

Security and getting access to the training infrastructure

Gergely Sipos

MTA SZTAKI

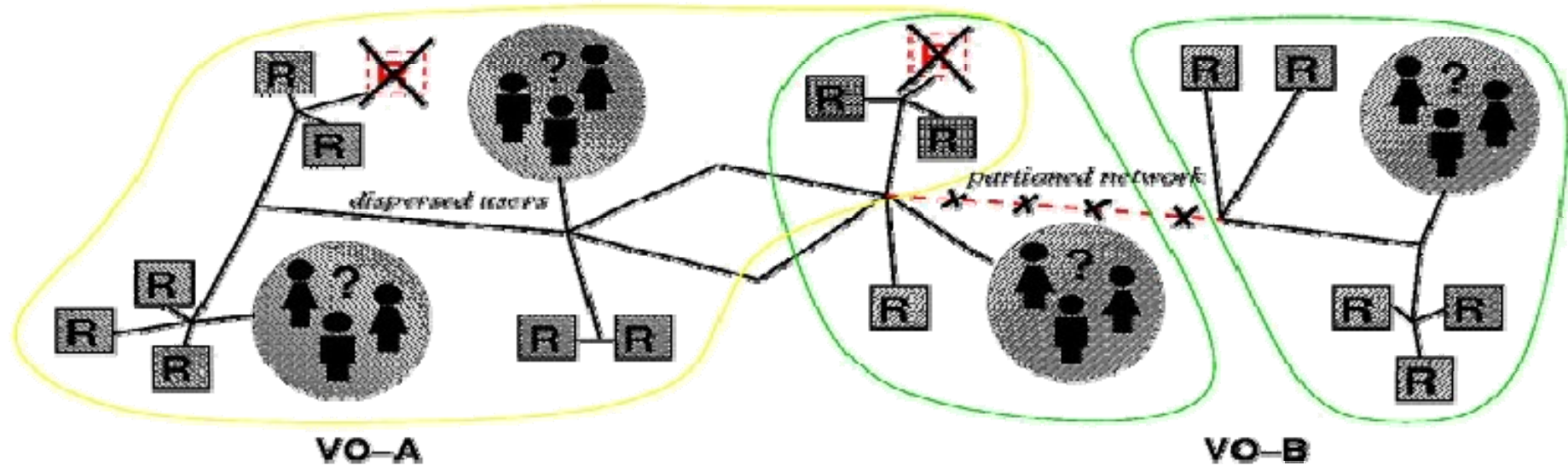
sipos@sztaki.hu

With thanks for some slides to EGEE and Globus colleagues

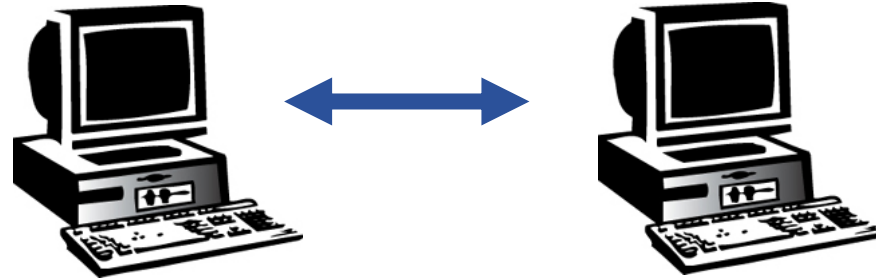
The Grid problem is to enable “coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations.”

From “The Anatomy of the Grid” by Ian Foster et al.

- So Grid Security is security to enable VOs
- What is needed in terms of security for a VO?



- VO for each application, workload or community
- The more dynamic the better...and the harder
- Security problems at two levels:
 - network level security
 - VO level security

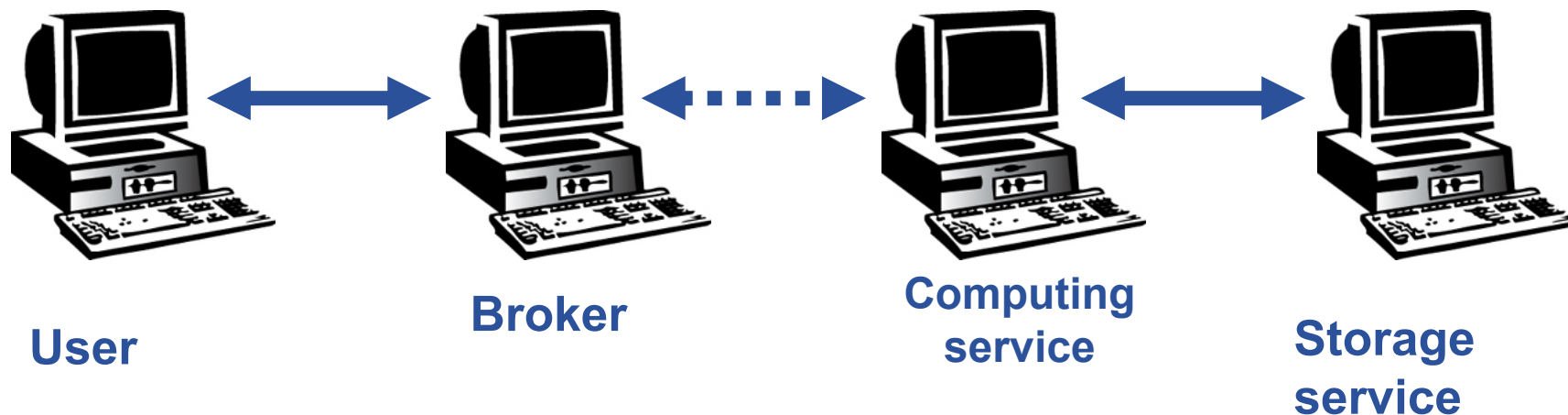


User

Grid service

Participants of a grid communicate over the Internet

- **How can communication endpoints be identified?**
 - Authentication
- **How can a secure channel established between two partners?**
 - Message encryption
 - Non-repudiation
 - Message integrity



- Which networked entity is / is not member of a VO?
- What are VO members allowed to do?
 - Authorization
- How can services act on behalf of a user?
 - How can a broker access the „user’s sites“?
 - How can a job which is started by the broker access the user’s private data?

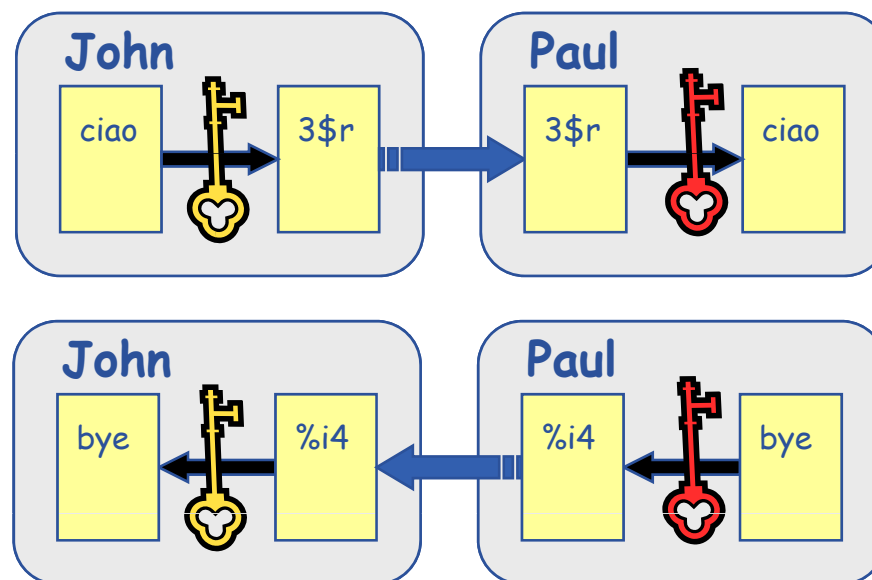
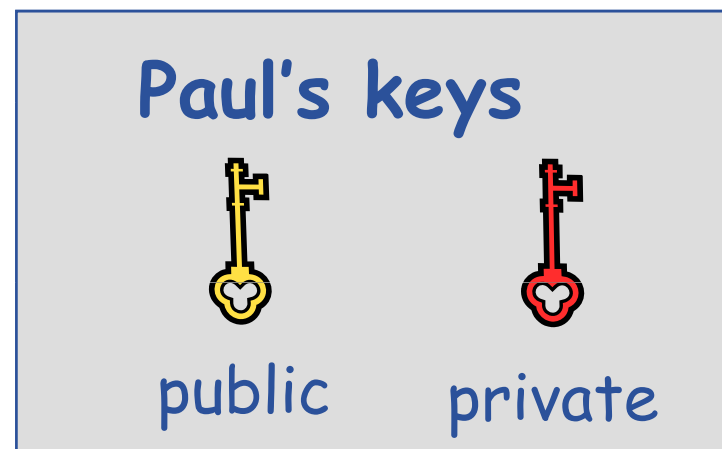
- **Launch attacks to other sites**
 - Large distributed farms of machines, perfect for launching a Distributed Denial of Service attack.
- **Illegal or inappropriate data distribution and access sensitive information**
 - Massive distributed storage capacity ideal for example, for swapping movies.
 - Growing number of users have data that must be private – biomedical imaging for example
- **Damage caused by viruses, worms etc.**
 - Highly connected infrastructure means worms could spread faster than on the internet in general.

Grid Security Infrastructure

based on

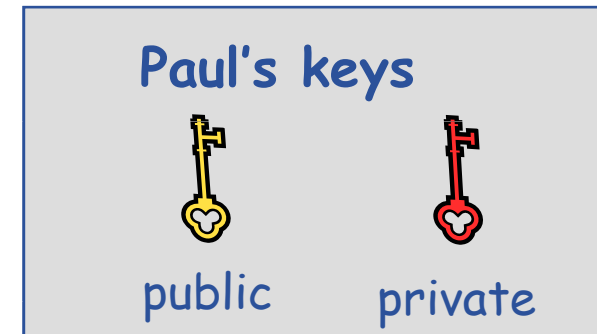
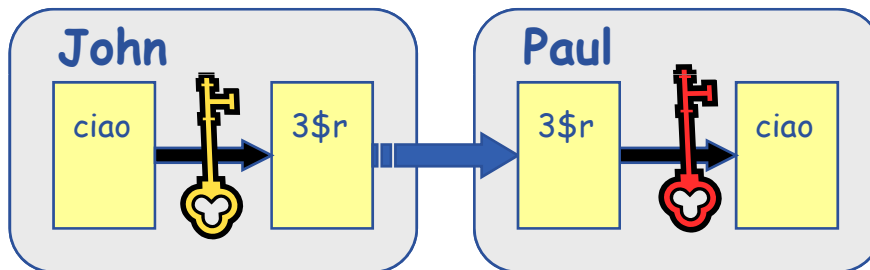
Public key infrastructure (PKI)

- Every networked entity (user/machine/software) is assigned with two keys: one **private key** and one **public key**
 - a message encrypted by one key can be decrypted **only** by the other one.
 - it is *impossible* to derive the private key from the public one
- **Concept (simplified version):**
 - Public keys are exchanged
 - The sender encrypts using receiver's public key
 - The receiver decrypts using their private key;



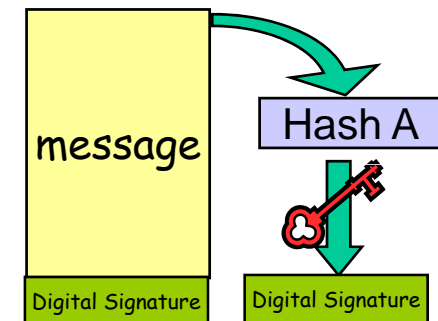
- **Encryption**

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

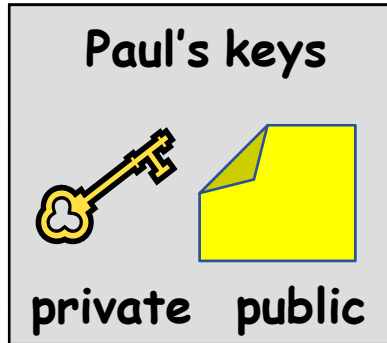


- **Non-repudiation**

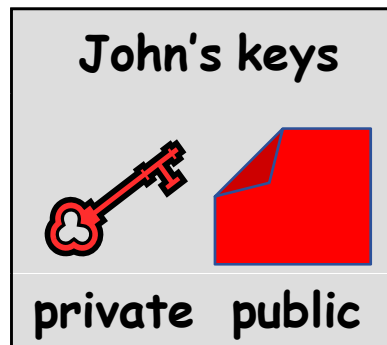
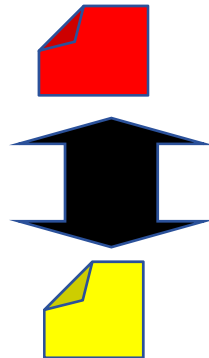
- **Naive approach:** encrypt message with sender's private key
 - Too costly for long messages
- **Solution:**
 - generate hash of the message
 - Encrypt hash with sender's private key
 - Attach encrypted hash to message → **Digital signature**
- Additional benefit: Integrity (hash is constant)



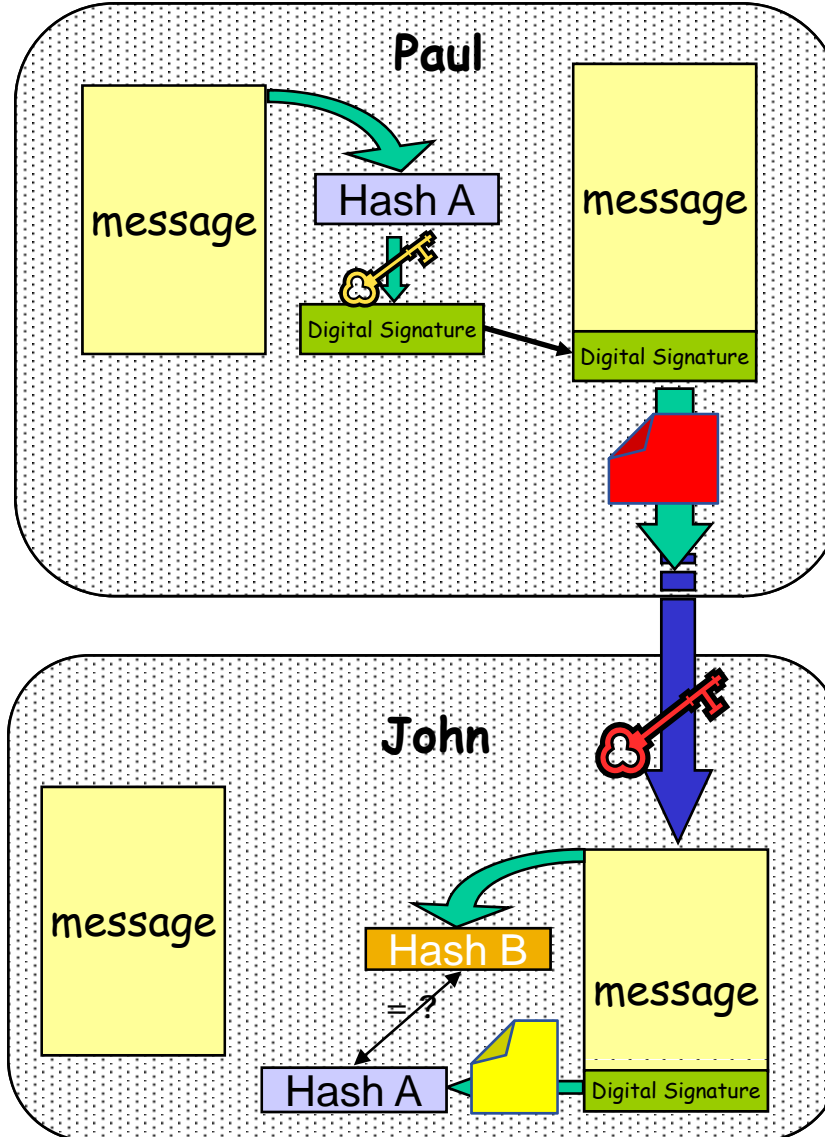
Hash function



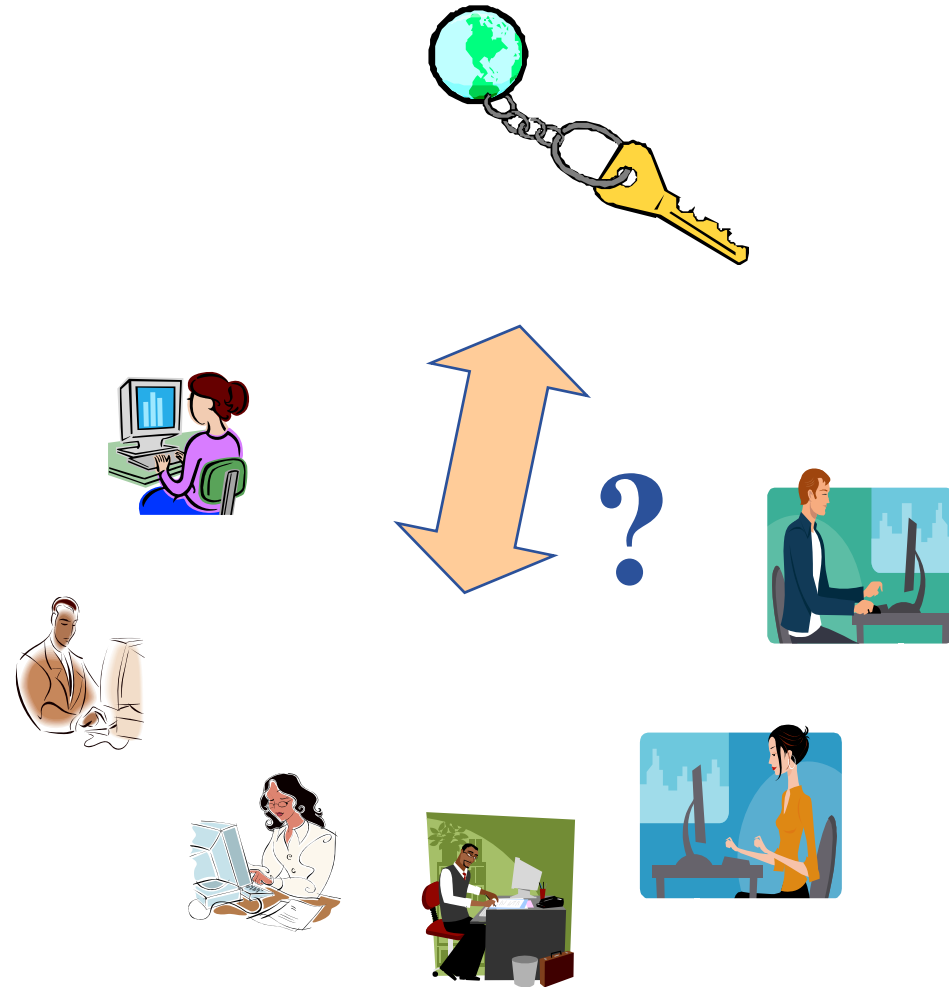
Mutual authentication and exchanging public keys: SSL protocol



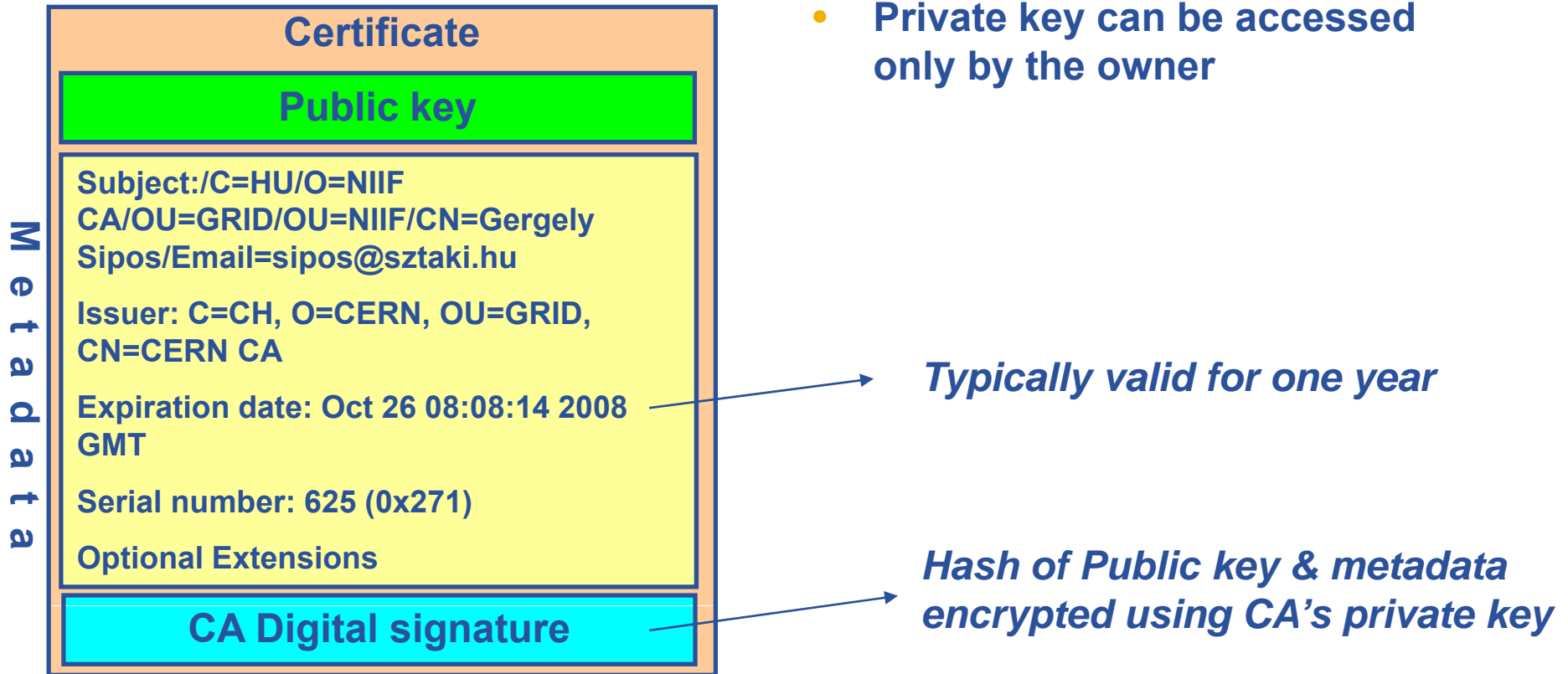
Hash function



- Since I'm the only one with access to my private key, you know I signed the data associated with it
- But, how do you know that you have **my** correct public key?

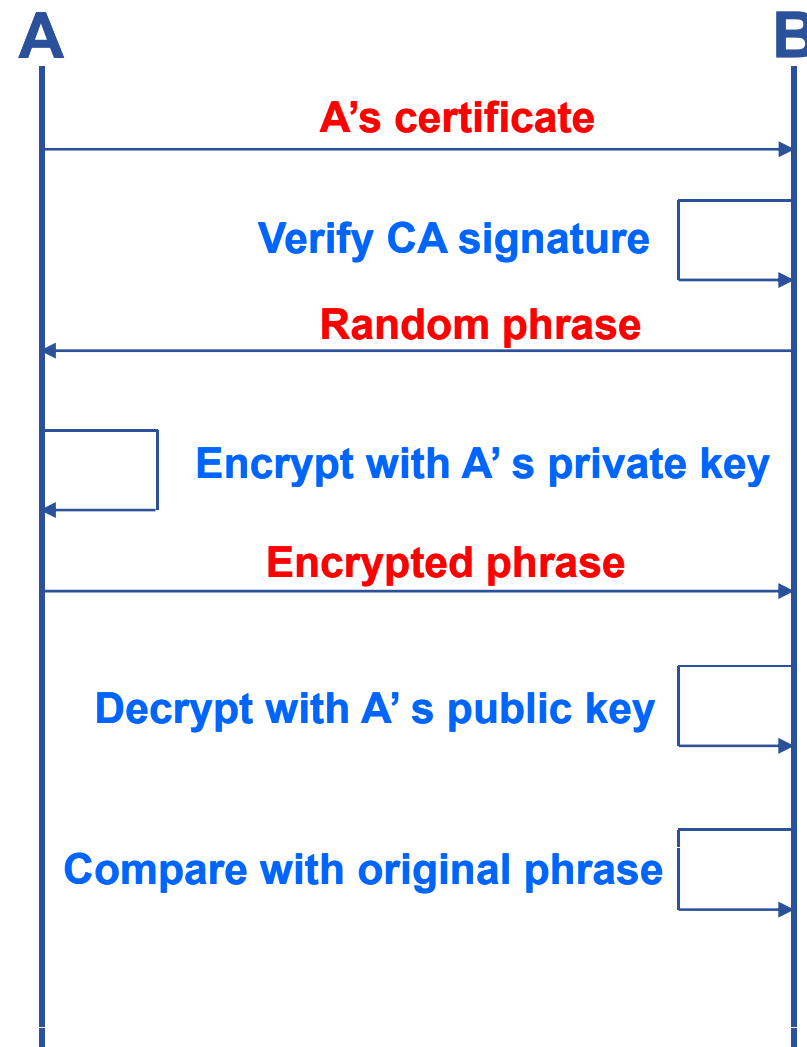


- **Public key** is wrapped into a “certificate”
- **Certificate** is created by trusted third parties: Grid Certification Authorities (CA)
- **Private key** is stored in an encrypted form – protected by a passphrase
- **Private key** is created by the grid user
- **Private key** can be accessed only by the owner



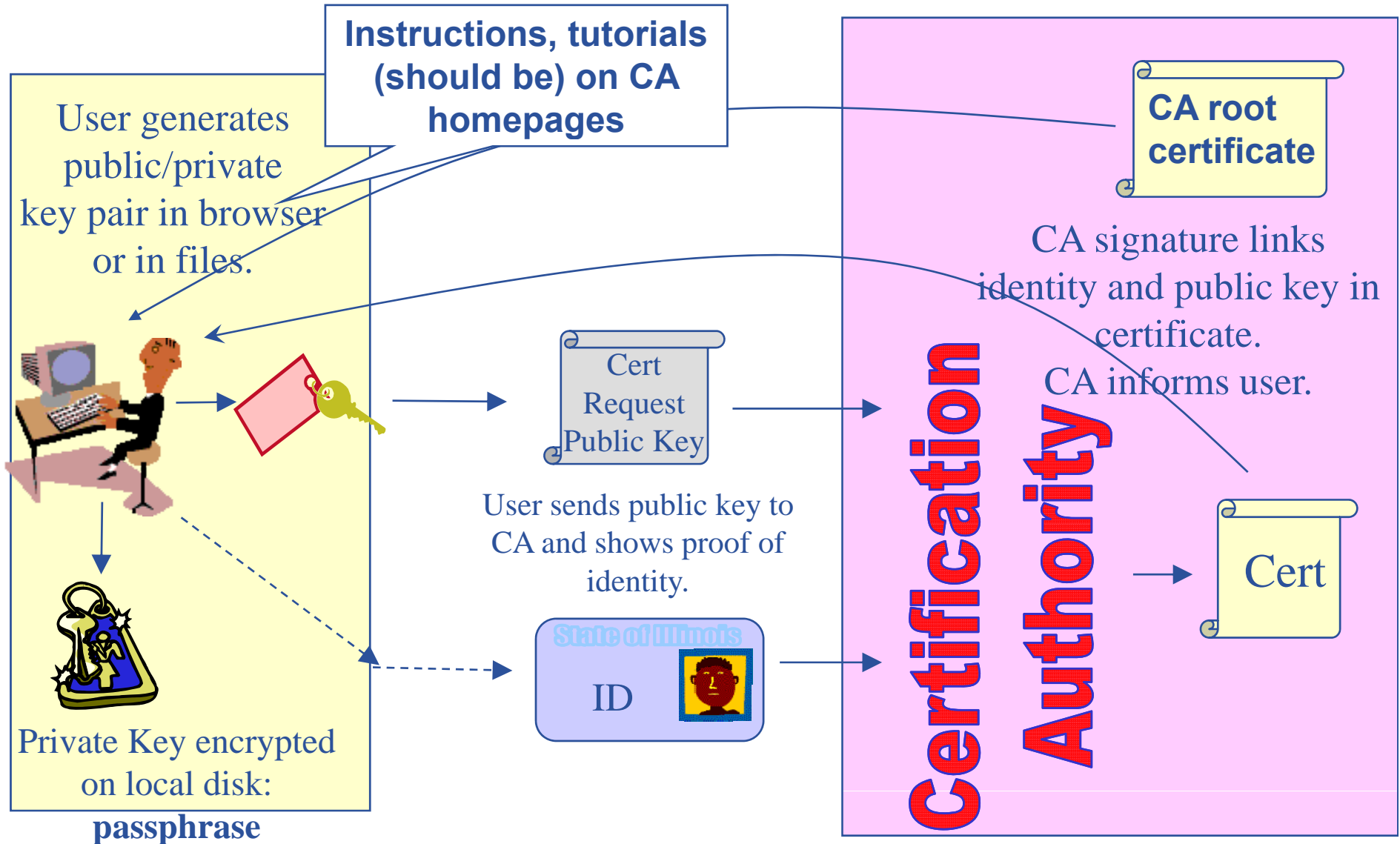
Based on X.509 PKI:

- every Grid transaction is mutually authenticated:
 1. A sends his certificate;
 2. B verifies signature in A's certificate using CA public certificate;
 3. B sends to A a challenge string;
 4. A encrypts the challenge string with his private key;
 5. A sends encrypted challenge to B
 6. B uses A's public key to decrypt the challenge.
 7. B compares the decrypted string with the original challenge
 8. If they match, B verified A's identity and A can not repudiate it.
 9. Repeat for A to verify B's identity



- **Grid user must generate private and public key**
- **Public key must be signed by a recognized CA**
 - CAs can establish a number of people “registration authorities” RAs: Personal visit to the nearest RA instead of the national CA
- **CAs recognized by EGEE: <http://www.gridpma.org/>**
 - Per continent
 - Per country
 - *Per region*

Issuing a grid certificate



- **Keep your private key secure**
 - if possible *on a USB drive only*
- **Do not loan your certificate to anyone**
- **Report to your CA if your certificate has been compromised.**
- **Private key and certificate can be:**
 - 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.


```
[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

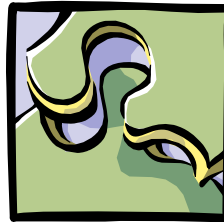
Delegated credentials will not be revoked

User Interface



Submit job
(Delegate proxy)

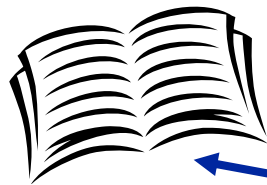
Resource Broker



create
proxy

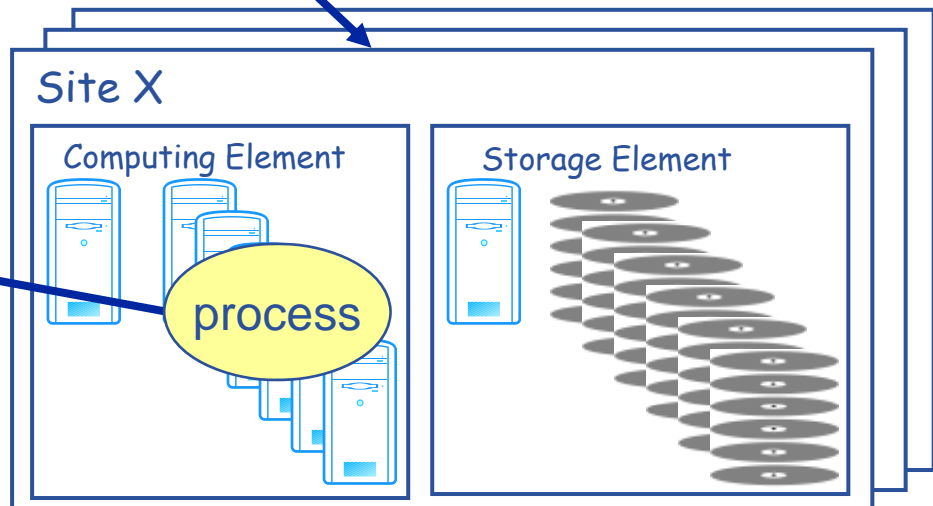
Submit job
(Delegate proxy)

File and Replica Catalog



Authorization Service
(VO Management Service)

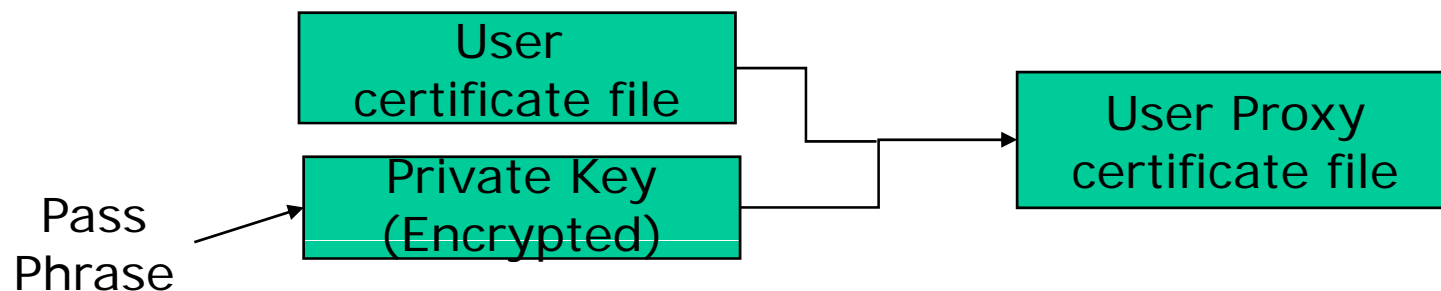
Read/write data



- Do not launch a delegation service for longer than your current task needs.

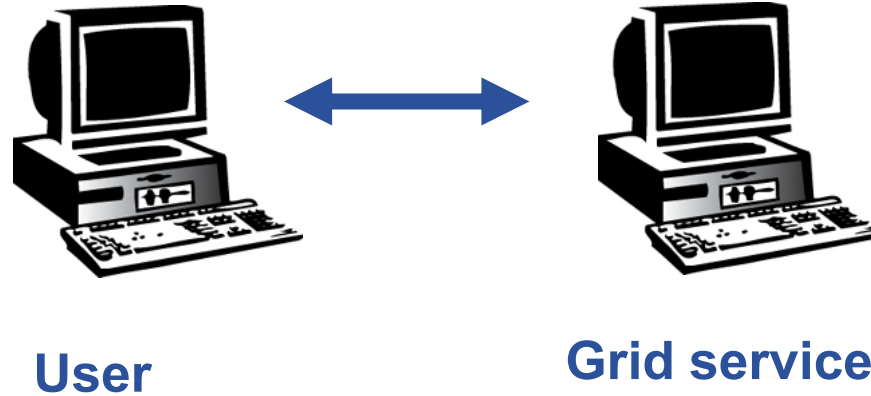
If your certificate *or delegated service* is used by someone other than you, it cannot be proven that it was not you.

- User enters pass phrase, which is used to decrypt private key.
- New private and new public key-pair generated and saved into proxy file
- Original private key is used to sign the proxy file
 - User's private key not exposed after proxy has been signed



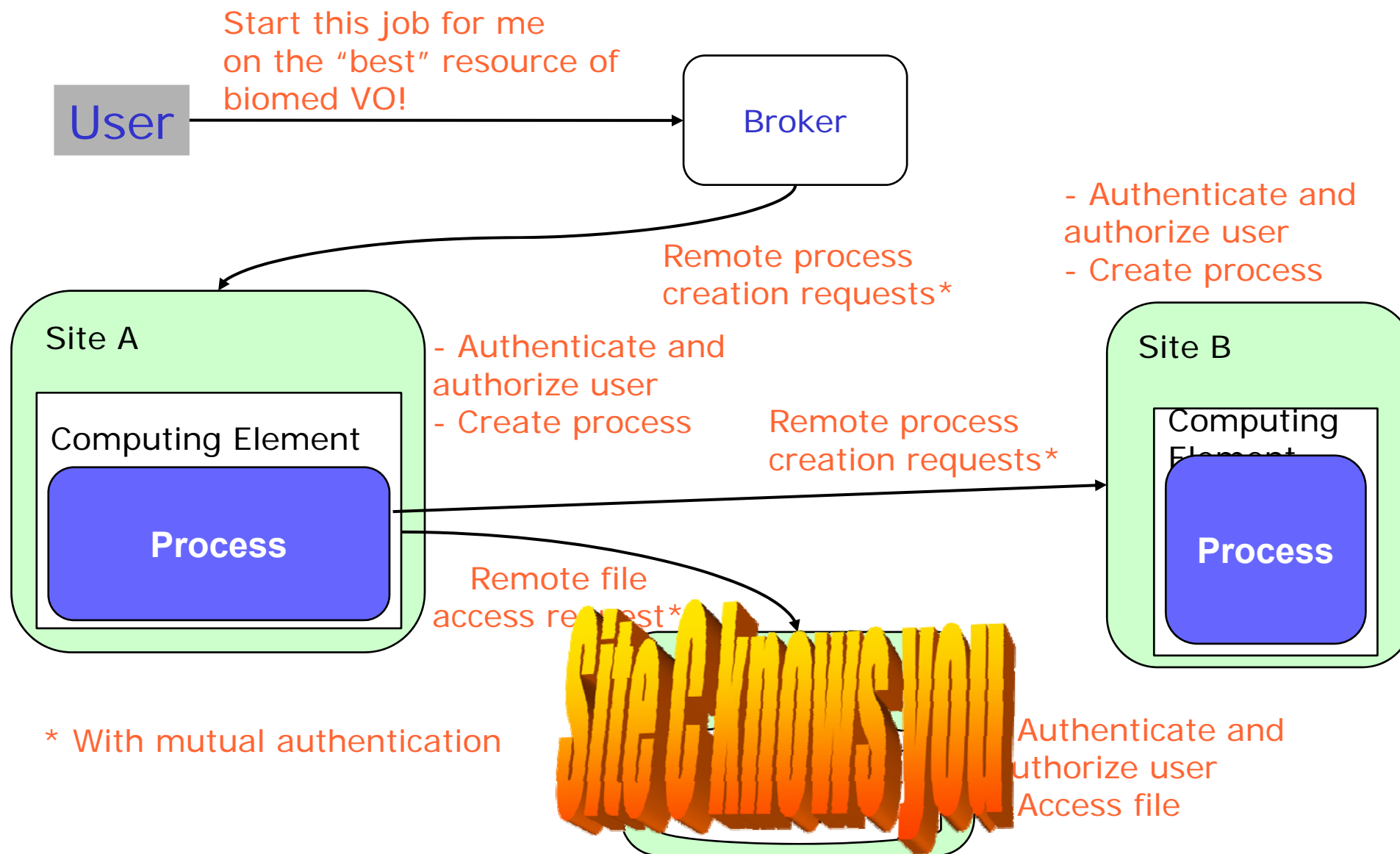
- Proxy file saved in `/tmp`
 - the private key part of the Proxy is *not* encrypted:
 - proxy lifetime is short (typically 12 h) to minimize security risks.
- NOTE: No network traffic during proxy creation!

- **voms-proxy-init** \equiv “login to the Grid”
- **To “logout” you have to destroy your proxy:**
 - `voms-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:**
 - `voms-proxy-info`
 - Options for printing proxy information
 - subject -issuer
 - type -timeleft
 - strength -help

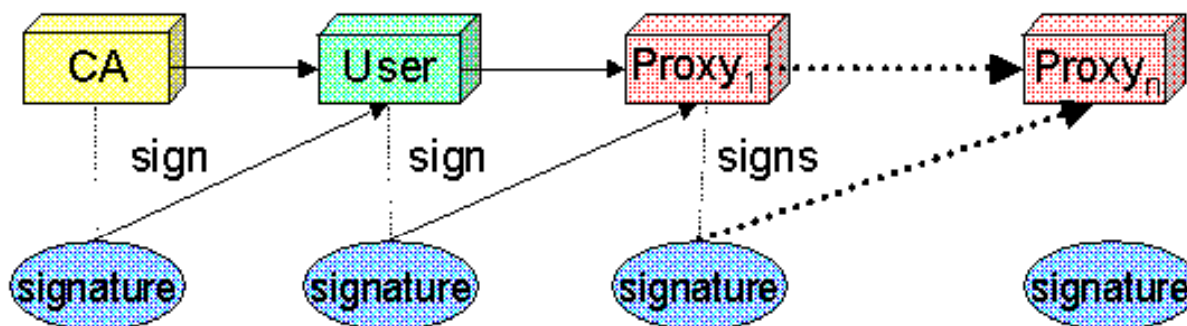


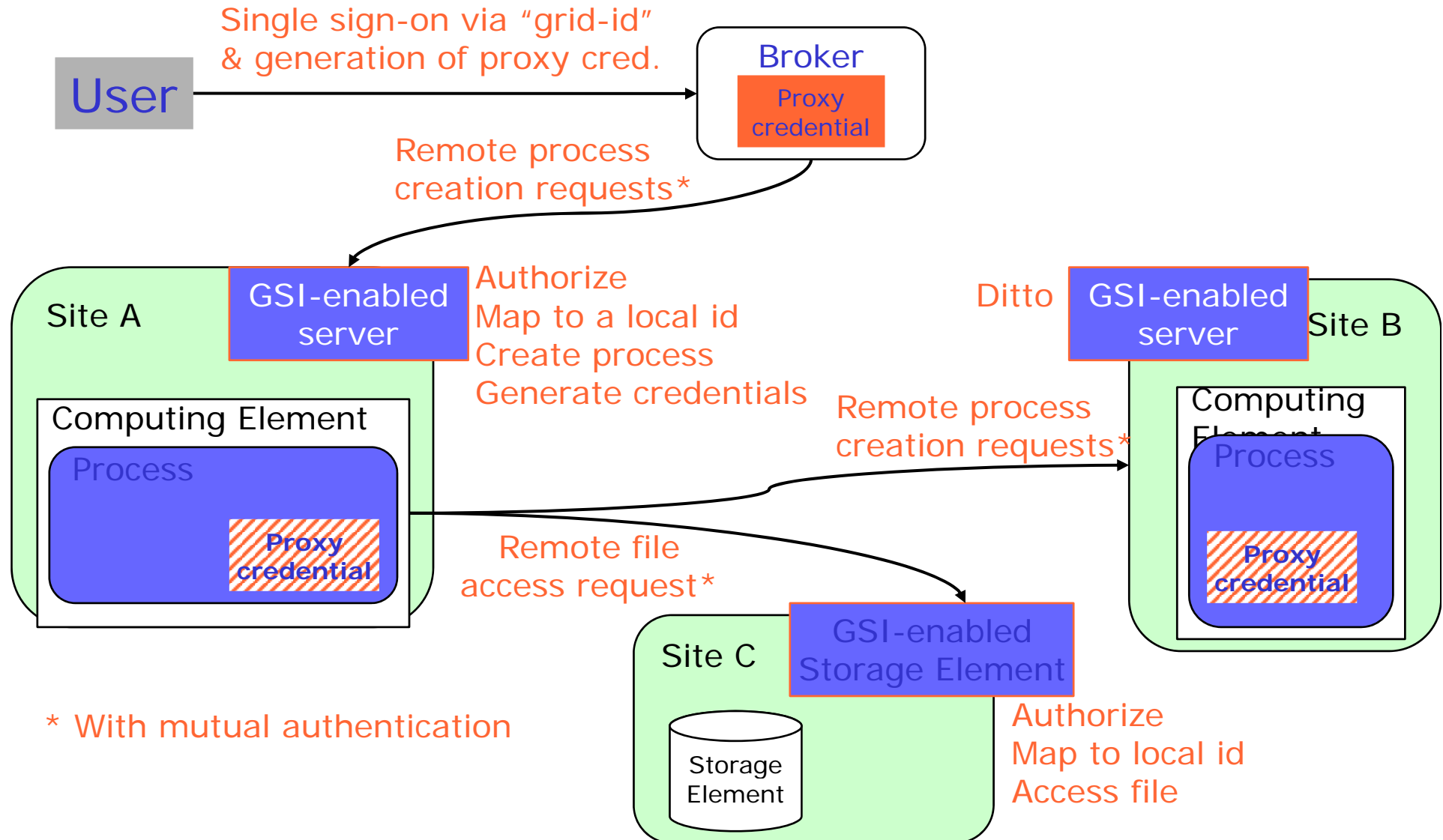
Members of a VO communicate over the Internet

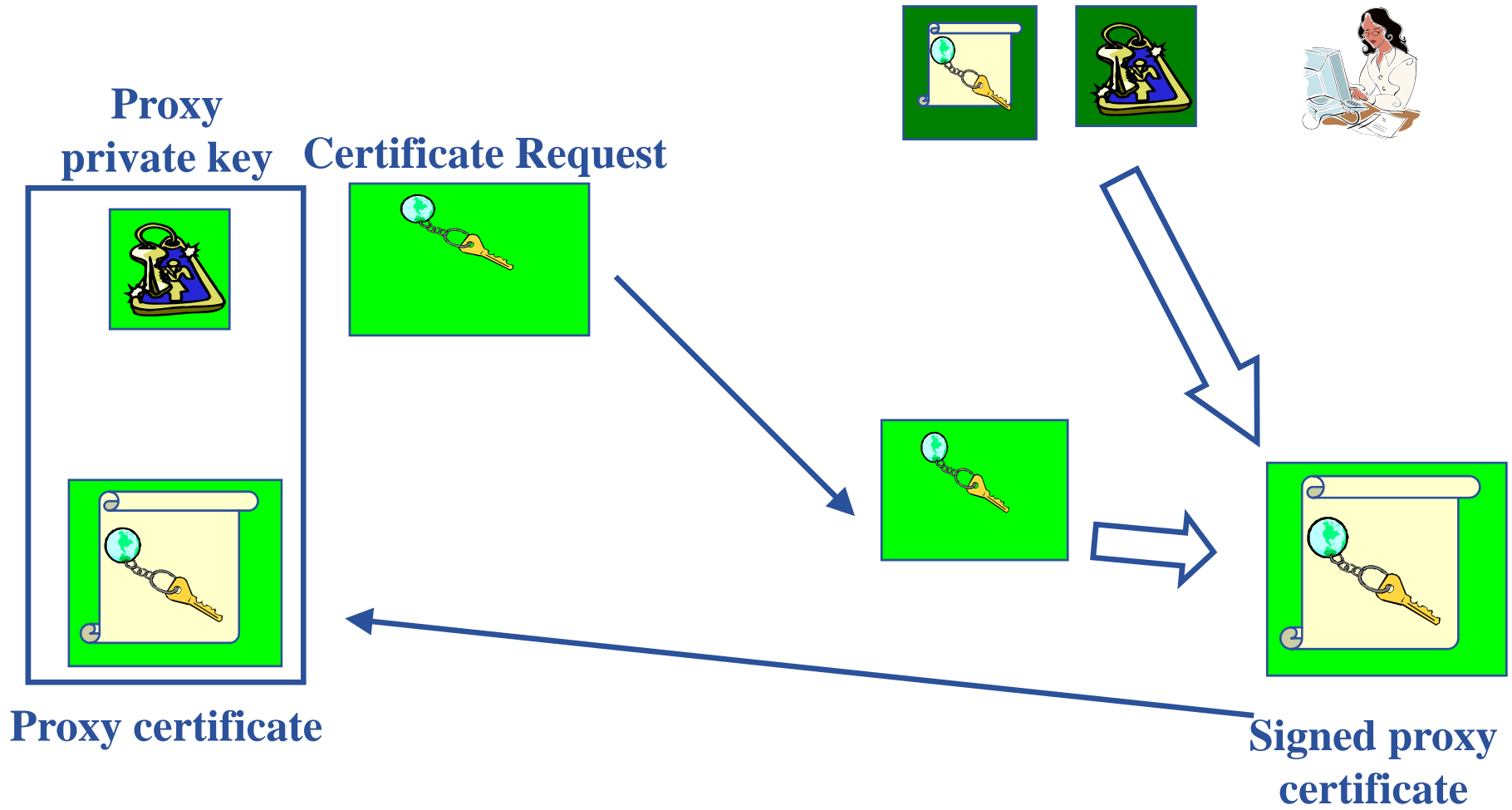
- How can communication endpoints be identified? ✓
 - Authentication
- How can a secure channel established between two partners?
 - Encryption ✓
 - Non-repudiation ✓
 - Integrity ✓



- **Delegation - allows remote process and services to authenticate **on behalf of the user****
 - Remote process/service “**impersonates**” 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







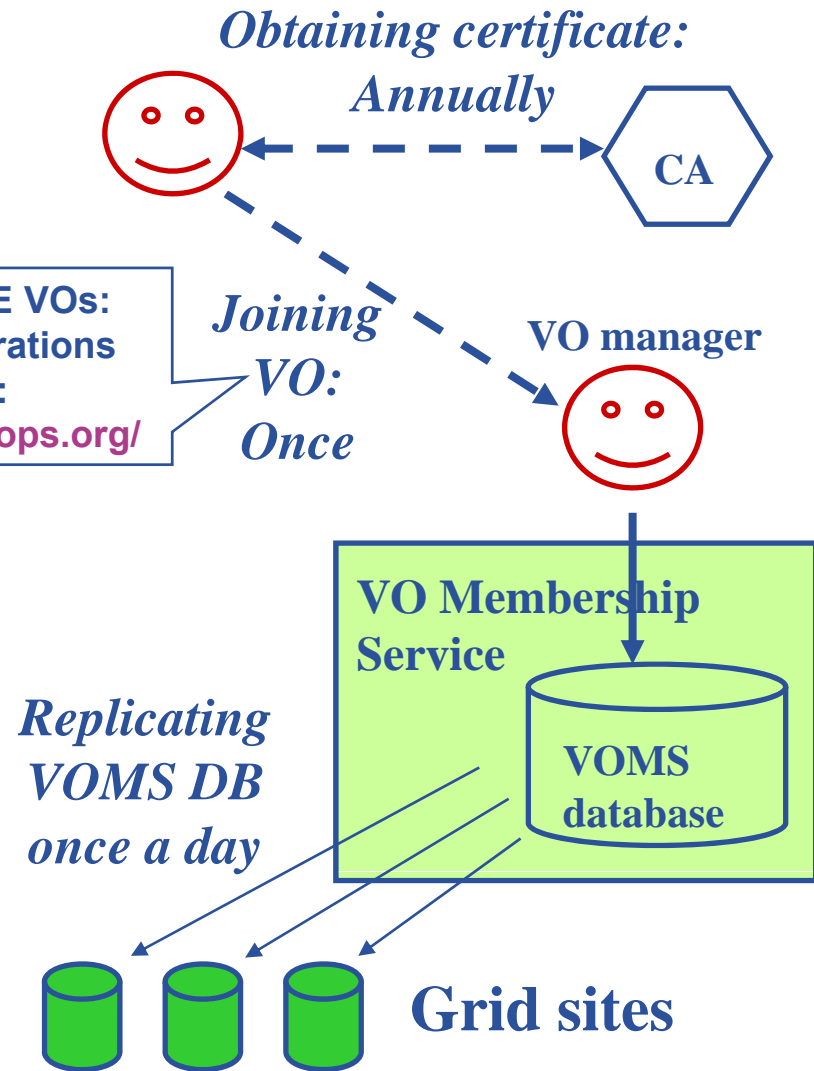
Security at VO level

- Users (and machines) are identified by certificates.
- VOMS keeps list of people who are registered to a VO

Steplist

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

List of EGEE VOs:
On CIC Operations Portal:
<http://cic.gridops.org/>

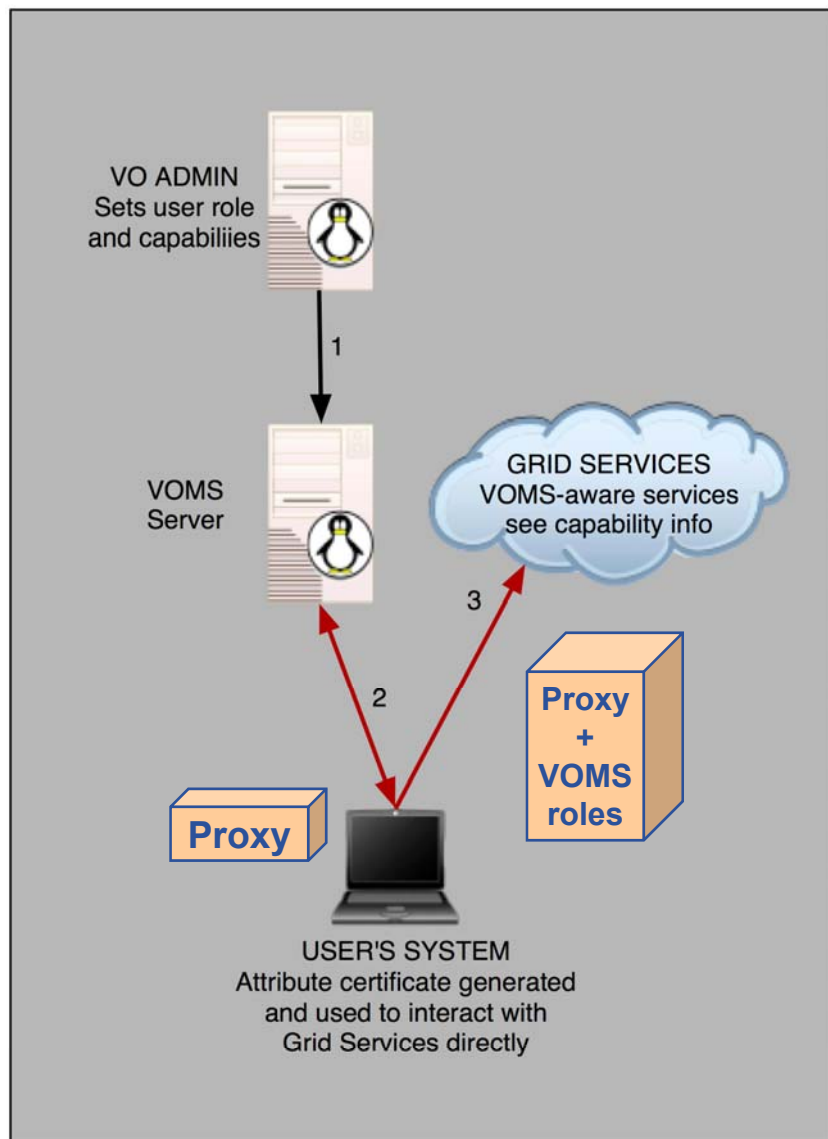


User's identity = Subject of certificate:

`$ grid-cert-info -subject`

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

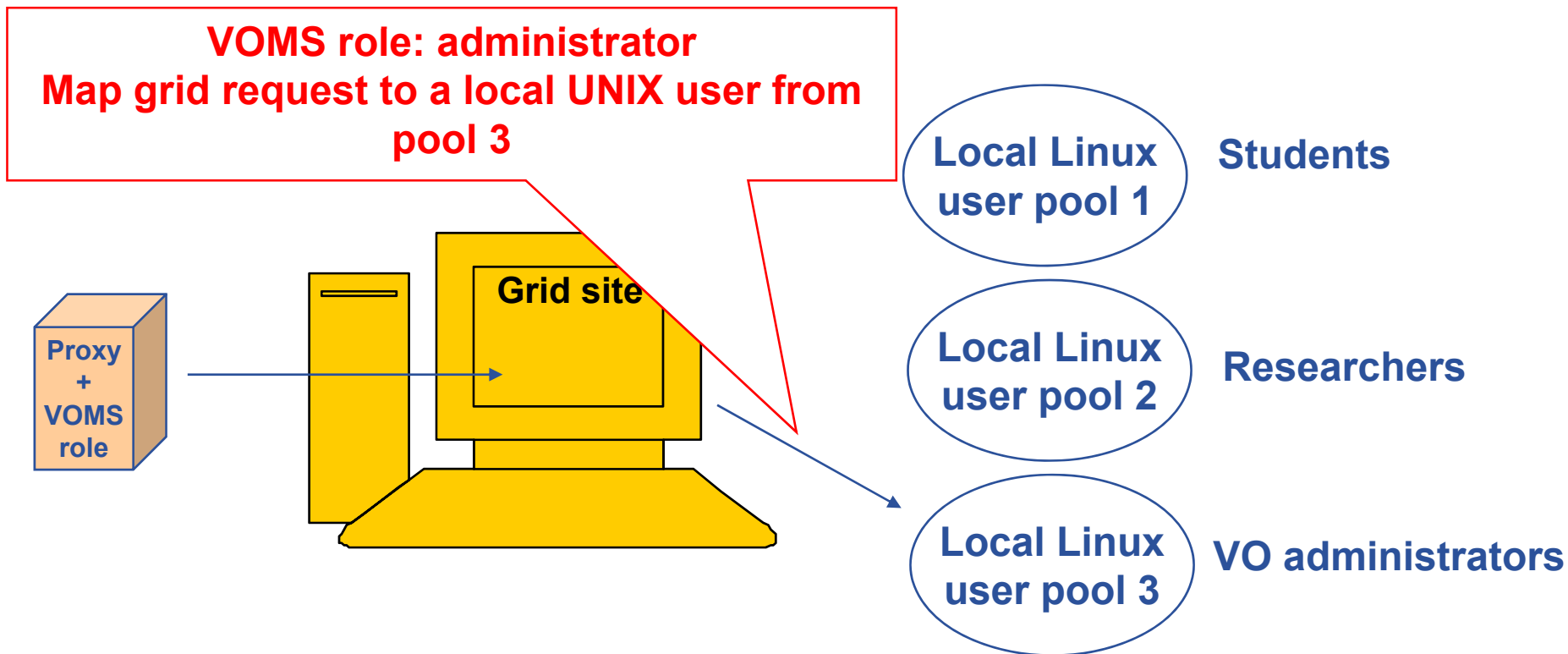
- **VO can have groups**
 - Different rights for each
 - Different groups of experimentalists
 - ...
 - Nested groups
- **VOMS has roles**
 - Assigned to specific purposes
 - E,g. system admin
 - When assume this role
- **VO members belong to one/more groups and can have extra roles**



- **voms-proxy-init**
 - Creates a proxy locally
 - Contacts the VOMS server and extends the proxy with a role
 - VOMS server signs the proxy
 - Sites of the VO recognise and accept signature of VOMS

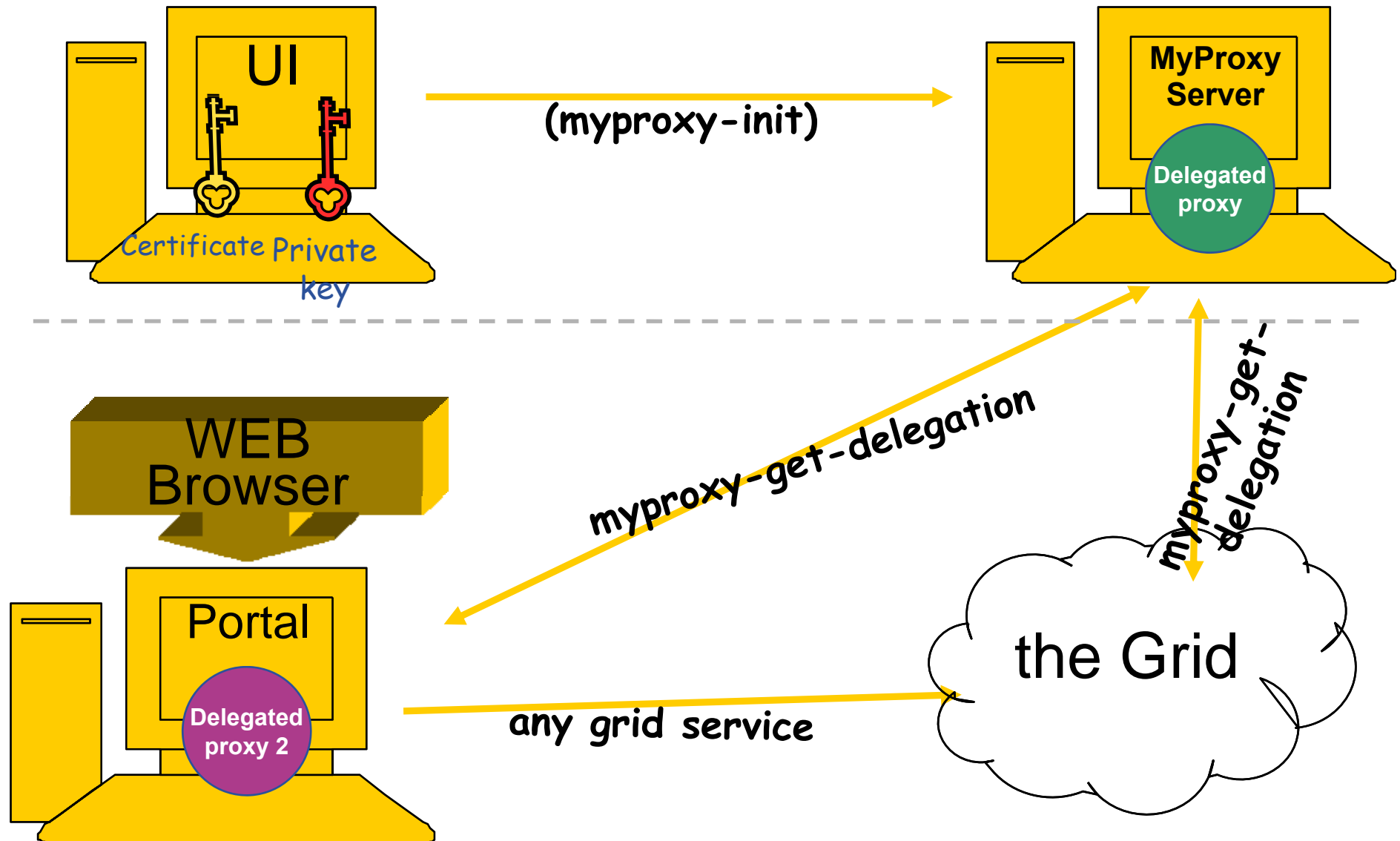
`voms-proxy-init -voms gilda`

- **Allows VOs to centrally manage user roles**



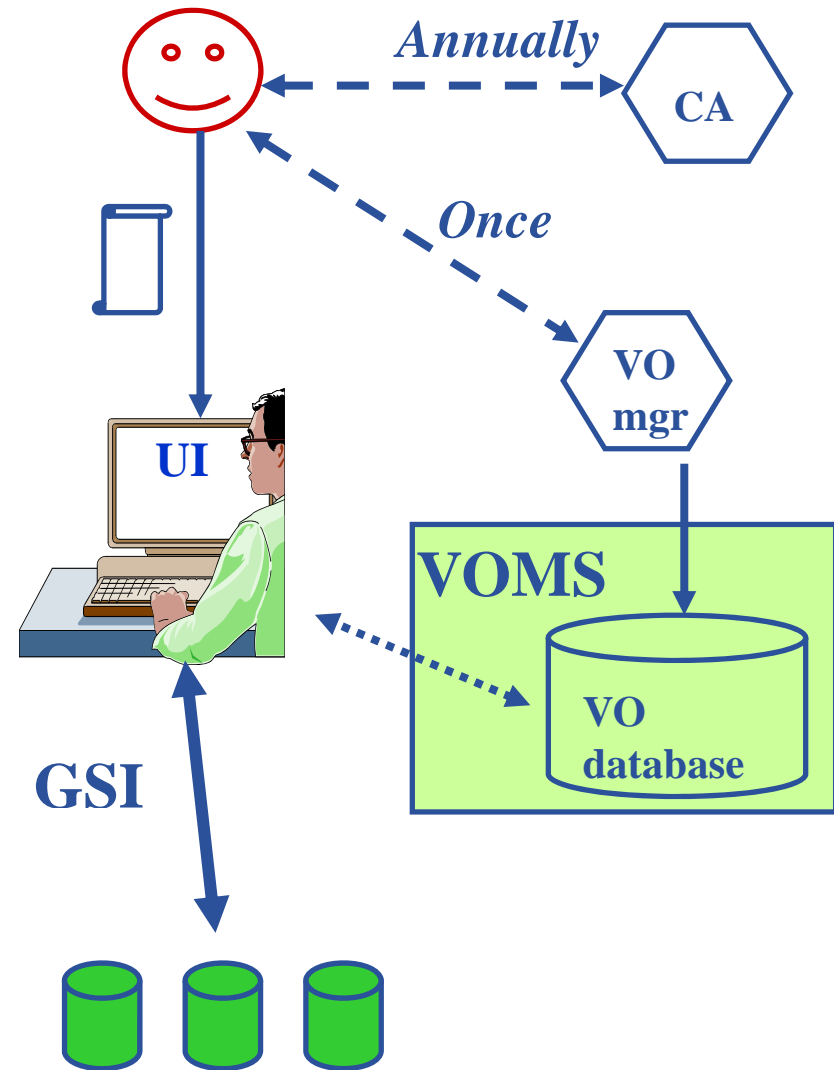
**The grid user can perform those actions on the site
that any Linux user from pool 3 is allowed to**

- **You may need:**
 - To interact with a grid from many machines
 - And you realise that you must NOT, EVER leave your certificate where anyone can find and use it....
 - Your job may need a long proxy
 - And you should keep the lifetime of delegated proxy short
- **Solution: you can store a long term proxy in a “MyProxy server” and derive a short living proxy certificate when needed**
- **MyProxy ~ storage for proxy files**



- **Obtain a certificate from a recognized CA:**
 - www.gridpma.org → 1 year long, renewable certificates, accepted in every EGEE VO
- **Find and register at a VO**
 - EGEE NA4 - CIC Operations portal: <http://cic.gridops.org/>
- **Use the grid:**
 - **command line clients and APIs installed on the User Interface**
(UI is maintained by the VO / your institute / you)
 - **voms-proxy-init -voms <voName>**
 - **voms-proxy-destroy**
 - **Portals and long-running jobs**
 - Typically involve interaction with MyProxy

- **User obtains certificate from Certificate Authority**
 - Import it into your browser
 - Have it on a User Interface
- **User selects and joins VO**
- **User connects to UI by ssh**
 - Create proxy
 - Submit jobs, manage files, ...



Security basics:

- Investigate your certificate
- Create proxy
- Investigate your proxy
- Destroy your proxy

- Create proxy again
- Submit job



Enabling Grids for E-scienceE

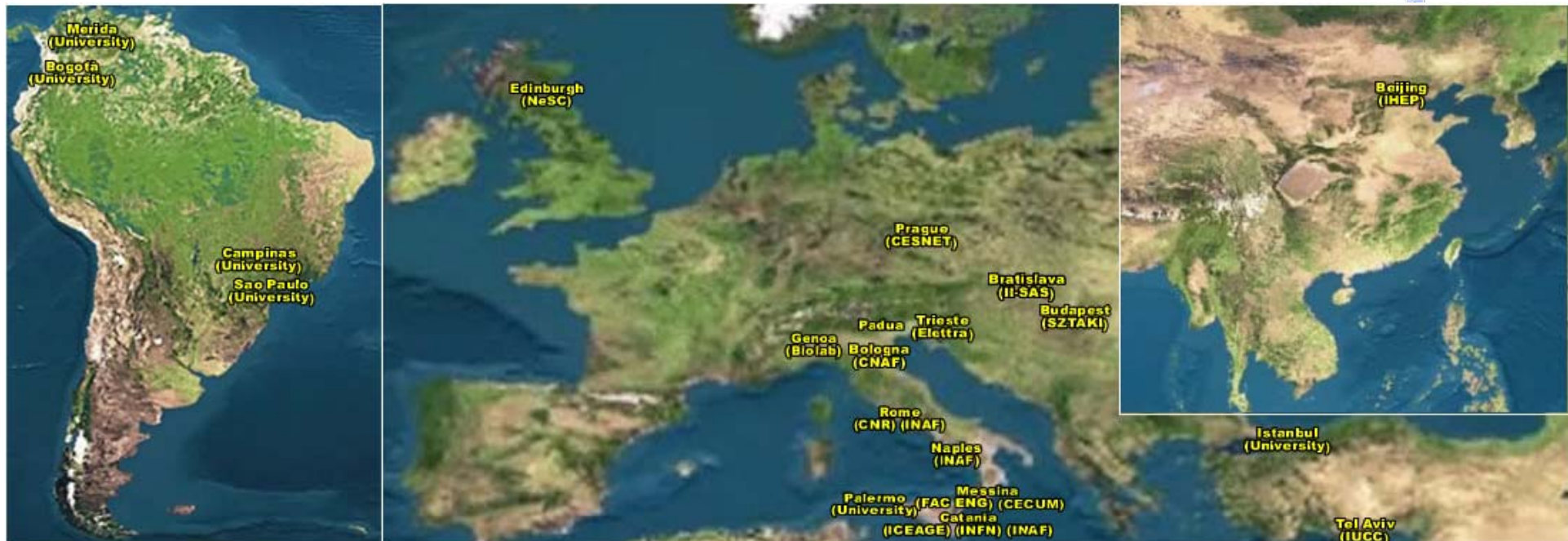
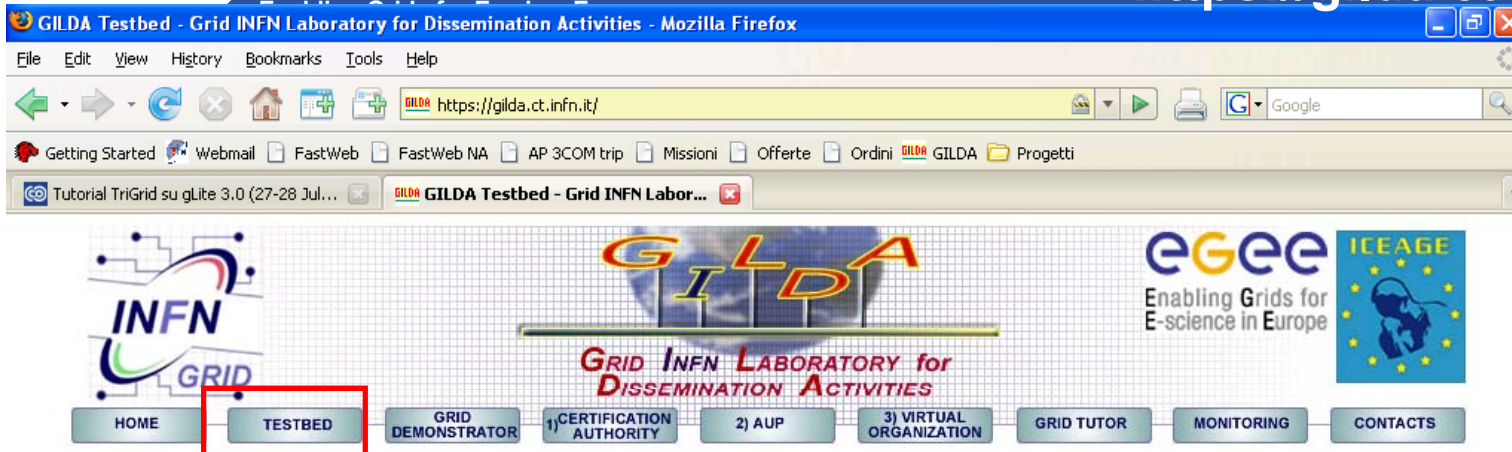
GILDA Training Infrastructure

www.eu-egee.org



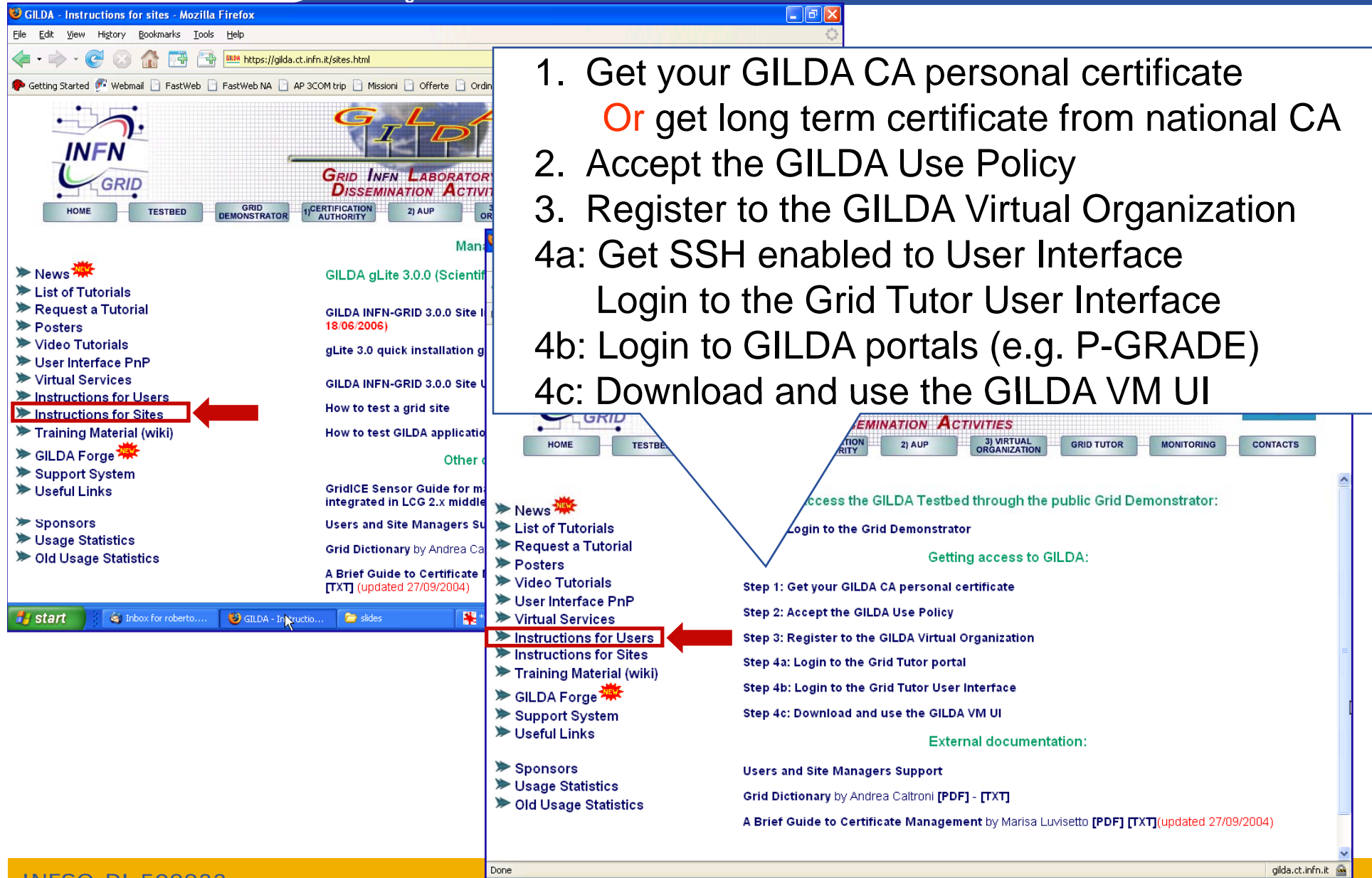
INFSO-RI-508833

- **Why t-infrastructure?**
 - Training is necessary!
 - Production VOs for production
 - T-Infrastructure for training
- **Need guaranteed response for tutorials; limit the vulnerability of production systems**
 - have a training CA – lightweight authentication
 - able to change middleware to prepare participants for future releases on production system
 - need safe resources for installation training
 - easy entry point for new communities



~10 sites in 3 continents

SERVICE	HOST
User Interface (UI)	glite-tutor.ct.infn.it
Backup User Interface (UI)	glite-tutor2.ct.infn.it
P-GRADE Portal	http://portal.p-grade.hu/gilda
LCG Resource Broker (RB)	glite-rb.ct.infn.it
gLite Resource Broker (WMS 3.0)	glite-rb2.ct.infn.it
gLite (WMproxy) Resource Broker (WMS 3.1)	glite-rb3.ct.infn.it
Information Index (BDII)	glite-rb.ct.infn.it:2170
VOMS server	voms.ct.infn.it:8443/voms/gilda
DGAS Price Authority	grid-demo1.ct.infn.it:56568
DGAS HLR	grid-demo1.ct.infn.it:56567
GridICE Monitoring System	alifarm7.ct.infn.it:50080
Services Availability Monitoring (SAM)	https://sam.ct.infn.it/sam/sam.py
Services Status (GStat)	http://goc.grid.sinica.edu.tw/gstat/gilda/
LCG File Catalog (LFC)	lfc-gilda.ct.infn.it
gLite File Transfer Service	fts.ct.infn.it
...	...



1. Get your GILDA CA personal certificate
 Or get long term certificate from national CA

2. Accept the GILDA Use Policy

3. Register to the GILDA Virtual Organization

4a: Get SSH enabled to User Interface
 Login to the Grid Tutor User Interface

4b: Login to GILDA portals (e.g. P-GRADE)

4c: Download and use the GILDA VM UI

Getting access to GILDA:

Step 1: Get your GILDA CA personal certificate

Step 2: Accept the GILDA Use Policy

Step 3: Register to the GILDA Virtual Organization

Step 4a: Login to the Grid Tutor portal

Step 4b: Login to the Grid Tutor User Interface

Step 4c: Download and use the GILDA VM UI

External documentation:

Users and Site Managers Support

Grid Dictionary by Andrea Caltroni [PDF] - [TXT]

A Brief Guide to Certificate Management by Marisa Luvisetto [PDF] [TXT] (updated 27/09/2004)

- **30 user certificates were obtained from GILDA CA**
 - One private key + one public key per person
- **Certificates have been registered at GILDA VO**
- **40 accounts were created on User Interface machine**
 - For command line tutorials (including GridWay and GANGA)
- **Certificate and private key are available on User Interface**
 - \$HOME/.globus/userkey.pem
 - \$HOME/.globus/usercert.pem
- **Certificates were uploaded into GILDA MyProxy server**
 - For P-GRADE Portal tutorial



Enabling Grids for E-scienceE

Thank you!

Questions?

www.eu-egee.org

