



Enabling Grids for E-science

Overview of EGEE and gLite Middleware

Presented by Min Tsai

With thanks to EGEE colleagues for many of these slides

www.eu-egee.org



- **EGEE Introduction**
- **gLite Middleware**
- **gLite Security**

- **Flagship European grid infrastructure project**
 - 2nd phase with 91 partners in 32 countries

- **Objectives**

- Large-scale, production-quality grid infrastructure for e-Science
- Attracting new resources and users from industry as well as science

- **Structure**

EGEE: 1 April 2004 – 31 March 2006

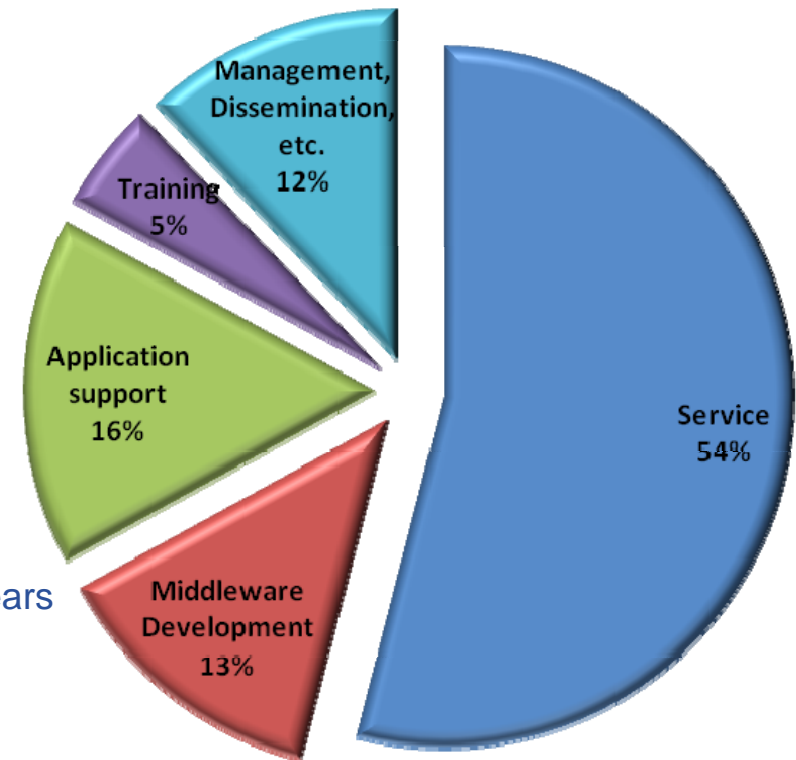
EGEE-II: 1 April 2006 – 31 March 2008

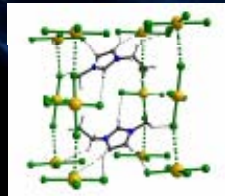
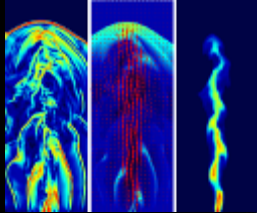
- Funded by the EC at a level of ~37 M Euros for 2 years

- **EGEE-III**: 1 April 2008 – 31 March 2010

- Transition to self-sustainable state

EGEE Project Activities

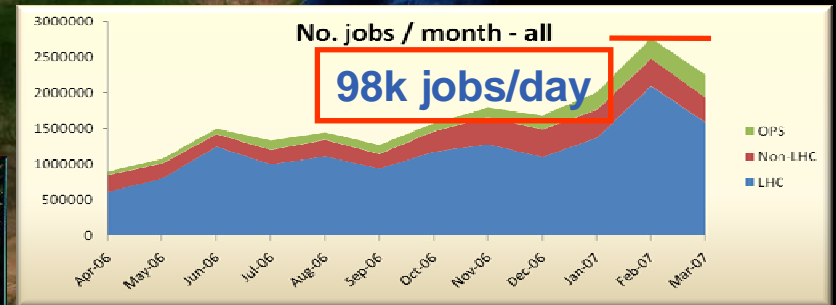




240 sites
45 countries
41,000 CPUs
5 PetaBytes
>10,000 users
>150 VOs
>100,000 jobs/day

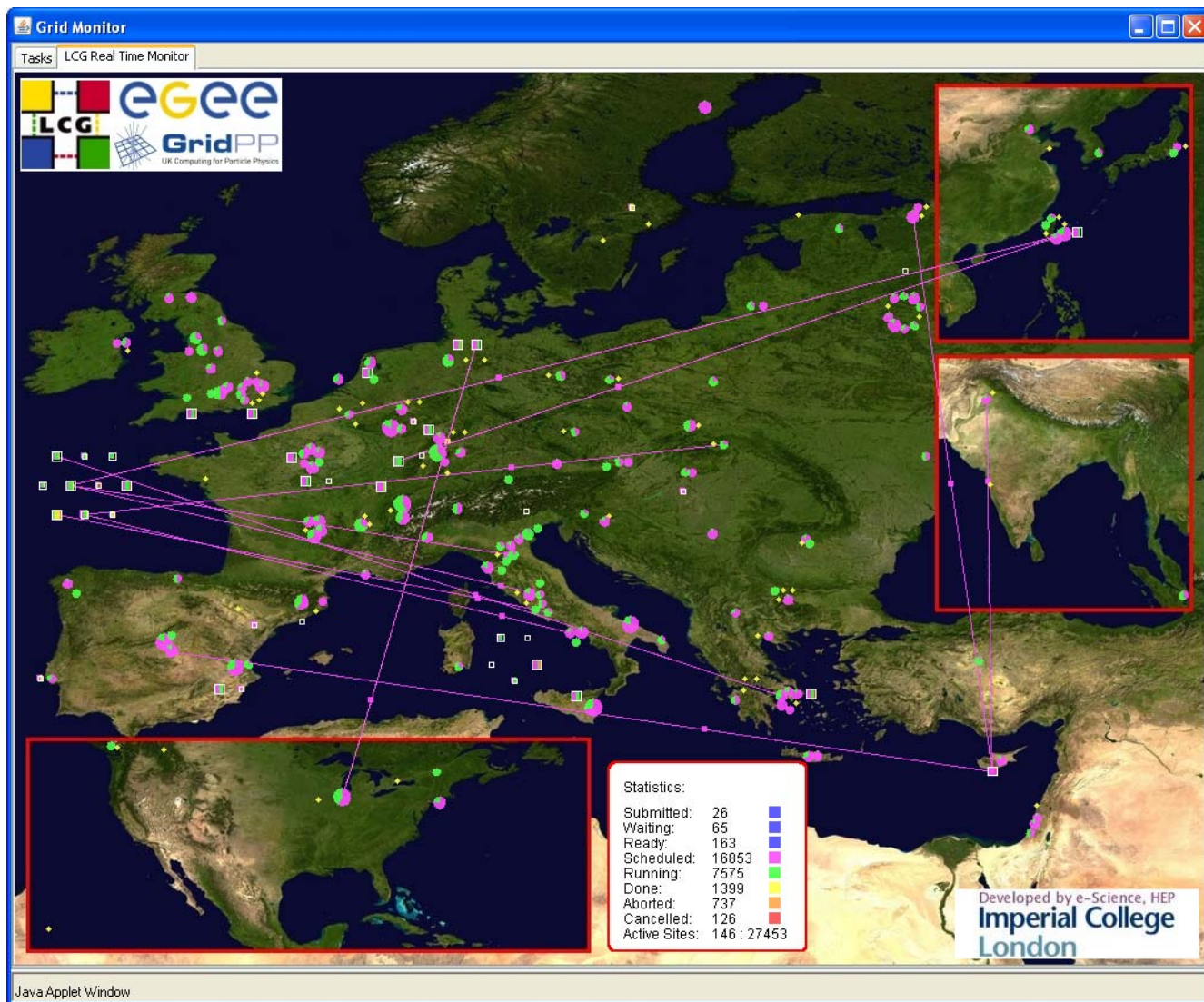
Archeology
Astronomy
Astrophysics
Civil Protection
Comp. Chemistry
Earth Sciences
Finance
Fusion
Geophysics
High Energy Physics
Life Sciences
Multimedia
Material Sciences

...



Real Time Monitor

- Java tool
- Displays jobs running (submitted through RBs)
- Shows jobs moving around world map in real time, along with changes in status



<http://gridportal.hep.ph.ic.ac.uk/rtm/>

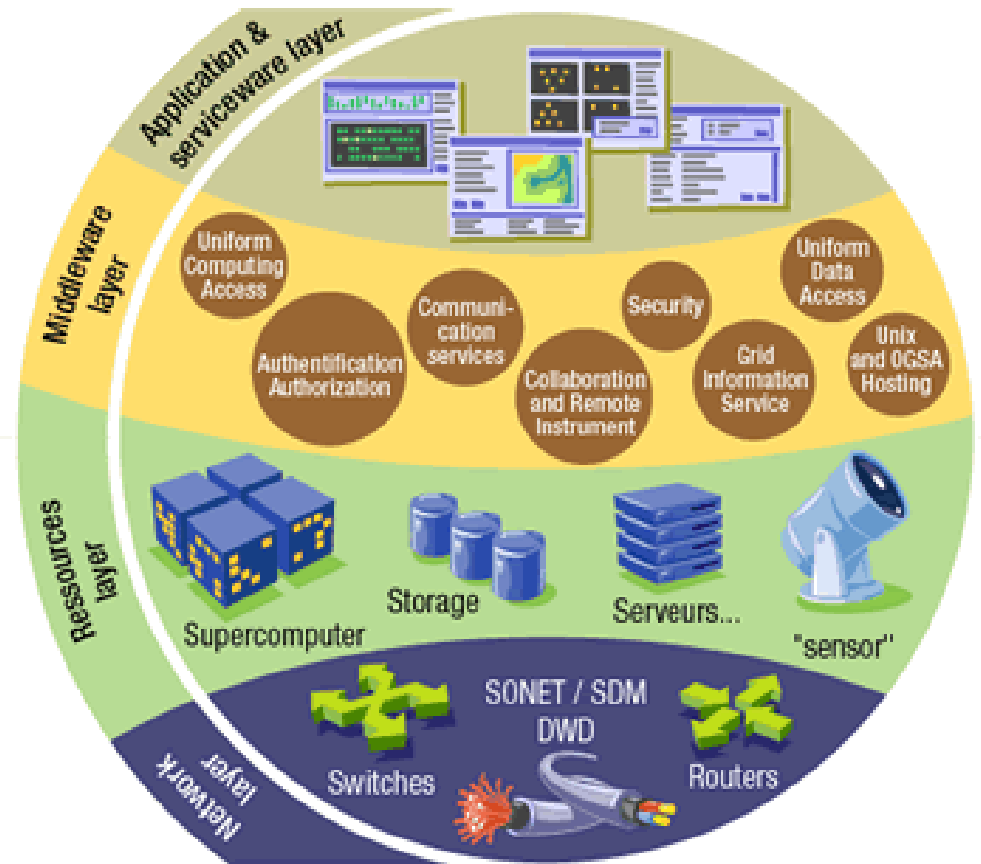
(snapshot 16 January 2007)

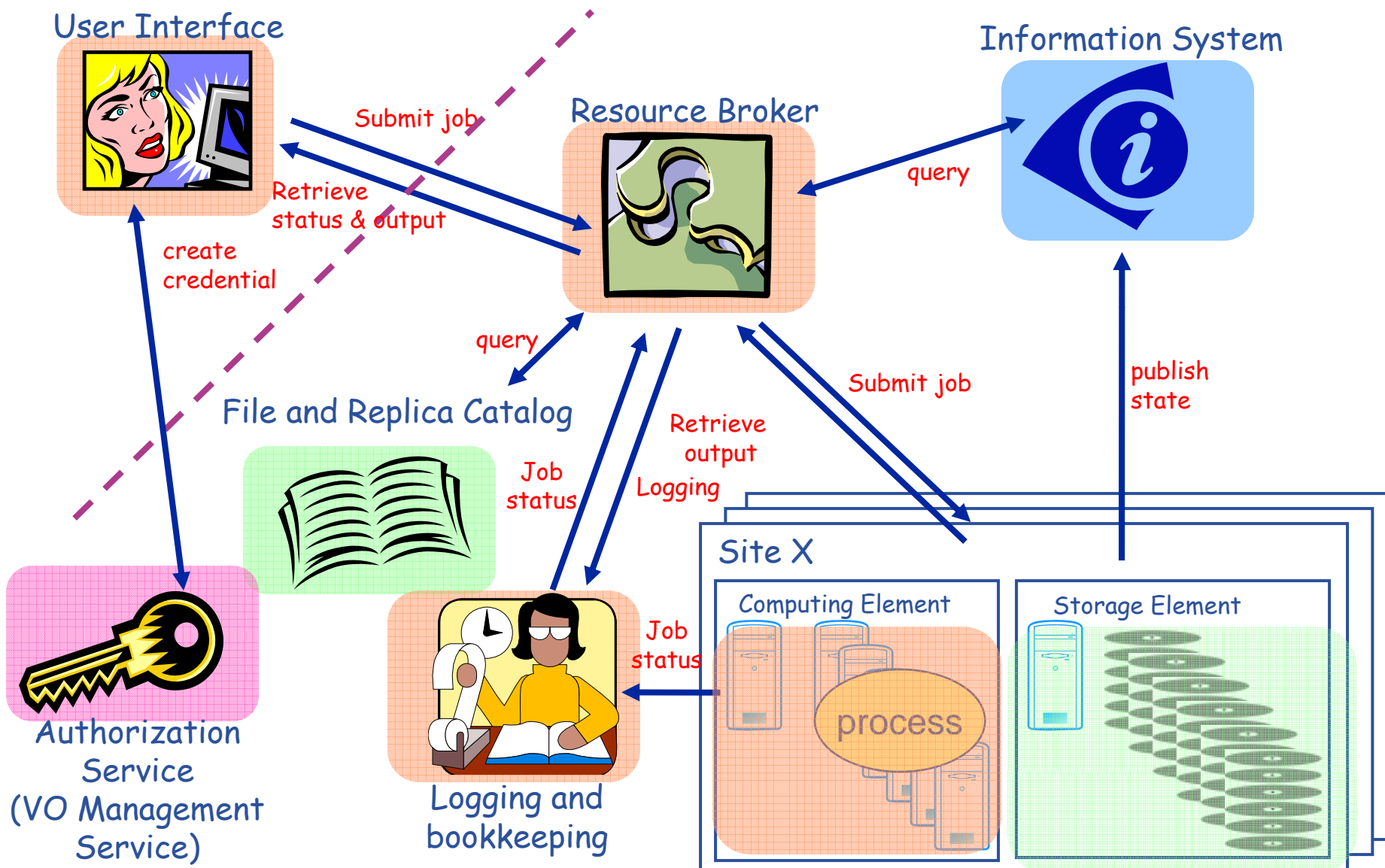
- **EGEE Introduction**
- **gLite Middleware**
- **gLite Security**

- The Grid relies on advanced software, called **middleware**, which interfaces between resources and the applications



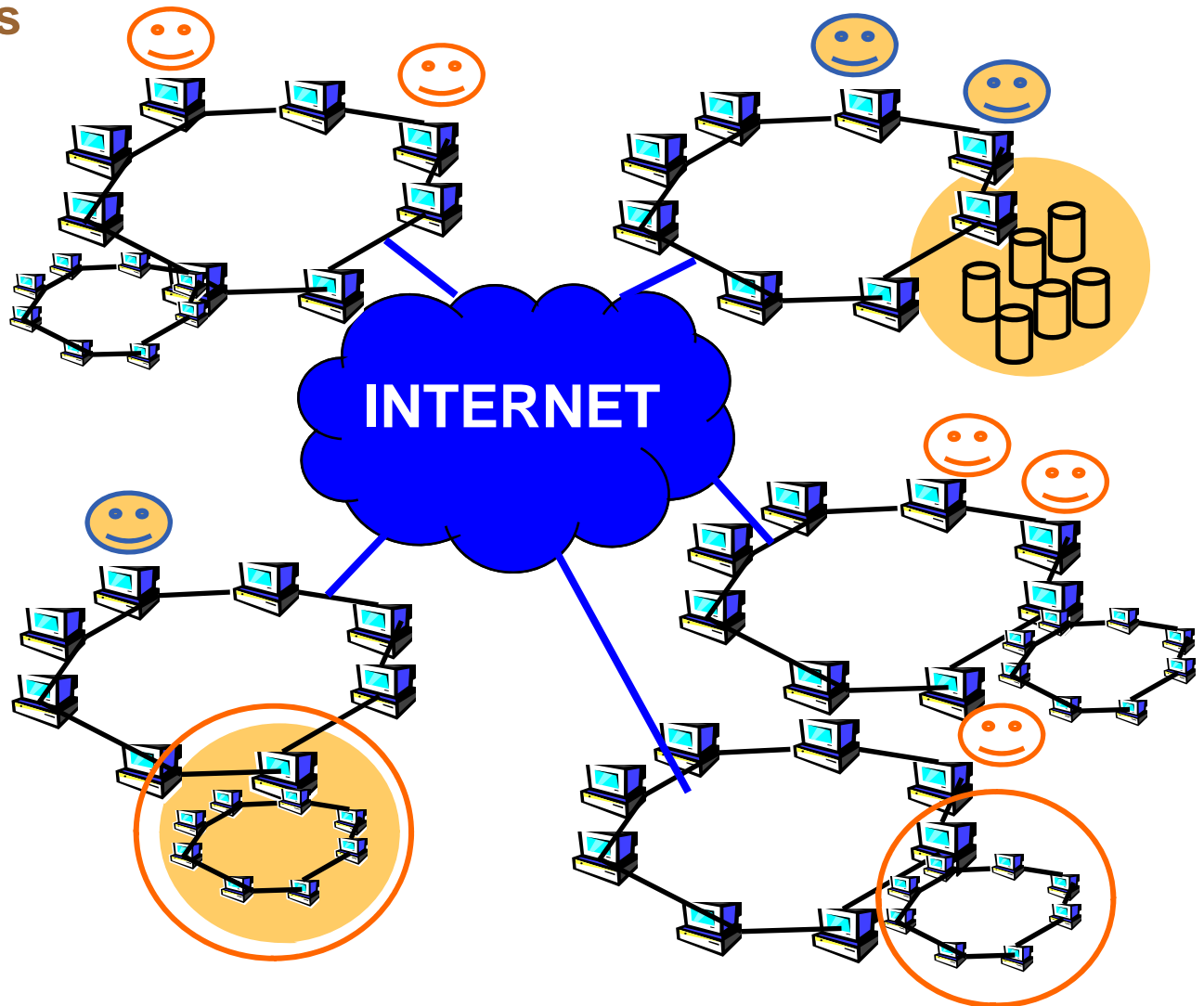
- gLite 3.1**
 - Scientific Linux 4
 - Exploits components from
 - VDT (Condor, Globus)
 - EDG/LCG, others



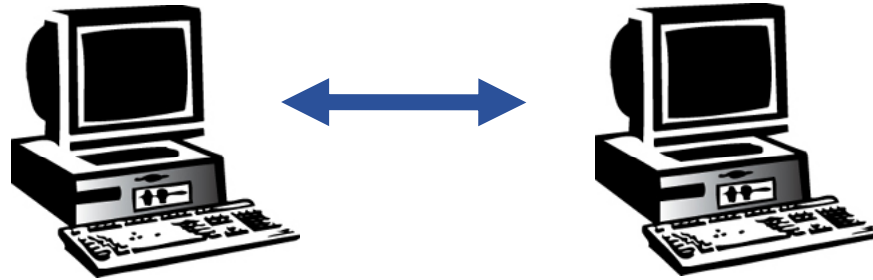


- **gLite middleware runs on each shared resource to provide**
 - Data services
 - Computation services
 - Security service

- **Resources and users form Virtual Organisations: basis for collaboration**



- **EGEE Introduction**
- **gLite Middleware**
- **gLite Security**



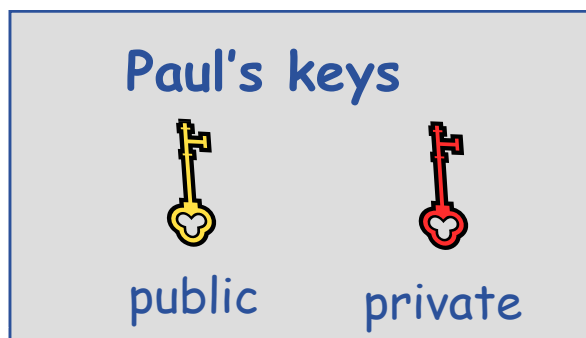
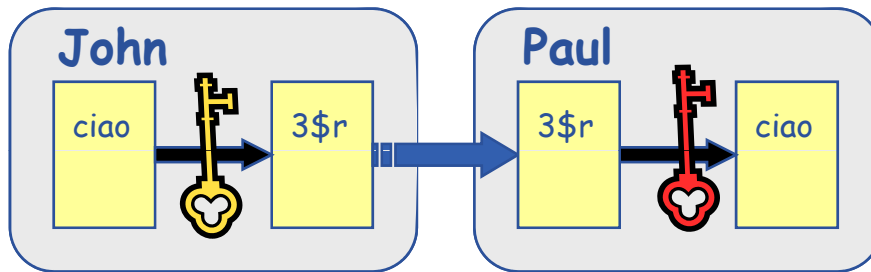
User

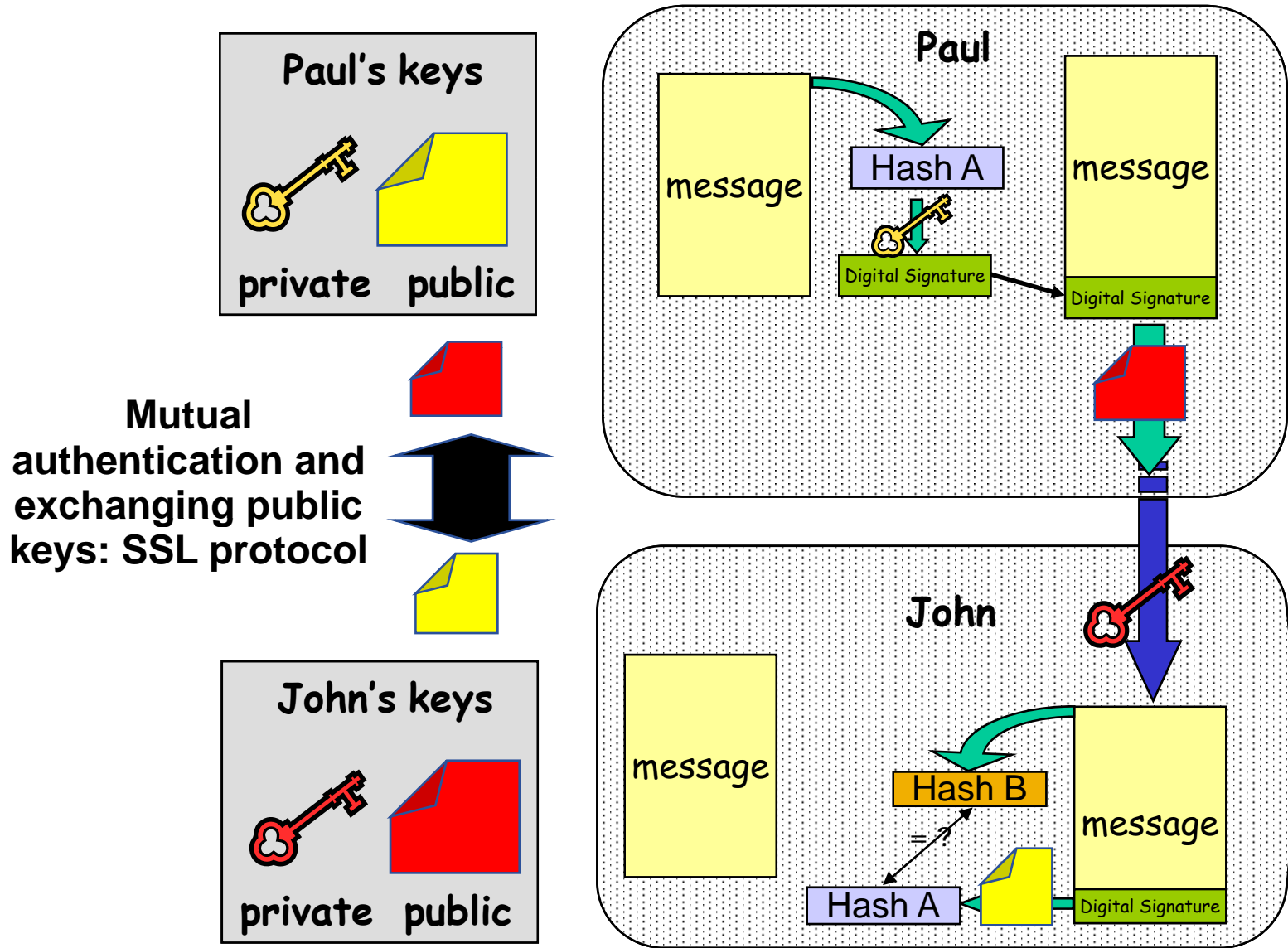
Grid service

- **How can communication endpoints be identified?**
 - Authentication
- **How can a secure channel established between two partners?**
 - Encryption
 - Non-repudiation
 - Integrity
- **Authorisation**
 - Who is allowed to access a Virtual Organisation's resources
 - What are VO members allowed to do?

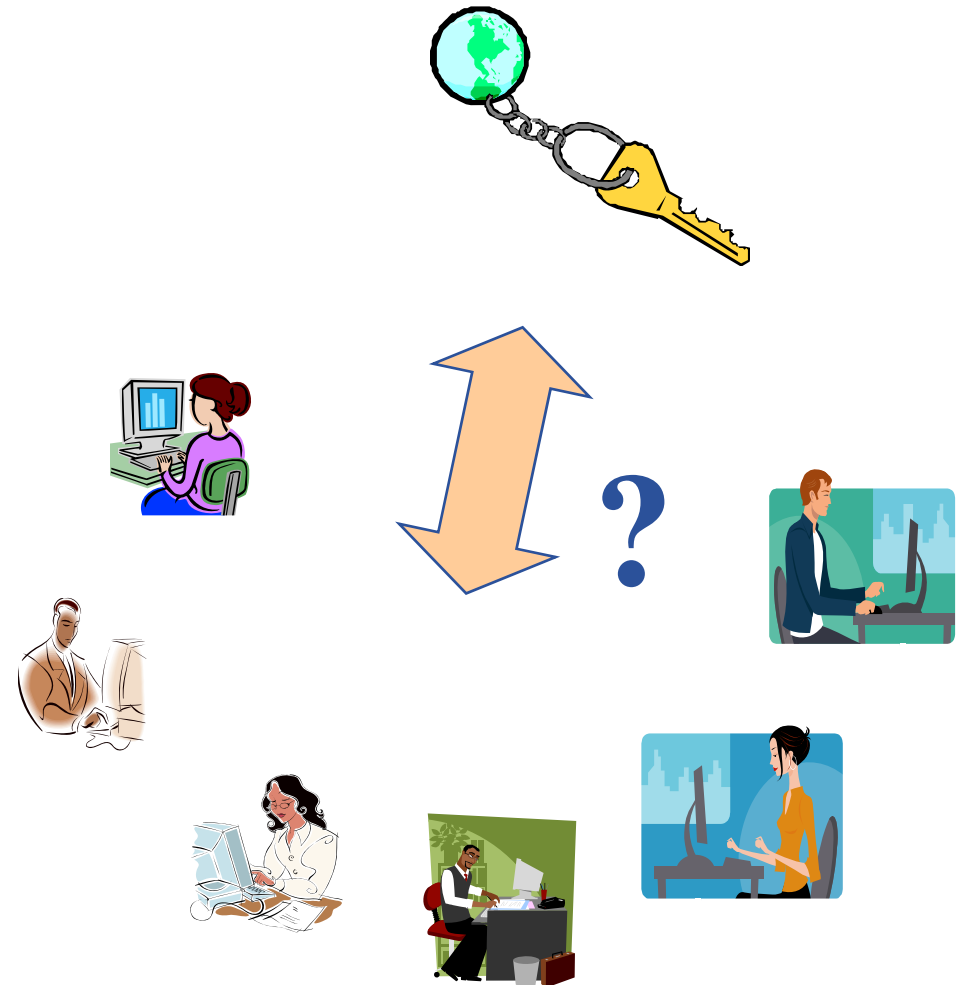
- **Encryption**

- Encryption with recipient's public key
- Only recipient can decrypt the message



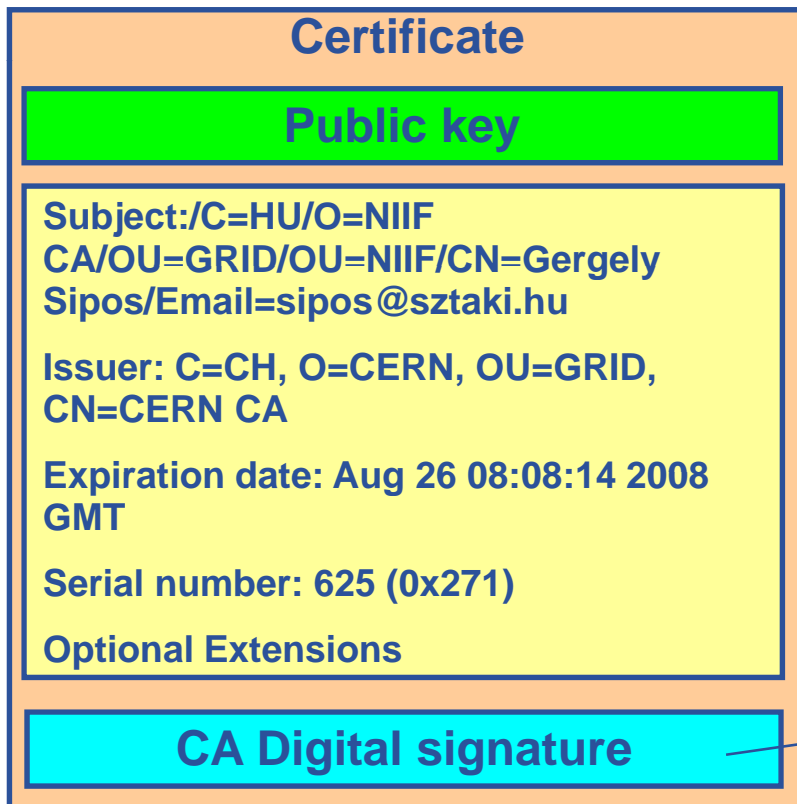


- Anyone can create a key pair.
- How can I trust the public key is yours?



- Private key is stored in encrypted file – protected by a passphrase

- Public key is wrapped into a “certificate file”
- Certificate files are created by trusted third parties: Grid Certification Authorities (CA)
- Certificates recognized by Grids
 - www.gridpma.org



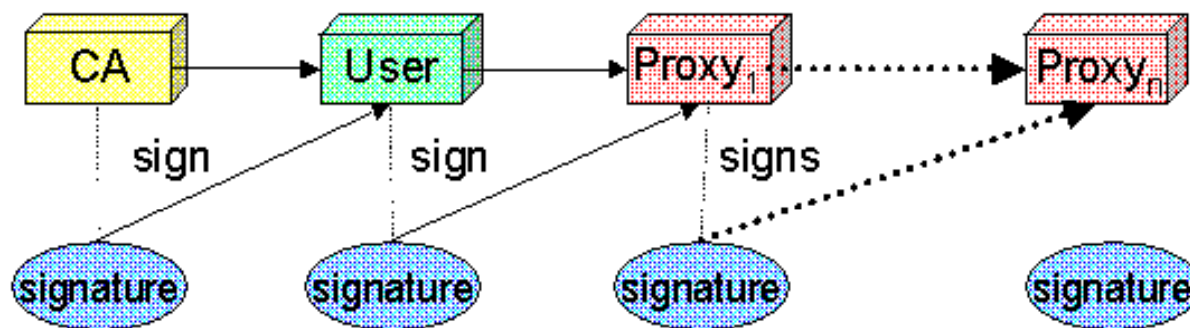
1. Hash of Public key & metadata,
2. Encrypt hash with CA's private key

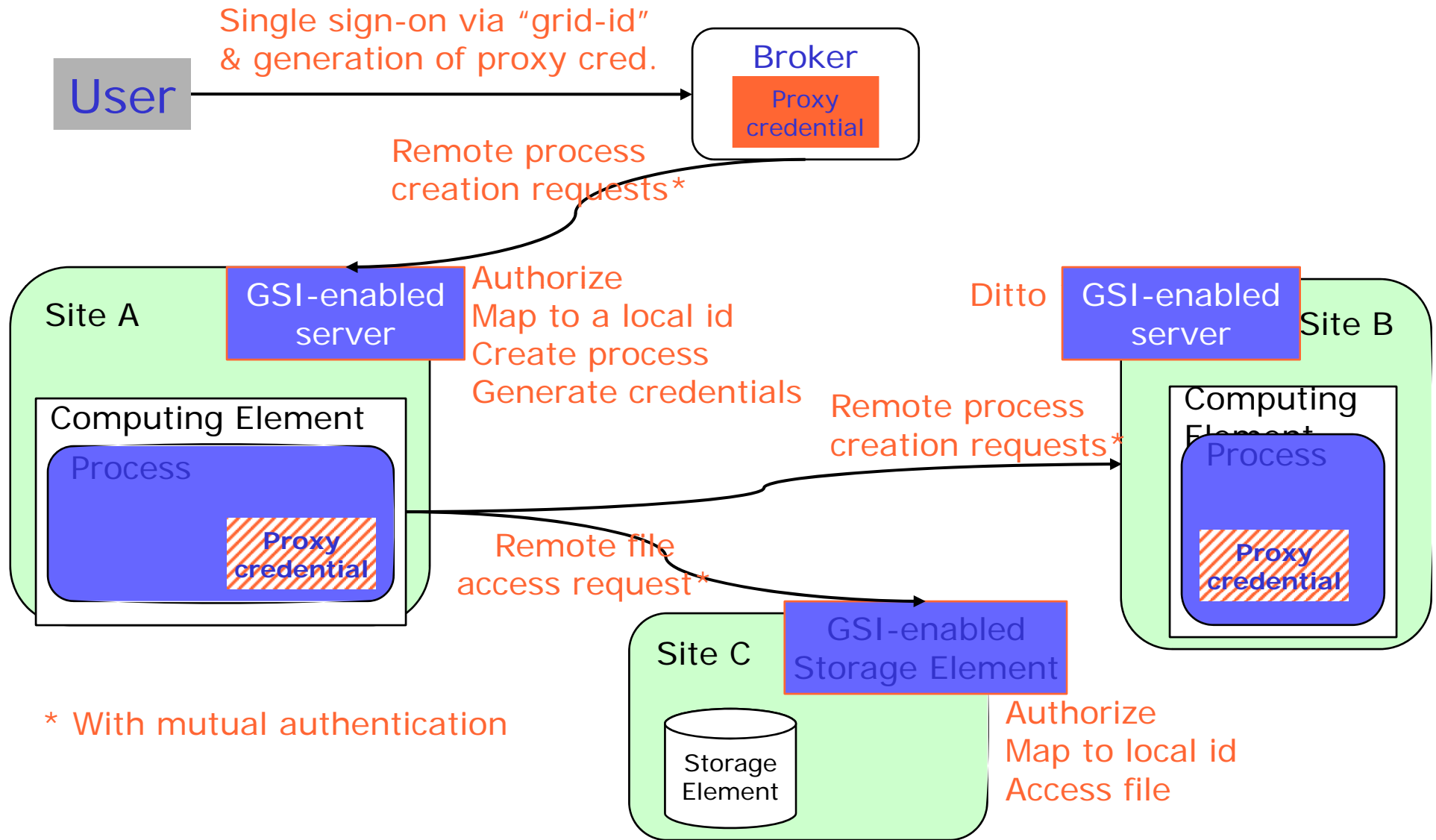
- **Private key and certificate can:**
 - Stored in your browser
 - Stored in files using different file format (PEM, P12, ...)
- **Typical situation on Globus, gLite, ARC middleware based grids:**

```
[sipos@glite-tutor sipos]$ ls -l .globus/  
total 8  
-rw-r--r--    1 sipos    users    1761 Oct 25  2006 usercert.pem  
-r-----    1 sipos    users    951  Oct 24  2006 userkey.pem
```

If your certificate is used by someone other than you, it cannot be proven that it was not you.

- Delegation - allows remote process and services to authenticate **on behalf of the user**
- Achieved by creation of next-level private key–certificate pair from the user’s private key–certificate.
 - New key-pair is a single file: **Proxy credential**
 - Proxy private key is not protected by password
 - Proxy may be valid for limited operations
 - Proxy has limited lifetime
- **The client can delegate proxies to services, processes**
 - Each service decides whether it accepts proxies for authentication





```
[sipos@glite-tutor sipos]$ voms-proxy-init --voms gilda
Enter GRID pass phrase: *****
Your identity: /C=HU/O=NIIF CA/OU=GRID/OU=NIIF/CN=Gergely
Sipos/Email=sipos@sztaki.hu
Creating temporary proxy ..... Done
Contacting voms.ct.infn.it:15001 [/C=IT/O=INFN/OU=Host/L=Catania/CN=voms.ct.infn.it]
"gilda" Done
Creating proxy ..... Done
Your proxy is valid until Sat Jun 23 04:55:19 2007
```

% voms-proxy-init → login to the Grid

Enter PEM pass phrase: ***** → private key is protected by a password

— Options for voms-proxy-init:

- VO name
- -hours <lifetime of new credential>
- -bits <length of key>
- -help

% voms-proxy-destroy → logout from the grid

Delegated credentials will not be revoked

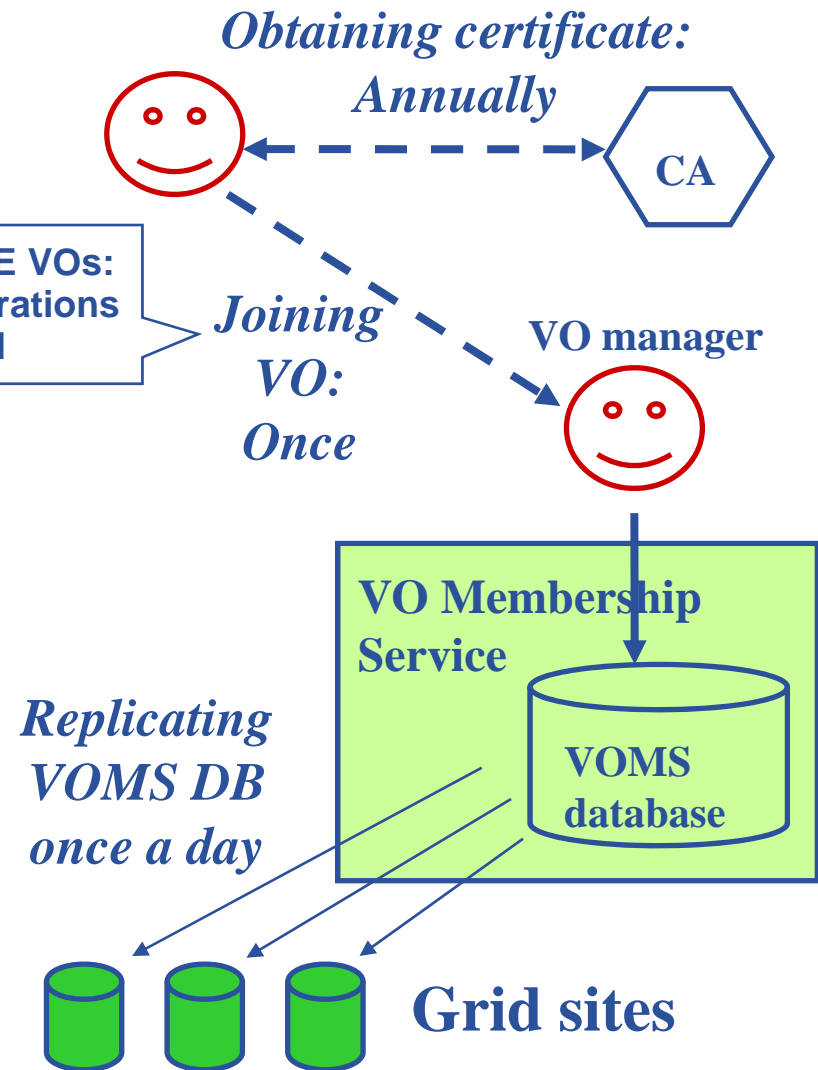
Joining a Virtual Organisation

- Users (and machines) are identified by certificates.

- **Steps**

- User obtains certificate from Certification Authority
- User registers at the VO
 - usually via a web form
- VO manager authorizes the user
 - VO DB updated
- User information is replicated onto VO resources within 24 hours

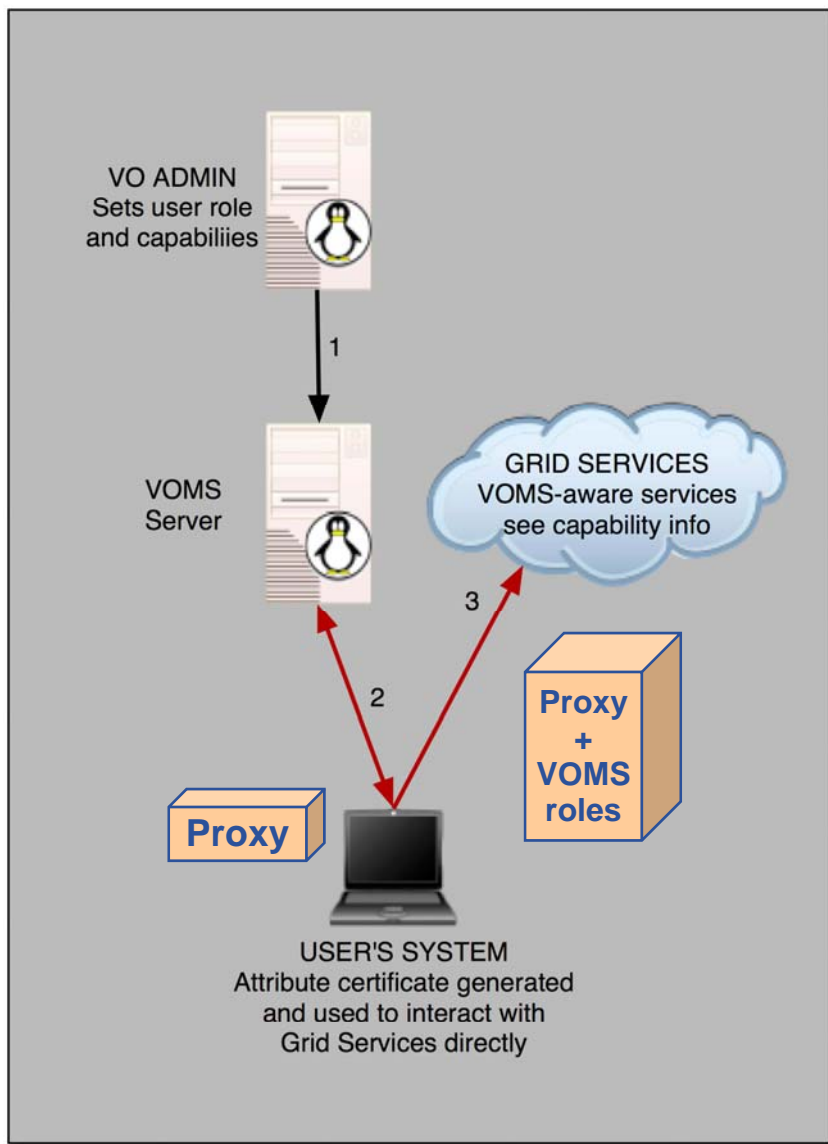
List of EGEE VOs:
On CIC Operations Portal



User's identity in the Grid = Subject of certificate:

/C=HU/O=NIIF CA/OU=GRID/OU=NIIF/CN=Gergely Sipos/Email=sipos@sztaki.hu

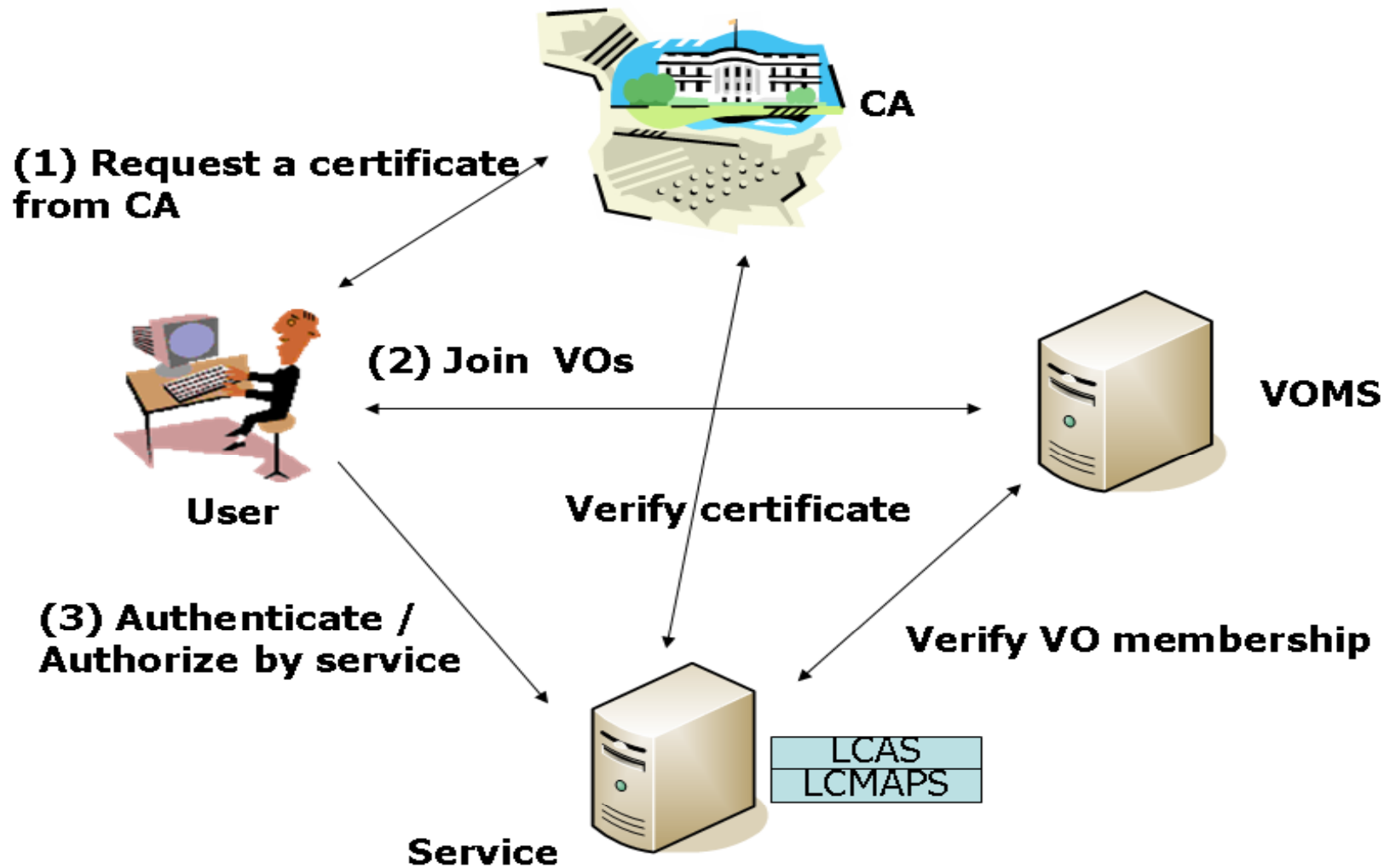
voms-proxy-init: what really happens in the background



- `voms-proxy-init`
 - Creates a proxy locally
 - Contacts the VOMS server and extends the proxy with a role
 - VOMS server signs the proxy

`voms-proxy-init -voms gilda`

- Allows VOs to centrally manage user roles



- **EGEE is running the largest multi-VO grid in the world!**
 - For both industry and science
 - EGEE III – transition to long term sustainability
- **EGEE's middleware consist of:**
 - Information system
 - Workload management system
 - Data management system
- **gLite Security**
 - Authentication depends on:
 - x509 certificates and Public Key Infrastructure
 - Authorization depends on:
 - VOMS

- **EGEE**
 - <http://www.eu-egee.org/>
- **gLite middleware**
 - <http://www.glite.org>
- **gLite manuals, documentation**
 - <http://glite.web.cern.ch/glite/documentation/>
(gLite user guide)
- **EGEE user and applications portal**
 - <http://egeena4.lal.in2p3.fr/>