Bezpečnosť v Gride
(Grid security)

Miroslav Dobrucký
Ústav informatiky
Slovenská akadémia vied
Bratislava

Obsah

- **Ako sa prihlásim do Gridu?**
  - Certifikáty - Autentifikácia
- **GSI**
  - Autorizácia
  - Delegované certifikáty
- **A walk-through – rekapitulácia**

Ako sa prihlásim do Gridu?

- **Zdroje sú distribuované: bezpečný prístup k nim je základnou požiadavkou**
  - Bezpečná komunikácia (SSL)
  - Bezpečnosť aj za organizačnými hranicami (PKI, X.509)
  - Iba jediné prihlásenie (zadanie hesla) pre používateľov Gridu (single sign-on)
- **Dva základné koncepty:**
- **Autentifikácia: Kto som?**
  - Ekvivalent ku OP, cestovnému pasu, ...
  - > Certifikáty
- **Autorizácia: Čo mám dovolené robiť?**
  - Určené povolenia, povinnosti, atď.
  - > Virtuálne organizácie

Zúčastnené entity

Certifikačná Autorita

dôvera

Používateľ

Žiadosť ->

<- Certifikát

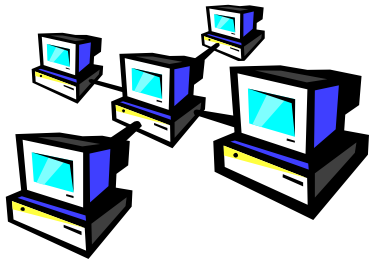
Žiadosť ->

<- Certifikát

Proxy certifikát ->

Privátny kľúč
Verejný kľúč
Certifikát

Zdroje
(strediská ponúkajúce služby)



Obsah

- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- A walk-through – rekapitulácia

Certifikáty

- Každý používateľ musí mať platný X.509 certifikát vydaný uznanou **Certification Authority** (CA)
- Pred vykonaním akejkoľvek činnosti v Gride sa používateľ musí prihlásiť na **User Interface** (UI) počítači a vytvorí si tzv. proxy certifikát
- **Proxy certifikát** má limitovanú časovú platnosť a používa sa na autentifikáciu používateľa (**delegated user credential**) bez nutnosti neskôr znova zadávať heslo (**pass phrase**) zakryptovaného privátneho kľúča
- **VOMS proxy** obsahuje rozšírenia ohľadne členstva vo VO a roliach, ktoré člen má

Ako vytvorím pár: kľúč/žiadosť

grid-cert-request príkaz

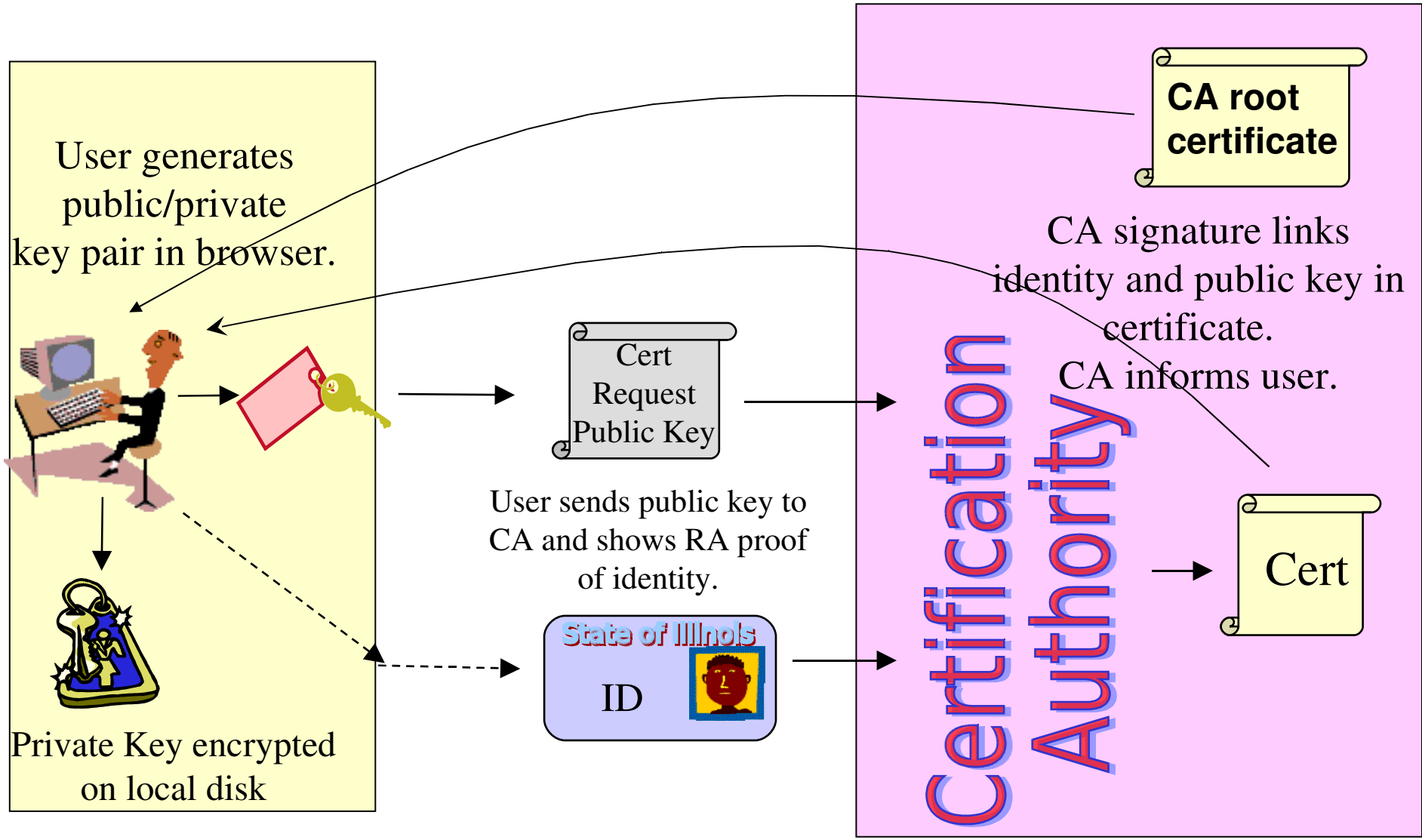
```
[miro@grid ~]$ grid-cert-request
Enter your name, e.g., John Smith: Miroslav Dobrucky
A certificate request and private key is being created.
You will be asked to enter a PEM pass phrase.
This pass phrase is akin to your account password,
and is used to protect your key file.
If you forget your pass phrase, you will need to
obtain a new certificate.

Using configuration from /etc/grid-security/globus-user-ssl.conf
Generating a 1024 bit RSA private key
.....................++++++
.........................++++++
writing new private key to '/home/miro/.globus/userkey.pem'
Enter PEM pass phrase:************
```

Poznámka: dá sa použiť aj priamo “openssl” alebo môj skript v linuxe (http://ups.savba.sk/ca/SlovakGrid_get_request).

Certificate Request

Courtesy of *Mike Mineter*



Ako získam certifikát

Doručím žiadosť relevantnej dôveryhodnej CA

```
[miro@grid ~]$ cat home/miro/.globus/usercert_request.pem | mail ca.ui@savba.sk
```

Používateľ musí doručiť svoju žiadosť relevantnej registračnej alebo certifikačnej autorite (RA alebo CA) a osobne sa preukázať svojím OP alebo podobným oficiálnym dokumentom obsahujúcim fotografiu. Mejlom doručená žiadosť bude skontrolovaná, či spĺňa požiadavky, ale je potrebné žiadosť doručiť aj osobne (USB pamäť, CD, disketa), alebo iným bezpečným kanálom.

RA následne doručí jej/jeho žiadosť certifikačnej autorite (CA), ktorá žiadosť podpíše a pošle naspäť mejlom ako certifikát, ktorý má platnosť 1 rok +1 mesiac a pred vypršaním platnosti môže byť využitý na podpísanie novej žiadosti, čo znamená, že sa už potom žiadateľ nemusí chodiť osobne preukazovať (aspoň raz za 5 rokov však musí).

Relevantné dôveryhodné CA

- C=SK, O=SlovakGrid, CN=SlovakGrid CA
- C=CZ, O=CESNET, CN=CESNET CA
- C=FR, O=CNRS, CN=CNRS
- C=GR, O=HellasGrid, CN=HellasGrid CA
- C=PT, O=LIPCA, CN=LIP Certification Authority
- C=ES, O=DATAGRID-ES, CN=DATAGRID-ES CA
- ...

Sú akreditované v združení "The European Policy Management Authority for Grid Authentication in e-Science" www.eugridpma.org, ktorá je členom svetovej IGTF federácie.

Nainštalovanie certifikátu

...na UI stroj do adresára ~/.globus

```
[miro@grid ~]$ ls –l .globus
-r--r--r-- 1 miro  miro 4774 Oct  8 13:11 usercert.pem
-r--r--r-- 1 miro  miro 1270 Oct  8 10:51 usercert_request.pem
-r-------- 1 miro  miro  963 Oct  8 10:51 userkey.pem
```

...do web prezerača:

```
openssl pkcs12 –export –in ~/.globus/usercert.pem \
   –inkey ~/.globus/userkey.pem –out user.p12 \
   –name 'Janko Mrkvicka'
```

A potom preniesť súbor user.p12 cez "Tools/Options/Advanced/ViewCertificates/Import" (Firefox).

Nezabudnúť mať nastavené hlavné heslo (MASTER PASSWORD).

Revokácia, CRL

- **Kedy je potrebné zrušiť platnosť certifikátu:**
  - Na žiadosť majiteľa – ak kľúč pokazil, stratil, alebo mu ho ukradli
  - Pri zistení, že majiteľ porušuje CP&CPS
- **Ako sa zruší platnosť certifikátu:**
  - Majiteľ doručí žiadosť o revokáciu dôveryhodnou cestou, napríklad osobne
  - Alebo CA rozhodne o nutnosti revokovať
  - CA vykoná revokačnú procedúru a okamžite vydá nový CRL
- **CRL (Certification Revocation List)**
  - CA pravidelne generuje CRL, ktorý má platnosť napr. 1 mesiac a publikuje ho (napr. na webe)
  - CE/SE (resources) pravidelne (častejšie než denne) sťahujú od všetkých dôveryhodných CA nimi vydané CRL

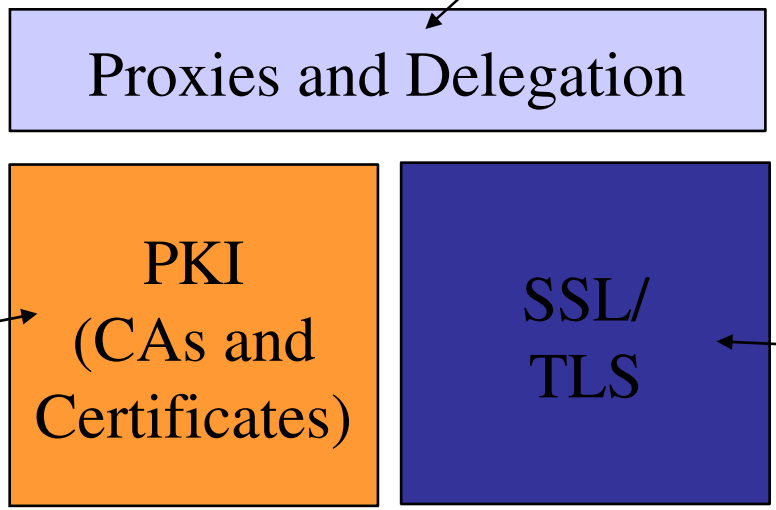
Obsah

- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- A walk-through – rekapitulácia

GSI - prehľad

Grid security infrastructure

Proxy a delegovanie (GSI rozšírenia) - pre bezpečné prihlásenie „single Sign-on“



PKI - pre poverovanie

SSL – pre autentifikáciu a ochranu posielaných údajov

Based on Slide from Globus Tutorial

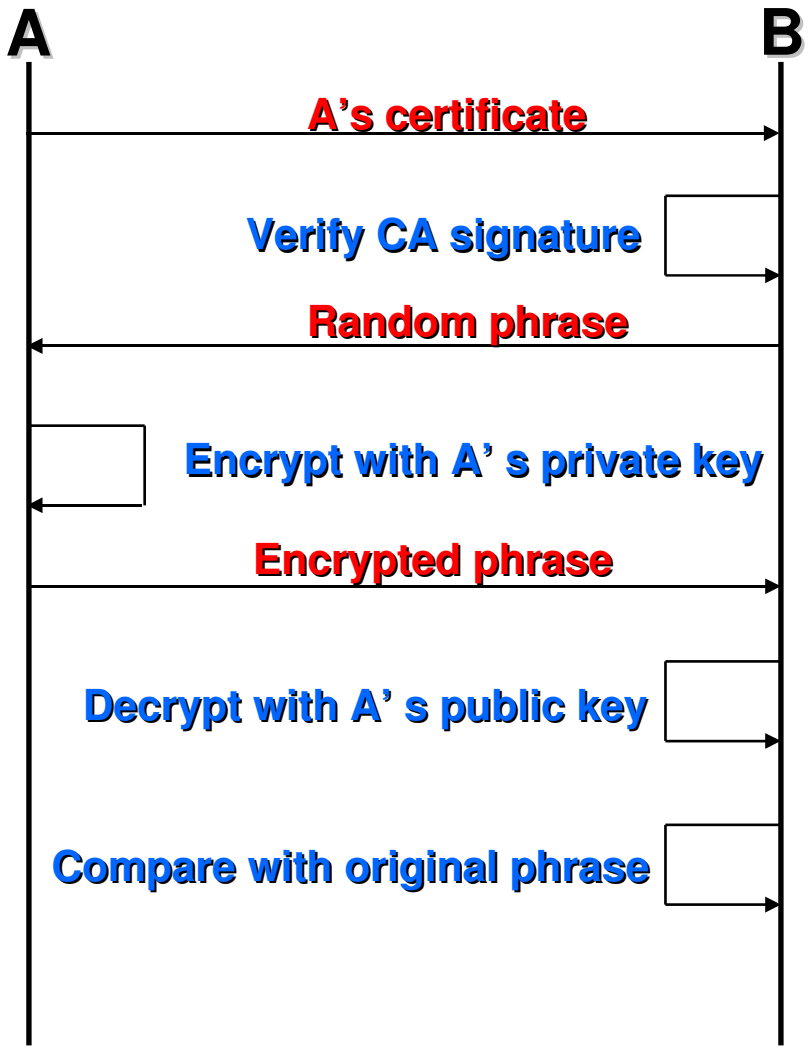
The Grid Security Infrastructure (GSI)

Courtesy of *Mike Mineter*

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

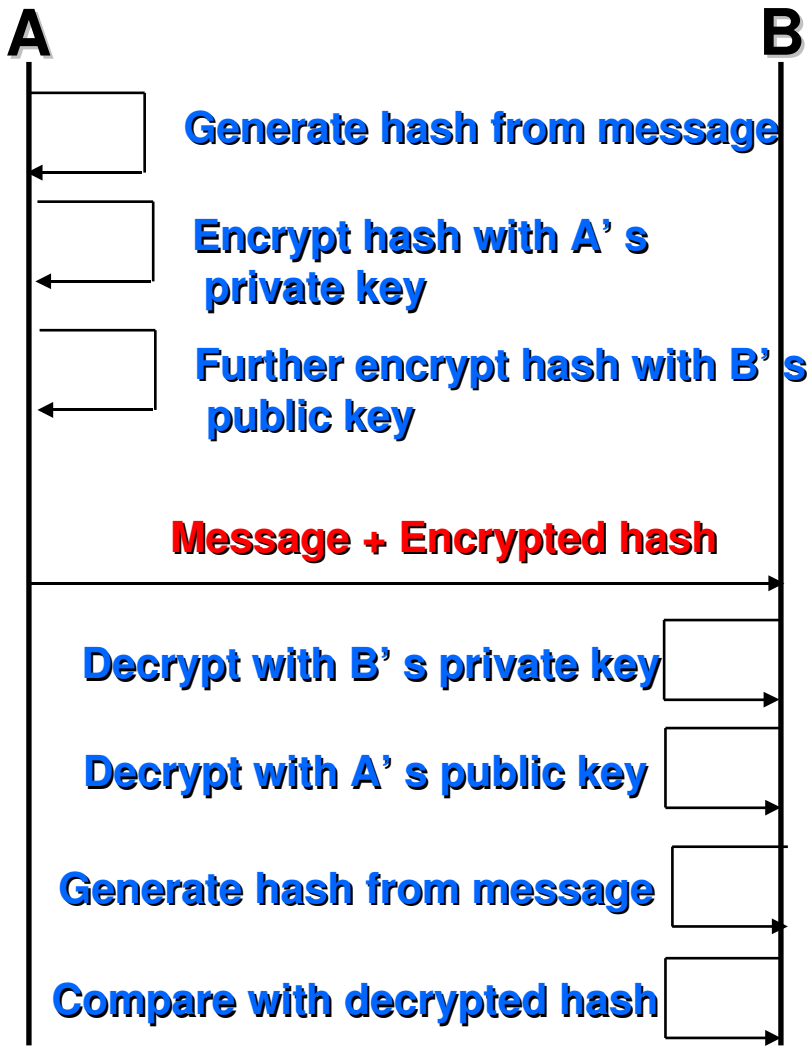


The Grid Security Infrastructure (GSI) …

Courtesy of *Mike Mineter*

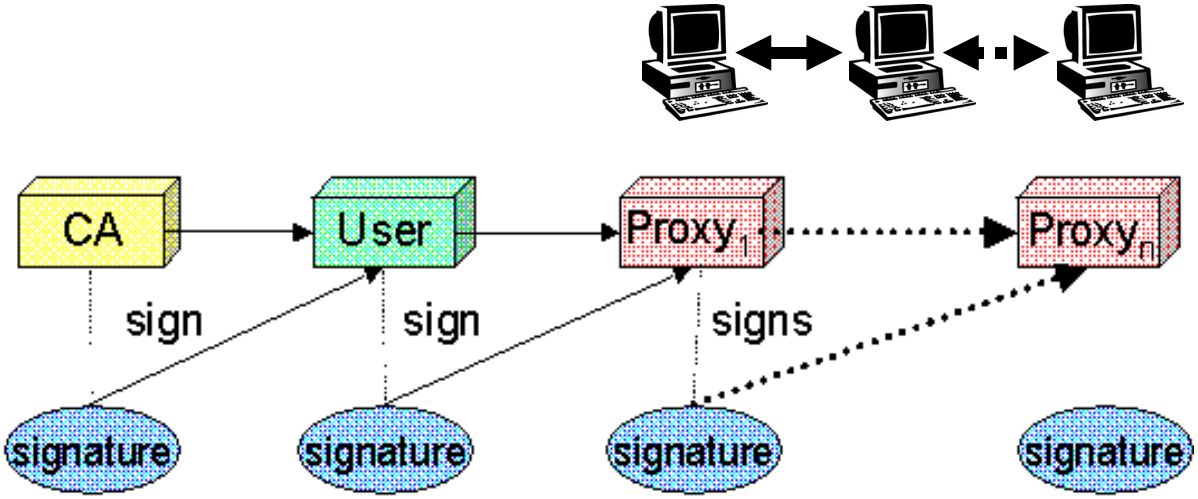
After A and B authenticated each other,
for A to send a message to B:

- Default: message integrity checking
  - Not private – a test for tampering



Grid Security Infrastructure - proxies

- **To support delegation: A delegates to B the right to act on behalf of A**
- **proxy certificates *extend X.509 certificates***
  - Short-lived certificates signed by the user's certificate or a proxy
  - Reduces security risk, enables delegation



User Responsibilities

Courtesy of *Mike Mineter*

- Keep your private key secure – *on USB drive only*
- Do not loan your certificate to anyone.
- Report to your local/regional contact if your certificate has been compromised.
- 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.

VOMS: Virtual Organization Membership Service

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

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

Obsah

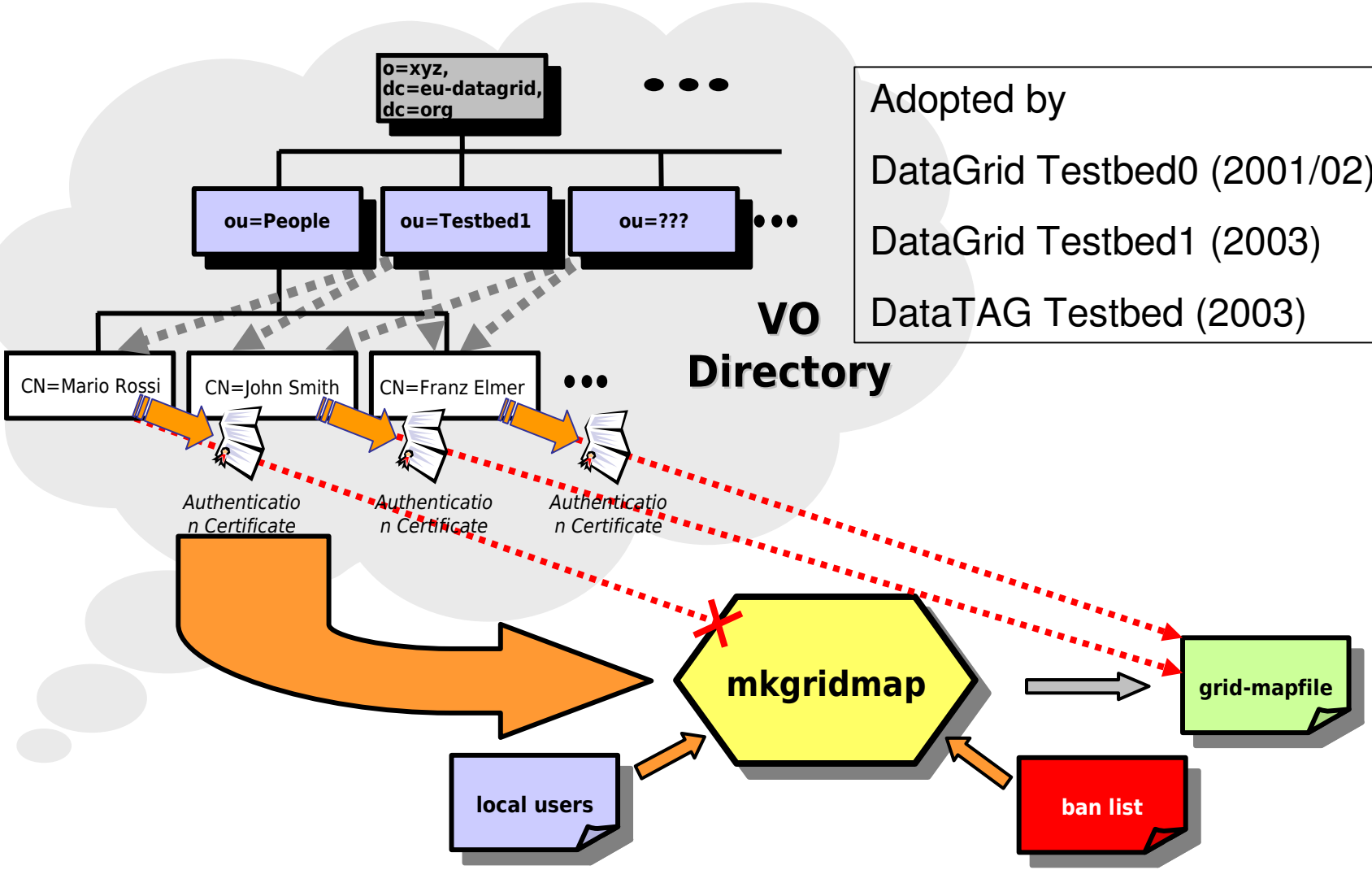
- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- A walk-through – rekapitulácia

Autorizácia

LDAP server

- **Udržuje zoznam členov VO**
- **CE/SE si pravidelne sťahuje aktuálny zoznam**
  - a generuje grid-mapfile
- **pri prvom prihlásení na CE/SE dostane používateľ jedno voľné konto**
  - z „pool accounts“
  - časom toto priradenie môže expirovať

príklad: VO-LDAP server na autorizáciu



Adopted by

DataGrid Testbed0 (2001/02)

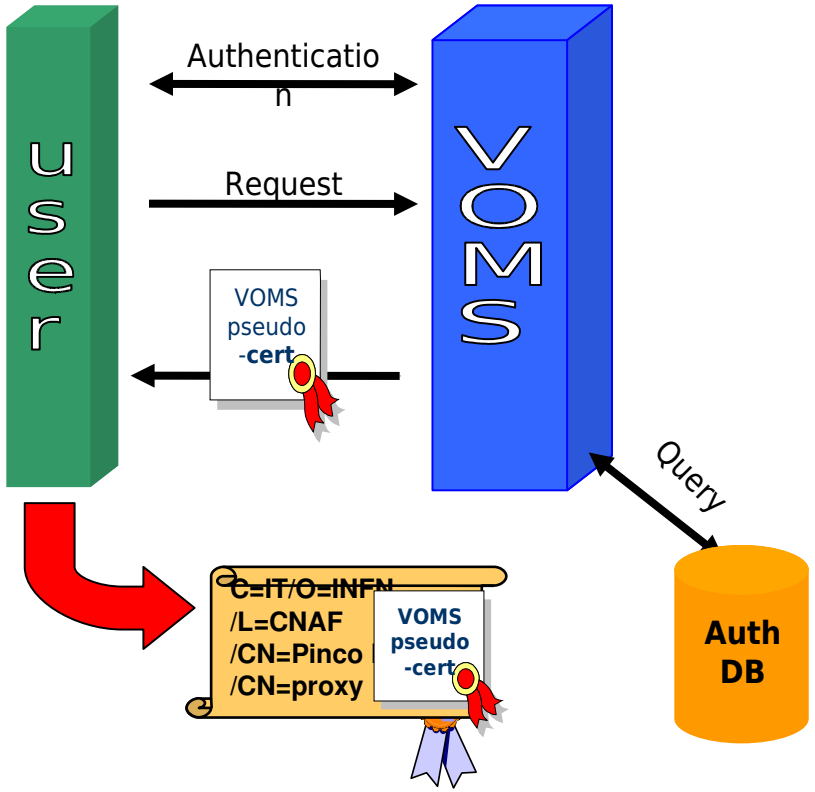
DataGrid Testbed1 (2003)

DataTAG Testbed (2003)

Zlepšenia / rozšírenia

- **Community Authorisation Service (CAS)**
  - od Globus Alliance
- **LCAS (Local Centre Authorization Service)**
  - DataGrid (EDG) plugin pre Globus
  - sysadmin môže blokovať prístup jednotlivým používateľom (ban list)
- **Virtual Organisation Membership Service (VOMS)**
  - od EU DataGrid a DataTAG projektov
  - VOMS proxy sa používa aj v gLite

VOMS



- **Mutual authentication Client-Server**
  - Secure communication channel via standard Globus API
- **Client sends request to VOMS Server**
- **Server checks correctness of request**
- **Server sends back the required info (signed by itself) in a "Pseudo-Certificate"**
- **Client checks the validity of the info received**
- **Optionally: [Client repeats process for other VOMS's]**
- **Client creates proxy certificates containing all the info received into a (non critical) extension**
- **Client may add user-supplied auth. info (kerberos tickets, etc…)**

Based on: http://www.slac.stanford.edu/econf/C0303241/proc/pres/317.PPT

Ako sa stať členom VO CE

- Mať naložený osobný certifikát vo web prezerači a navštíviť stránku
  - https://voce-register.farm.particle.cz/voce/

Návody ako na to:

- http://egee.cesnet.cz/en/voce/

Obsah

- Ako sa prihlásim do Gridu?
- Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- A walk-through – rekapitulácia

Delegované certifikáty

- **Proxy certifikát**
  - Krátko-dobý (12 hodín), s obmedzenými právomocami, odvodený z dlhodobého (1 rok) X.509 certifikátu
  - Podpísaný používateľovým certifikátom alebo iným proxy
  - Umožňuje procesu pôsobiť v mene používateľa
  - Je nezakryptovaný - preto musí byť uložený a dopravovaný bezpečnými spôsobmi
- **MyProxy server**
  - Udržuje stredne-dobý proxy (7 dní)
  - Chránený heslom
  - Generuje na požiadanie z neho krátkodobý proxy
  - Vhodné pre prácu z portálu (“internet café”)
  - Alebo pre dlhšie trvajúce úlohy (bežný proxy expiruje)
    - Proxy certifikát je automaticky obnovovaný počas celého behu úlohy

Vytvorenie proxy certifikátu

grid-proxy-init príkaz

```
[miro@grid ~]$ grid-proxy-init
 Your identity: /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
 Enter GRID pass phrase for this identity:
 Creating proxy ..................................... Done
 Your proxy is valid until: Fri Oct 19 22:37:05 2007
```

grid-proxy-info

grid-proxy-destroy

MyProxy (2): vloženie proxy certifikátu na server

myproxy-init príkaz

```
[miro@grid ~]$ myproxy-init –s myproxy.cern.ch
Your identity: /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
Enter GRID pass phrase for this identity:
Creating proxy ..................................... Done
Proxy Verify OK
Your proxy is valid until: Fri Oct 26 12:05:40 2007
Enter MyProxy pass phrase:
Verifying password - Enter MyProxy pass phrase:
A proxy valid for 168 hours (7.0 days) for user miro now exists on
  myproxy.cern.ch.
```

MyProxy (3): vyzdvihnutie proxy certifikátu

myproxy-get-delegation príkaz

```
[miro@grid miro]$ myproxy-get-delegation –s \
    myproxy.cern.ch
Enter MyProxy pass phrase:
A proxy has been received for user miro in /tmp/x509up_u1001
```

myproxy-info

myproxy-destroy

Poznámka: myproxy-destroy vyžaduje mať u seba na disku svoj ‘lokálny’ proxy v /tmp

Vytvorenie VOMS proxy certifikátu

VOMS-proxy-init príkaz

```
[miro@grid ~]$ voms-proxy-init –voms voce
Enter GRID pass phrase:
Your identity: /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
Creating temporary proxy ..................................... Done
Contacting  skurut19.cesnet.cz:7001
[/DC=cz/DC=cesnet-ca/O=CESNET/CN=skurut19.cesnet.cz] "voce" Done
Creating proxy ............................................... Done
Your proxy is valid until Sat Oct 20 00:01:13 2007
```

voms-proxy-info

voms-proxy-destroy

Poznámka: na MyProxy sa ukladá len štandardný proxy, nedá sa tam vložiť rozšírený VOMS proxy.

VOMS proxy certifikát

```
[miro@grid ~]$ voms-proxy-info -all
subject   : /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky/CN=proxy
issuer    : /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
identity  : /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
type      : proxy
strength  : 512 bits
path      : /tmp/x509up_u1001
timeleft  : 11:59:31
=== VO voce extension information ===
VO        : voce
subject   : /C=SK/O=SlovakGrid/O=IISAS/CN=Miroslav Dobrucky
issuer    : /DC=cz/DC=cesnet-ca/O=CESNET/CN=skurut19.cesnet.cz
attribute : /voce/Role=NULL/Capability=NULL
timeleft  : 11:59:31
```

Poznámka: gLite-voms-proxy-* sú len ‘symlink’ na príkazy voms-proxy-*

gLite - WMProxy

[miro@grid ~]$ glite-wms-job-delegate-proxy –d mojprvy

Connecting to the service
https://wms.ui.savba.sk:7443/glite_wms_wmproxy_server

========== glite-wms-job-delegate-proxy Success ==========

Your proxy has been successfully delegated to the WMProxy:

https://wms.ui.savba.sk:7443/glite_wms_wmproxy_server

with the delegation identifier: mojprvy

==========

Alebo sa dá delegovať až pri spustení úlohy (jobu).

Informácia o stave delegáta (proxy) sa v gLite 3.1 dá zistiť príkazom:

glite-wms-job-info -d mojprvy

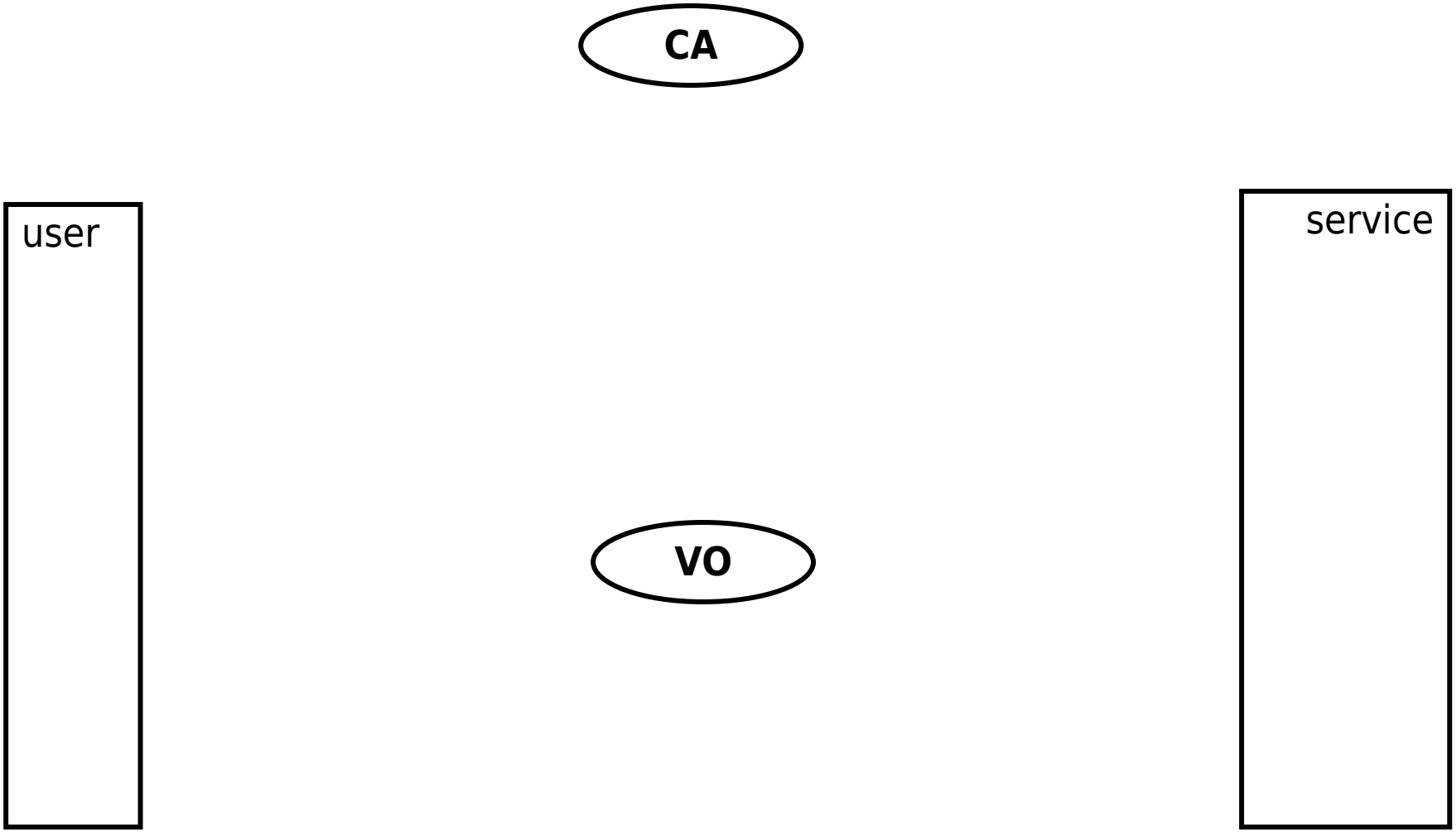
Ako sa dá delegát zmazať? Asi zatiaľ nijako.

Obsah

- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- **A walk-through – rekapitulácia**

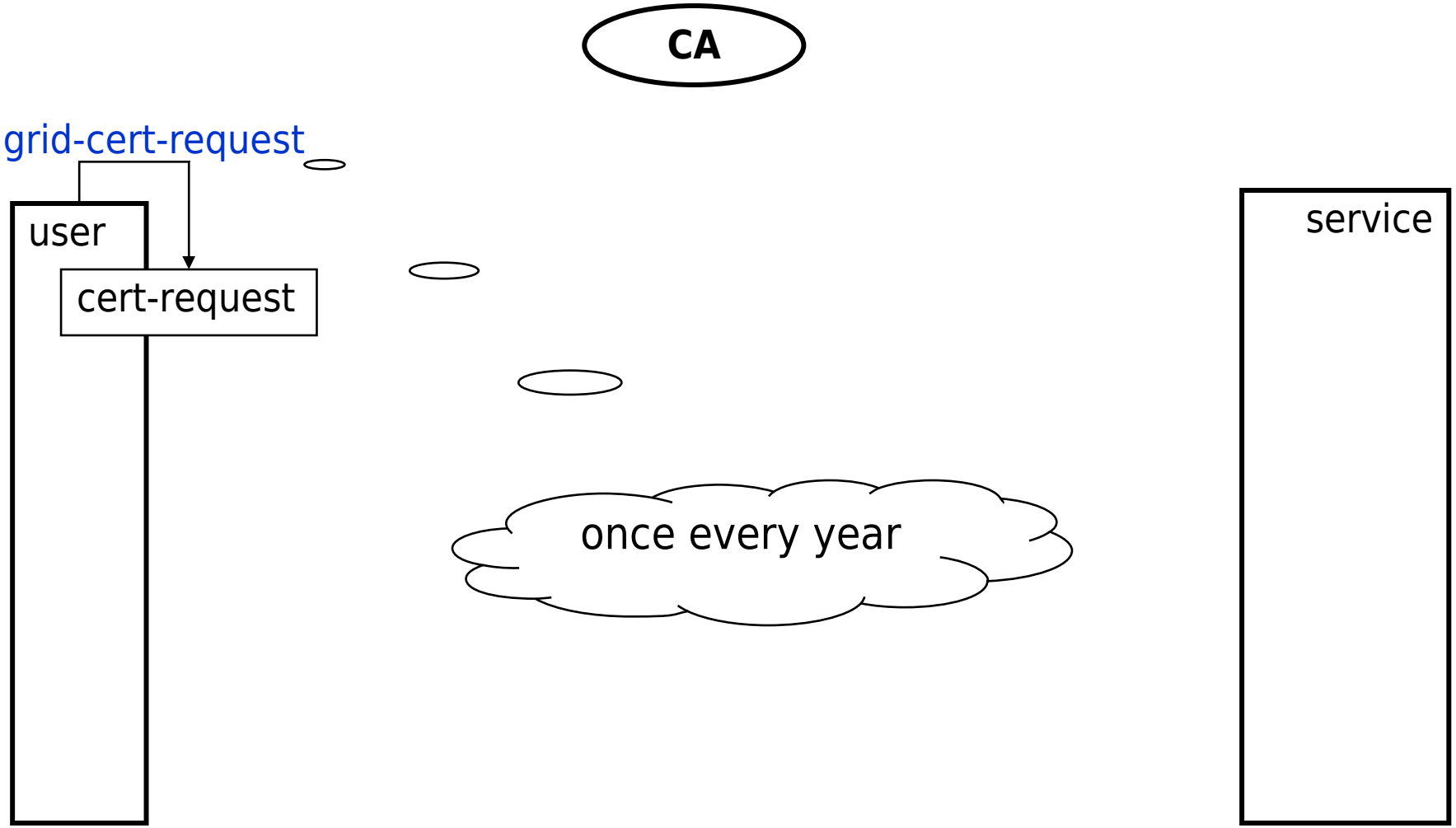
A walk-through

Courtesy of *David Groep*



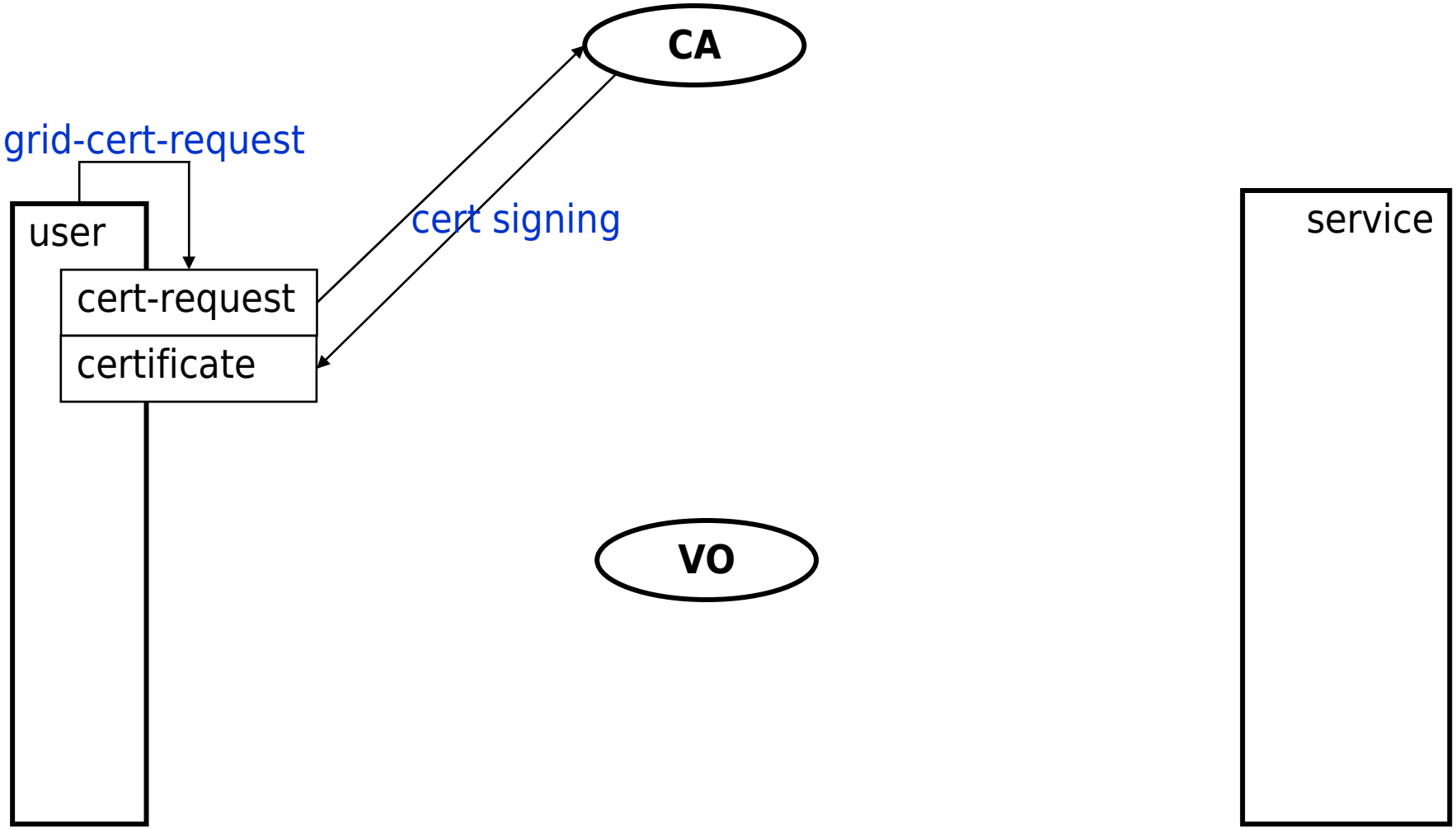
Certificate request

Courtesy of *David Groep*



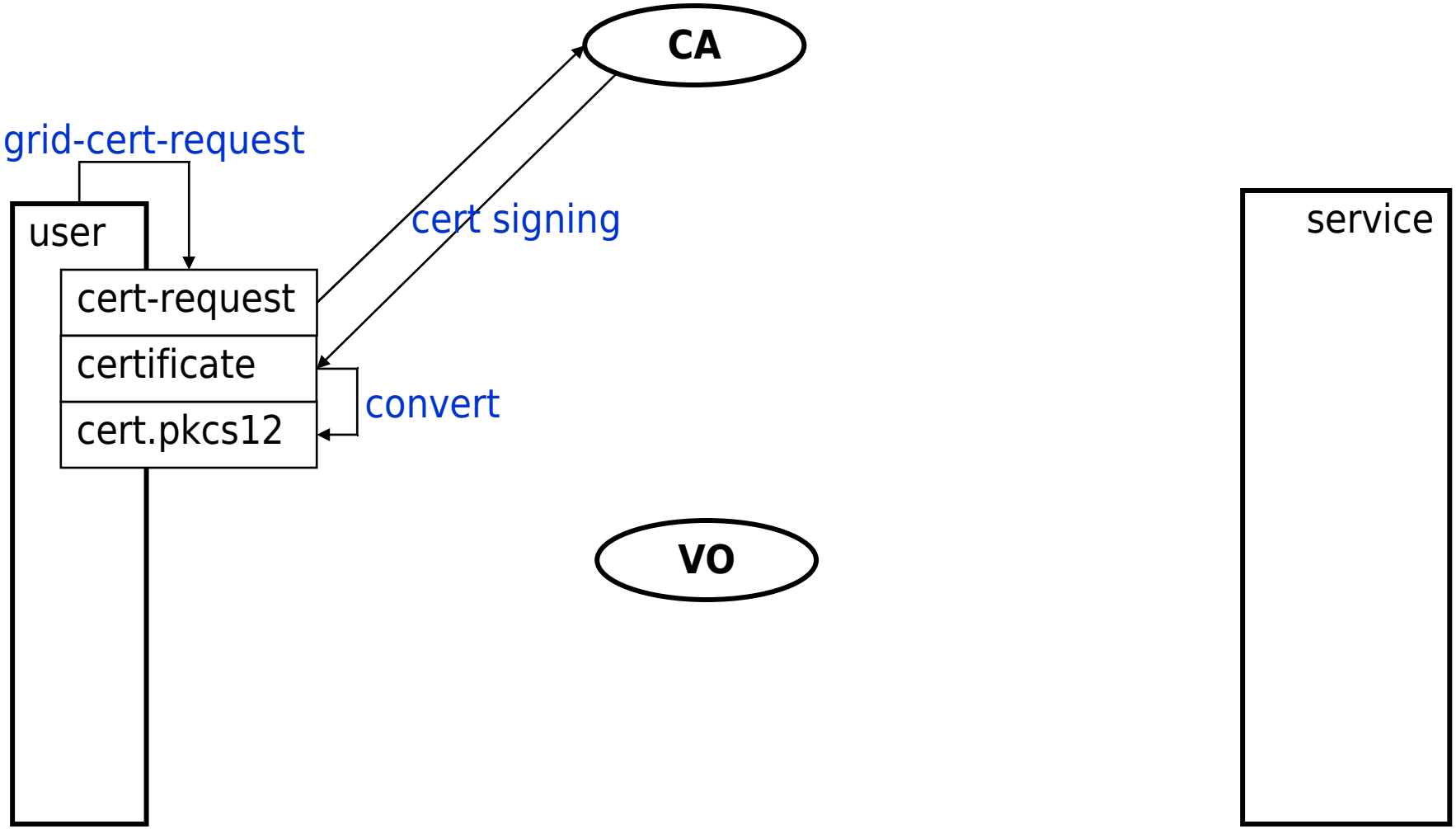
Certificate signing

Courtesy of *David Groep*



Importing your certificate in the browser

Courtesy of *David Groep*

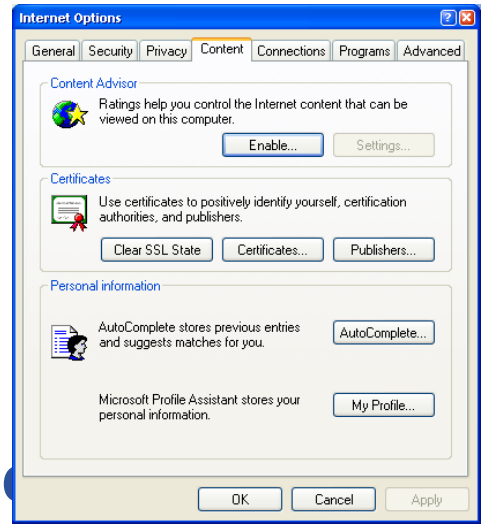


Browser certificates

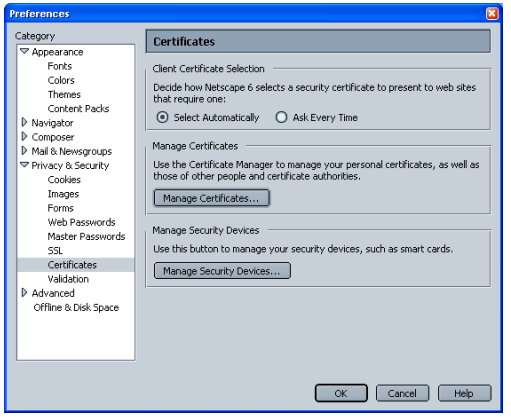
Courtesy of *David Groep*

- **Your our certificate must be in *PKCS#12* format**

```
openssl pkcs12 –export \
    –in ~/.globus/usercert.pem \
    –inkey ~/.globus/userkey.pem \
    –out user.p12 \
    –name ’Joe Smith’
```



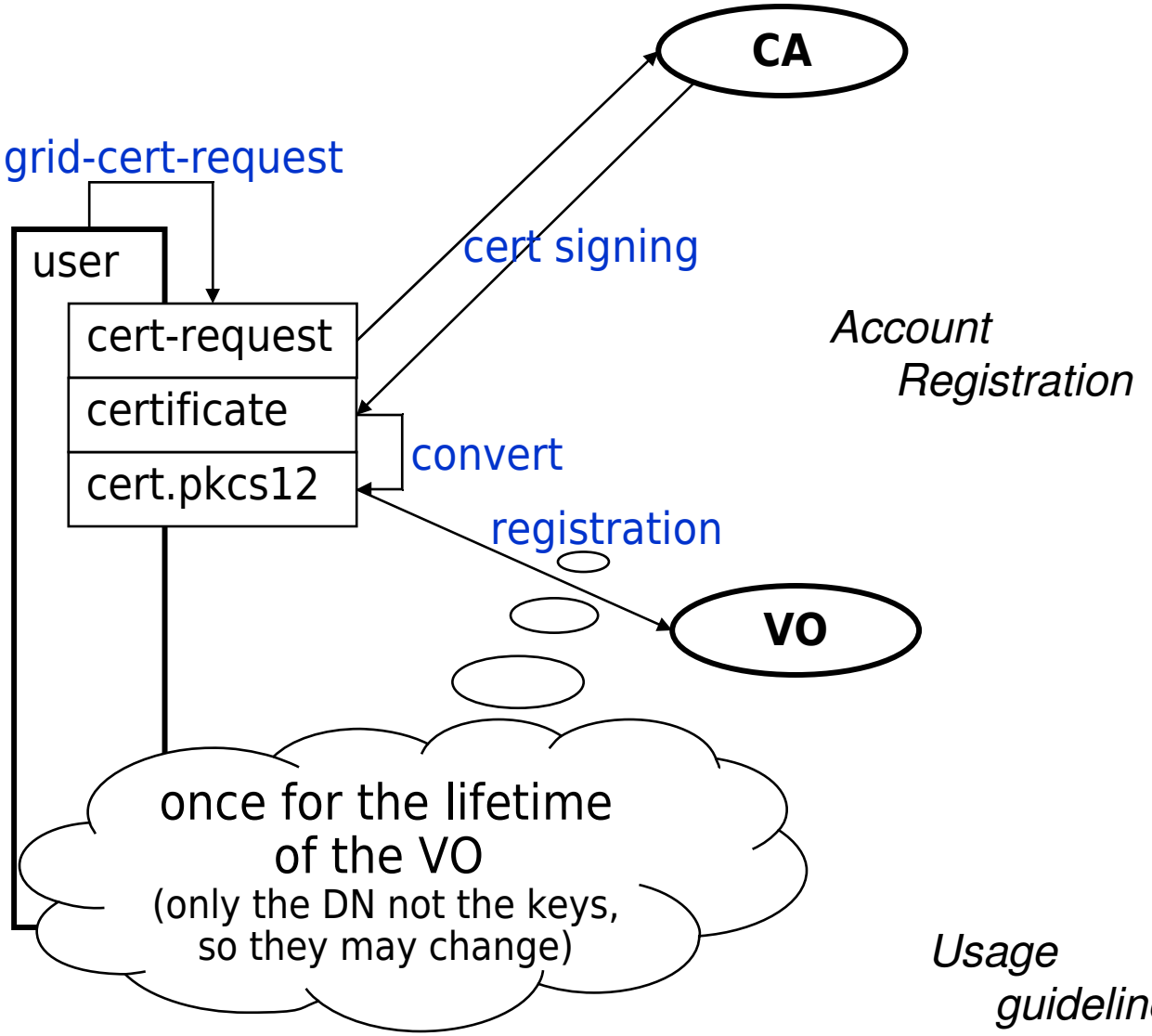
- **Use the “certificate store” of your brows**
  - Windows: double-click on the “.p12” file
  - Explorer: Internet Options – tab: Content
  - Netscape 6: Preferences – Privacy&Sec – Certificates, then use “Restore”



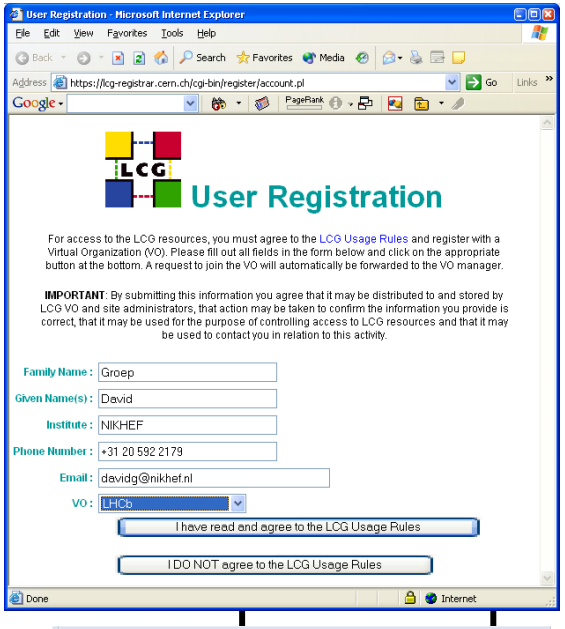
- **And SET THE MASTER PASSWORD**

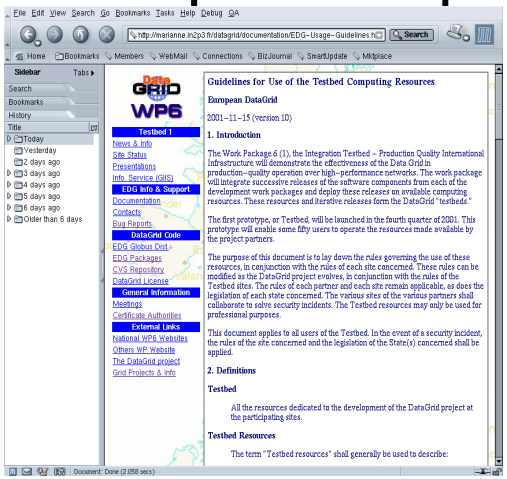
Usage Guidelines

Courtesy of *David Groep*



Account Registration

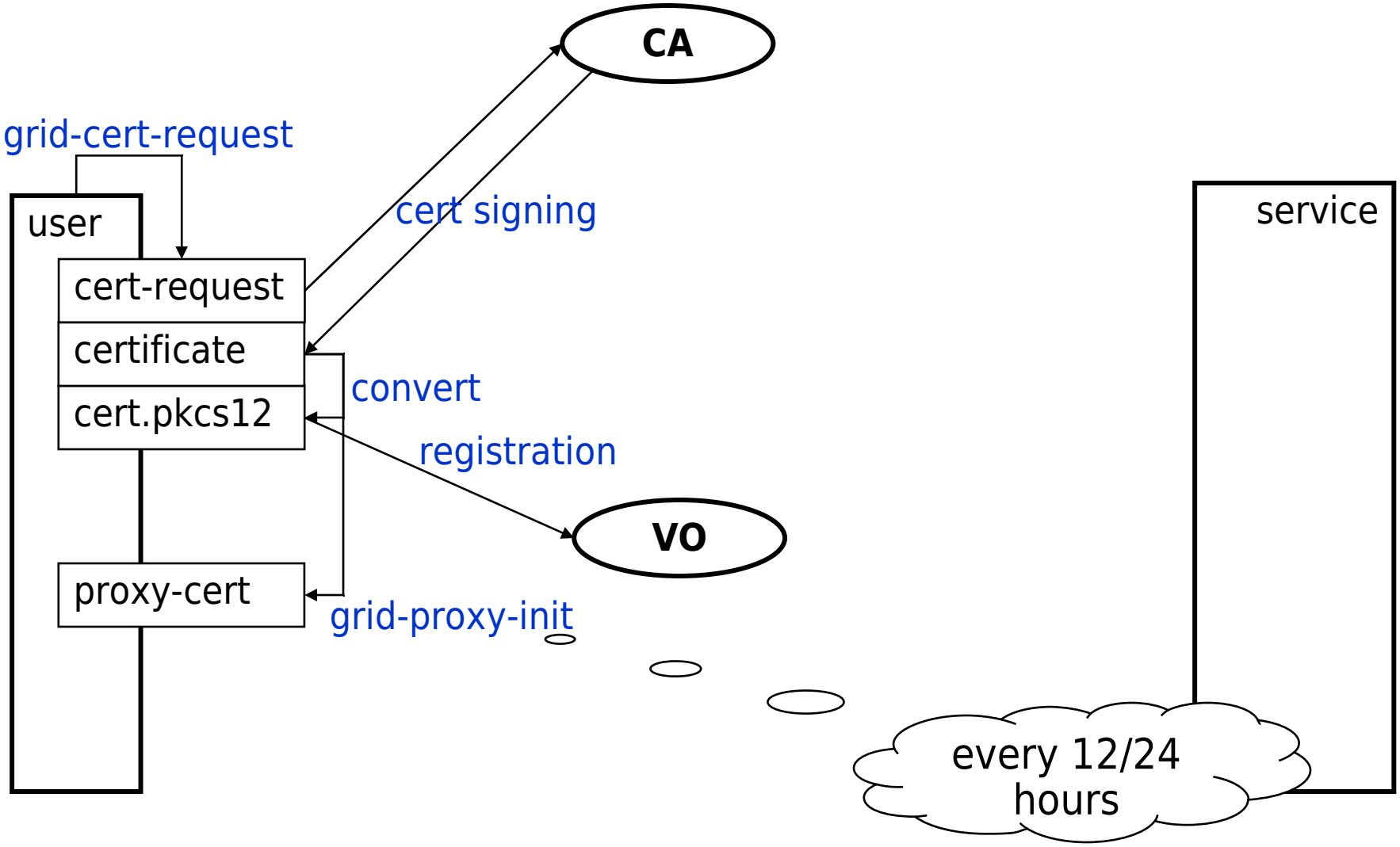




Usage guidelines

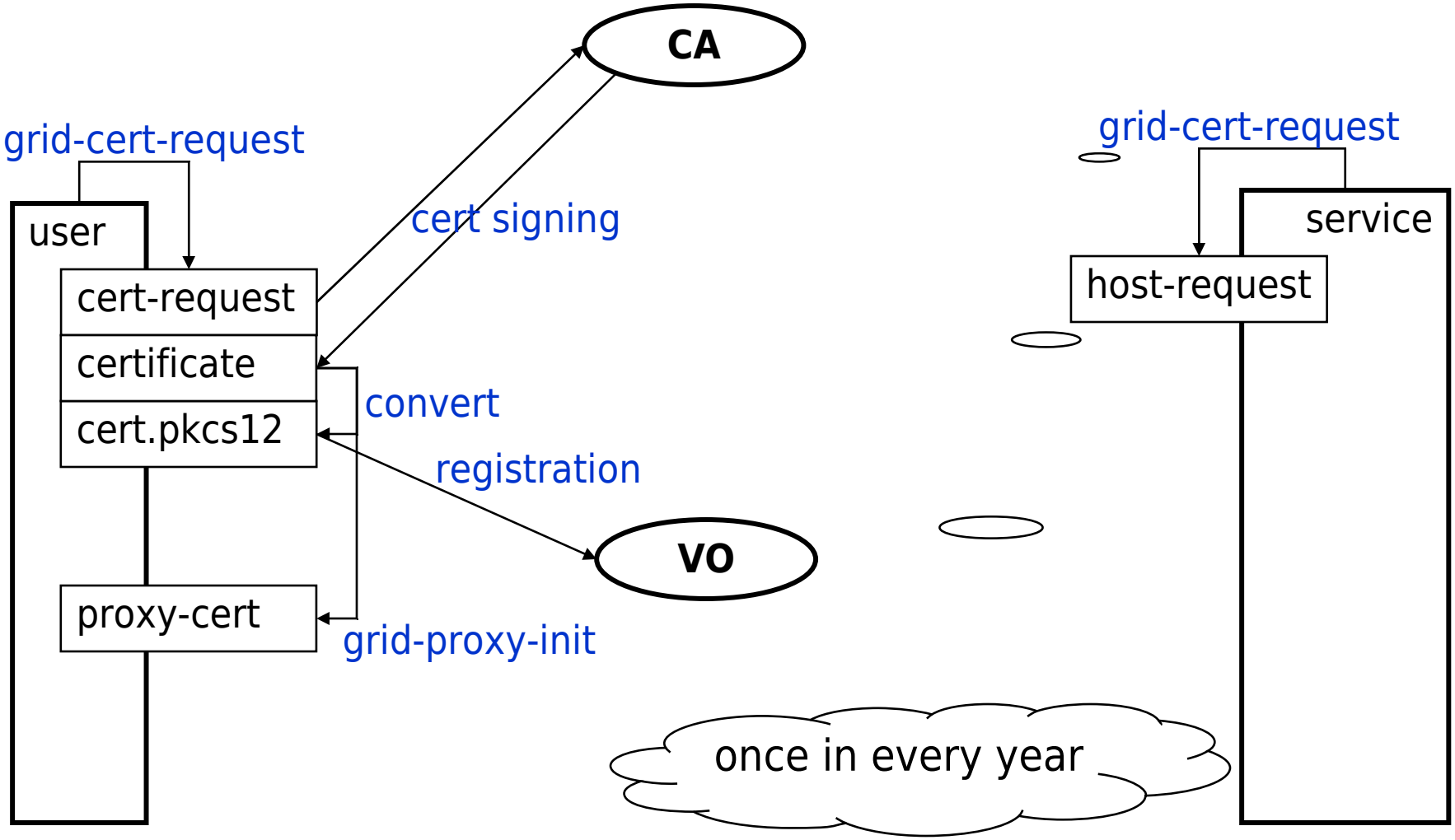
Starting a session

Courtesy of *David Groep*



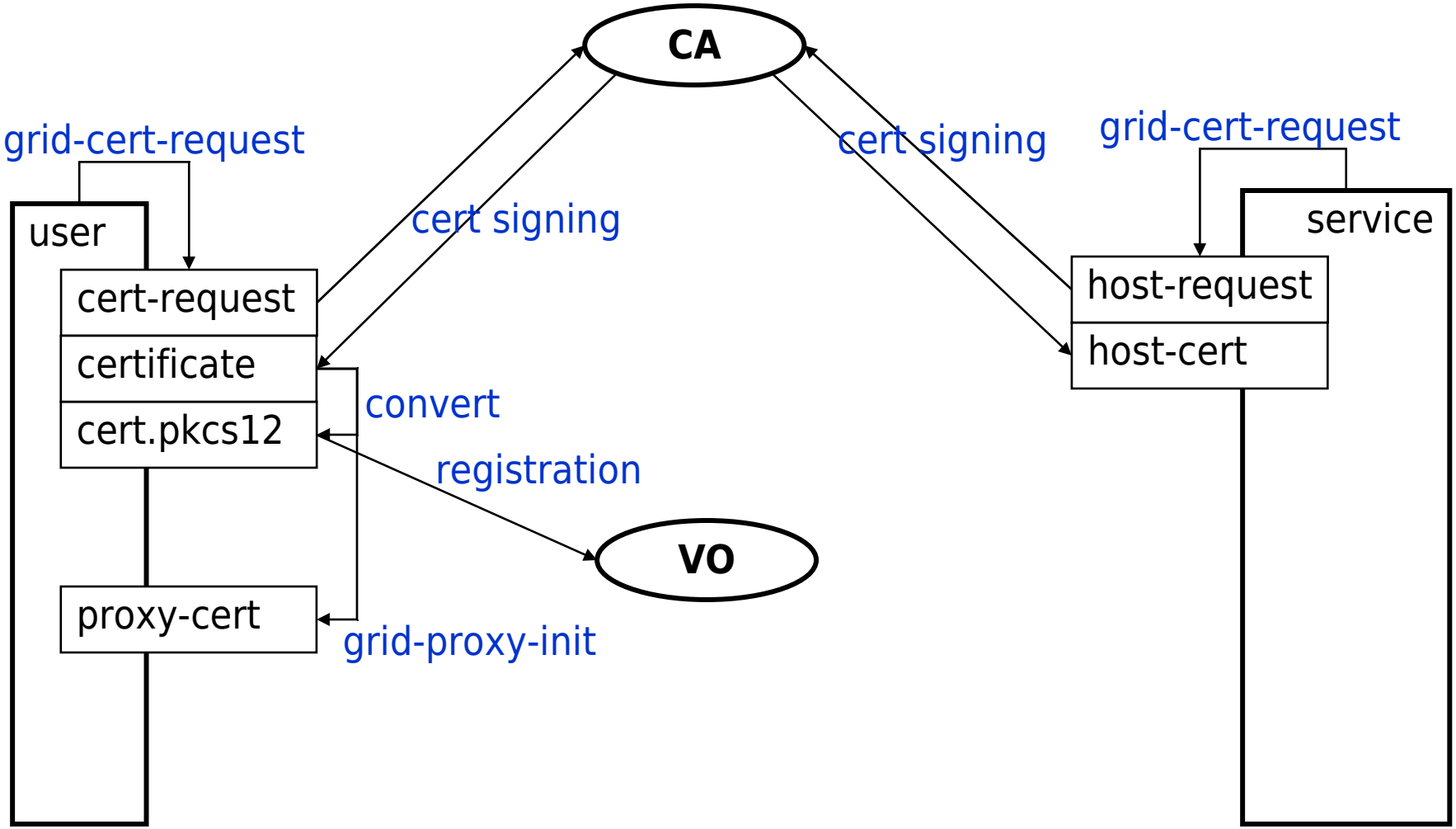
Certificate Request for a Host

Courtesy of *David Groep*



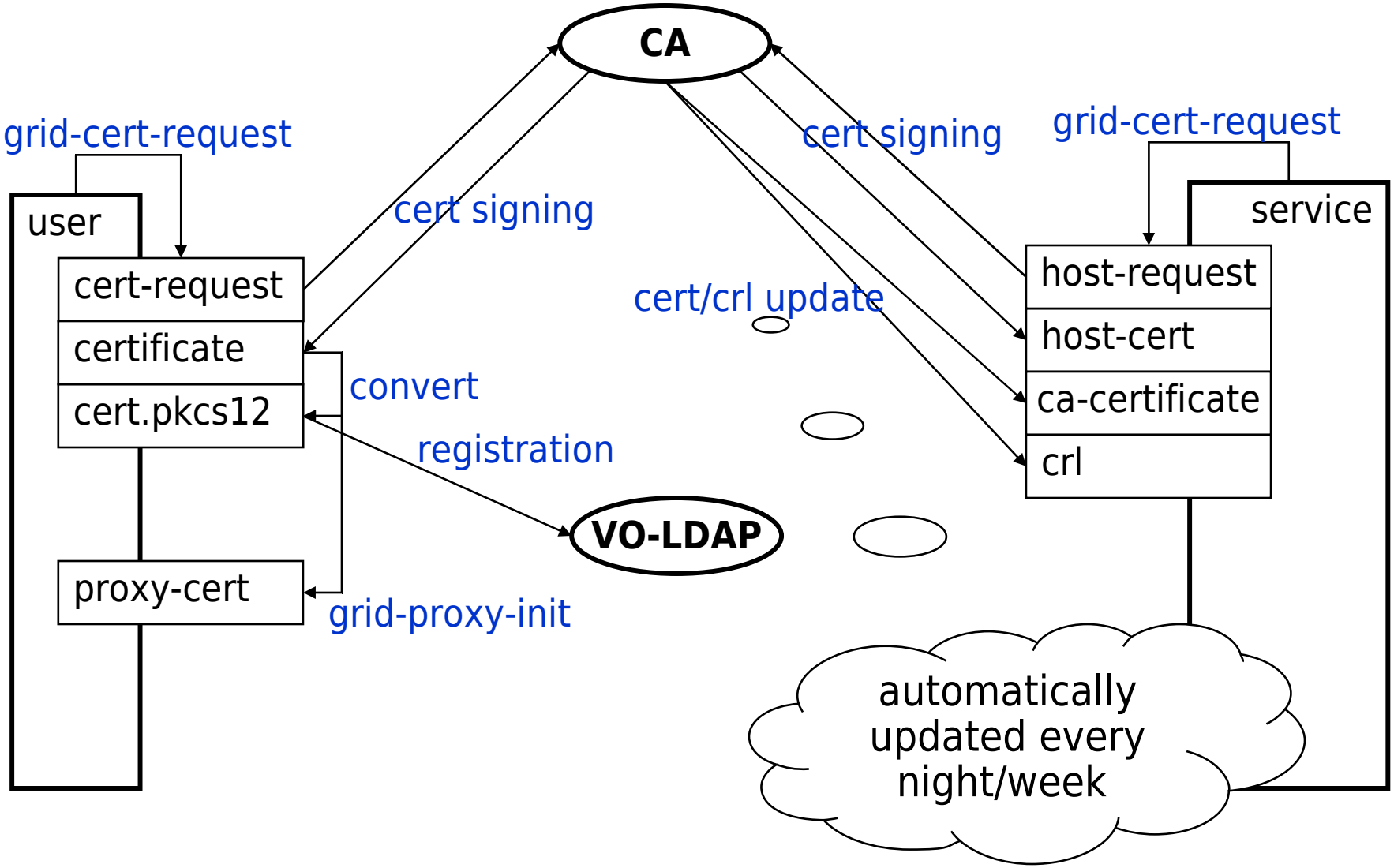
Signing the Certificate

Courtesy of *David Groep*



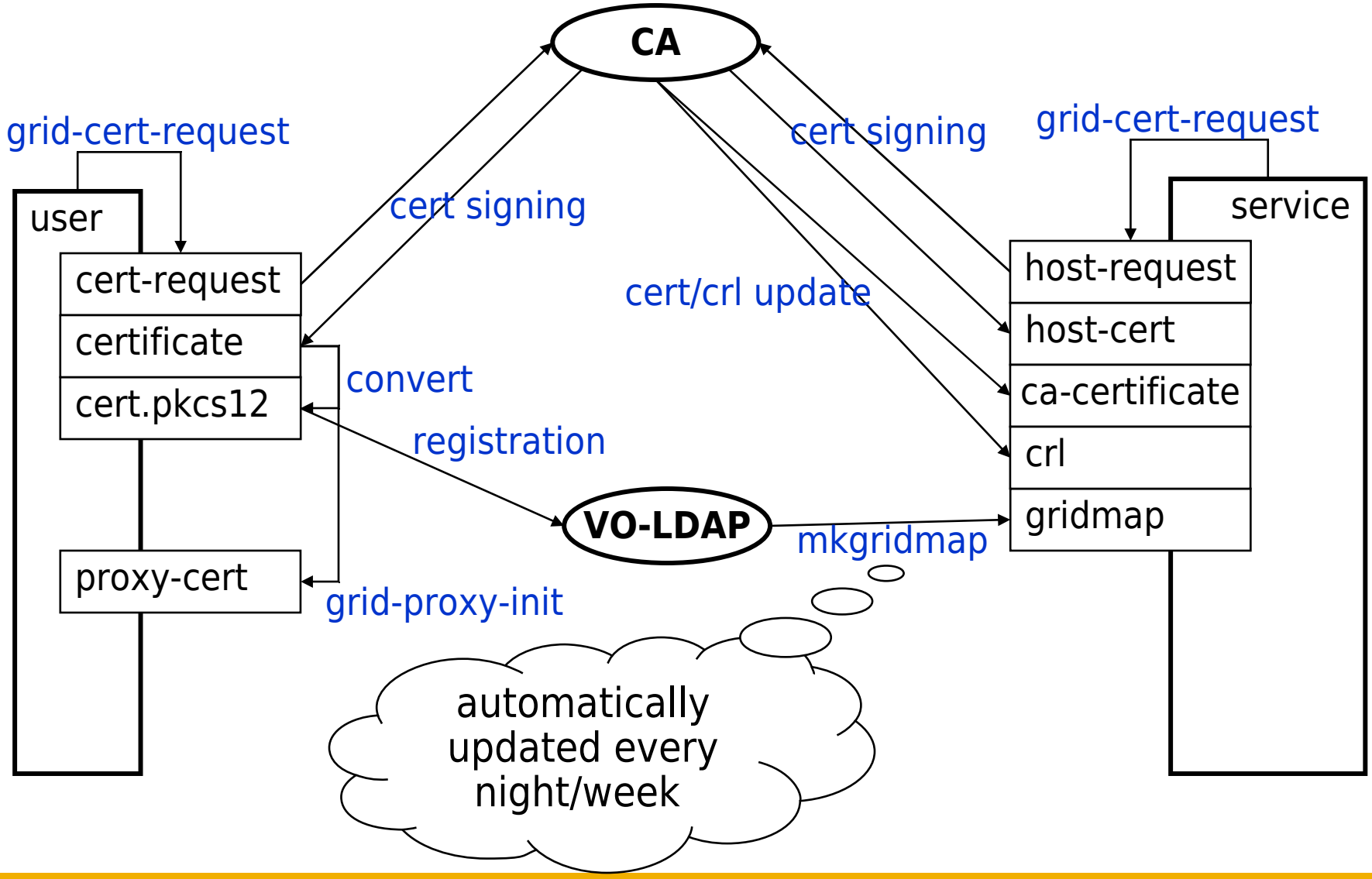
Configuration on the Server

Courtesy of *David Groep*

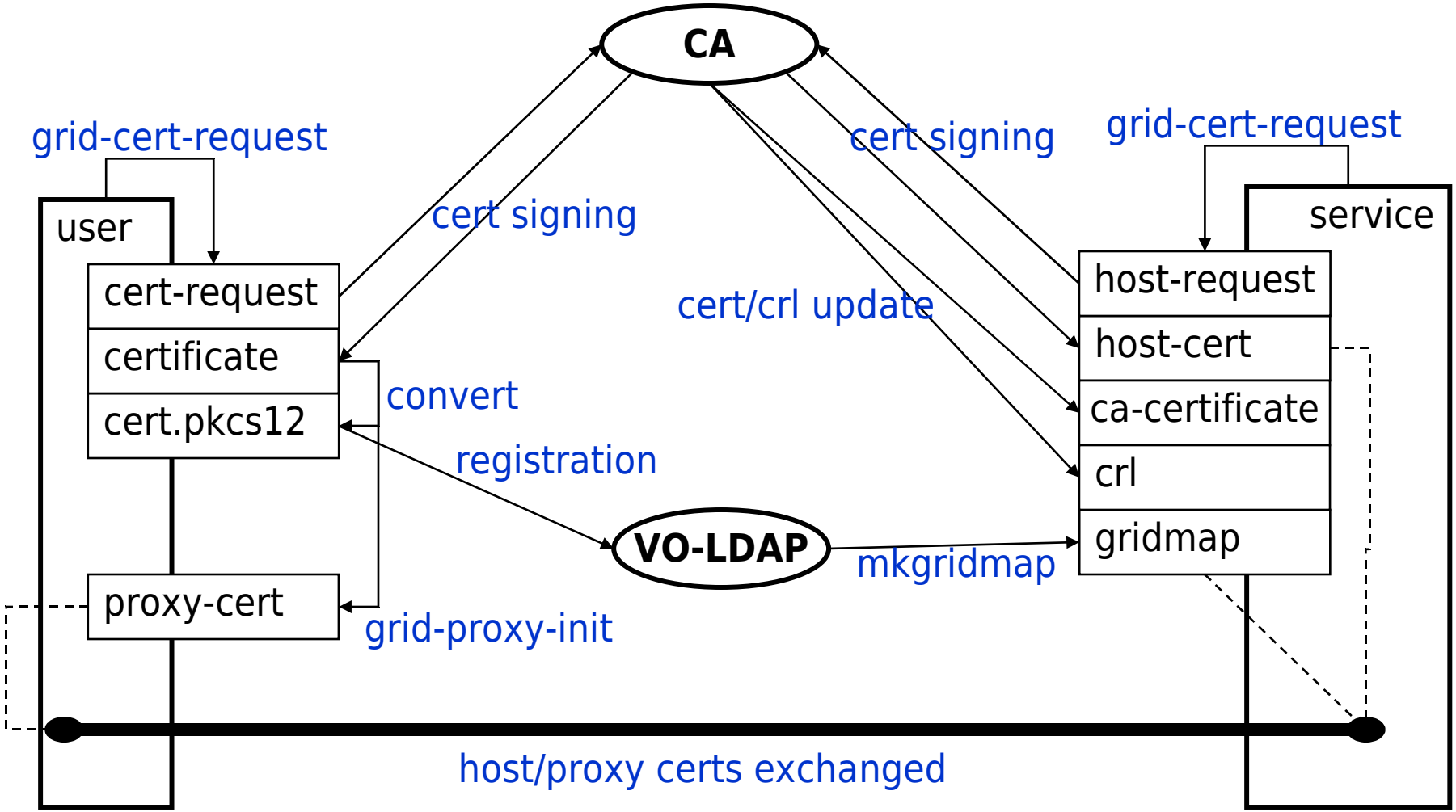


Authorization Information

Courtesy of *David Groep*



Using a Service



Ďakujem za pozornosť

egee.ui{AT}sav.sk

http://www.ui.sav.sk-egee

Miroslav Dobrucký

Ústav informatiky

Slovenská akadémia vied

Bratislava