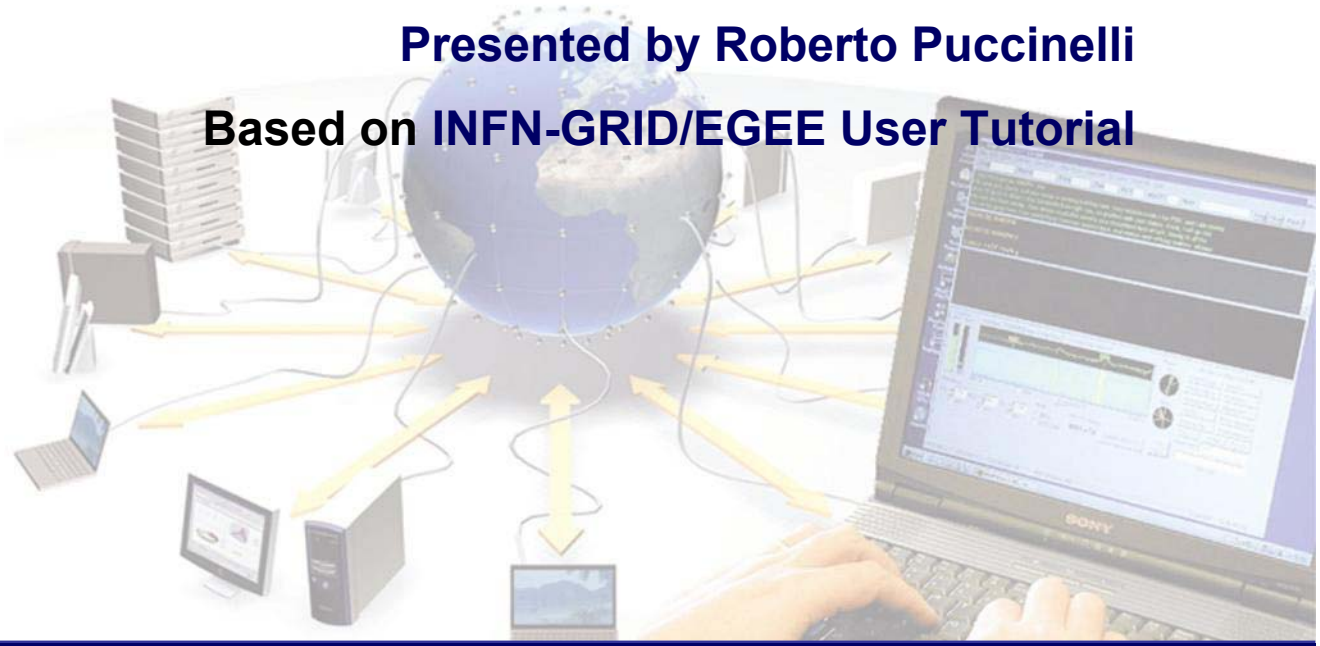
Enabling Grids for E-science in Europe

ESRIN Grid Workshop Tutorial
Introduction to Grid Computing
Frascati, 3 February 2005

Security on Grid:

Presented by Roberto Puccinelli

Based on INFN-GRID/EGEE User Tutorial



EGEE is a project funded by the European Union under contract IST-2003-508833

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 Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS
- Security in action

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 Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS
- Security in action

Glossary

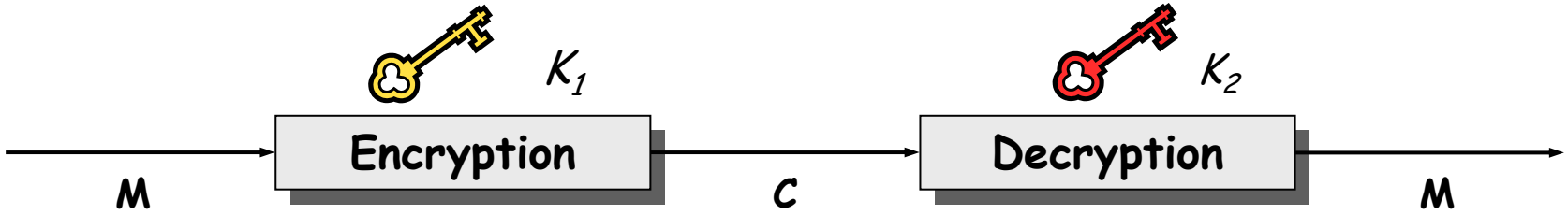
Enabling Grids for E-science in Europe

- Principal
  - An entity: a user, a program, or a machine
- Credentials
  - Some data providing a proof of identity
- Authentication
  - Verify the identity of the 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

Overview

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

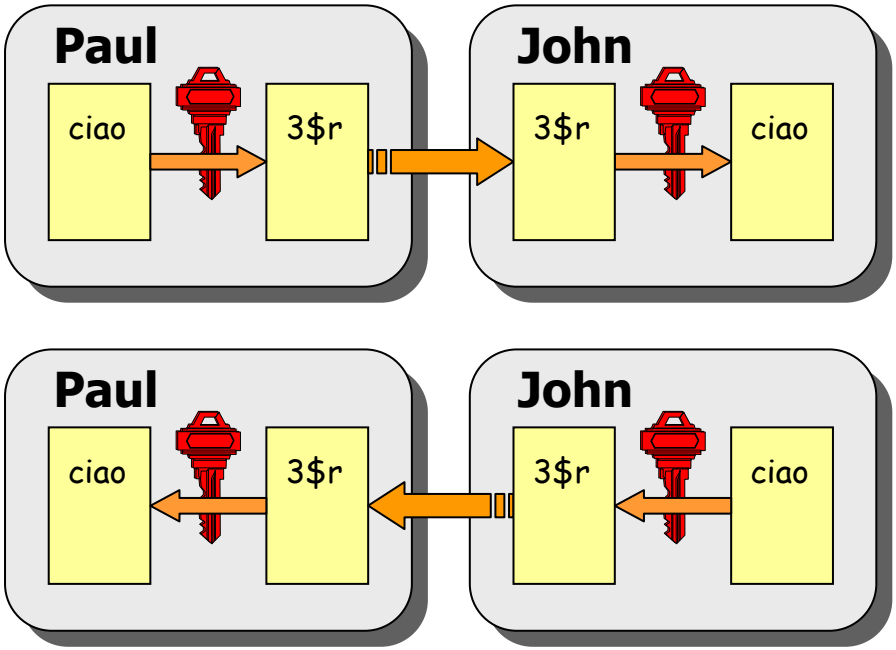
Cryptography



- Mathematical algorithm that provides 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**: $K_1 \neq K_2$

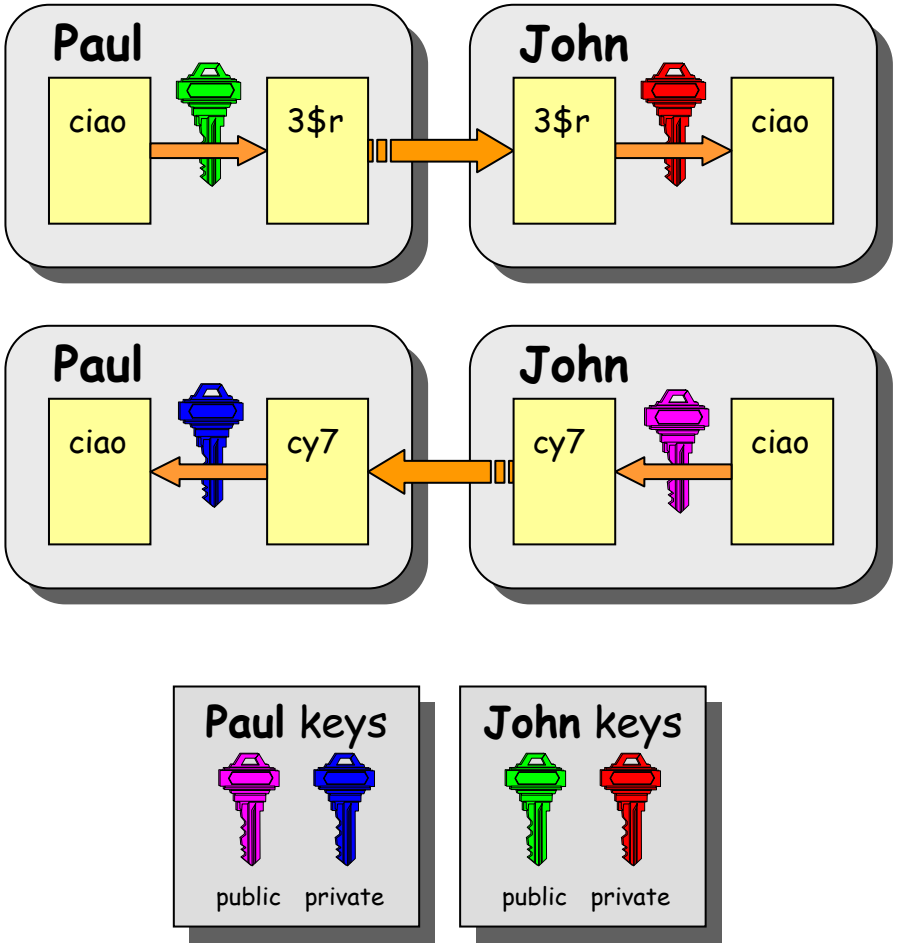
Symmetric Algoritms

- 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 decripted **only** by the other one.
- No exchange of secrets is necessary
  - the sender cyphers using the *public* key of the receiver;
  - the receiver decripts using his *private* key;
  - the number of keys is O(n).
- Examples:
  - **Diffie-Helmann** (1977)
  - **RSA** (1978)



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 Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS
- Security in action

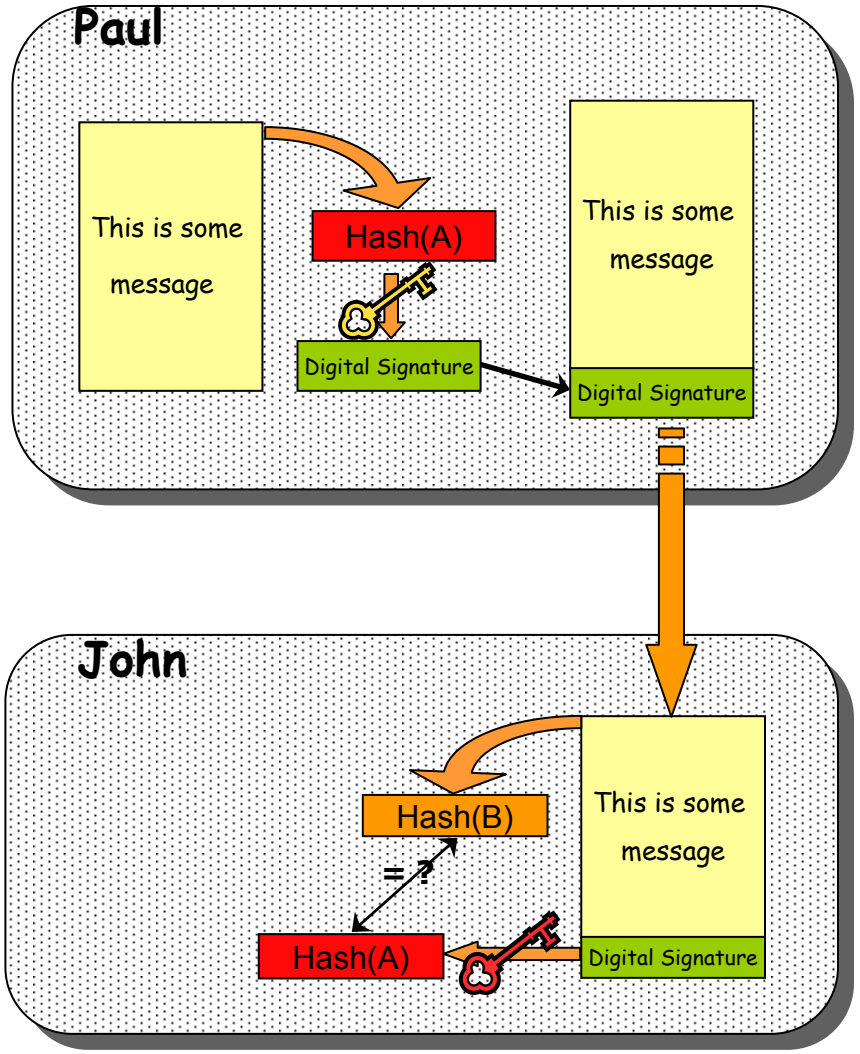
One-Way Hash Functions

Enabling Grids for E-science in Europe

- Functions (*H*) that given as input a variable-length message (*M*) produce as output a string of fixed length (*h*)
  - the length of *h* must be at least 128 bits (to avoid *birthday attacks*)
  1. given *M*, it **must be easy** to calculate $H(M) = h$
  2. given *h*, it **must be difficult** to calculate $M = H^{-1}(h)$
  3. given *M*, it **must be difficult** to find *M'* such that $H(M) = H(M')$
- Examples:
  - **SNEFRU**: hash of 128 or 256 bits;
  - **MD4/MD5**: hash of 128 bits;
  - **SHA** (Standard FIPS): hash of 160 bits.

Digital Signature

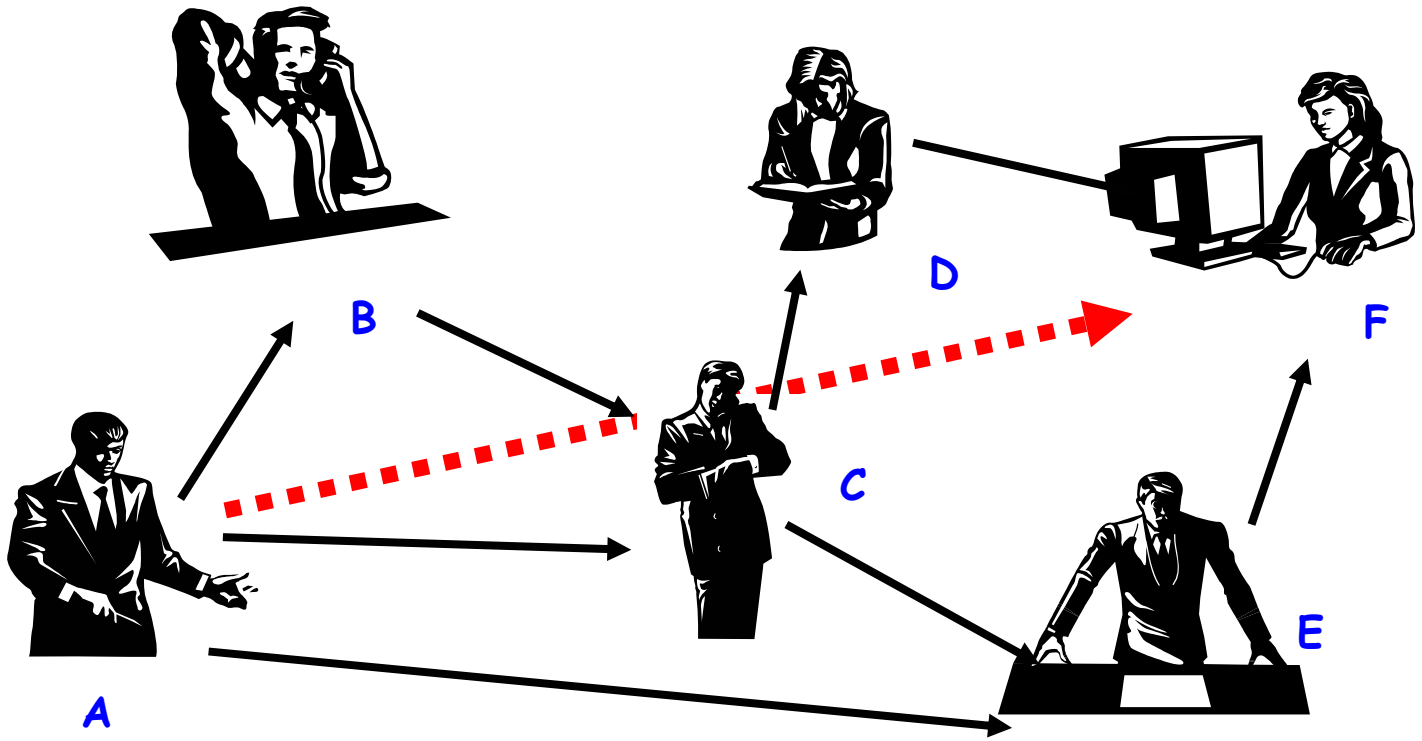
- **Paul** calculates the ***hash*** of the message
- **Paul** encrypts the hash using his ***private*** key: the encrypted hash is the ***digital signature*****.**
- **Paul** sends the signed message to **John.**
- **John** calculates the hash of the message and ***verifies*** it with the one received by A and decyphered with A'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**.

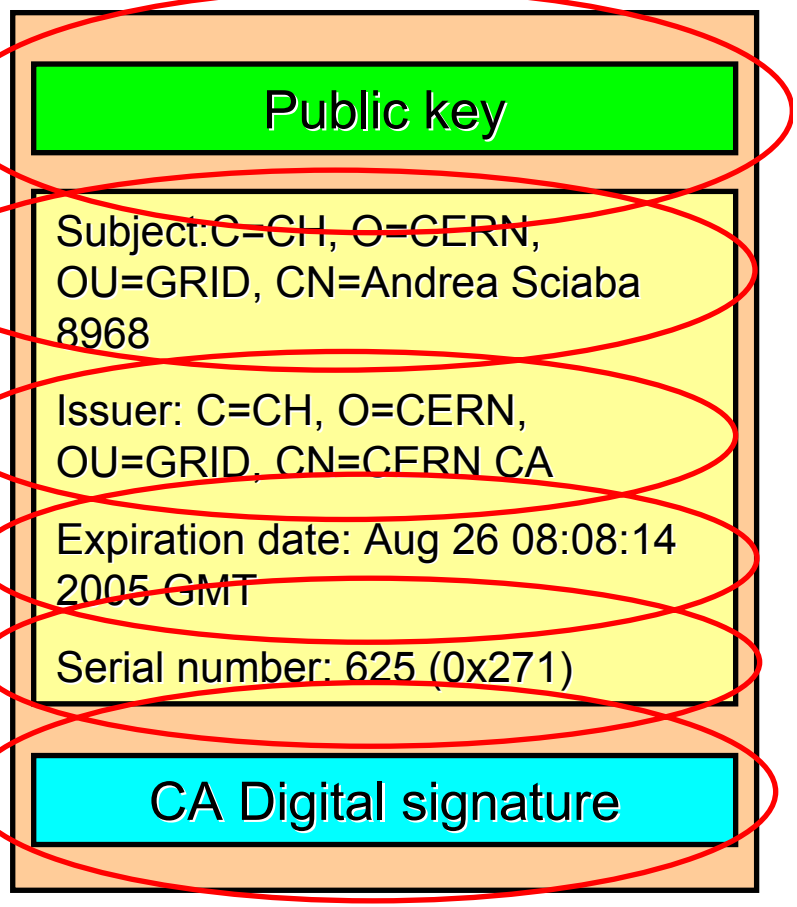
X.509

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

- Issue **Digital Certificates** for users, programs and machines
- Check the 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



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 Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS
- Security in action

GRID Security: the players

Enabling Grids for E-science in Europe

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*

Grid

Sites

- *Heterogeneous Resources*
- *Access Patterns*
- *Local policies*
- *Membership*

The Risks

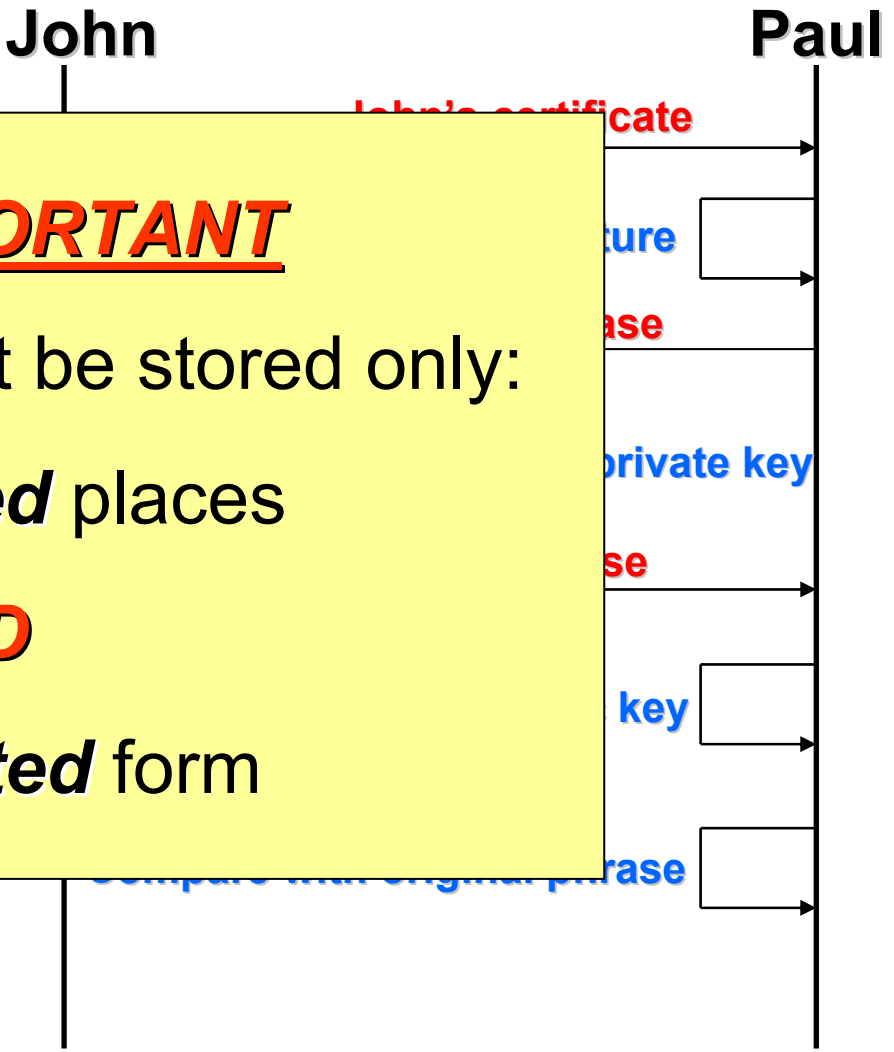
- Launch attacks to other sites
  - Large distributed farms of machines
- Illegal or inappropriate data distribution and access sensitive information
  - Massive distributed storage capacity
- Disruption by exploiting security holes
  - Complex, heterogeneous and dynamic environment
- Damage caused by viruses, worms etc.
  - Highly connected and novel infrastructure

The Grid Security Infrastructure (GSI)

Enabling Grids for E-science in Europe

Based on X.509 PKI:

- every us
  certificat
- certificat
  local site
- every Gr
  authenti
  1. John
  2. Paul
     certif
  3. Paul
  4. John
     his p
  5. John
  6. Paul
     chall
  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

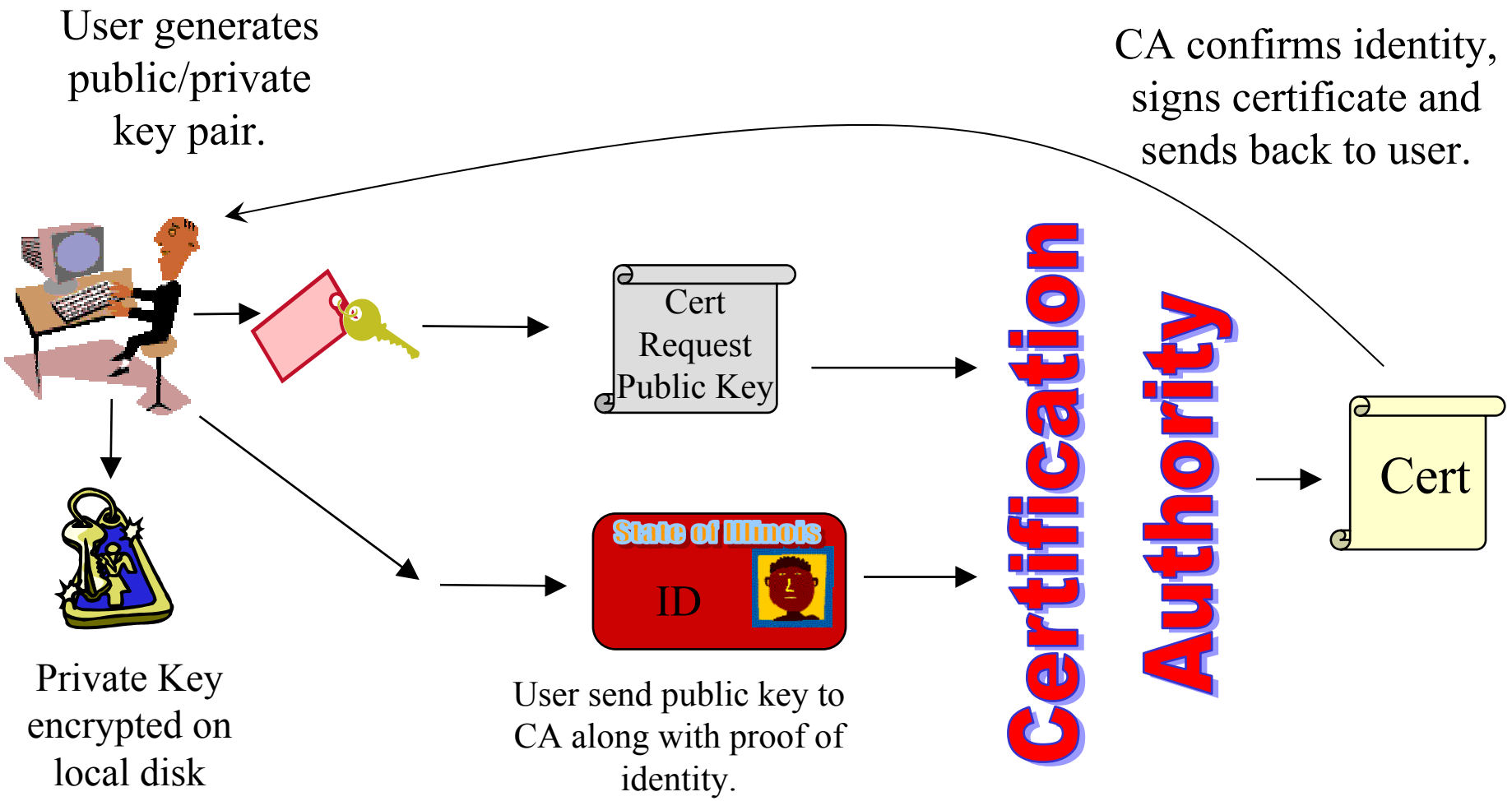
Private keys must be stored only:

in ***protected*** places

AND

in ***encrypted*** form

Certificate Request



Certificate Information

Enabling Grids for E-science in Europe

- To get cert information run grid-cert-info

```
[scampana@grid019:~]$  grid-cert-info -subject

/C=CH/O=CERN/OU=GRID/CN=Simone Campana 7461
```

- Options for printing cert information

-all	-startdate
-subject	-enddate
-issuer	-help

X.509 Proxy Certificate

Enabling Grids for E-science in Europe

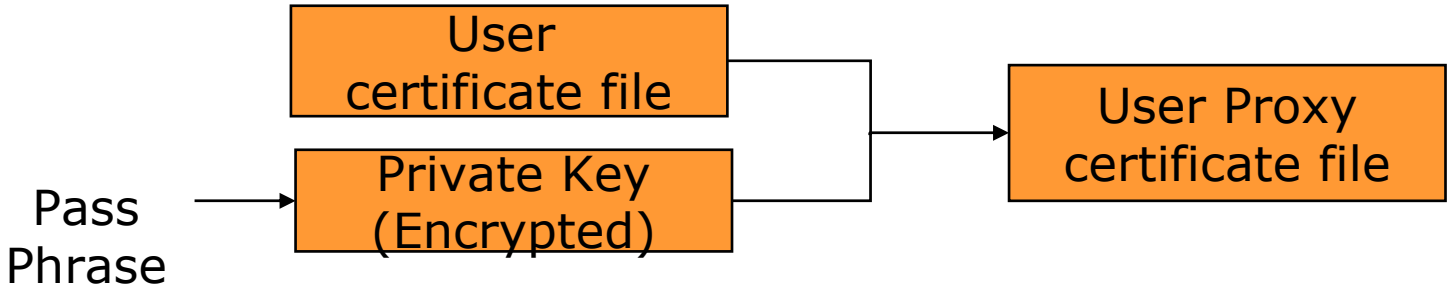
- GSI extension to X.509 Identity Certificates
  - signed by the normal end entity cert (or by another proxy).
- Enables single sign-on
- Support some important features
  - Delegation
  - Mutual authentication
- Has a limited lifetime (minimized risk of “compromised credentials”)
- It is created by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

Enabling Grids for E-science in Europe

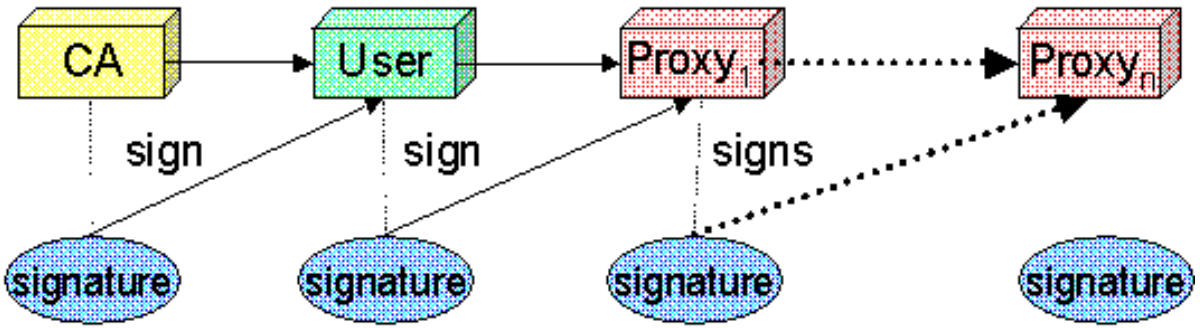
- grid-proxy-init ≡ “login to the Grid”
- To “logout” you have to destroy your proxy:
  - grid-proxy-destroy
  - This does *NOT* destroy any proxies that were delegated from this proxy.
  - You cannot revoke a remote proxy
  - Usually create proxies with short lifetimes
- To gather information about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

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

Delegation and limited proxy

Enabling Grids for E-science in Europe

- 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
- The client can elect to delegate a “limited proxy”
  - Each service decides whether it will allow authentication with a limited proxy
  - Job manager service requires a full proxy
  - GridFTP server allows either full or limited proxy to be used



Long term proxy

Enabling Grids for E-science in Europe

- 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
  - contacts the myproxy server

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_USER_CERT (default: `/etc/grid-security/hostcert.pem`)
  - Private key: X509_USER_KEY (default: `/etc/grid-security/hostkey.pem`)
- Trusted certification authority certificates:
  - X509_CERT_DIR (default: `/etc/grid-security/certificates`)

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 Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS
- Security in action

Virtual Organizations and authorization

Enabling Grids for E-science in Europe

- Grid users MUST belong to Virtual Organizations
  - What we previously called “Groups”
  - Sets of users belonging to a collaboration
  - List of supported VOs:
    - https://lcg-registrar.cern.ch/virtual_organization.html
- VOs maintain a list of their members
  - 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
...
```

/etc/grid-security/grid-mapfile

  - Sites decide which VOs to accept

On the side: user Registration in a VO

- 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 egee/LCG UI)
    - `openssl pkcs12 -export -in usercert.pem -inkey userkey.pem -out my_cert.p12 -name 'My Name'`
- Sign the usage guidelines for the VO
  - You will be registered in the VO-LDAP server (wait for notification)

- Gilda (and other VO):
  - You receive already a PKCS12 certificate (can import it directly into 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`

VOMS, LCAS, LCMAPS

Enabling Grids for E-science in Europe

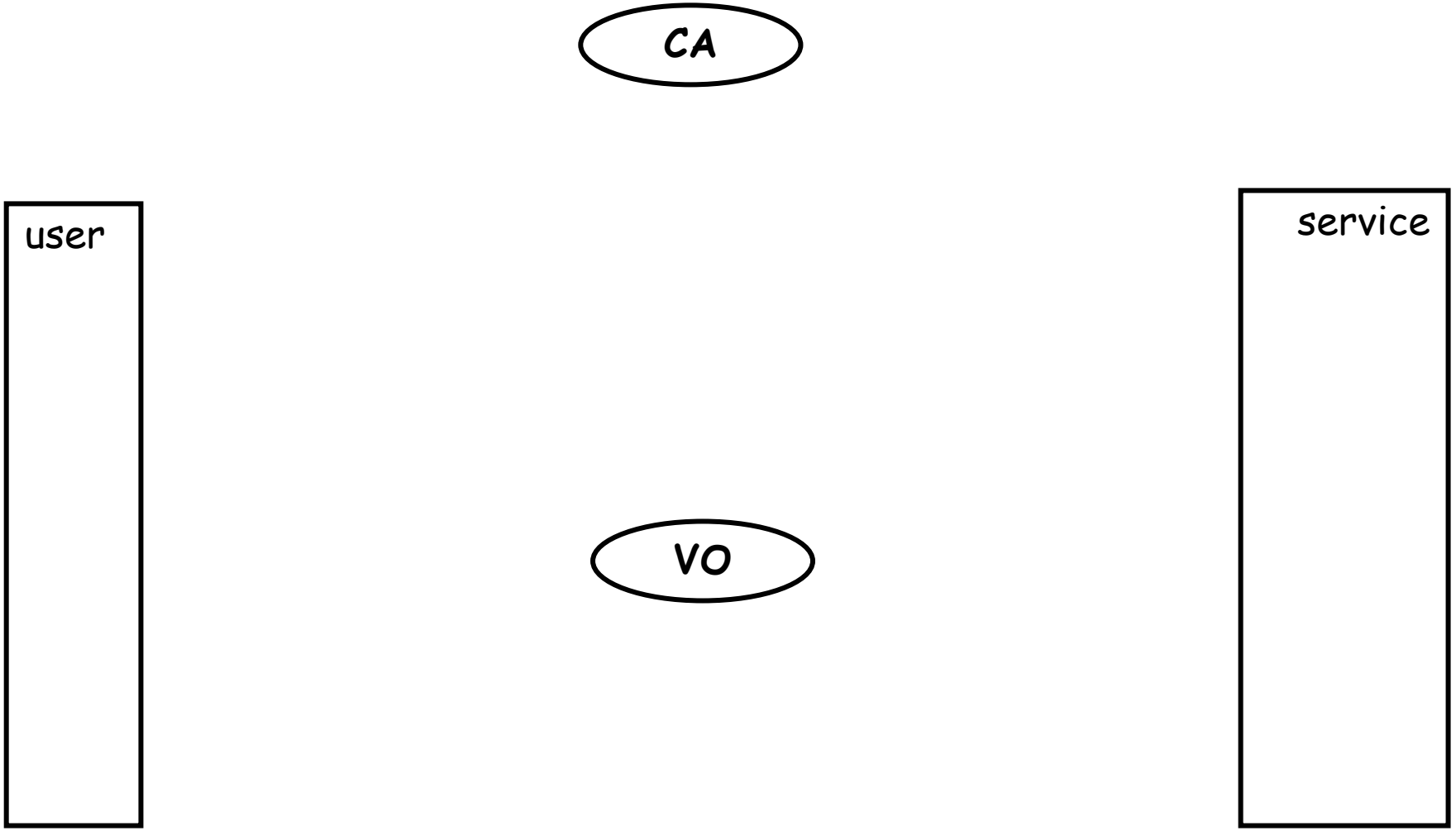
- Virtual Organization Membership Service
  - Extends the proxy info with VO membership, group, role and capabilities
- Local Centre Authorization Service (LCAS)
  - Checks if the user is authorized (currently using the grid-mapfile)
  - Checks if the user is banned at the site
  - Checks if at that time the site accepts jobs
- Local Credential Mapping Service (LCMAPS)
  - Maps grid credentials to local credentials (eg. UNIX uid/gid, AFS tokens, etc.)
  - Currently uses the grid-mapfile (based only on certificate subject)
  - In the near future will map also VOMS group and roles

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

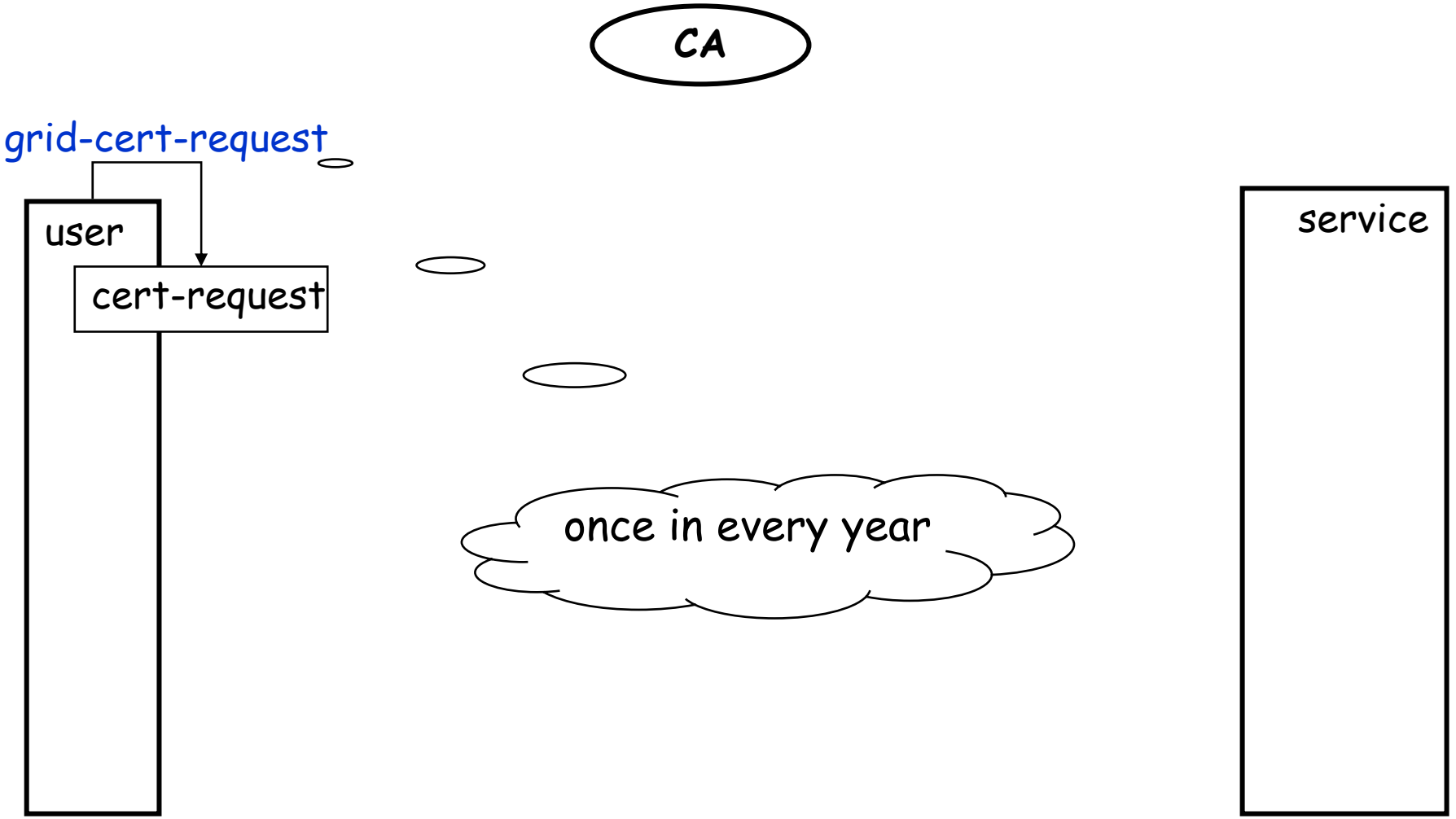
Overview

- 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 Organisation
  - Concept of VO and authorization
  - VOMS, LCAS, LCMAPS
- Security in action

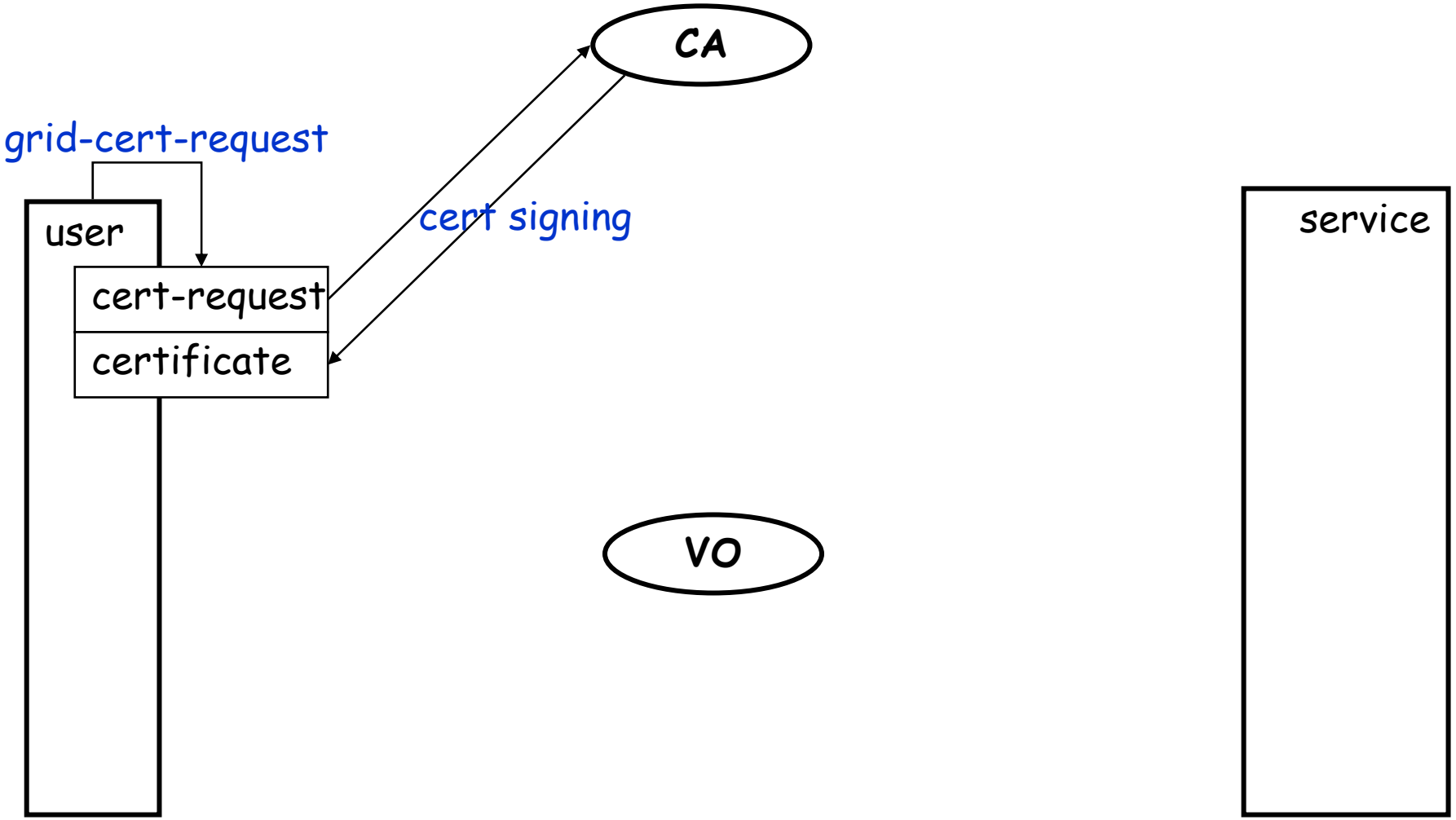
Authentication Overview



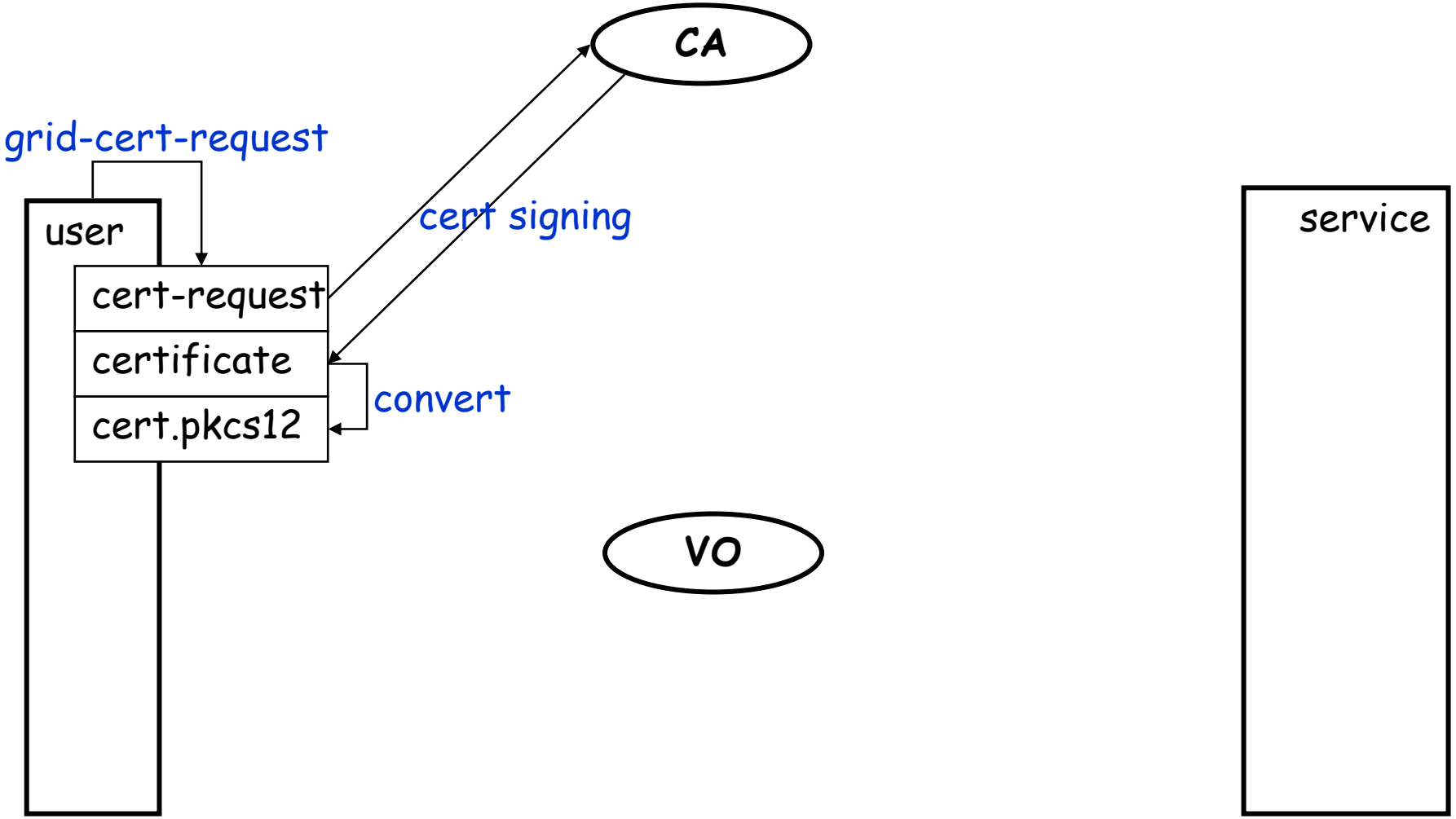
Certificate Request



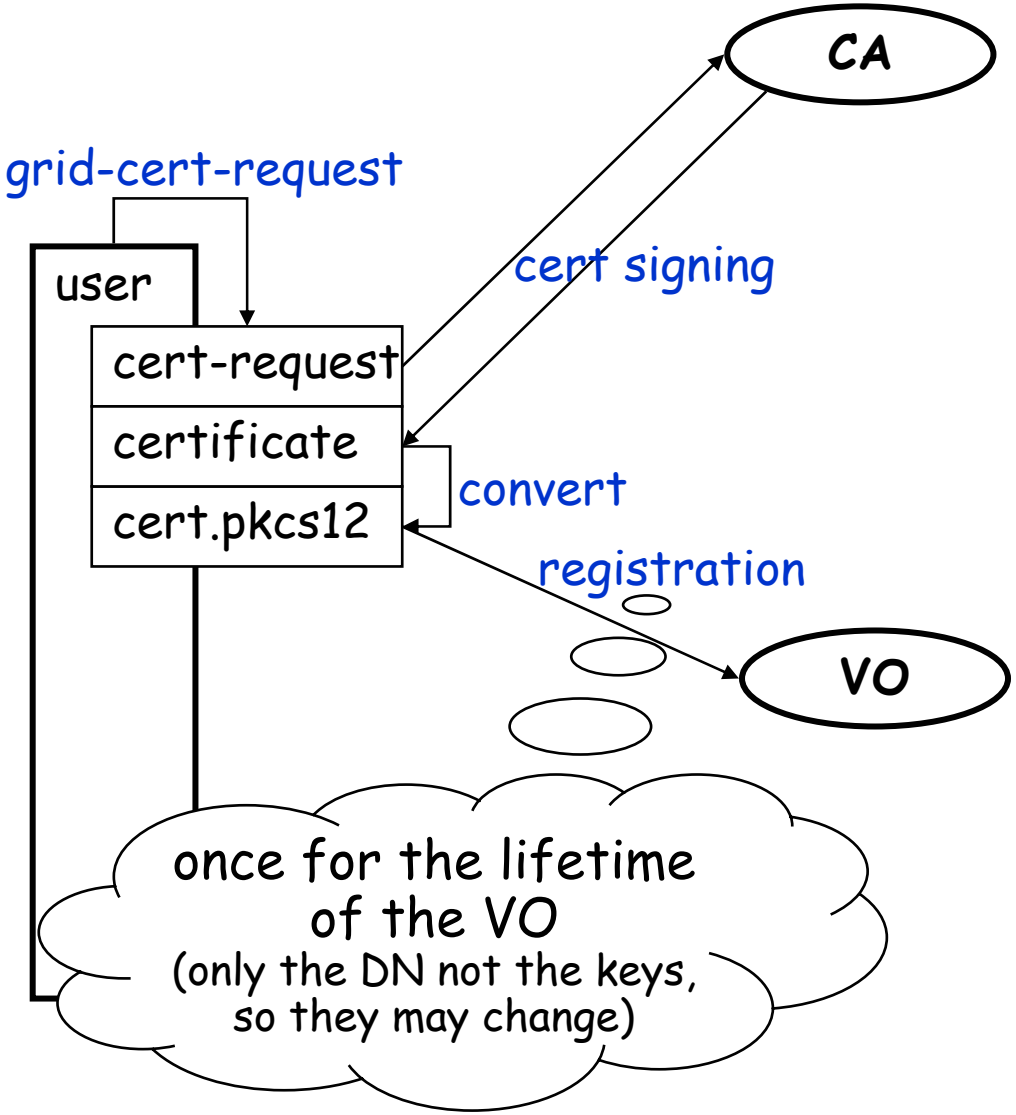
Certificate Signing



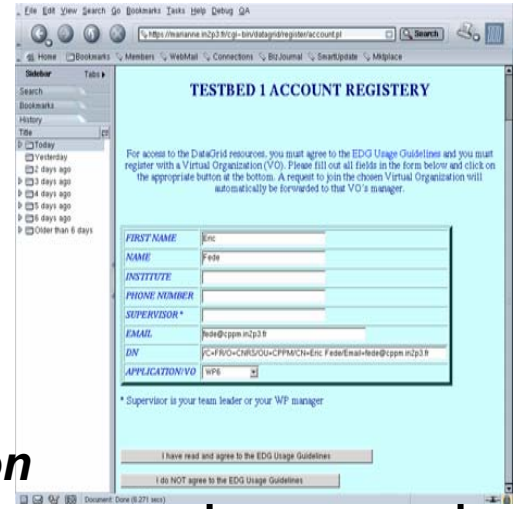
Preparation for Registration



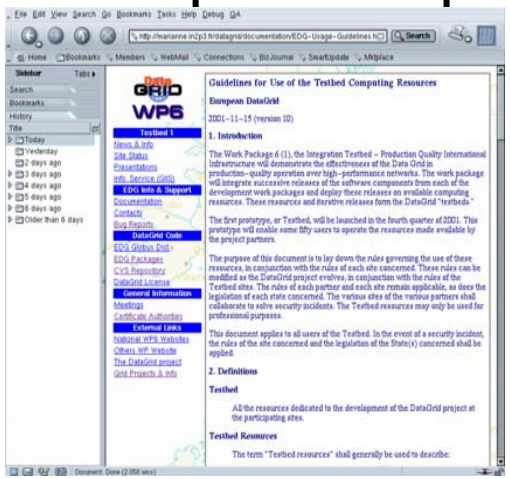
Registration



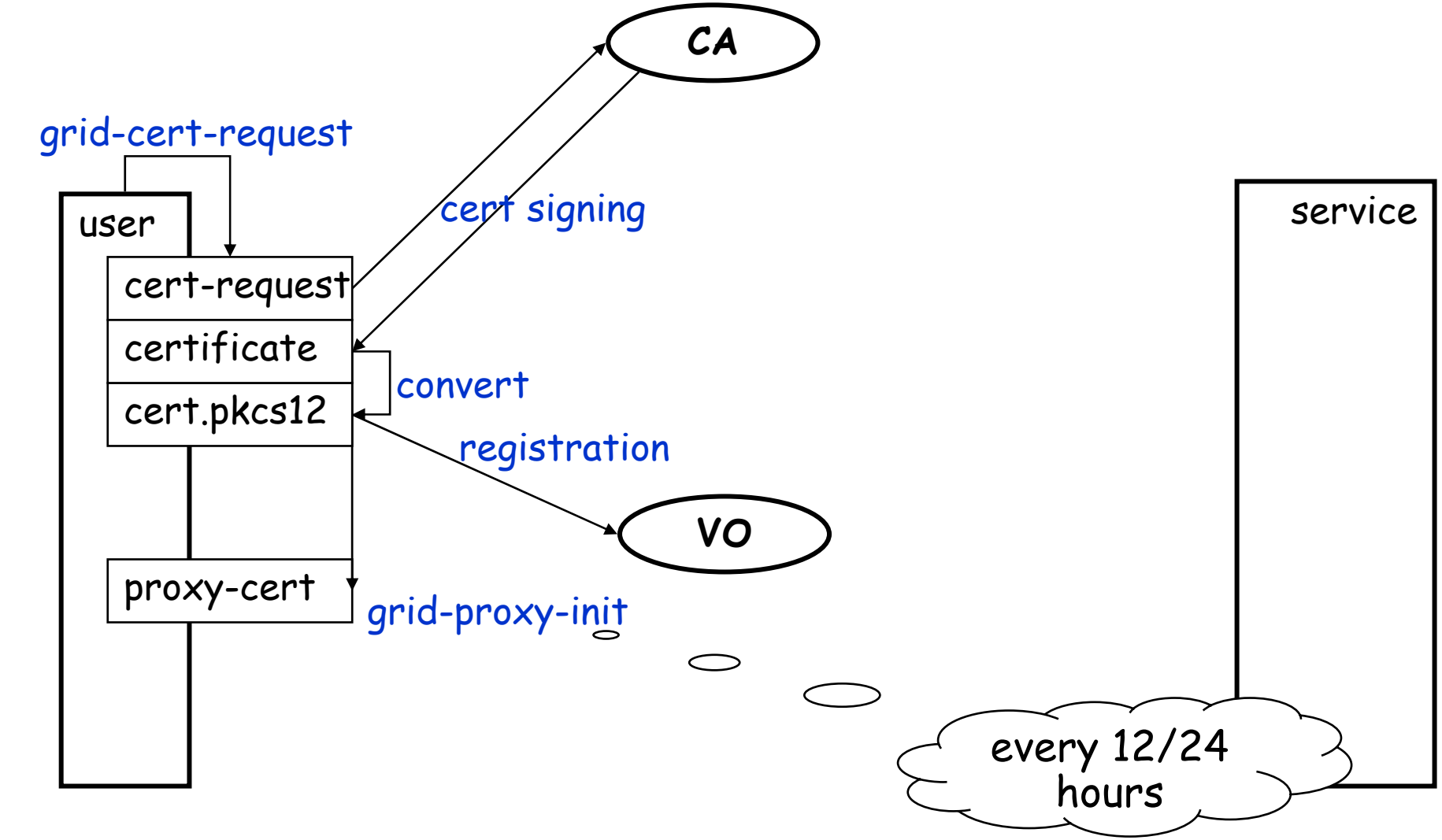
Account Registration



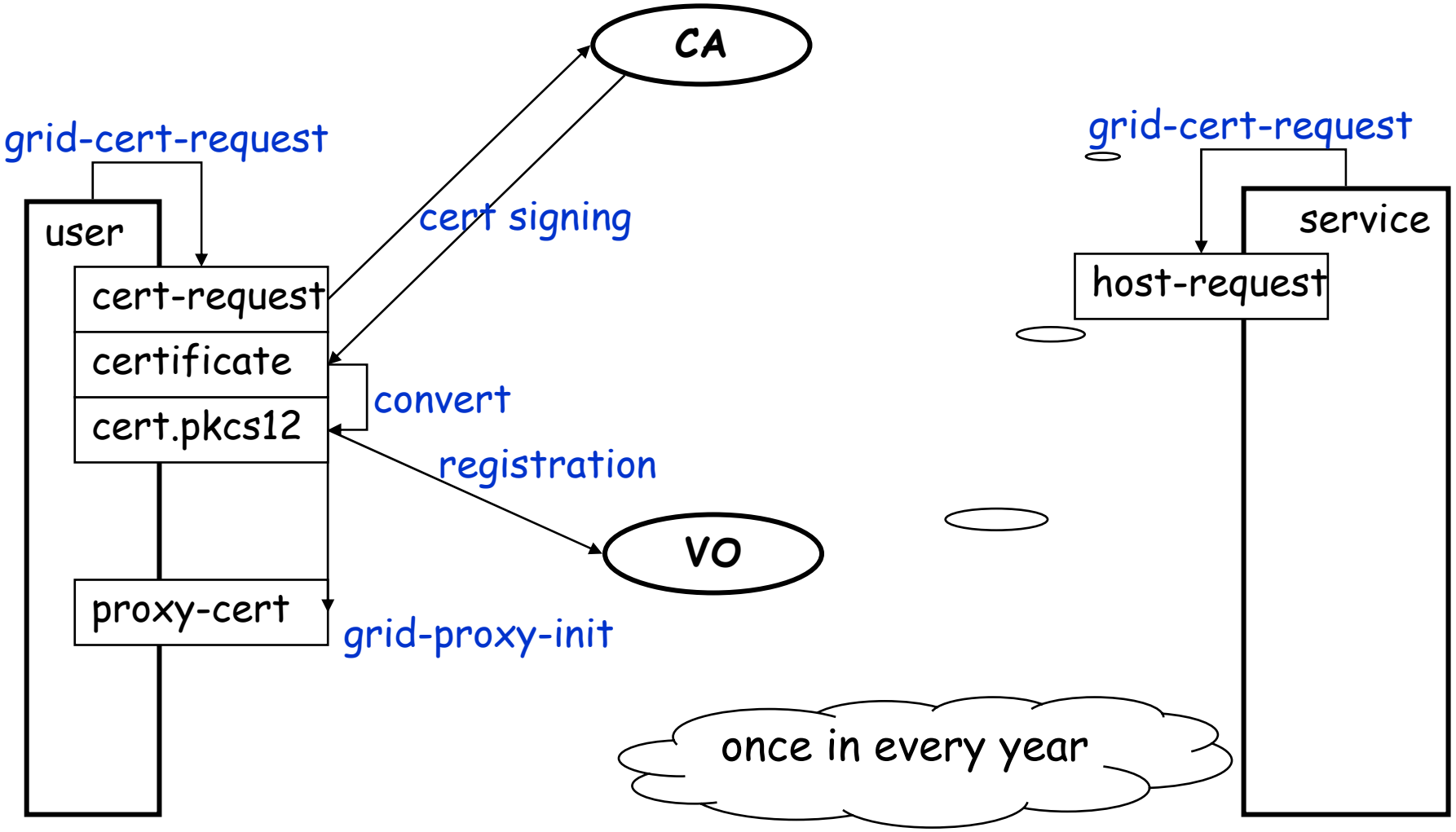
Usage guidelines



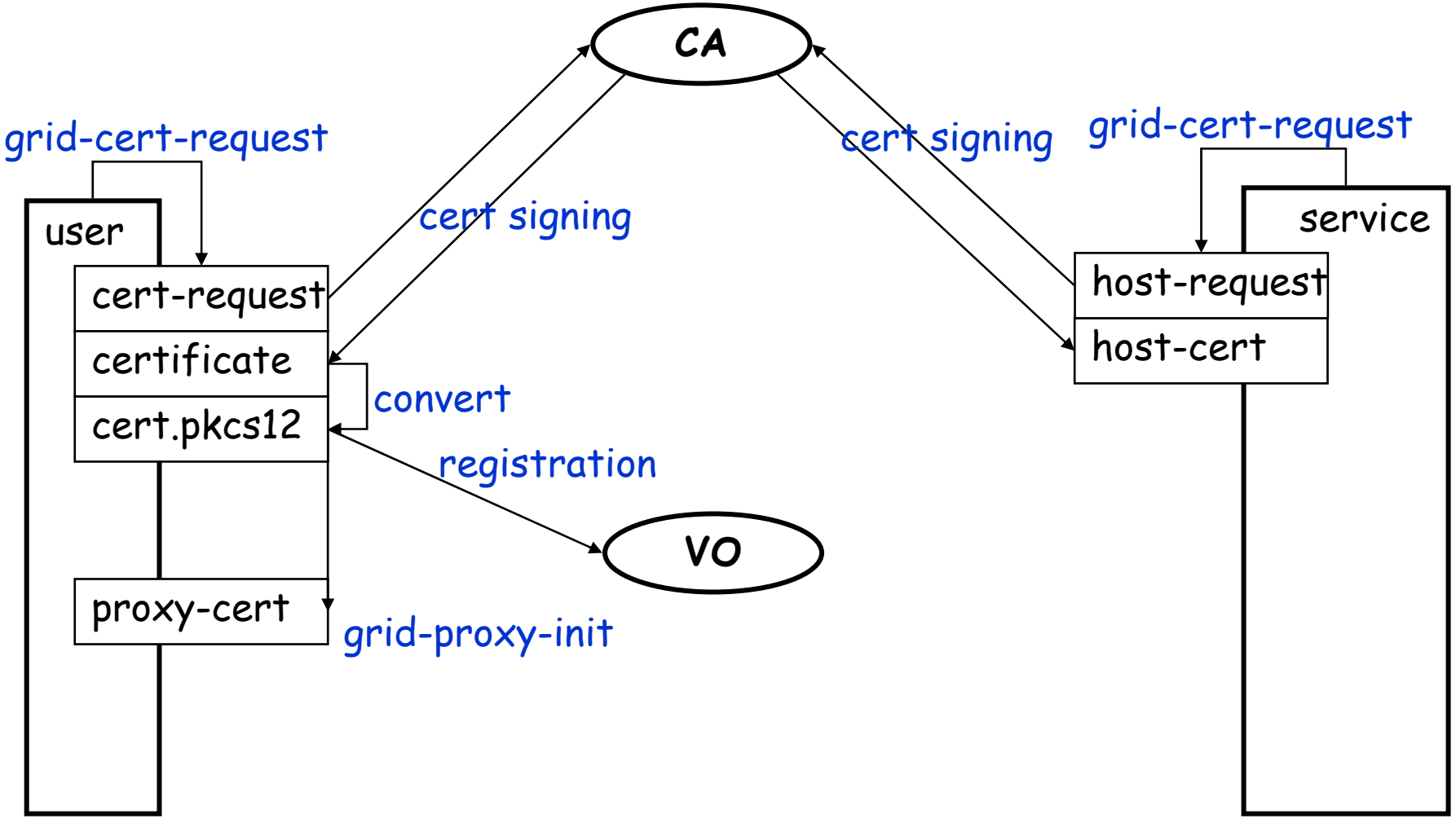
Starting a Session



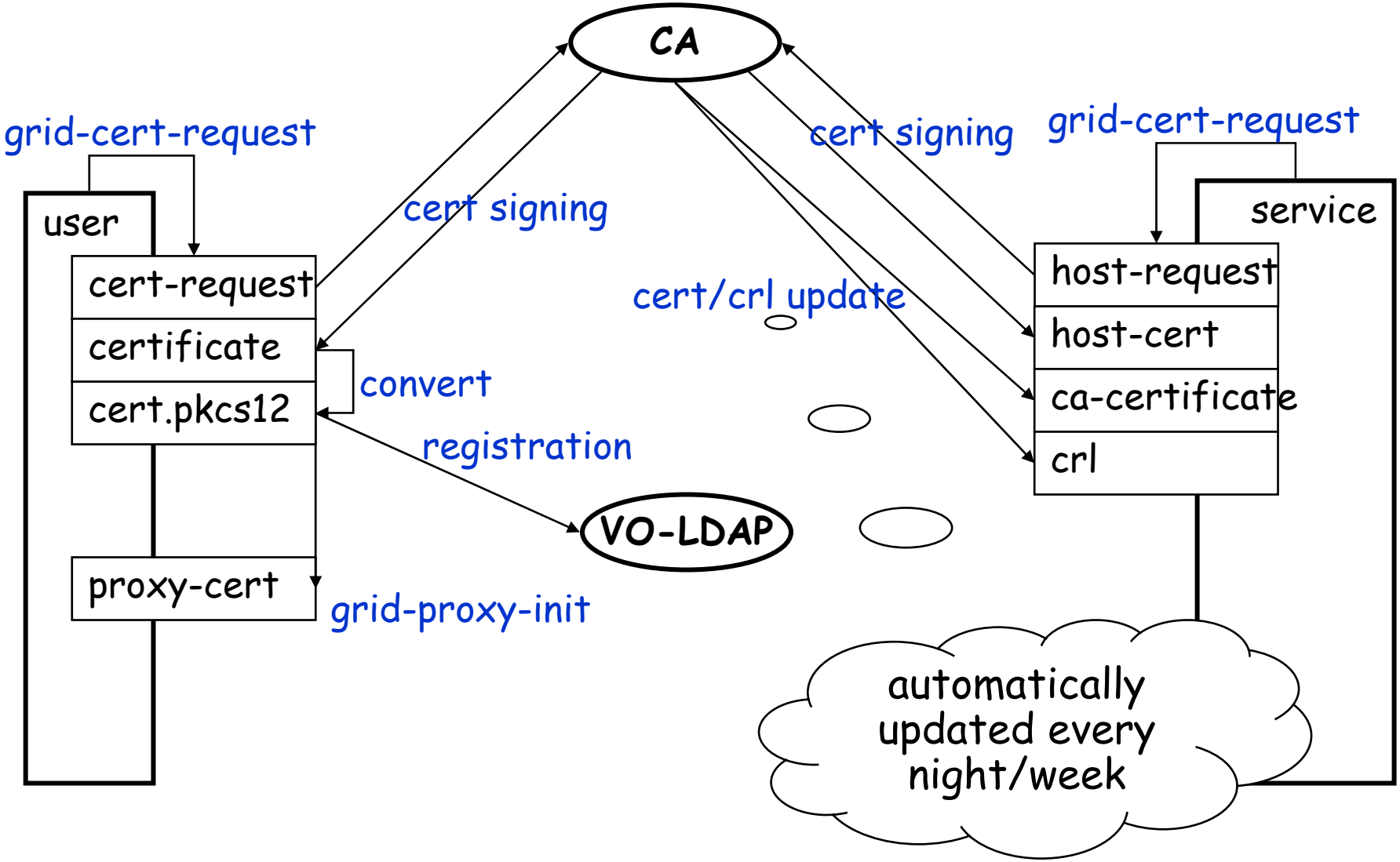
Certificate Request for a Host



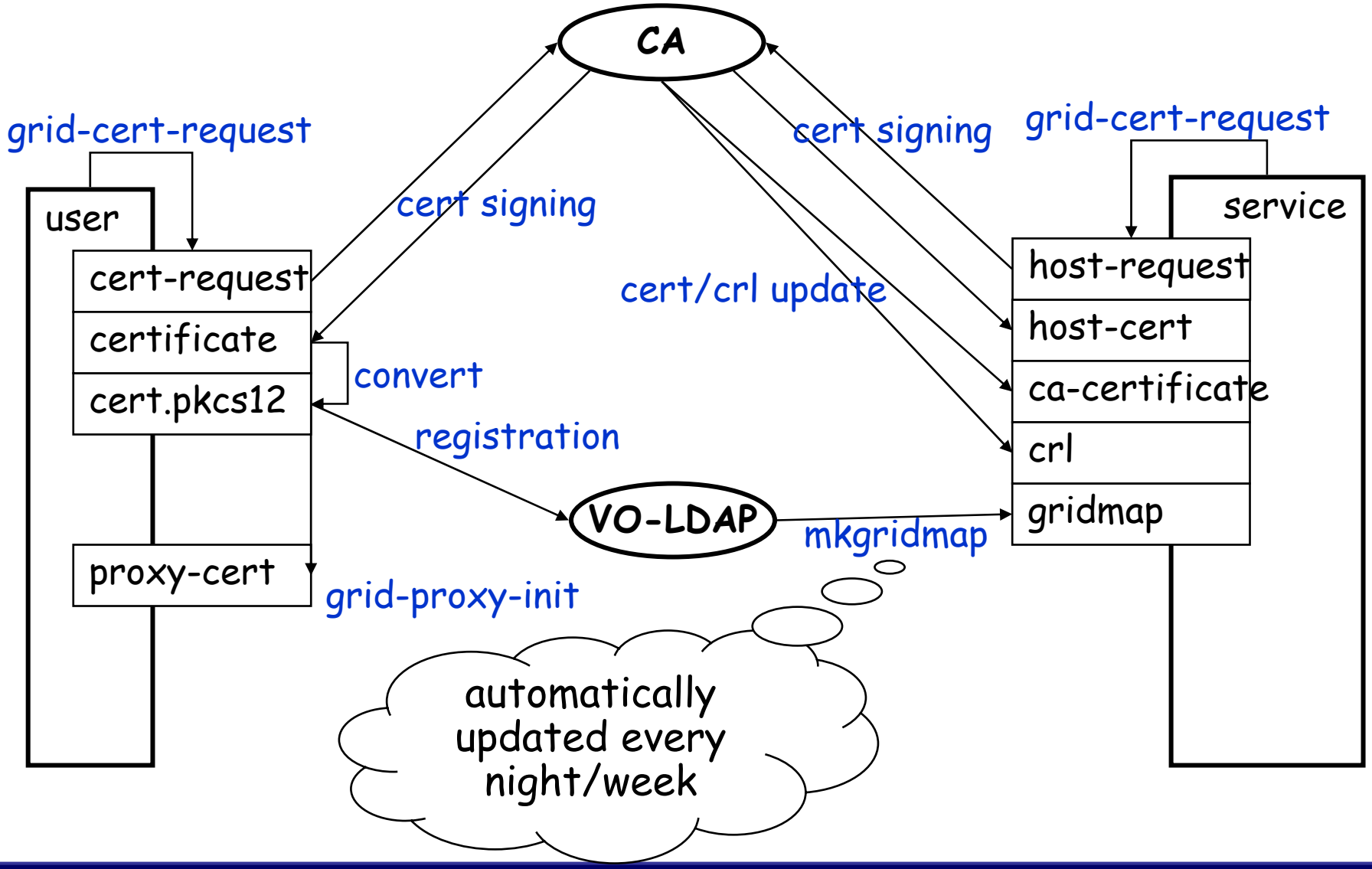
Signing the Certificate



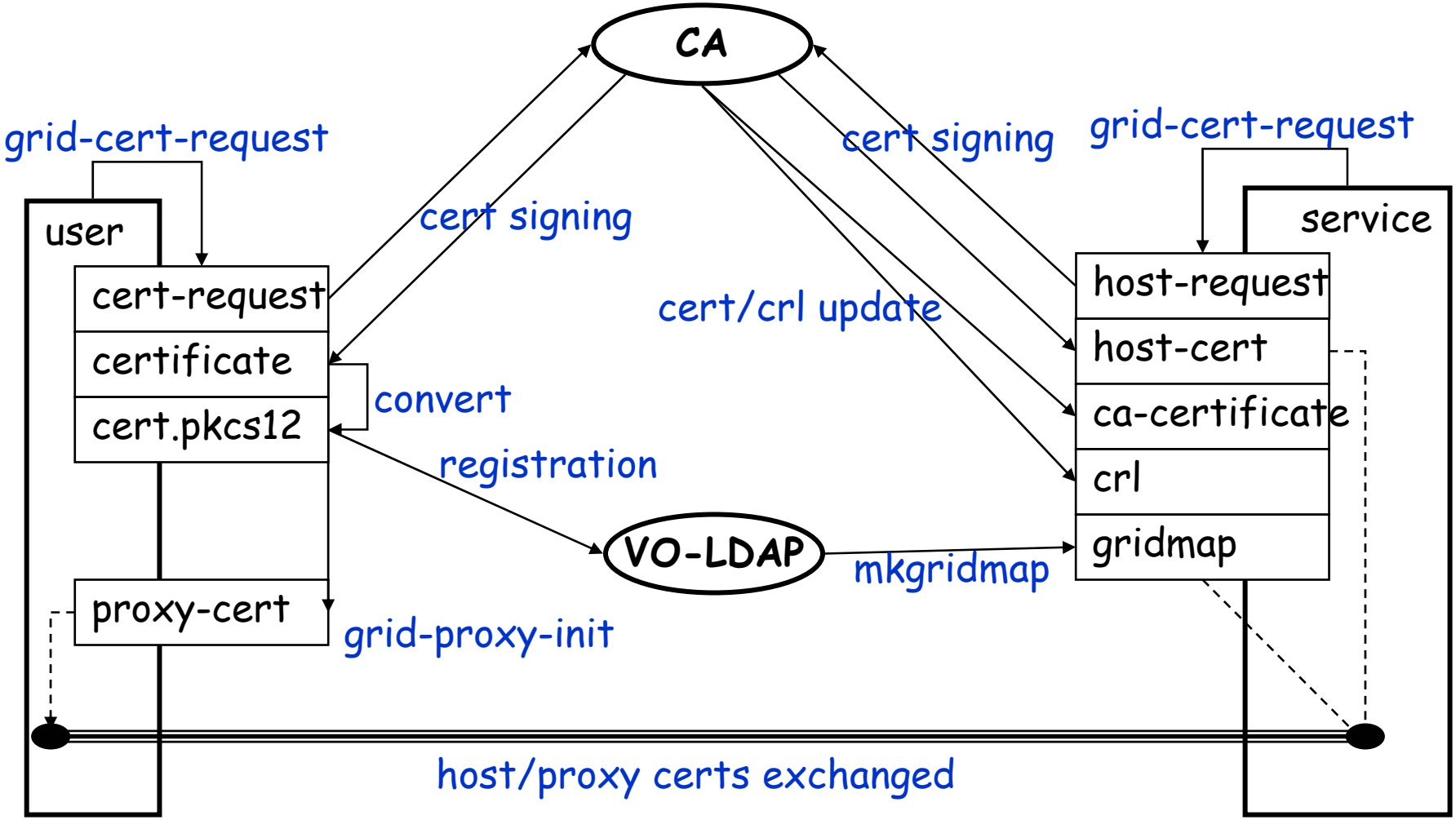
Configuration on the Server



Authorization Information



Using a Service



Further Information

Enabling Grids for E-science in Europe

Grid

- LCG Security: http://proj-lcg-security.web.cern.ch/proj-lcg-security/
- LCG Registration: http://lcg-registrar.cern.ch/
- Globus Security: http://www.globus.org/security/

Background

- GGF Security: http://www.gridforum.org/security/
- GSS-API: http://www.faqs.org/faqs/kerberos-faq/general/section-84.html
- GSS-API: http://docsun.cites.uiuc.edu/sun_docs/C/solaris_9/SUNWdev/ \ GSSAPIPG/toc.html
- IETF PKIX charter: http://www.ietf.org/html.charters/pkix-charter.html
- PKCS: http://www.rsasecurity.com/rsalabs/pkcs/index.html