



# Security Mechanisms



The European DataGrid Project Team

<http://www.eu-datagrid.org>

---



# Overview

- User side
  - Getting a certificate
  - Becoming a member of the VO
  
- Server side
  - Authentication / CA
  - Authorization / VO

(with some examples)



# Authentication/Authorization

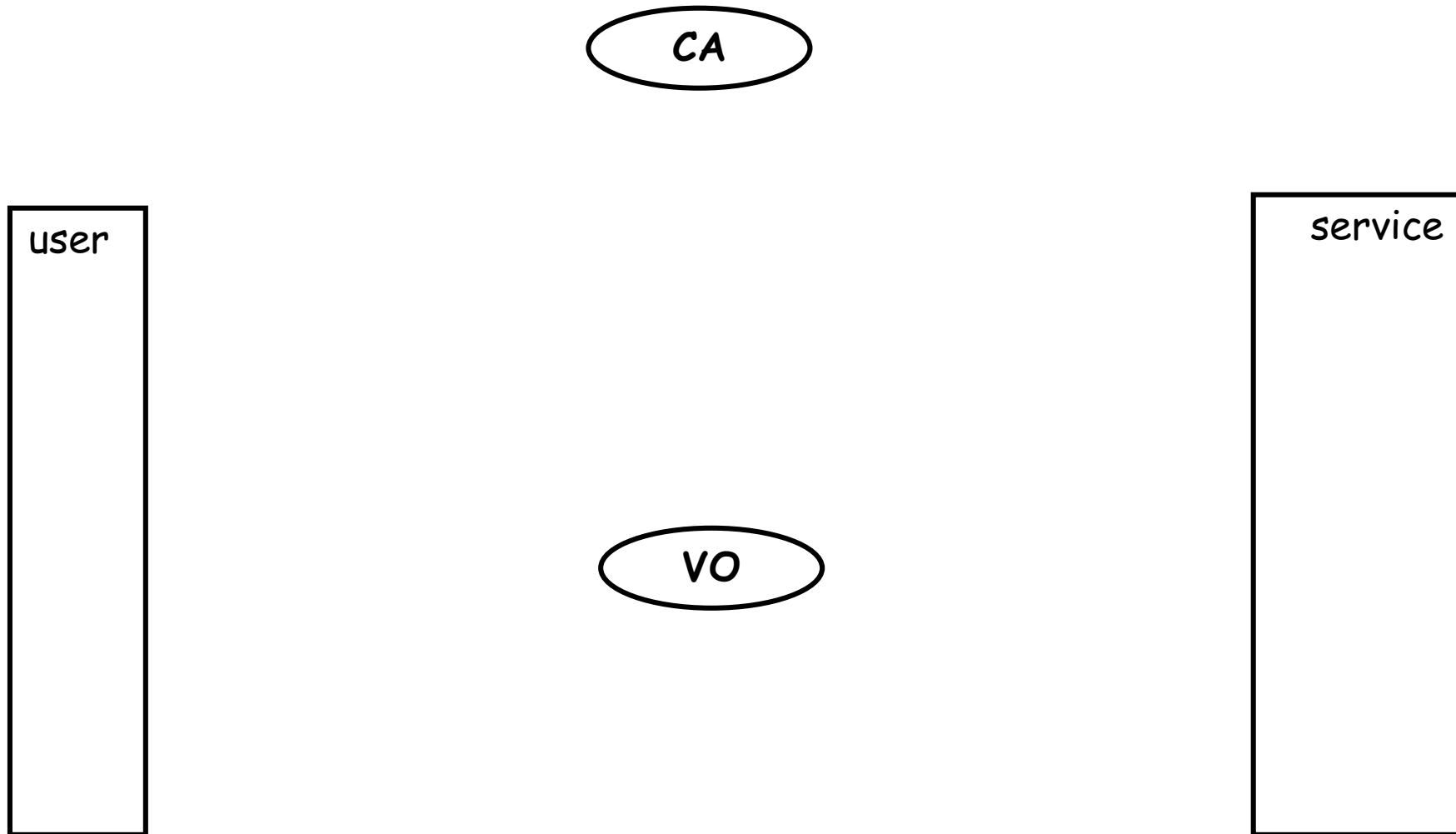
- Authentication (CA Working Group)
  - 16 national certification authorities + CrossGrid CAs
  - policies & procedures → mutual trust
  - users identified by CA's certificates
- Authorization (Authorization Working Group)
  - Based on Virtual Organizations (VO).
  - Management tools for VO membership lists.
  - 6+2 Virtual Organizations

VO's	
ALICE	Earth Obs.
ATLAS	Biomedical
CMS	Testbed
LHCb	Tutorial

CA's
CERN
CESNET
CNRS (3)
GermanGrid
Grid-Ireland
INFN
NIKHEF
NorduGrid
LIP
Russian DataGrid
DATAGRID-ES
GridPP
US-DOE Root CA
US-DOE Sub CA
CrossGrid (*)



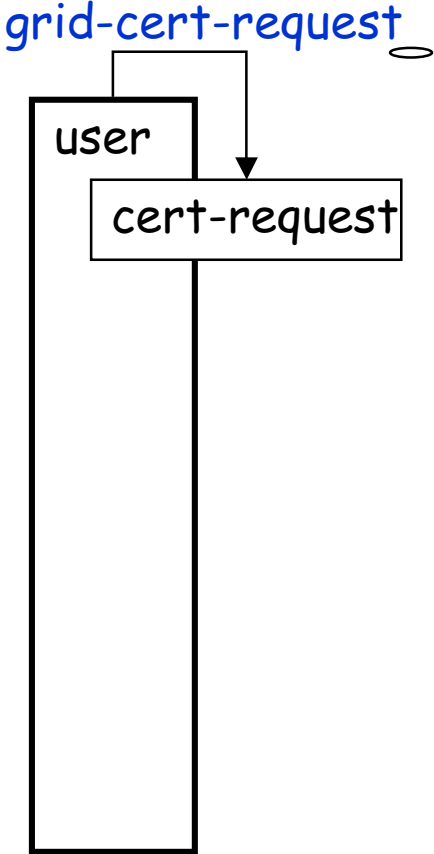
# Authentication Overview



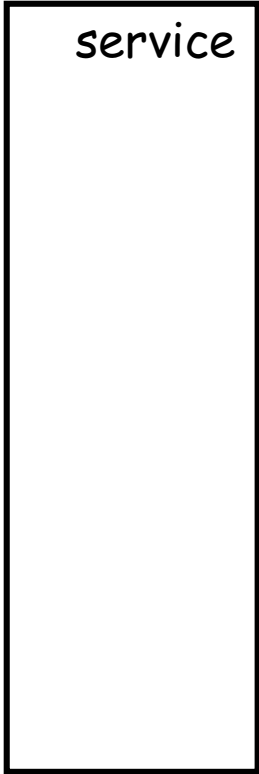


# Certificate Request

CA



once in every year





# Requesting a Certificate

## ➤ **grid-cert-request**

A certificate request and private key is being created.

[...]

Using configuration from `/usr/local/grid/globus/etc/globus-user-ssleay.conf`

Generating a 1024 bit RSA private key

[...]

A private key and a certificate request has been generated with the subject:

**`/O=Grid/O=CERN/OU=cern.ch/CN=Akos Frohner`**

[...]

Your private key is stored in `.../.globus/userkey.pem`

Your request is stored in `.../.globus/usercert_request.pem`

Please e-mail the certificate request to the CERN CA

**`cat .../.globus/usercert_request.pem | mail cern-globus-ca@cern.ch`**

Your certificate will be mailed to you within two working days.



# Request Details...

example

➤ `openssl req -in ~/.globus/usercert_request.pem -text`

Data:

Version: 0 (0x0)

Subject: O=Grid, O=CERN, OU=cern.ch, CN=Akos Frohner [User information](#)

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ba:ae:e2:9a:98:be:94:f5:f5:9e:e7:f7:06:58: [...]

[Public key](#)

Exponent: 65537 (0x10001)

Signature Algorithm: md5WithRSAEncryption

29:87:63:40:65:af:1b:39:e9:71:b9:3f:70:80:0c:27:71:0e: [...]

[Signature on the public](#)

[key and user information](#)

-----BEGIN CERTIFICATE REQUEST-----

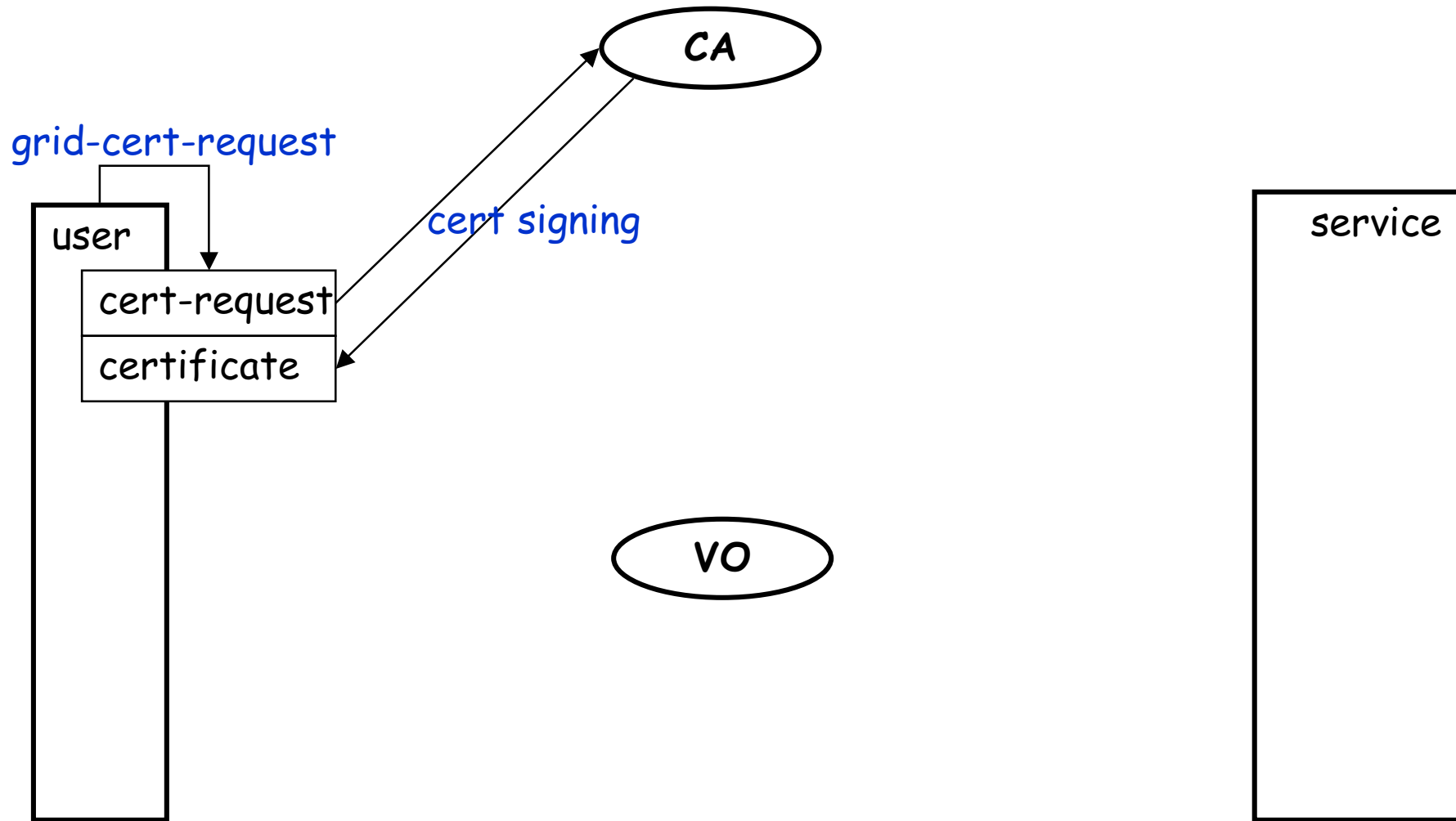
[PEM encoded request](#)

MIIBhjCB8AIBADBHMQ0wCwYDVQQKEwRHcmIkMQ0wC [...]

-----END CERTIFICATE REQUEST-----



# Certificate Signing







# Signing a Request

example

Upon a certificate request from the user

- checking the identity of the user (Registration Authority)
- signing the request and sending back the result
  - `openssl ca -in usercert_request.pem -out usercert.pem`
- if something goes wrong: revocation of a certificate -> CRL
  
- the issued certificates are described in the Certificate Policy (CP)
- the process is described in the Certificate Practice Statement (CPS)



# Private Key

example

➤ **openssl rsa -in ~/.globus/userkey.pem -text**

Enter PEM pass phrase:

Private-Key: (1024 bit)

modulus: [...]

publicExponent: ..... (0x.....)

privateExponent: [...]

prime1: [...]

private parameters

prime2: [...]

exponent1: [...]

exponent2: [...]

coefficient: [...]

writing RSA key

-----BEGIN RSA PRIVATE KEY-----

PEM encoded private key

-----END RSA PRIVATE KEY-----



# Certificate Details 1.

example

➤ `openssl x509 -in ~/.globus/usercert.pem -text`

Certificate:

Data:

Version: 3 (0x2)

X509.3 – with extensions

Serial Number: 199 (0xc7)

Signature Algorithm: md5WithRSAEncryption

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

Issuer CA

Validity

Not Before: Jun 11 08:25:59 2002 GMT

long term certificate

Not After : Sep 29 11:22:33 2002 GMT

Subject: O=Grid, O=CERN, OU=cern.ch, CN=Akos Frohner

user information

Subject Public Key Info:

[...]

same as in the request



# Certificate Details 2.

example

X509v3 extensions:

Netscape Base Url:

<http://home.cern.ch/globus/ca>

Certificate extensions

Netscape Cert Type:

SSL Client, S/MIME, Object Signing

client/user certificate

Netscape Comment:

For DataGrid use only

Netscape Revocation Url:

<http://home.cern.ch/globus/ca/cern.crl.pem>

CRL information

Netscape CA Policy Url:

<http://home.cern.ch/globus/ca/CPS.pdf>

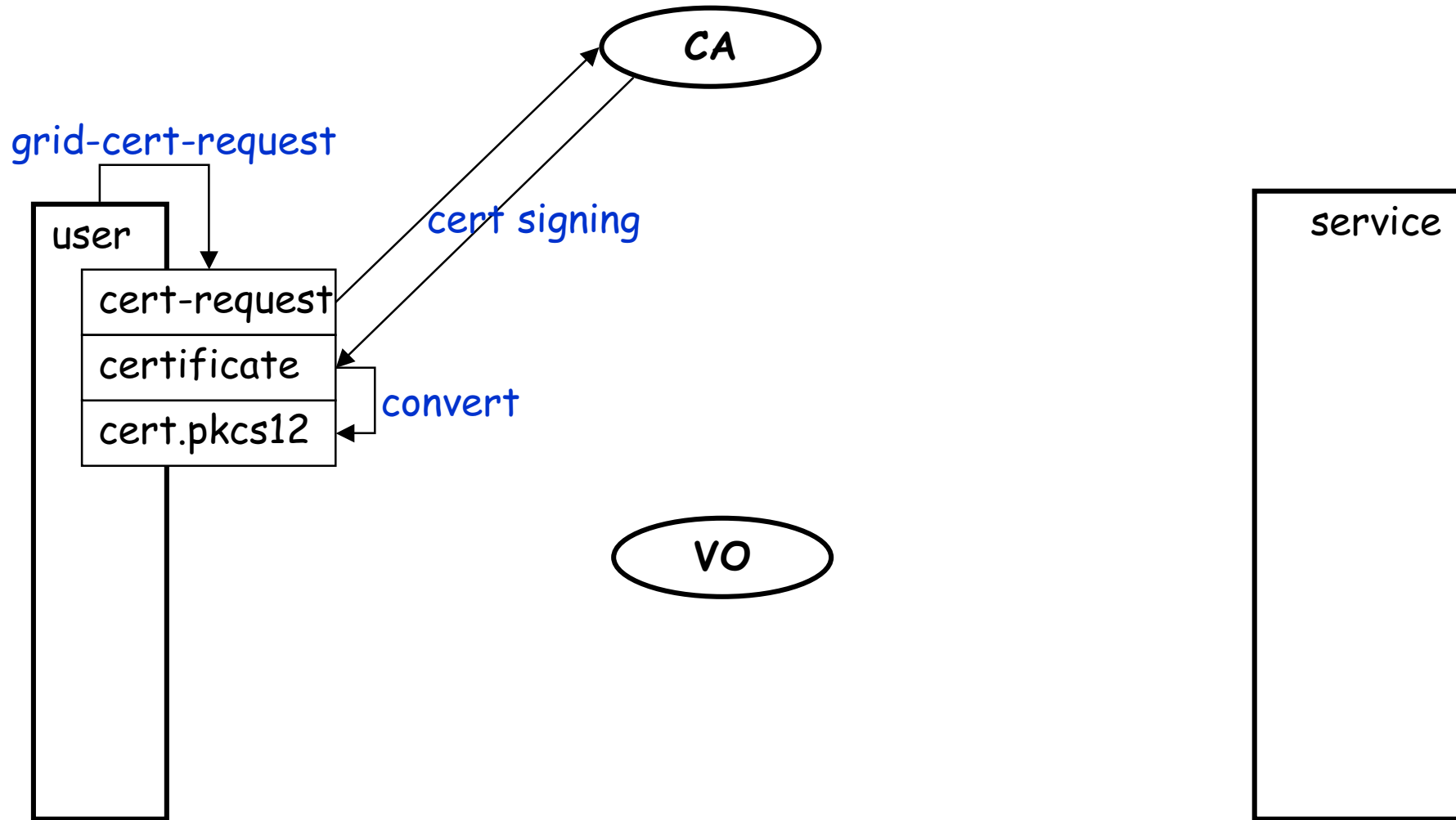
Policy information

Signature Algorithm: md5WithRSAEncryption

54:8b:66:e8:dc:60:cd:e3:dc:43:a7:c9:3a:12:2c:73:05:13: [...] Signature on the information



# Preparation for Registration





# Registration/Authorization

User registration in an EDG Virtual Organisation

➤ convert your certificate:

- `openssl pkcs12 -export -in ~/.globus/usercert.pem -inkey ~/.globus/userkey.pem -out user.p12 -name 'Joe Smith'`

➤ import your certificate in your browser

➤ sign the usage guidelines:

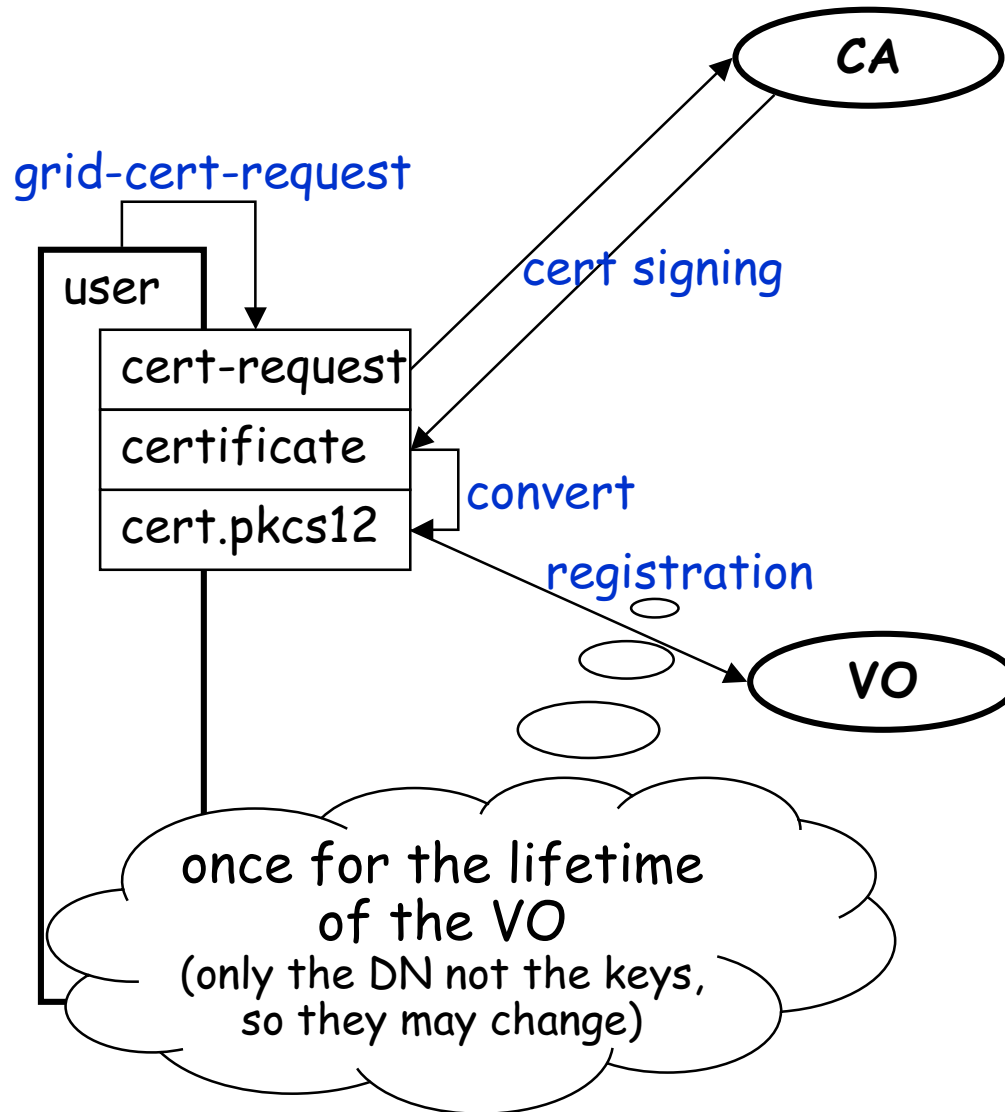
<https://marianne.in2p3.fr/cgi-bin/datagrid/register/account.pl>

➤ ask an account from your VO administrator by email

-> You are registered in the VO-LDAP server and have a user account.

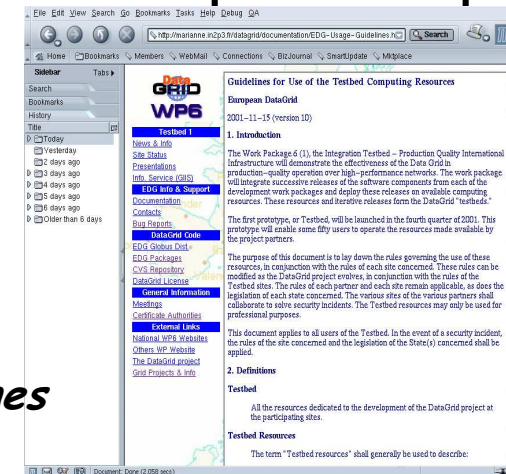
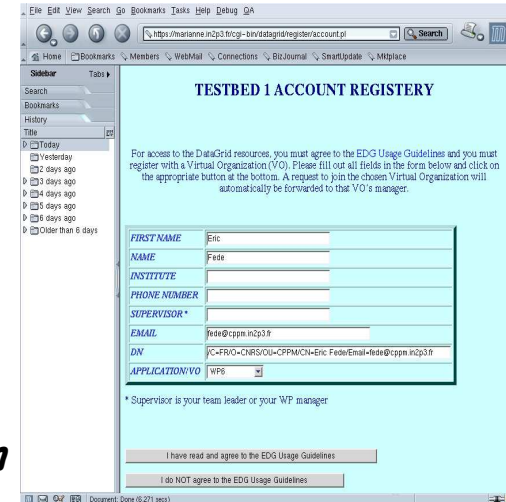


# Registration



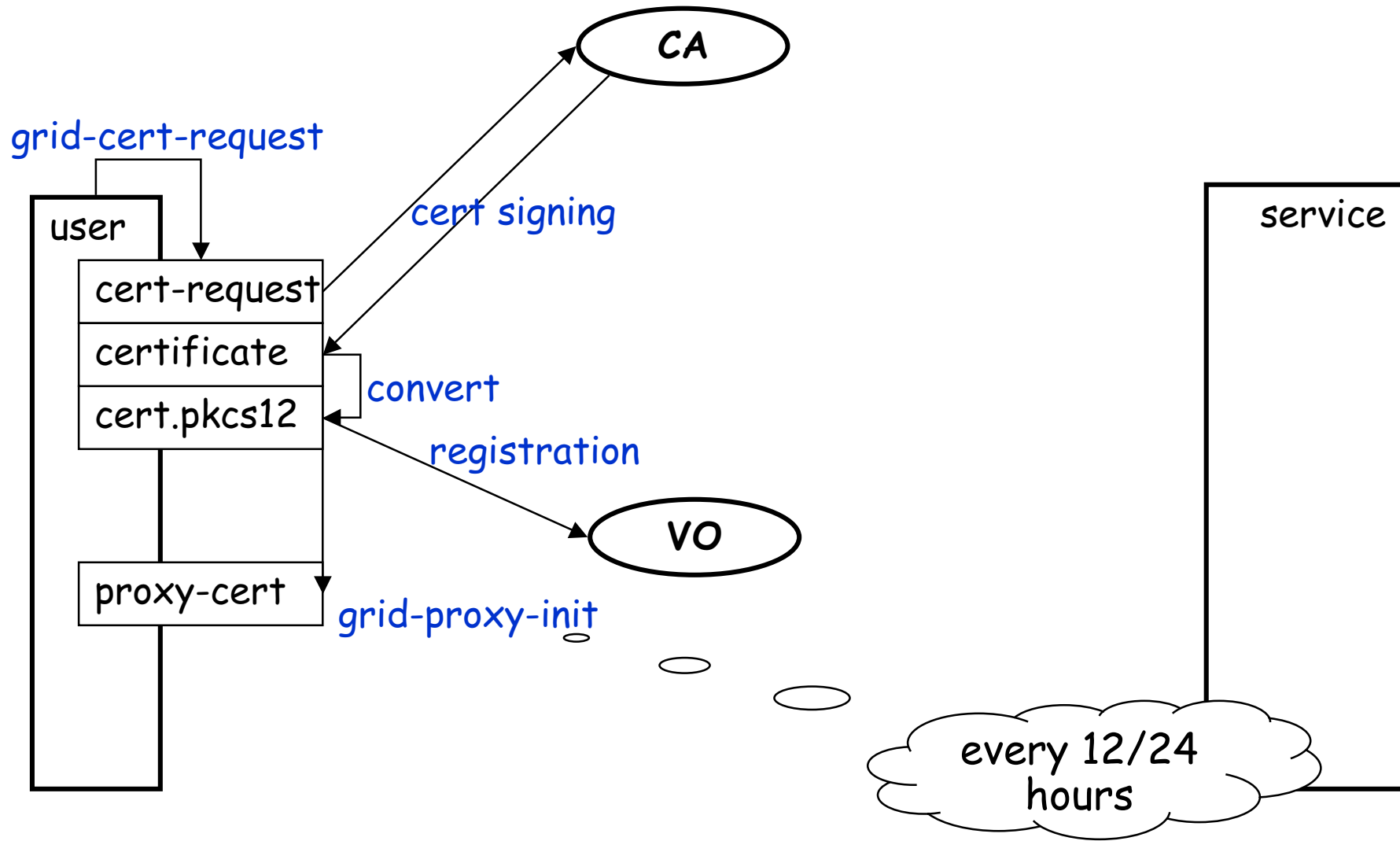
*Account Registration*

*Usage guidelines*





# Starting a Session







# Usage

You must have a valid certificate from a trusted CA!

➤ „login“: **grid-proxy-init**

short lifetime certificate: 24 hours

Enter PEM pass phrase:

.....+++++

.....+++++

➤ checking the proxy: **grid-proxy-info -subject**

/O=Grid/O=CERN/OU=cern.ch/CN=Akos Frohner/CN=proxy

➤ „logout“: **grid-proxy-destroy**

-> use the grid services



# Proxy Certificate details

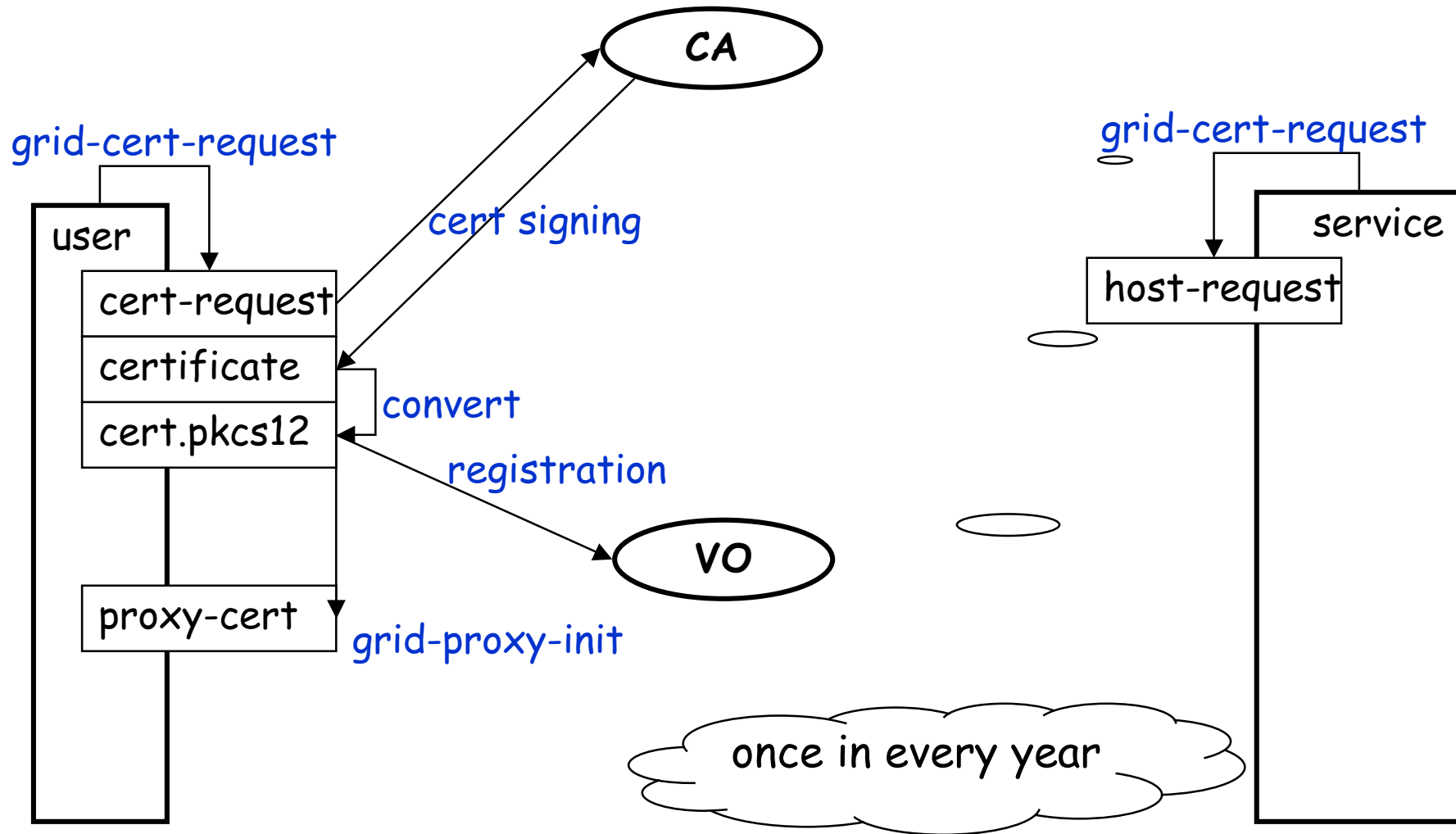
example

➤ `openssl x509 -in /tmp/x509up_u`id -u` -text`

Data: [...]   
 Issuer: O=Grid, O=CERN, OU=cern.ch, CN=Akos Frohner   
 Issuer is the user not a CA   
 Validity   
 Not Before: Jul 22 09:44:39 2002 GMT   
 short time certificate: 1 day   
 Not After : Jul 22 21:49:39 2002 GMT   
 Subject: O=Grid, O=CERN, OU=cern.ch, CN=Akos Frohner, CN=proxy   
 extra tag: proxy   
 Subject Public Key Info:   
 new (shorter) key(s)   
 Public Key Algorithm: rsaEncryption   
 RSA Public Key: (512 bit)   
 Modulus (512 bit):   
 00:e9:7c:f4:d0:5d:8a:4c:91:8b:df:a7:16:78:1f: [...]   
 Exponent: 65537 (0x10001)   
 X509v3 extensions: [...] same as earlier   
 Signature Algorithm: md5WithRSAEncryption [...] signed by the user

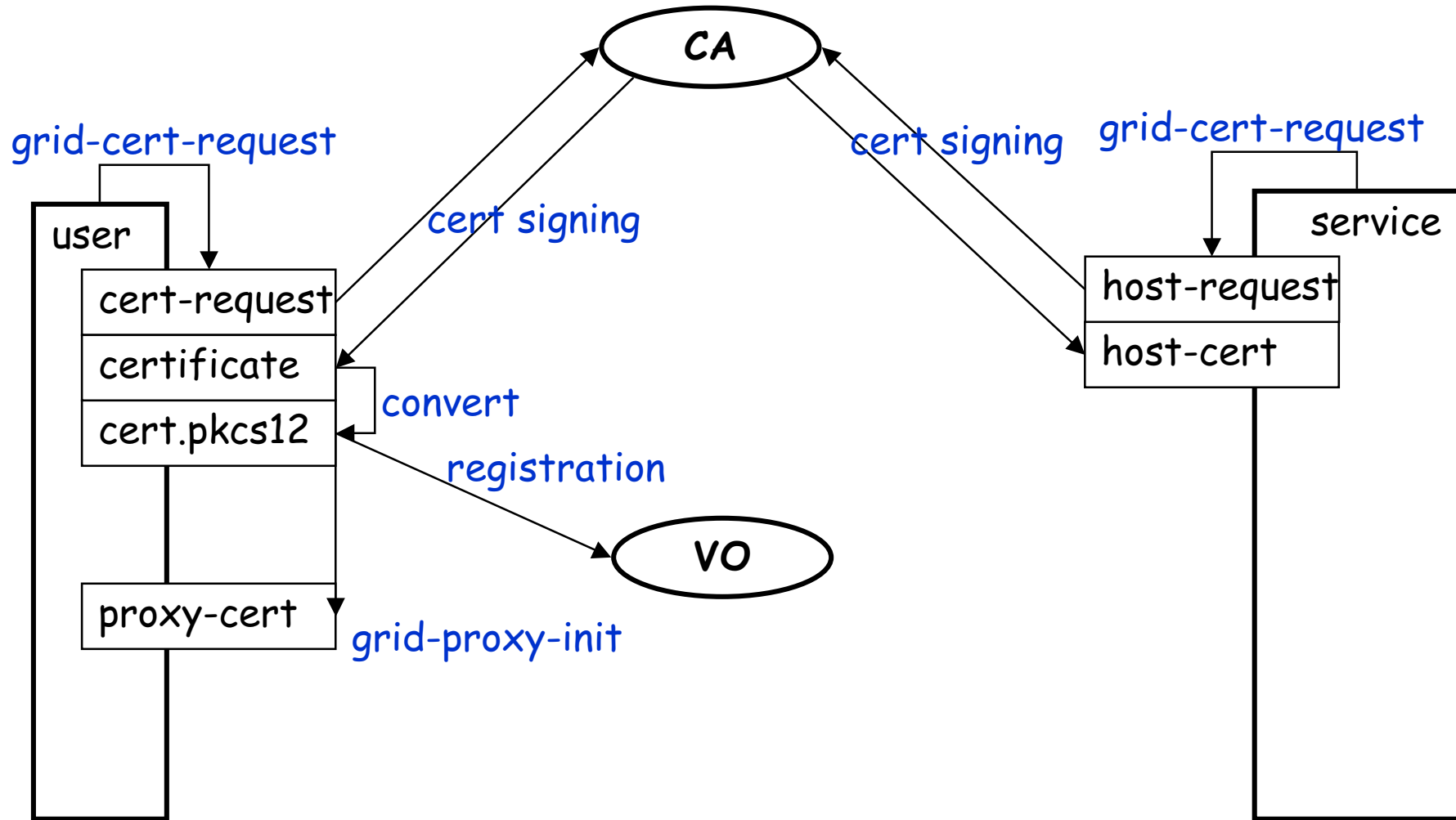


# Certificate Request for a Host



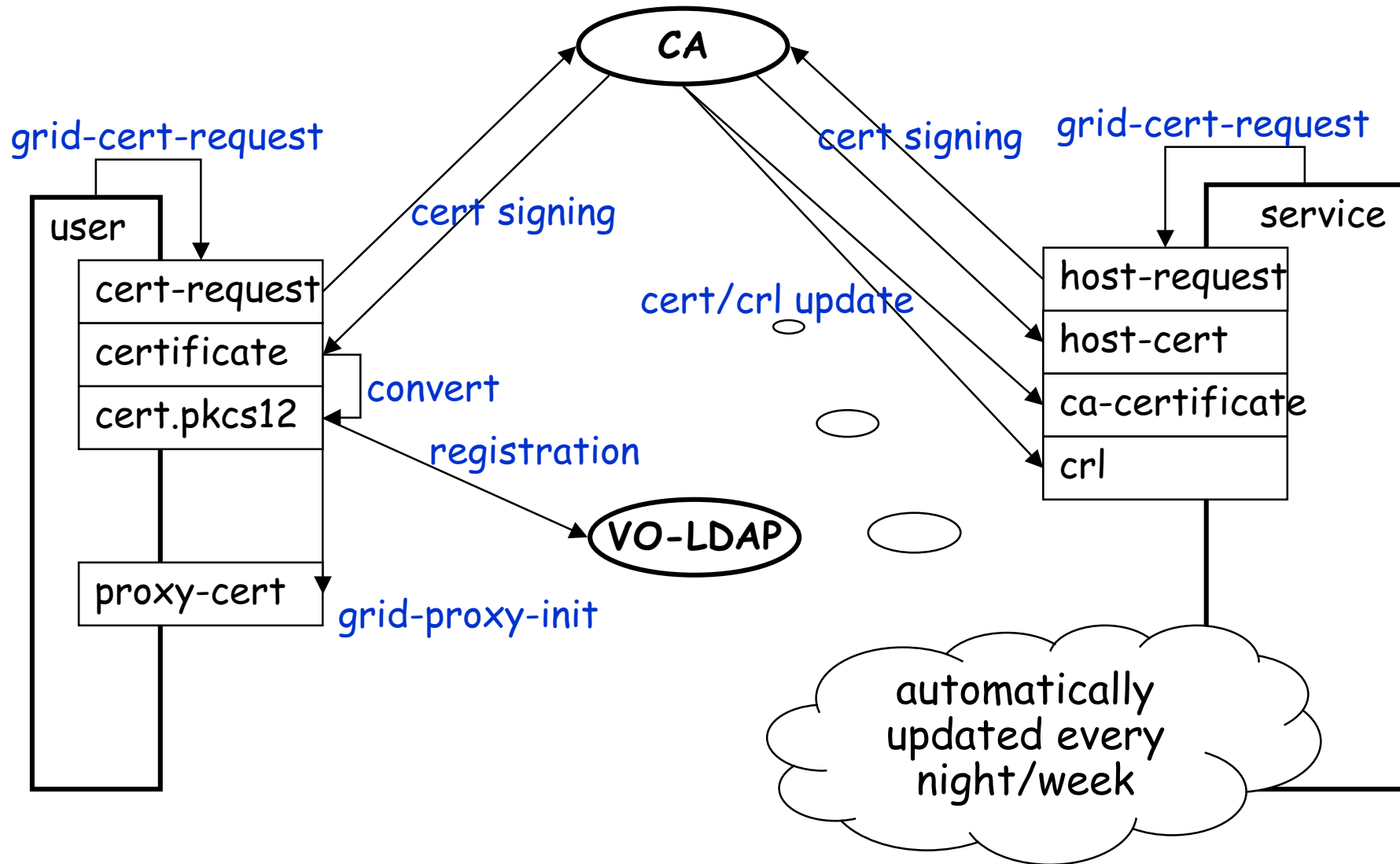


# Signing the Certificate





# Configuration on the Server





## Service

info

You must have the trusted CA certificates in files and the VO-LDAP server(s) URL configured.

- registering a trusted CA
  - /etc/grid-security/certificates: hashed cert, crl and url
- generating a gridmap file: mkgridmap
  - /etc/grid-security/gridmap: DN -> userid/gid mapping
- generating host/service certificate:  
grid-cert-request -host  
(see user certificates for the whole process)

Start the service!



# Service: CA Certificates

example

## ➤ **ls /etc/grid-security/certificates**

0ed6468a.0	c35c1972.0	d64ccb53.0
0ed6468a.crl_url	c35c1972.crl_url	d64ccb53.crl_url
0ed6468a.r0	c35c1972.r0	d64ccb53.r0
0ed6468a.signing_policy	c35c1972.signing_policy	d64ccb53.signing_policy
16da7552.0	cf4ba8c8.0	df312a4e.0
16da7552.crl_url	cf4ba8c8.crl_url	df312a4e.crl_url
16da7552.r0	cf4ba8c8.r0	df312a4e.r0
16da7552.signing_policy	cf4ba8c8.signing_policy	df312a4e.signing_policy

## ➤ **cat c35c1972.crl\_url**

<http://globus.home.cern.ch/globus/ca/cern.crl.pem>



# Service: a certificate

example

## ➤ `cat c35c1972.signing_policy`

```
# EACL CERN CA
```

```
access_id_CA          X509          '/C=CH/O=CERN/CN=CERN CA'
```

```
pos_rights            globus        CA:sign
```

```
cond_subjects         globus        ""/C=ch/O=CERN/*" ""/C=CH/O=CERN/*"  
                    ""/O=Grid/O=CERN/*" ""/O=CERN/O=Grid/"
```

## ➤ `openssl x509 -in c35c1972.0 -text`

Issuer: C=CH, O=CERN, CN=CERN CA [...] the issuer and the subject are  
the same

Subject: C=CH, O=CERN, CN=CERN CA [...] self signed certificate

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE [...] it may be used to sign other certificates

Netscape Cert Type:

SSL CA, S/MIME CA, Object Signing CA it is a CA certificate





# Service: Revocation List

example

➤ `openssl crl -in c35c1972.r0 -text`

Certificate Revocation List (CRL):

Version 1 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: /C=CH/O=CERN/CN=CERN CA

the issuer is the CA itself

Last Update: Jul 1 17:53:17 2002 GMT

Next Update: Aug 5 17:53:17 2002 GMT

next update: shall be checked

Revoked Certificates:

Serial Number: 5A

the revoked certificate's number

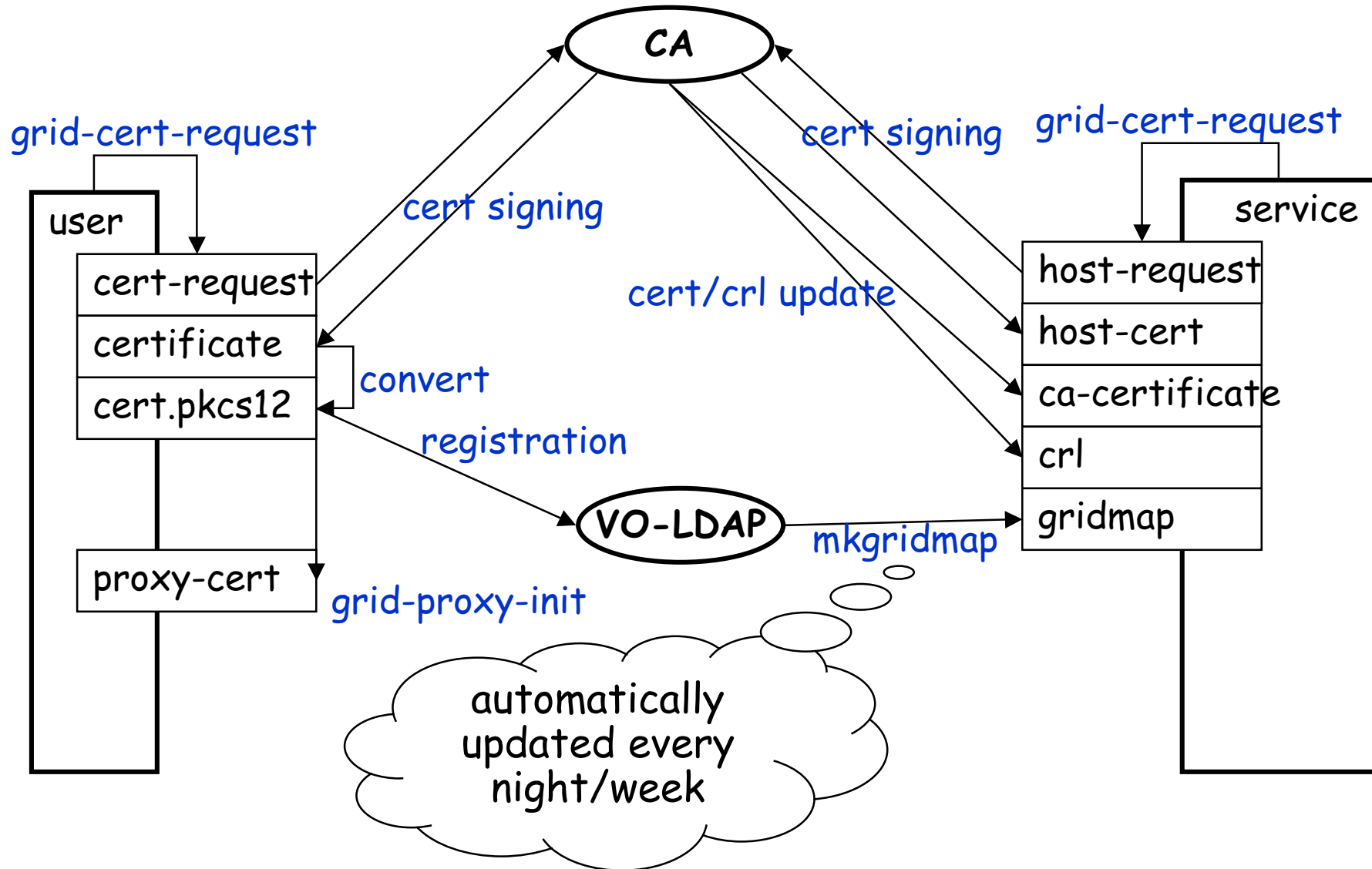
Revocation Date: May 24 16:45:52 2002 GMT

Signature Algorithm: md5WithRSAEncryption

Signature – as usual



# Authorization Information





# Gridmap file: configuration

example

➤ **cat /etc/grid-security/mkgridmap.conf**

```
auth ldap://marianne.in2p3.fr/ou=People,o=testbed,dc=eu-datagrid,dc=org
```

```
# EDG Standard Virtual Organizations
```

```
group ldap://grid-vo.nikhef.nl/ou=testbed1,o=alice,dc=eu-datagrid,dc=org .alice
```

```
group ldap://grid-vo.nikhef.nl/ou=testbed1,o=atlas,dc=eu-datagrid,dc=org .atlas
```

```
group ldap://grid-vo.nikhef.nl/ou=tb1users,o=cms,dc=eu-datagrid,dc=org .cms
```

```
group ldap://grid-vo.nikhef.nl/ou=tb1users,o=lhcb,dc=eu-datagrid,dc=org .lhcb
```

```
group ldap://grid-vo.nikhef.nl/ou=tb1users,o=biomedical,dc=eu-datagrid,dc=org .biome
```

```
group ldap://grid-vo.nikhef.nl/ou=tb1users,o=earthob,dc=eu-datagrid,dc=org .eo
```

```
group ldap://marianne.in2p3.fr/ou=ITeam,o=testbed,dc=eu-datagrid,dc=org .iteam
```

```
group ldap://marianne.in2p3.fr/ou=wp6,o=testbed,dc=eu-datagrid,dc=org .wpsix
```

```
default_lcluser AUTO
```



# Generated Gridmap file

example

➤ **cat /etc/grid-security/gridmap**

```
"/O=Grid/O=Globus/OU=cern.ch/CN=Geza Odor" odor
```

```
"/O=Grid/O=CERN/OU=cern.ch/CN=Pietro Paolo Martucci" pietro
```

```
"/C=IT/O=INFN/L=Bologna/CN=Franco Semeria/Email=Franco.Semeria@bo.infn.it" aliproduct
```

```
"/C=IT/O=INFN/L=Bologna/CN=Marisa Luvisetto/Email=Marisa.Luvisetto@bo.infn.it" aliproduct
```

```
"/O=Grid/O=CERN/OU=cern.ch/CN=Bob Jones" jones
```

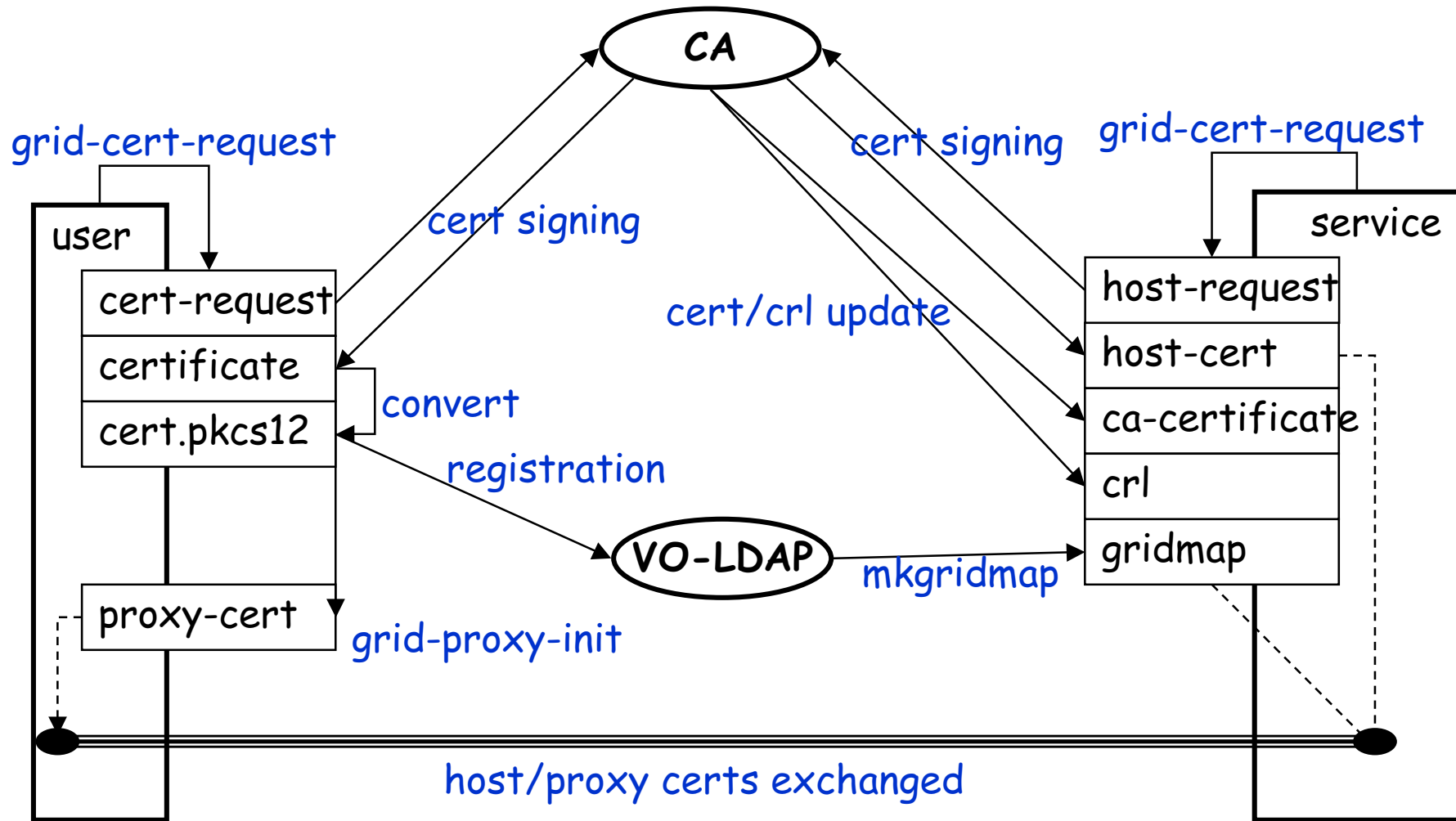
```
"/O=Grid/O=CERN/OU=cern.ch/CN=Brian Tierney" btierney
```

```
"/O=Grid/O=CERN/OU=cern.ch/CN=Tofigh Azemoun" azemoun
```

```
"/C=FR/O=CNRS/OU=LPC/CN=Yannick Legre/Email=legre@clermont.in2p3.fr" yannick
```



# Using a Service





# Summary

Obtaining a certificate from a CA

see <http://marianne.in2p3.fr/datagrid/ca/> for CAs

- new certificate: **grid-cert-request**
    - new files in ~/.globus: usercert\_request.pem userkey.pem
  - mail it to the appropriate CA (e.g. [cern-globus-ca@cern.ch](mailto:cern-globus-ca@cern.ch))
  - save the answer
    - ~/.globus/usercert.pem
  - new proxy certificate: **grid-proxy-init**
    - /tmp/x509up\_u<uid>
- > You have a certificate signed by an EDG CA.



# Further Information

## Grid

- EDG CAs: <http://marianne.in2p3.fr/datagrid/ca>
- Globus Security: <http://www.globus.org/security/>
- EDG WP2: <http://grid-data-management.web.cern.ch/grid-data-management/security/>
- EDG D7.5: <http://edms.cern.ch/document/340234>

## Background

- GGF Security: <http://www.gridforum.org/security/>
- GSS-API: <http://www.faqs.org/faqs/kerberos-faq/general/section-84.html>
- IETF PKIX charter: <http://www.ietf.org/html.charters/pkix-charter.html>
- PKCS: <http://www.rsasecurity.com/rsalabs/pkcs/index.html>