
  - One server can have more than one certificate
- **Certificates must not be shared among end entities**
  - A certificate cannot be shared with other users
  - CAs and RAs must immediately revoke these certificates when such a violation of the CP/CPS is detected

CA profile: CP/CPS Identification

- **Every CA must have a Certification Policy and Certificate Practice Statement**
- **For new CAs the CP/CPS documents must be structured as defined in RFC 3647**
  - This is a new format. Most CP/CPS were written in RFC 2527
  - Examples:
    - PkirisGrid
    - AustrianGrid
- **Major CP/CPS changes must be:**
  - announced to the accrediting PMA
  - approved before signing any certificates under the new CP/CPS
- **All the CP/CPS under which valid certificates are issued must be available on the web (many examples can be found at http://www.eugridpma.org/members and http://www.tagpma.org/members)**

RA operations

- **The operation of the RAs must be:**
  - in accordance with the CA CP/CPS
  - defined in a document for each RA
- **The RA operation in general:**
  - Each RA must have one responsible person (manager)
    - A deputy is advisable
  - The manager can nominate one or more operators
  - Both the manager and the operators can authorize requests
  - All RA personnel must be trained in CA/RA operations and security
  - The selection method of the personnel should be defined
  - The CA must be informed officially of any change of RA personnel (eg: a letter signed and stamped)
  - The first manager must be identified/authenticated by the CA in person
  - Each RA should have a unique namespace (subject DN prefix) to avoid DN name collisions
  - The community supported by the RA must be well defined
  - The method used to identify subjects must be fully described including the enforcement of any additional requirements imposed by the CA or by the RA (eg. relation with an organization)

CA/RA namespaces

- **The namespace definition is of the responsibility of the CA however depending on this definition the RA can also be involved eg. (just an example based on the LIP CA namespace ...)**
  - /C=PT/O=LIPCA/
    - CA prefix should be unique across CAs
  - /C=PT/O=LIPCA/O=UMINHO
    - The second /O= designates the organization of the subject and also the RA
  - /C=PT/O=LIPCA/O=UMINHO/OU=DI
    - The /OU=DI in the LIP case is optional and can be used to identify a department within the organization
    - It is used to designate an RA within the organization when an organization has multiple RAs

CA/RA namespaces

- **About the CN and full DN:**
  - /C=PT/O=LIPCA/O=UMINHO/OU=DI/CN=Jose A Sousa
    - each DN must be unique:
      - *Long enough to avoid collisions*
      - *Add something (number,...) when duplications are found*
      - *Possibly using the person full name is the best option*
    - each DN must be bound to the same subject for the lifetime of the CA
    - The CN must have a clear direct relation with the DN
    - Don’t forget that the certificates are for grid computing, don’t create names (or extensions) that may create problems for the middleware
    - Please don’t use accents
    - Some characters may have special meanings for the applications (eg. The “-” character is recognized by globus as an wildcard)
    - Some characters are not allowed (eg. “/” and “.” in user certificates)

Renewal

- **Two types of renewals:**
  - End entities certificate renewals
  - CA certificate renewals
- **End entities:**
  - The certificates maximum lifetime is 1 year + 1 month
  - The idea is that at the end of the year (12th month) a new certificate is issued
  - Users (EE) should be warned about the coming expiration and the need to renew
  - Since the new certificate will be issued at the end of the 12th month (or beginning of the 13th) there will be an overlap of two certificates:
    - this is used to avoid a situation where the certificate will expire rendering the service or the user without grid access
    - don't forget there are users submitting jobs that may take days or weeks
    - during this period there will be two certificates with the same DN
  - Don't revoke a certificate to issue a new one unless the certificate has been compromised or the user has ceased his activity or liaison which entitles him to have a certificate

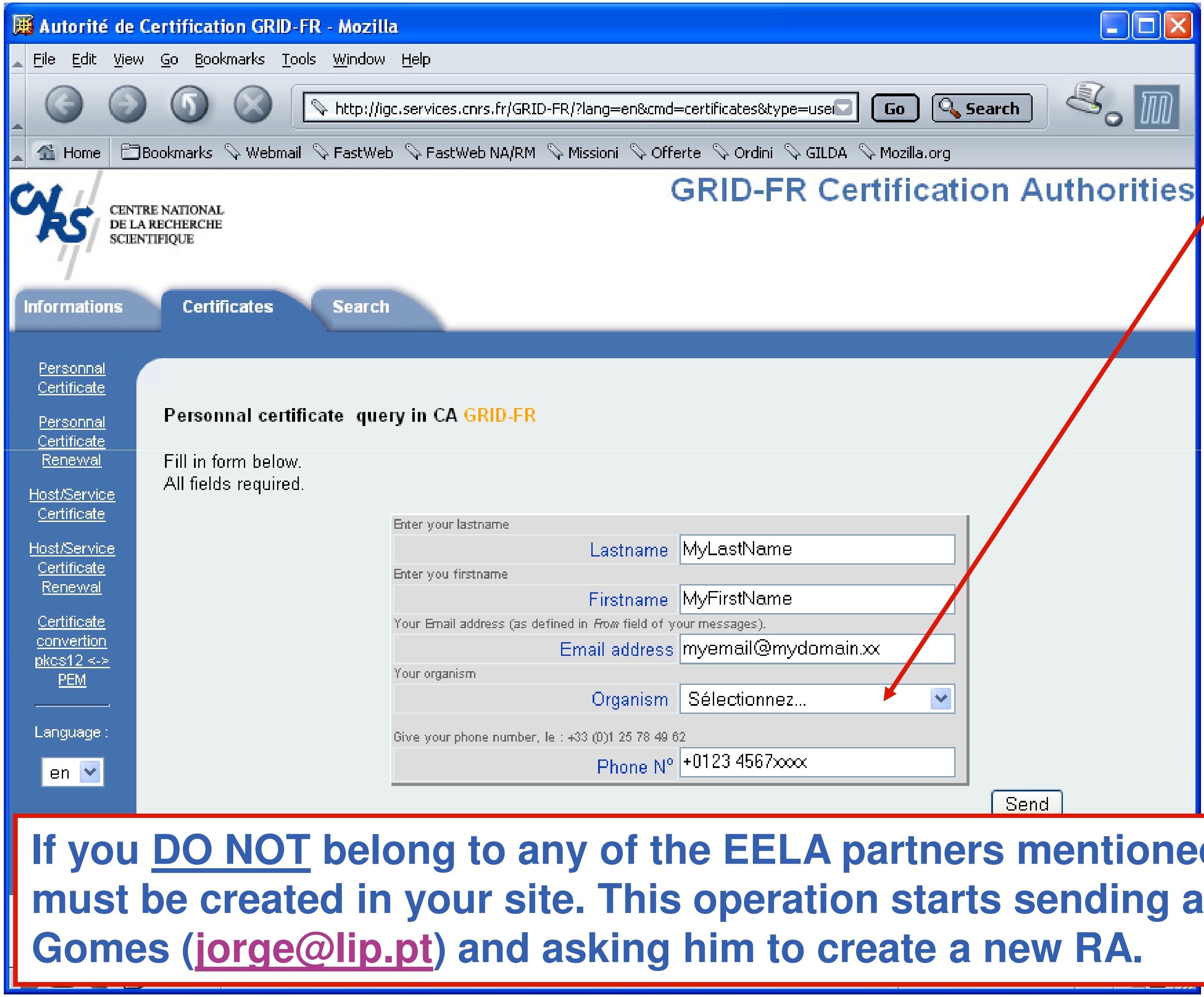
Renewal

- **End entities:**
  - During a renewal it is not required to make the EE to pass through the identification procedure:
    - This is a big advantage for both the EE and the RA
    - However a maximum renewal number without identification is advisable (for instance: every two years the EE must pass through the identification again)
    - However the relation with the organization should still be performed (if this requirement is being used)
  - In order not to pass through the identification the renewal request must be signed with the user certificate, examples:
    - Email signed with user certificate
    - CA/RA Web interface that would identify the user certificate
  - If the user certificate expires before renewal the procedure for a new certificate must be followed

Request a Personal Certificate to Work in EELA

- If you are **Italian** go to:
  - https://security.fi.infn.it/CA/en/RA/
- If you are **Portuguese** go to:
  - http://ca.lip.pt/
- If you are **Spanish** go to:
  - http://www.irisgrid.es/pki/
- If you are **not any of the above** go to:
  - http://igc.services.cnrs.fr/GRID-FR/?lang=en&cmd=certificates&type=usercert

Request a Certificate to the GRID-FR CA


Autorité de Certification GRID-FR - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://igc.services.cnrs.fr/GRID-FR/?lang=en&cmd=certificates&type=user
Go
Search
Home
Bookmarks
Webmail
FastWeb
FastWeb NA/RM
Missioni
Offerte
Ordini
GILDA
Mozilla.org
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
GRID-FR Certification Authorities
Informations
Certificates
Search
Personnal Certificate
Personnal Certificate Renewal
Host/Service Certificate
Host/Service Certificate Renewal
Certificate convertion pkcs12 <-> PEM
Language :
en
Send

Personnal certificate query in CA GRID-FR

Fill in form below.
All fields required.

Enter your lastname
Lastname: MyLastName

Enter you firstname
Firstname: MyFirstName

Your Email address (as defined in *From* field of your messages).
Email address: myemail@mydomain.xx

Your organism
Organism: Sélectionnez...

Give your phone number, ie : +33 (0)1 25 78 49 62
Phone N°: +0123 4567xxxx

Working RA's are:

1. ICN-UNAM
2. REUNA
3. UFF
4. UFRJ
5. ULA

If you DO NOT belong to any of the EELA partners mentioned above, a new RA must be created in your site. This operation starts sending an email to Jorge Gomes (jorge@lip.pt) and asking him to create a new RA.

Certificate management

- Import your certificate in your browser
  - If you received a .pem certificate you need to convert it to PKCS12
  - Use *openssl* command line (available in each UI)
    - `openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out my_cert.p12 -name 'My Name'`

- GILDA (and other VOs, among which EELA):
  - You receive already a PKCS12 certificate (can import it directly into the web browser)
  - For future use, you will need *usercert.pem* and *userkey.pem* in a directory ~/.globus on your UI
  - Export the PKCS12 cert to a local dir on UI and use again *openssl:*
    - `openssl pkcs12 -nocerts -in my_cert.p12 -out userkey.pem`
    - `openssl pkcs12 -clcerts -nokeys -in my_cert.p12 -out usercert.pem`

X.509 Proxy Certificate

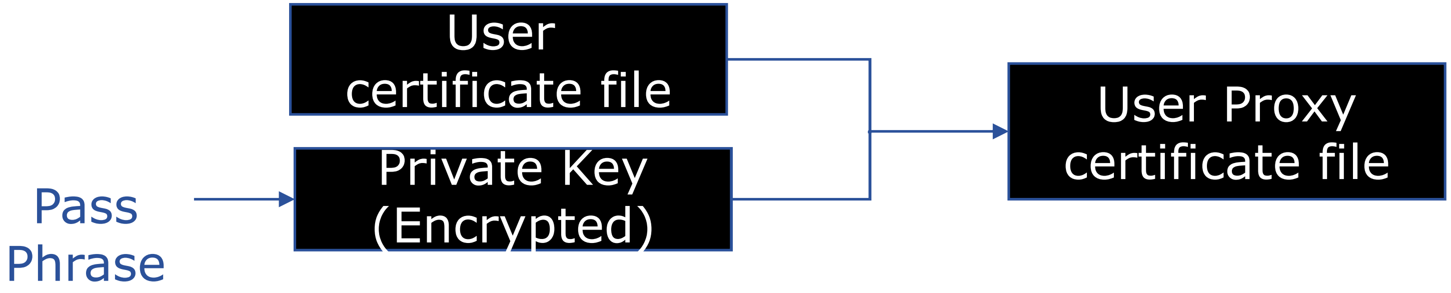
- GSI extension to X.509 Identity Certificates
  - signed by the normal end entity cert (or by another proxy).
- Enables single sign-on
- Support some important features
  - Delegation
  - Mutual authentication
- Has a limited lifetime (minimized risk of “compromised credentials”)
- It is created by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

```
% grid-proxy-init
Enter PEM pass phrase: ******
```

  - Options for grid-proxy-init:
    - -hours <lifetime of credential>
    - -bits <length of key>
    - -help

grid-proxy-init

- User enters pass phrase, which is used to decrypt private key.
- Private key is used to sign a proxy certificate with its own, new public/private key pair.
  - User's private key not exposed after proxy has been signed



- Proxy placed in /tmp
  - the private key of the Proxy is *not* encrypted:
  - stored in local file: must be readable **only** by the owner;
  - proxy lifetime is short (typically 12 h) to minimize security risks.
- NOTE: *No* network traffic!

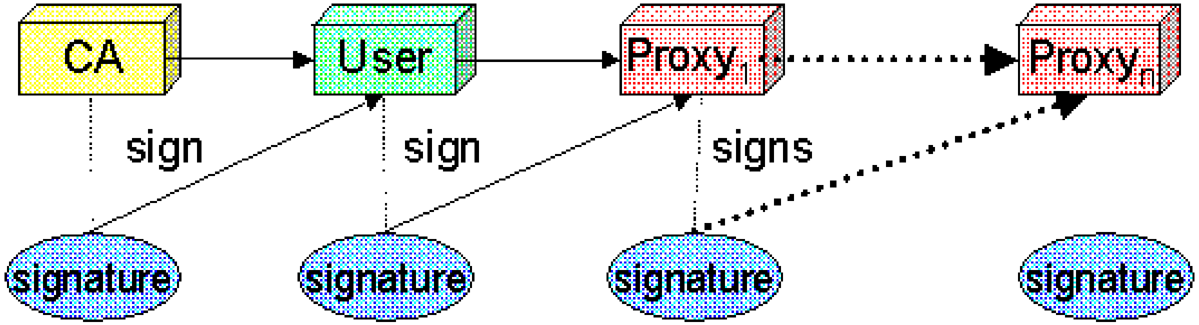
Proxy again ...

- grid-proxy-init ≡ “login to the Grid”
- To “logout” you have to destroy your proxy:
  - `grid-proxy-destroy`
  - This does *NOT* destroy any proxies that were delegated from this proxy.
  - You cannot revoke a remote proxy
  - Usually create proxies with short lifetimes
- To gather information about your proxy:
  - `grid-proxy-info`
  - Options for printing proxy information

    -subject
    -type
    -strength
    -issuer
    -timeleft
    -help

Delegation

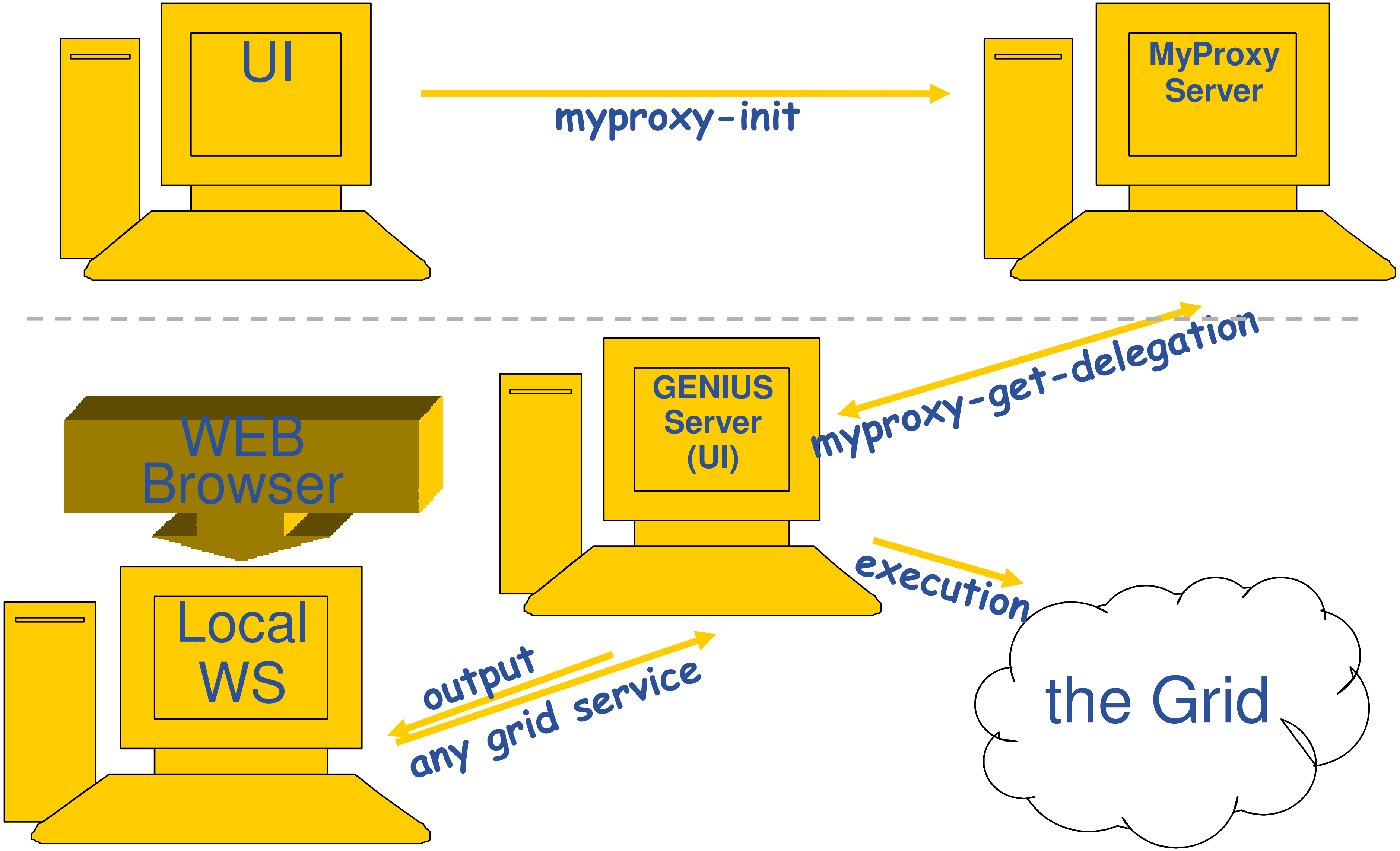
- Delegation = remote creation of a (second level) proxy credential
  - New key pair generated remotely on server
  - Client signs proxy cert and returns it
- Allows remote process to authenticate on behalf of the user
  - Remote process "impersonates" the user



Long term proxy

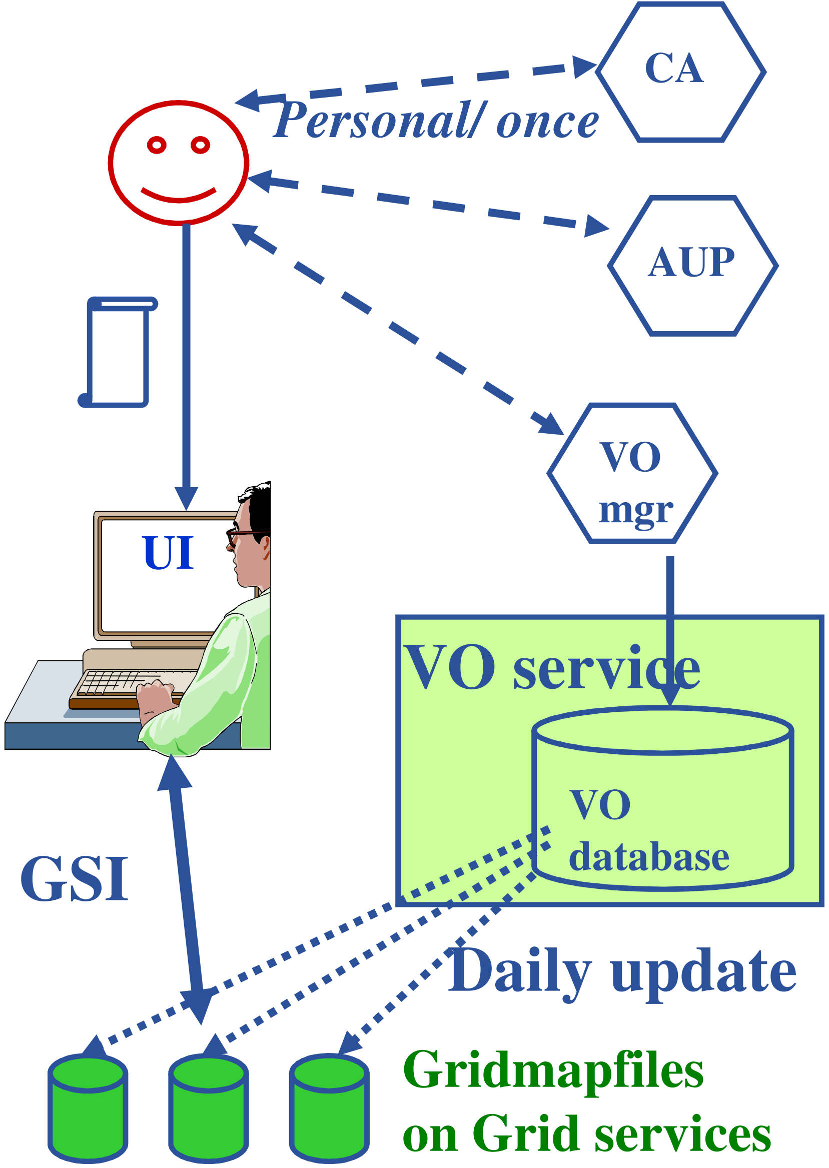
- Proxy has limited lifetime (default is 12 h)
  - Bad idea to have longer proxy
- However, a grid task might need to use a proxy for a much longer time
  - Grid jobs in HEP Data Challenges on LCG last up to 2 days
- myproxy server:
  - Allows to create and store a long term proxy certificate:
  - myproxy-init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

Grid authentication with MyProxy



Authentication, Authorisation: pre-VOMS

- **Authentication**
  - User receives certificate signed by CA
  - Connects to "UI" by ssh
  - Downloads certificate
  - **Single logon to Grid** – create proxy - then **Grid Security Infrastructure identifies user to other machines**
- **Authorisation**
  - User joins Virtual Organisation
  - VO negotiates access to Grid nodes and resources
  - Authorisation tested by CE
  - gridmapfile maps user to local account



VOs and authorization

- Grid users MUST belong to virtual organizations
  - What we previously called “groups”
  - Sets of users belonging to a collaboration
  - User must sign the usage guidelines for the VO
  - You will be registered in the VO server (wait for notification)

- VOs maintained a list of their members on a LDAP Server
  - The list is downloaded by grid machines to map user certificate subjects to local “pool” accounts

```
...
"/C=CH/O=CERN/OU=GRID/CN=Simone Campana 7461" .dteam
"/C=CH/O=CERN/OU=GRID/CN=Andrea Sciaba 8968" .cms
"/C=CH/O=CERN/OU=GRID/CN=Patricia Mendez Lorenzo-ALICE" .alice
...
```

  - Sites decide which vos to accept
    - /etc/grid-security/grid-mapfile

Evolution of VO management

Before VOMS

- User is authorised as a member of a single VO
- All VO members have same rights
- Gridmapfiles are updated by VO management software: map the user's DN to a local account
- grid-proxy-init – derives proxy from certificate – the "single sign-on to the grid"

VOMS

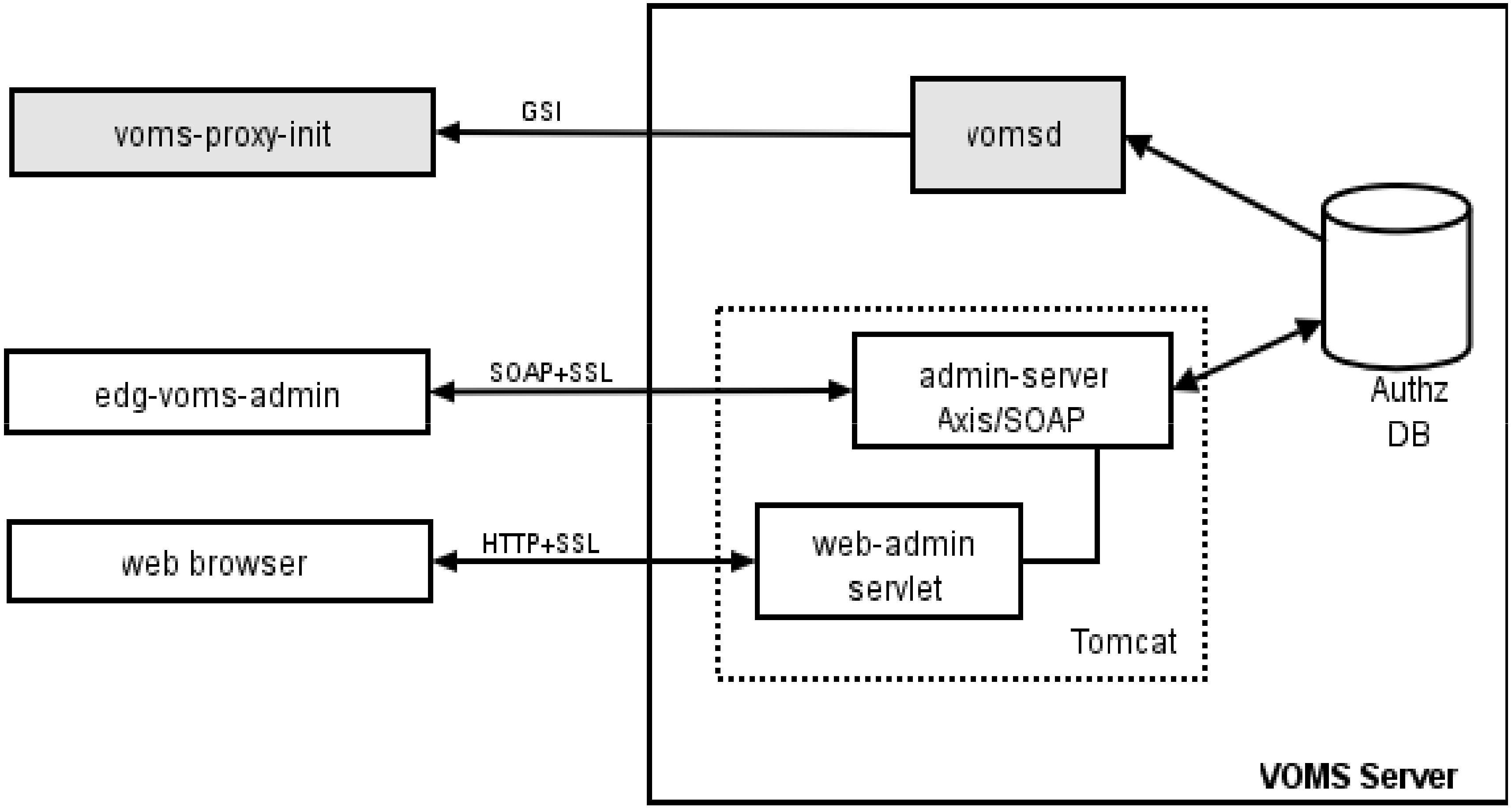
- User can be in multiple VOs
  - Aggregate rights
- VO can have groups
  - Different rights for each
    - Different groups of experimentalists
    - …
  - Nested groups
- VO has roles
  - Assigned to specific purposes
    - E,g. system admin
    - When assume this role
- Proxy certificate carries the additional attributes
- voms-proxy-init

VOMS: concepts

- Virtual Organization Membership Service
  - Extends the proxy with info on VO membership, group, roles
  - Fully compatible with Globus Toolkit
  - Each VO has a database containing group membership, roles and capabilities informations for each user
  - User contacts voms server requesting his authorization info
  - Server send authorization info to the client, which includes them in a proxy certificate

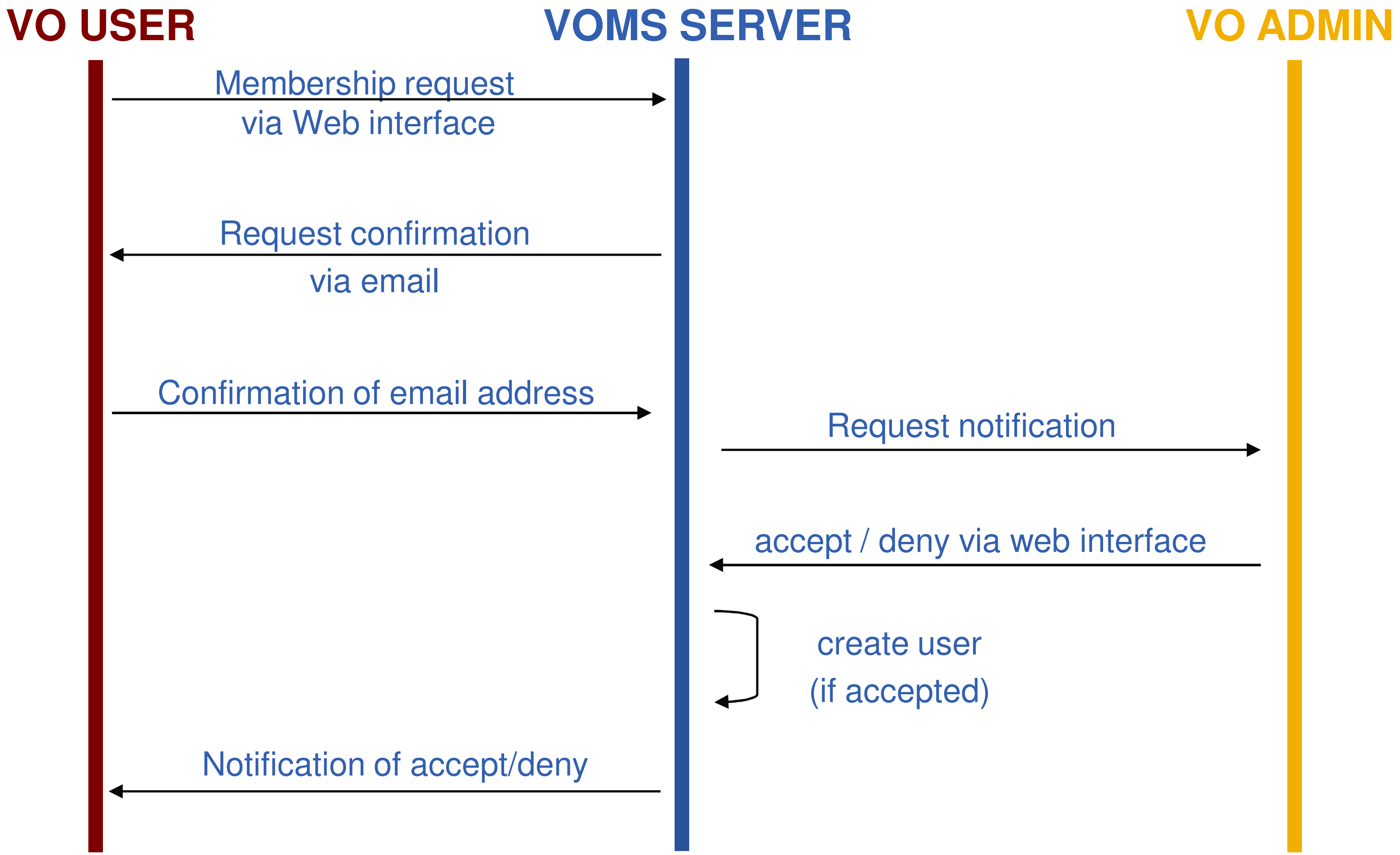
```
[glite-tutor] /home/giorgio > voms-proxy-init --voms gilda
Cannot find file or dir: /home/giorgio/.glite/vomses
Your identity: /C=IT/O=GILDA/OU=Personal
Certificate/L=INFN/CN=Emidio
Giorgio/Email=emidio.giorgio@ct.infn.it
Enter GRID pass phrase:
Your proxy is valid until Mon Jan 30 23:35:51 2006
Creating temporary proxy...............................Done
Contacting  voms.ct.infn.it:15001 [/C=IT/O=GILDA/OU=Host/L=INFN
Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it]
"gilda"
Creating proxy ...................................... Done
Your proxy is valid until Mon Jan 30 23:35:51 2006
```

VOMS - components



- **Authz DB is a RDBMS (currently MySQL and Oracle are supported).**

Registration process



VO USER

VOMS SERVER

VO ADMIN

Membership request via Web interface

Request confirmation via email

Confirmation of email address

Request notification

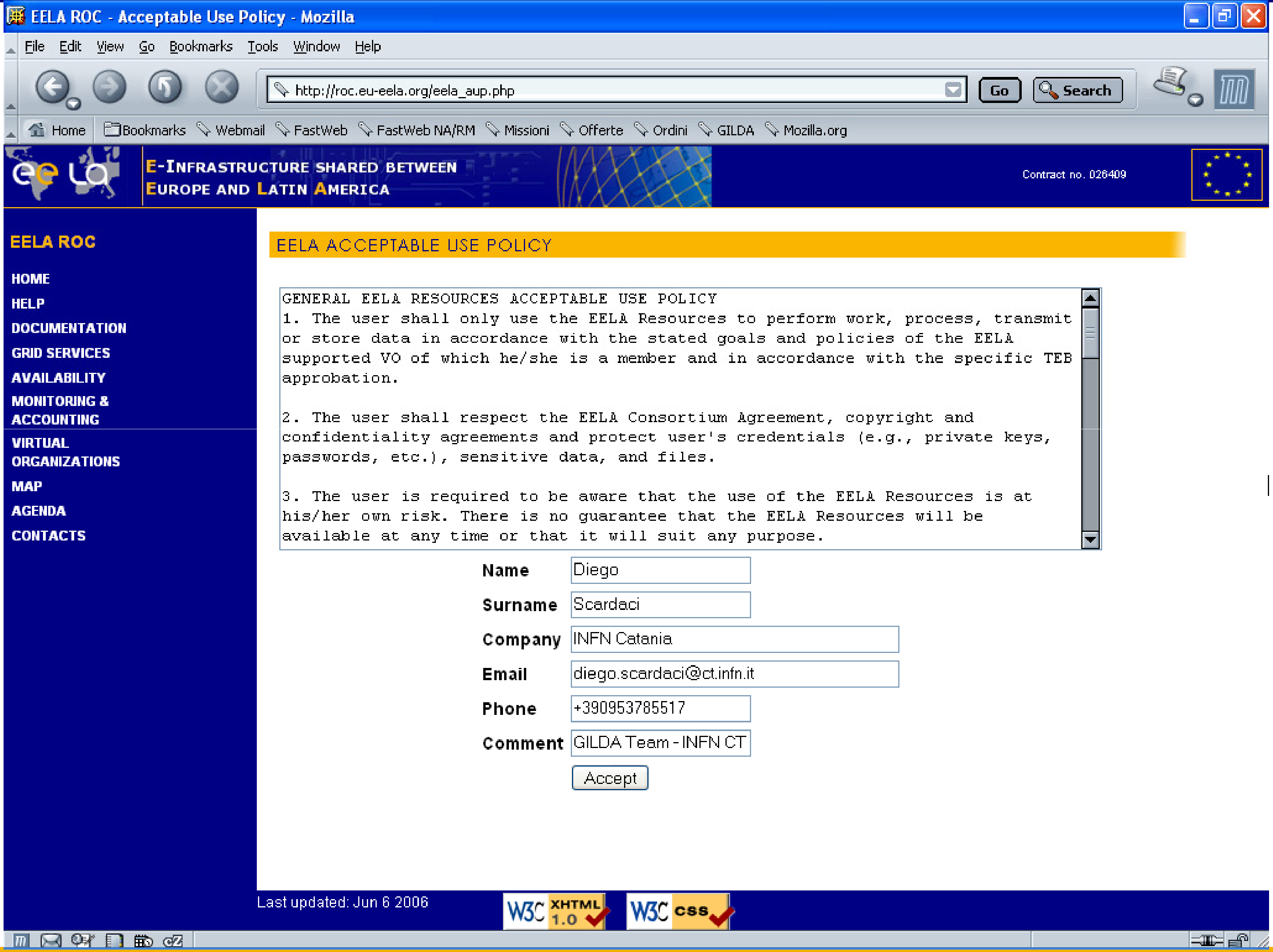
accept / deny via web interface

create user (if accepted)

Notification of accept/deny

EELA VO Usage Rules (http://roc.eu-eela.org/eela_aup.php)

E-infrastructure shared between Europe and Latin America


EELA ROC - Acceptable Use Policy - Mozilla
File Edit View Go Bookmarks Tools Window Help
http://roc.eu-eela.org/eela_aup.php
Go
Search
Home Bookmarks Webmail FastWeb FastWeb NA/RM Missioni Offerte Ordini GILDA Mozilla.org
E-Infrastructure shared between Europe and Latin America
Contract no. 026409
EELA ROC
HOME
HELP
DOCUMENTATION
GRID SERVICES
AVAILABILITY
MONITORING & ACCOUNTING
VIRTUAL ORGANIZATIONS
MAP
AGENDA
CONTACTS

EELA ACCEPTABLE USE POLICY

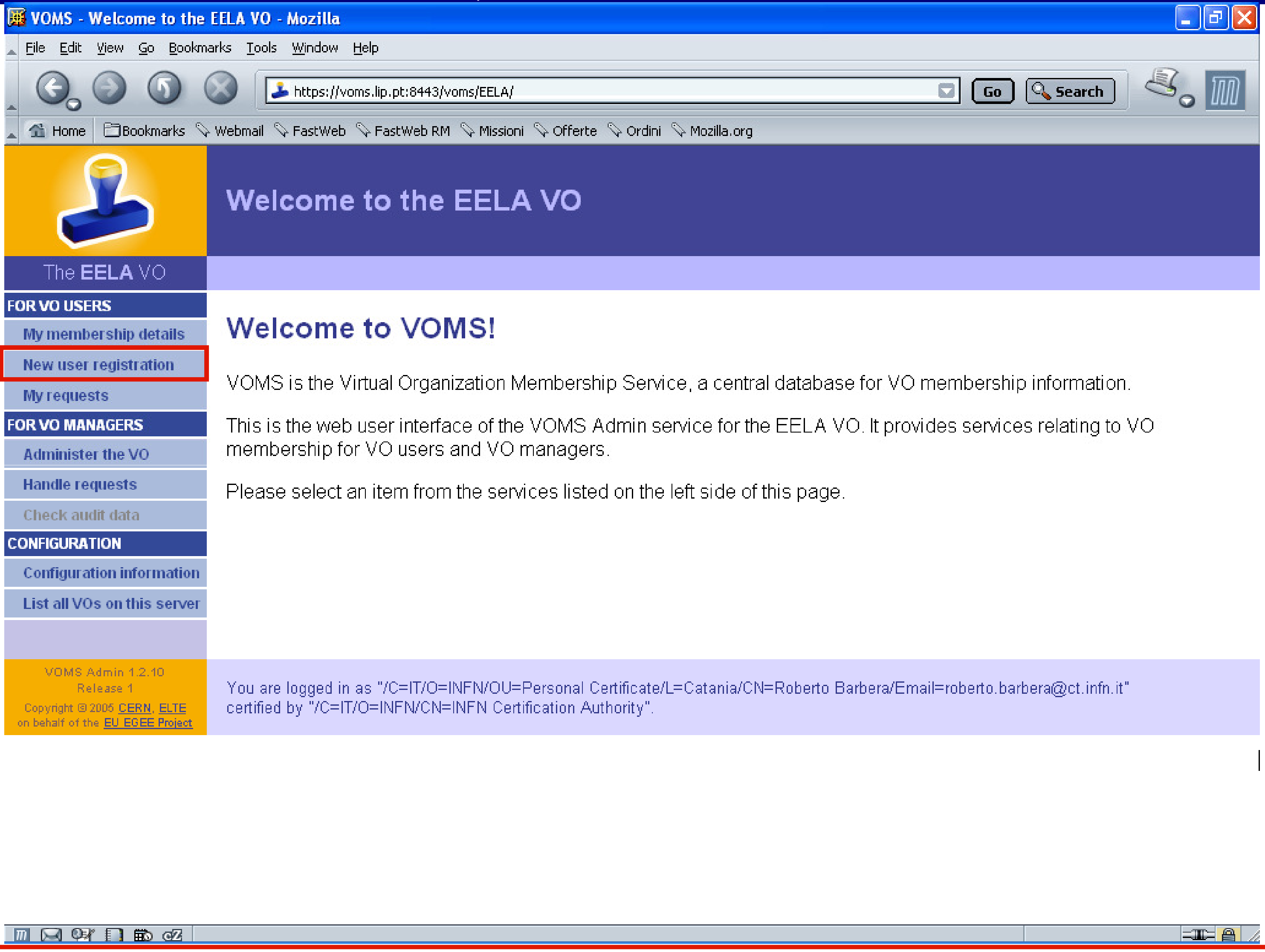
```
GENERAL EELA RESOURCES ACCEPTABLE USE POLICY
1. The user shall only use the EELA Resources to perform work, process, transmit
or store data in accordance with the stated goals and policies of the EELA
supported VO of which he/she is a member and in accordance with the specific TEB
approbation.

2. The user shall respect the EELA Consortium Agreement, copyright and
confidentiality agreements and protect user's credentials (e.g., private keys,
passwords, etc.), sensitive data, and files.

3. The user is required to be aware that the use of the EELA Resources is at
his/her own risk. There is no guarantee that the EELA Resources will be
available at any time or that it will suit any purpose.
```

Name	Diego
Surname	Scardaci
Company	INFN Catania
Email	diego.scardaci@ct.infn.it
Phone	+390953785517
Comment	GILDA Team - INFN CT

EELA VOMS
(https://voms.lip.pt:8443/voms/EELA/)


VOMS - Welcome to the EELA VO - Mozilla
File Edit View Go Bookmarks Tools Window Help
https://voms.lip.pt:8443/voms/EELA/
Go
Search
Home
Bookmarks
Webmail
FastWeb
FastWeb RM
Missioni
Offerte
Ordini
Mozilla.org

Welcome to the EELA VO

The EELA VO

FOR VO USERS
- My membership details
- New user registration
- My requests

FOR VO MANAGERS
- Administer the VO
- Handle requests
- Check audit data

CONFIGURATION
- Configuration information
- List all VOs on this server

Welcome to VOMS!

VOMS is the Virtual Organization Membership Service, a central database for VO membership information.

This is the web user interface of the VOMS Admin service for the EELA VO. It provides services relating to VO membership for VO users and VO managers.

Please select an item from the services listed on the left side of this page.

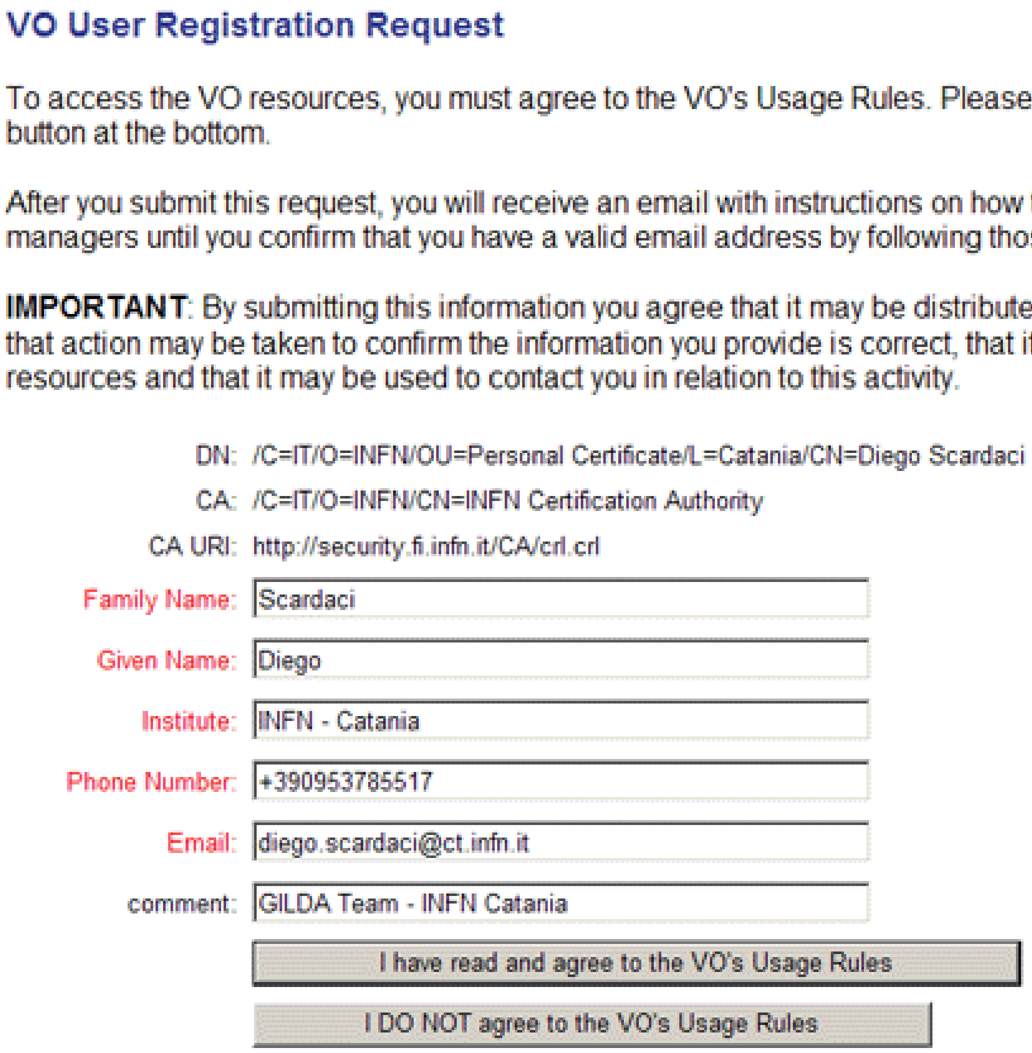
VOMS Admin 1.2.10
Release 1
Copyright © 2005 CERN, ELTE
on behalf of the EU EGEE Project

You are logged in as "/C=IT/O=INFN/OU=Personal Certificate/L=Catania/CN=Roberto Barbera/Email=roberto.barbera@ct.infn.it" certified by "/C=IT/O=INFN/CN=INFN Certification Authority".

New registrations at: https://voms.lip.pt:8443/voms/EELA/webui/request/user/create

EELA Registration (1/6)

(https://voms.lip.pt:8443/voms/eela/webui/request/user/create)



VO User Registration Request

To access the VO resources, you must agree to the VO's Usage Rules. Please fill out all fields in the form below and click on the appropriate button at the bottom.

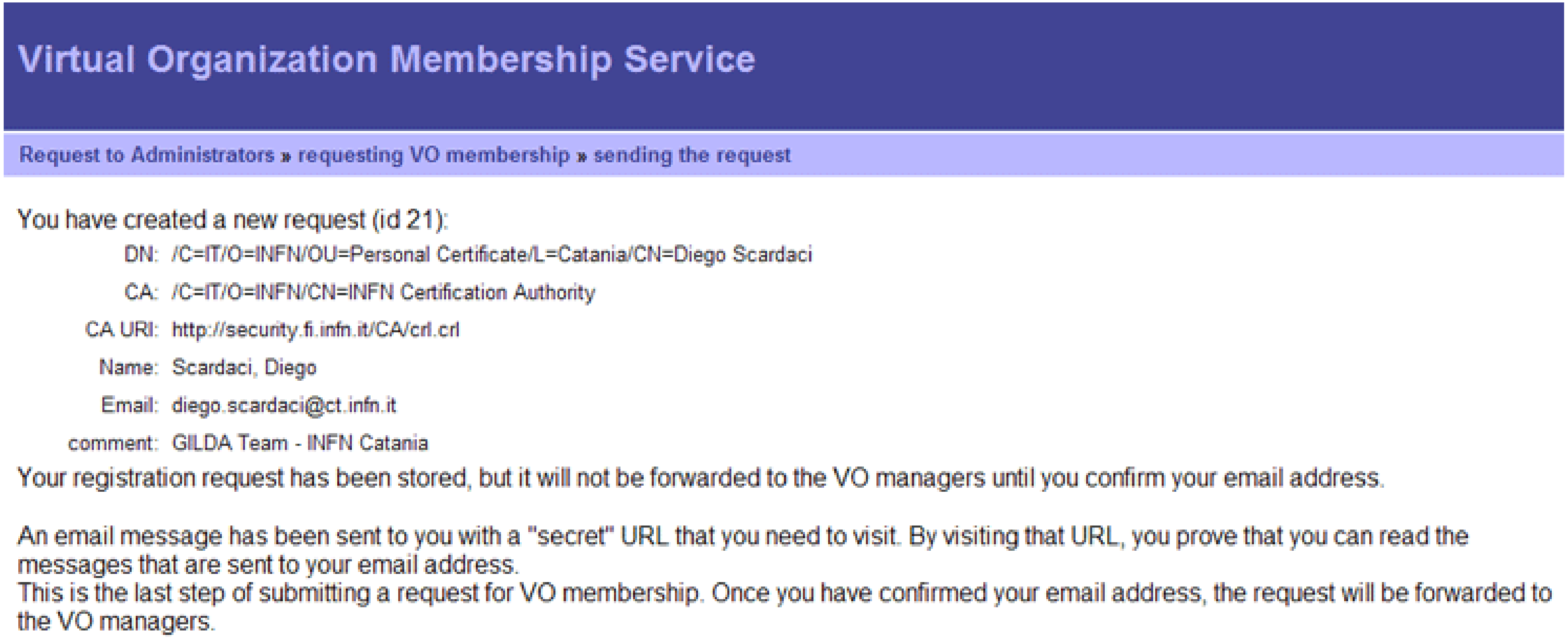
After you submit this request, you will receive an email with instructions on how to proceed. Your request will not be forwarded to the VO managers until you confirm that you have a valid email address by following those instructions.

IMPORTANT: By submitting this information you agree that it may be distributed to and stored by VO and site administrators. You also agree that action may be taken to confirm the information you provide is correct, that it may be used for the purpose of controlling access to VO resources and that it may be used to contact you in relation to this activity.

DN:	/C=IT/O=INFN/OU=Personal Certificate/L=Catania/CN=Diego Scardaci
CA:	/C=IT/O=INFN/CN=INFN Certification Authority
CA URI:	http://security.fi.infn.it/CA/crl.crl
Family Name:	Scardaci
Given Name:	Diego
Institute:	INFN - Catania
Phone Number:	+390953785517
Email:	diego.scardaci@ct.infn.it
comment:	GILDA Team - INFN Catania

I have read and agree to the VO's Usage Rules
I DO NOT agree to the VO's Usage Rules

EELA Registration (2/6)



Virtual Organization Membership Service

Request to Administrators » requesting VO membership » sending the request

You have created a new request (id 21):

DN:	/C=IT/O=INFN/OU=Personal Certificate/L=Catania/CN=Diego Scardaci
CA:	/C=IT/O=INFN/CN=INFN Certification Authority
CA URI:	http://security.fi.infn.it/CA/crl.crl
Name:	Scardaci, Diego
Email:	diego.scardaci@ct.infn.it
comment:	GILDA Team - INFN Catania

Your registration request has been stored, but it will not be forwarded to the VO managers until you confirm your email address.

An email message has been sent to you with a "secret" URL that you need to visit. By visiting that URL, you prove that you can read the messages that are sent to your email address.
This is the last step of submitting a request for VO membership. Once you have confirmed your email address, the request will be forwarded to the VO managers.

EELA Registration (3/6)

E-mail address confirmation for VO eela

A request for a VO membership on eela has been made using this email address.

If you have not made this request please ignore this message. It would be helpful if you would contact the VO registrar and tell us about this bogus request.

If the request was made by you, please click on the following URL to confirm this email address,

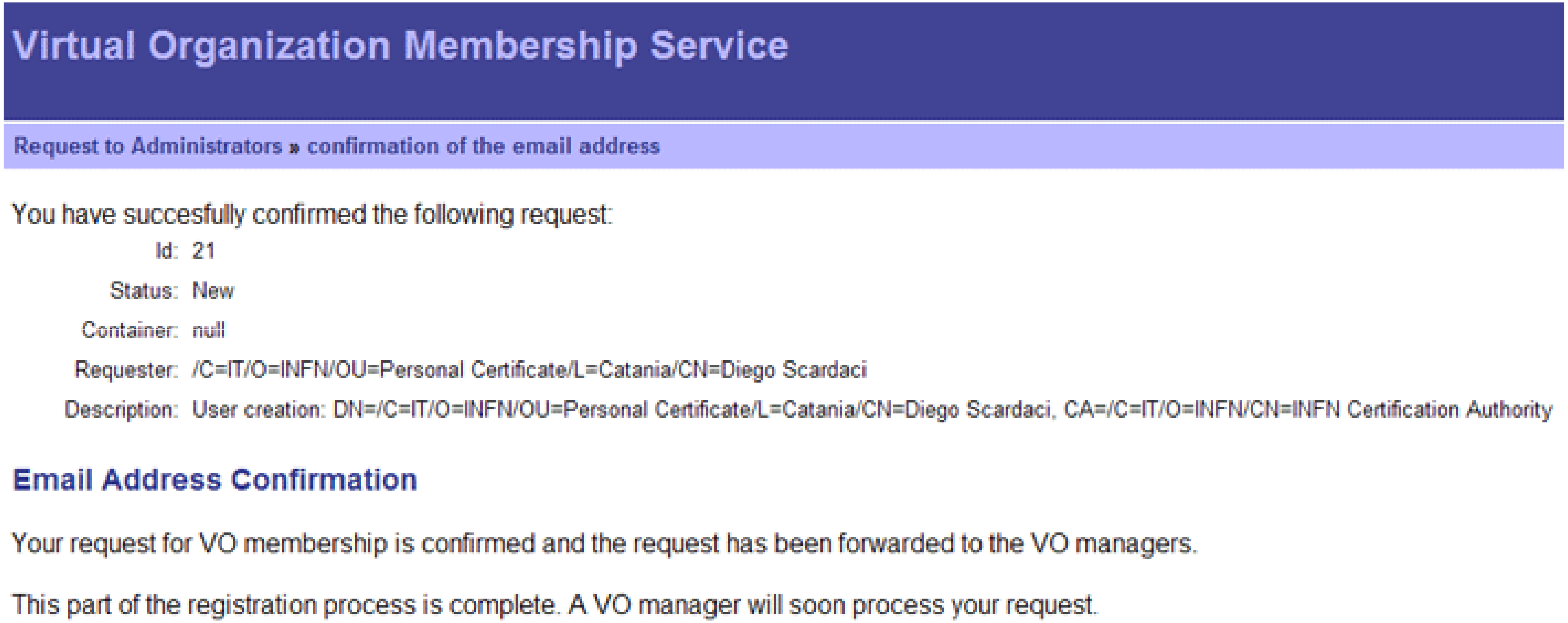
https://voms.lip.pt:8443/voms/eela/webui/request/user/confirm?cookie=xlqi8oy6fudv0wod&reqid=21

Make sure you have your client certificate loaded in your browser.
One way to ensure this is to copy and paste the above URL into the same browser that you used to submit the request.

If you wish to confirm the request another way, then you need the following information:

Request number : 21
Confirmation cookie: xlqi8oy6fudv0wod

EELA Registration (4/6)



Virtual Organization Membership Service

Request to Administrators » confirmation of the email address

You have succesfully confirmed the following request:

Id:	21
Status:	New
Container:	null
Requester:	/C=IT/O=INFN/OU=Personal Certificate/L=Catania/CN=Diego Scardaci
Description:	User creation: DN=/C=IT/O=INFN/OU=Personal Certificate/L=Catania/CN=Diego Scardaci, CA=/C=IT/O=INFN/CN=INFN Certification Authority

Email Address Confirmation

Your request for VO membership is confirmed and the request has been forwarded to the VO managers.

This part of the registration process is complete. A VO manager will soon process your request.

EELA Registration (5/6)

Dear Scardaci, Diego,

Thank you for confirming your email address. Your request for an account on VO eela has been sent to the VO administrators.

A VO administrator will probably contact you to confirm account creation.

If you find any problems regarding the account registration, then please contact the VO registrar.

Thank You,
VO Registration

EELA Registration (6/6)

Welcome to the eela VO!

Dear Scardaci, Diego,

Your request (21) for the eela VO has been accepted and allowed by the VO Administrator.

From this point you can use the voms-proxy-init command to acquire the VO specific credentials, which will enable you to use the resources of this VO.

Good Luck,
VO Registration

FQAN and AC

- short for Fully Qualified Attribute Name, is what VOMS uses to express membership and other authorization info
- Groups membership, roles and capabilities may be expressed in a format that bounds them together
  <group>/Role=[<role>][/Capability=<capability>]

```
[glite-tutor] /home/giorgio > voms-proxy-info -fqan
/gilda/Role=NULL/Capability=NULL
/gilda/tutors/Role=NULL/Capability=NULL
```

- FQAN are included in an Attribute Certificate
- Attribute Certificates are used to bind a set of attributes (like membership, roles, authorization info etc) with an identity
- AC are digitally signed
- VOMS uses AC to include the attributes of a user in a proxy certificate

VOMS and AC

- Server creates and sign an AC containing the FQAN requested by the user, if applicable

- AC is included by the client in a well-defined, non critical, extension assuring compatibility with GT-based mechanism

```
/home/giorgio > voms-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      : proxy
strength  : 512 bits
path      : /tmp/x509up_u513
timeleft  : 11:59:52
=== VO gilda extension information ===
VO        : gilda
subject   : /C=IT/O=GILDA/OU=Personal Certificate/L=INFN/CN=Emidio
Giorgio/Email=emidio.giorgio@ct.infn.it
issuer    : /C=IT/O=GILDA/OU=Host/L=INFN
Catania/CN=voms.ct.infn.it/Email=emidio.giorgio@ct.infn.it
attribute : /gilda/tutors/Role=NULL/Capability=NULL
attribute : /gilda/Role=NULL/Capability=NULL
timeleft  : 11:59:45
```

Groups

- **The number of users of a VO can be very high:**
  - E.g. the experiment ATLAS has 2000 member

- **Make VO manageable by organizing users in groups:**

  Examples:
  - VO GILDA
    - Group Catania
      - *INFN*
        - Group Barbera
      - *University*
    - Group Padua
  - VO GILDA
    - /GILDA/TUTORS can write to normal storage
    - /GILDA/STUDENT only write to volatile space

- **Groups can have a hierarchical structure, indefinitely deep**

Roles

- **Roles are specific roles a user has and that distinguishes him from others in his group:**
  - Software manager
  - VO-Administrator

- **Difference between roles and groups:**
  - Roles have no hierarchical structure – there is no sub-role
  - Roles are not used in ‘normal operation’
    - They are not added to the proxy by default when running *voms-proxy-init*
    - But they can be added to the proxy for special purposes when running *voms-proxy-init*

- **Example:**
  - User Emidio has the following membership
    - VO=gilda, Group=tutors, Role=SoftwareManager
  - During normal operation the role is not taken into account, e.g. Emidio can work as a normal user
  - For special things he can obtain the role “Software Manager”

LCAS & LCMAPS

- At resources level, authorization info are extracted from the proxy and processed by *LCAS* and *LCMAPS*

- Local Centre Authorization Service (LCAS)
  - Checks if the user is authorized (currently using the grid-mapfile)
  - Checks if the user is banned at the site
  - Checks if at that time the site accepts jobs

- Local Credential Mapping Service (LCMAPS)
  - Maps grid credentials to local credentials (eg. UNIX uid/gid, AFS tokens, etc.)
  - Map also VOMS group and roles (full support of FQAN)

```
"/VO=cms/GROUP=/cms"                     .cms
"/VO=cms/GROUP=/cms/prod"                .cmsprod
"/VO=cms/GROUP=/cms/prod/ROLE=manager"   .cmsprodman
```

GSI environment variables

- User certificate files:
  - Certificate: **$X509_USER_CERT** (default: `$HOME/.globus/usercert.pem`)
  - Private key: **$X509_USER_KEY** (default: `$HOME/.globus/userkey.pem`)
  - Proxy: **$X509_USER_PROXY** (default: `/tmp/x509up_u<id>`)
- Host certificate files:
  - Certificate **$X509_HOST_CERT** (default: `/etc/grid-security/hostcert.pem`)
  - Private key **$X509_HOST_KEY** (default: `/etc/grid-security/hostkey.pem`)
- Trusted certification authority certificates:
  - **$X509_CERT_DIR** (default: `/etc/grid-security/certificates`)
- Voms server public keys
  - **$X509_VOMS_DIR** (default: `/etc/grid-security/vomsdir`)

References

- Grid
  - LCG Security: http://proj-lcg-security.web.cern.ch/proj-lcg-security/
  - EELA VOMS Registration: https://voms.lip.pt:8443/voms/EELA/webui/request/user/create
  - EELA ROC: http://roc.eu-eela.org
  - Globus Security Infrastructure: http://www.globus.org/security/
  - VOMS: http://infnforge.cnaf.infn.it/projects/voms
  - CA: http://www.tagpma.org/

- Background
  - GGF Security: http://www.gridforum.org/security/
  - IETF PKIX charter: http://www.ietf.org/html.charters/pkix-charter.html
  - PKCS: http://www.rsasecurity.com/rsalabs/pkcs/index.html