

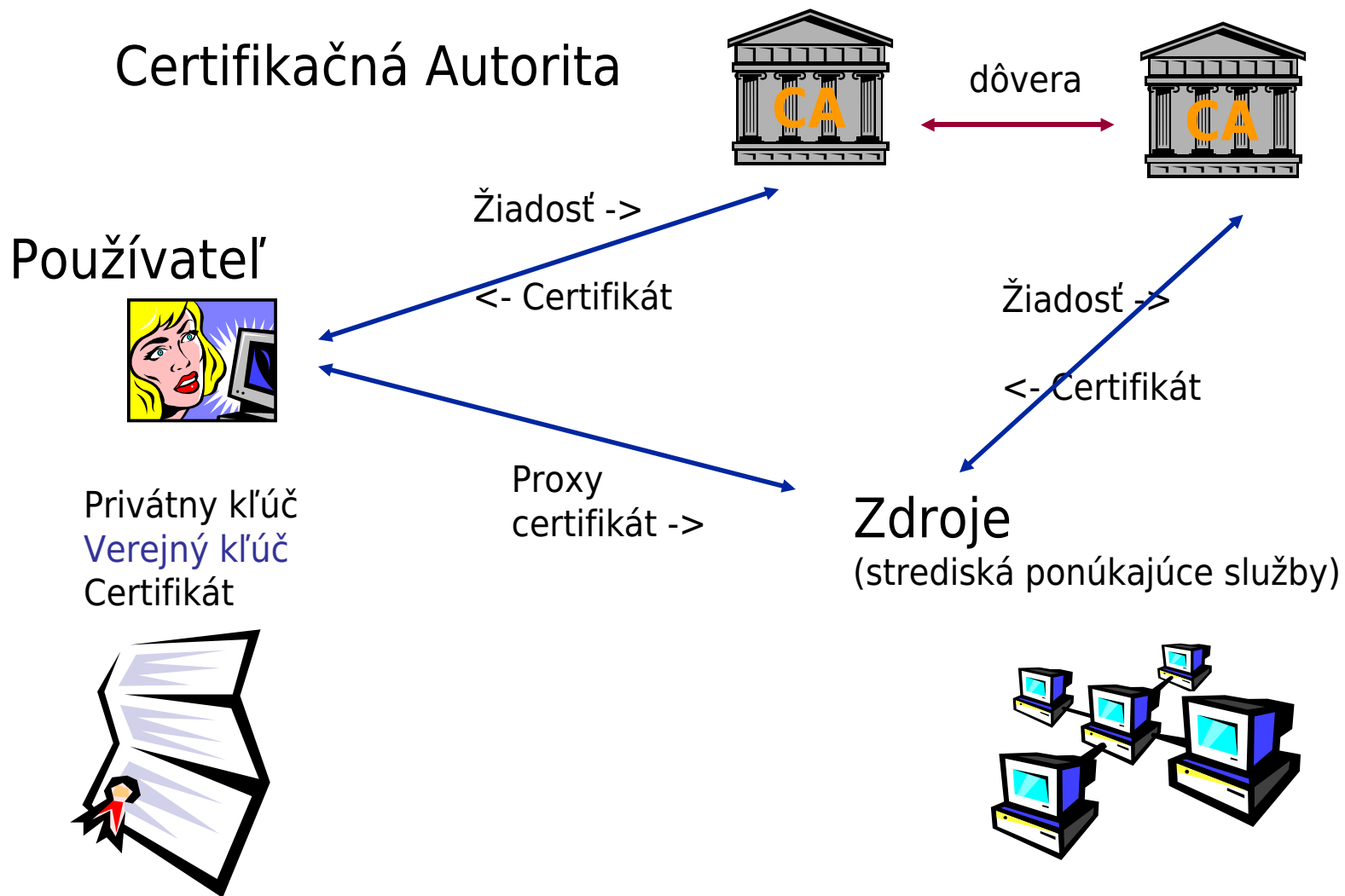
# Prístup do Gridu a bezpečnosť v Gride

**Miroslav Dobrucký**  
Ústav informatiky  
Slovenská akadémia vied  
Bratislava

- **Ako sa prihlásim do Gridu?**
  - Certifikáty - Autentifikácia
- **GSI**
  - Autorizácia
  - Delegované certifikáty
- **Rekapitulácia**

- 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

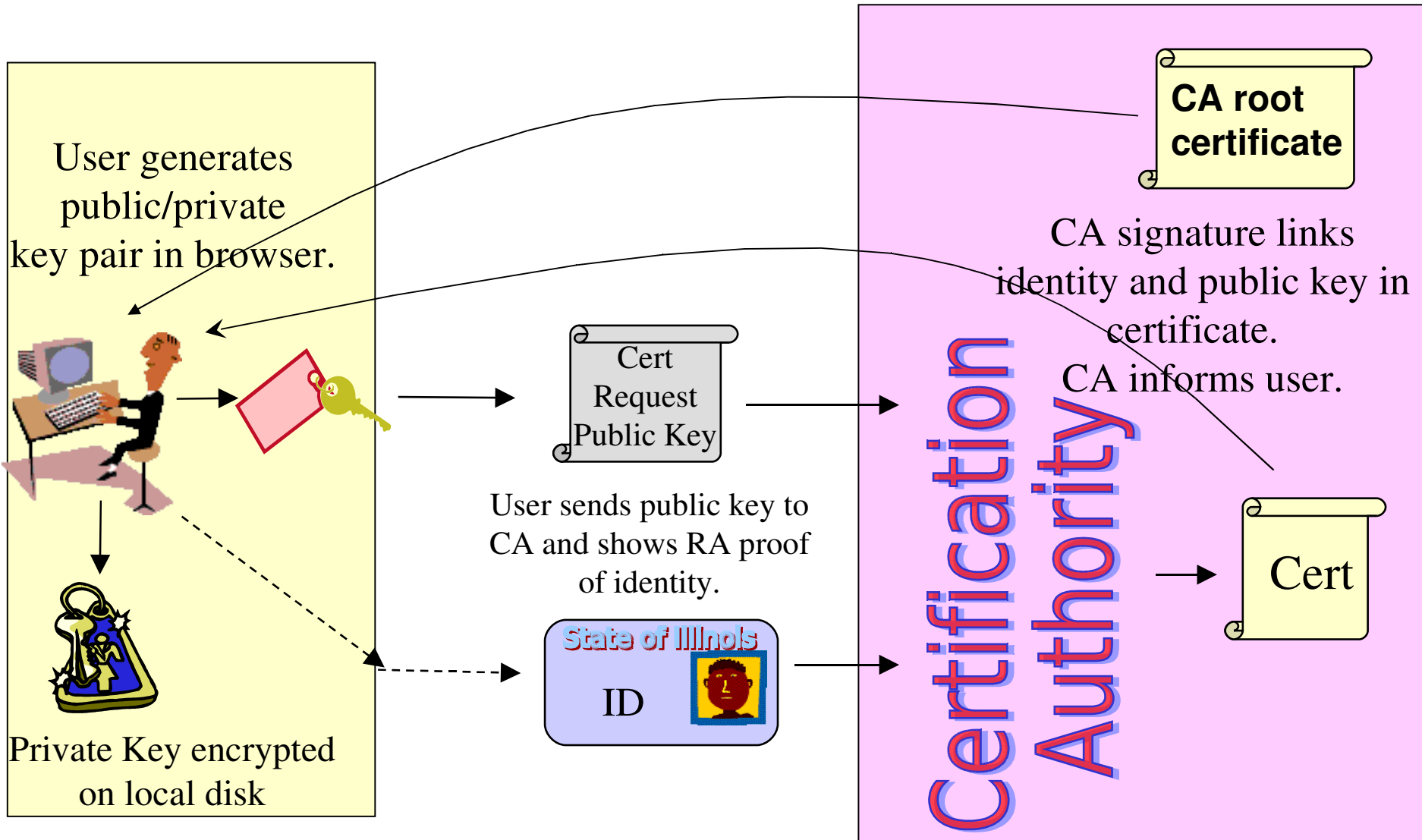




- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- Rekapitulácia

- 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)** počítača 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**) zakrytovaného privátneho kľúča
- **VOMS proxy** obsahuje rozšírenia ohľadne členstva vo VO a informáciu o roliach, ktoré člen má

# Certificate Request



## 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](http://ups.savba.sk/ca/SlovakGrid_get_request)).



## 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 svojim 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).

- 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](http://www.eugridpma.org), ktorá je členom svetovej IGTf federácie.*

## ...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).

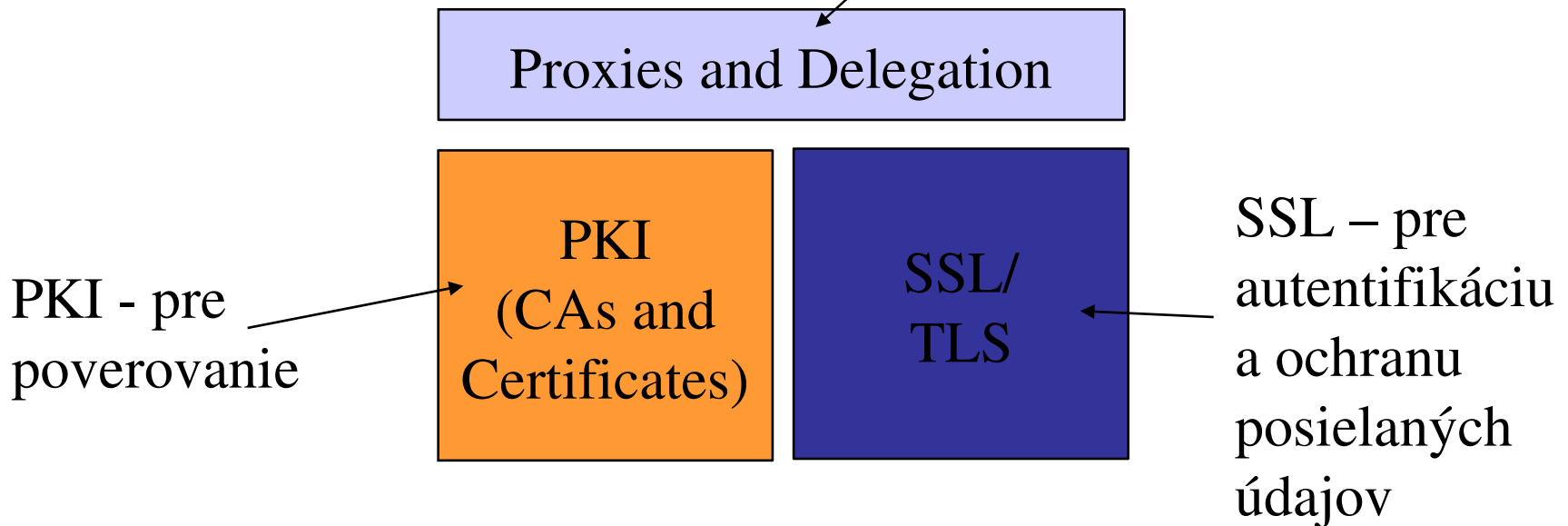
**Nezabudnúť mať nastavené hlavné heslo (MASTER PASSWORD).**

- **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

- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- **GSI**
  - Autorizácia
  - Delegované certifikáty
- **Rekapitulácia**

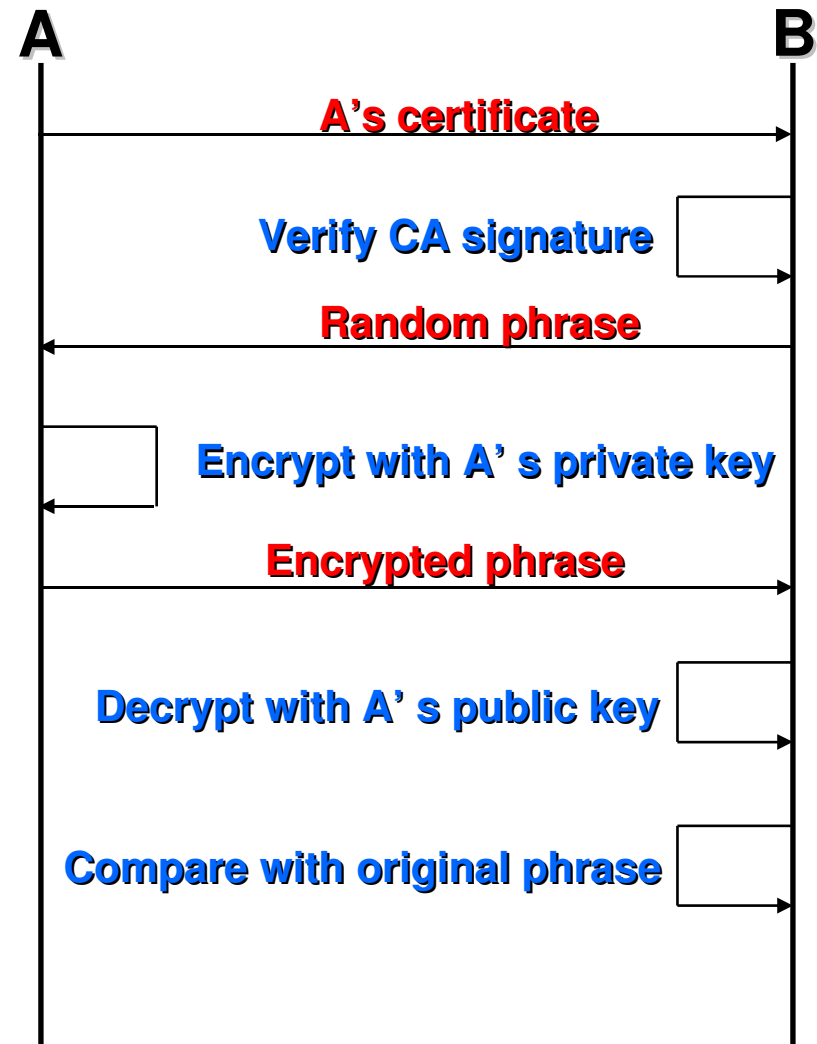
## Grid security infrastructure

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



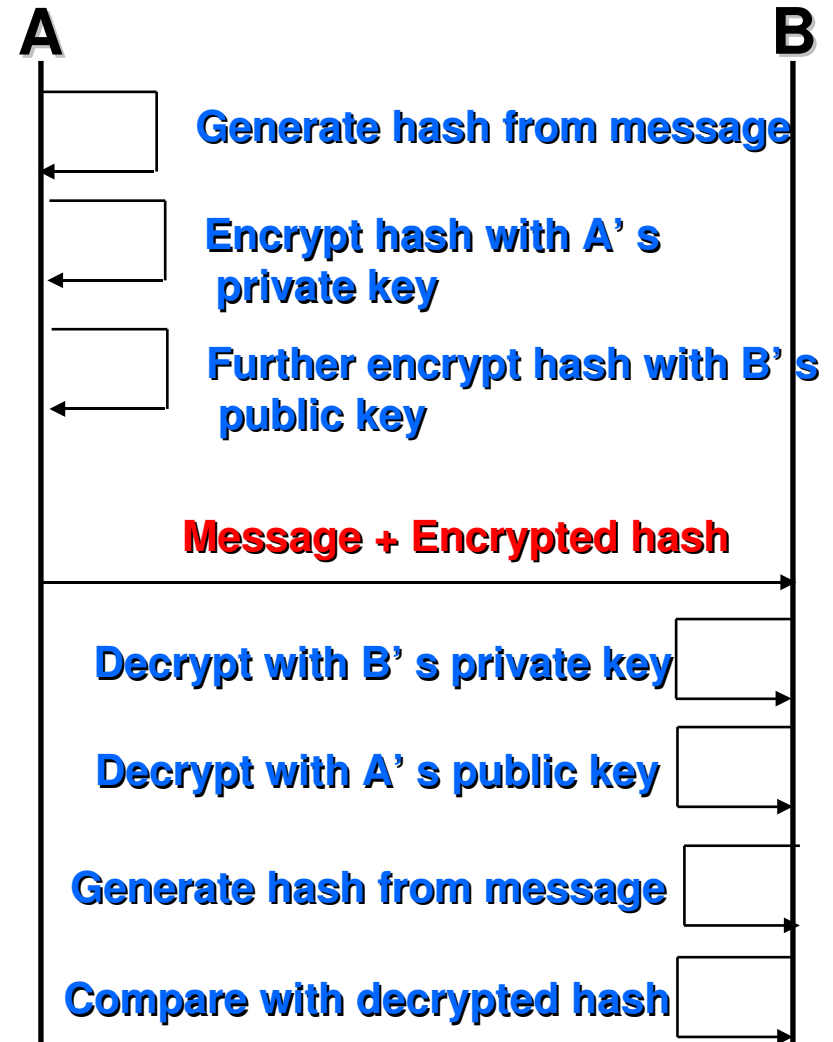
Based on X.509 PKI:  
every Grid transaction is mutually authenticated:

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



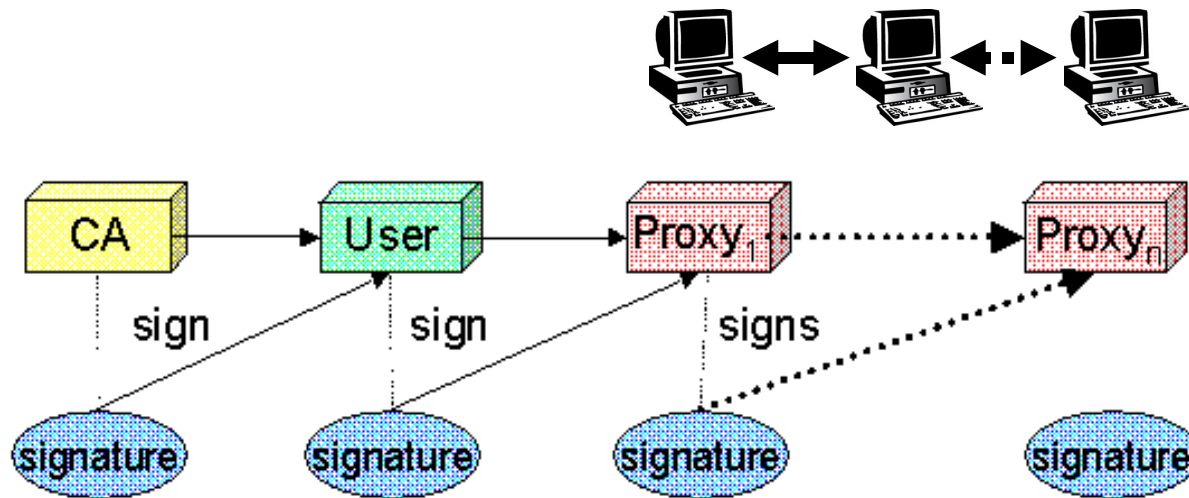
After A and B authenticated each other,  
for A to send a message to B:

- Default: message integrity checking
  - Not private – a test for tampering
- For private communication:
  - Encrypt all the message (not just hash) - Slower





- 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



- Mať bezpečne uložený privátny kľúč – *na USB pamäti*
- Nedať ho k dispozícii nikomu
- Reportovať lokálnej RA/CA ak bol kľúč odcudzený/zneužitý
- Nenechať delegovaný proxy dlhšie než potrebuje Vaša práve spustená úloha

**Ak je Váš certifikát (privátny kľúč) alebo delegovaná služba (proxy) použitý niekým iným, nemôžete dokázať, že ste to neboli Vy.**

## pred VOMS

- Používateľ je autorizovaný ako člen **jedinej** VO
- Všetci členovia VO majú rovnaké práva (oprávnenia)
- Grid-mapfiles sú spravované VO manažérom (sw): mapuje používateľské meno (DN) na lokálne konto
- grid-proxy-init

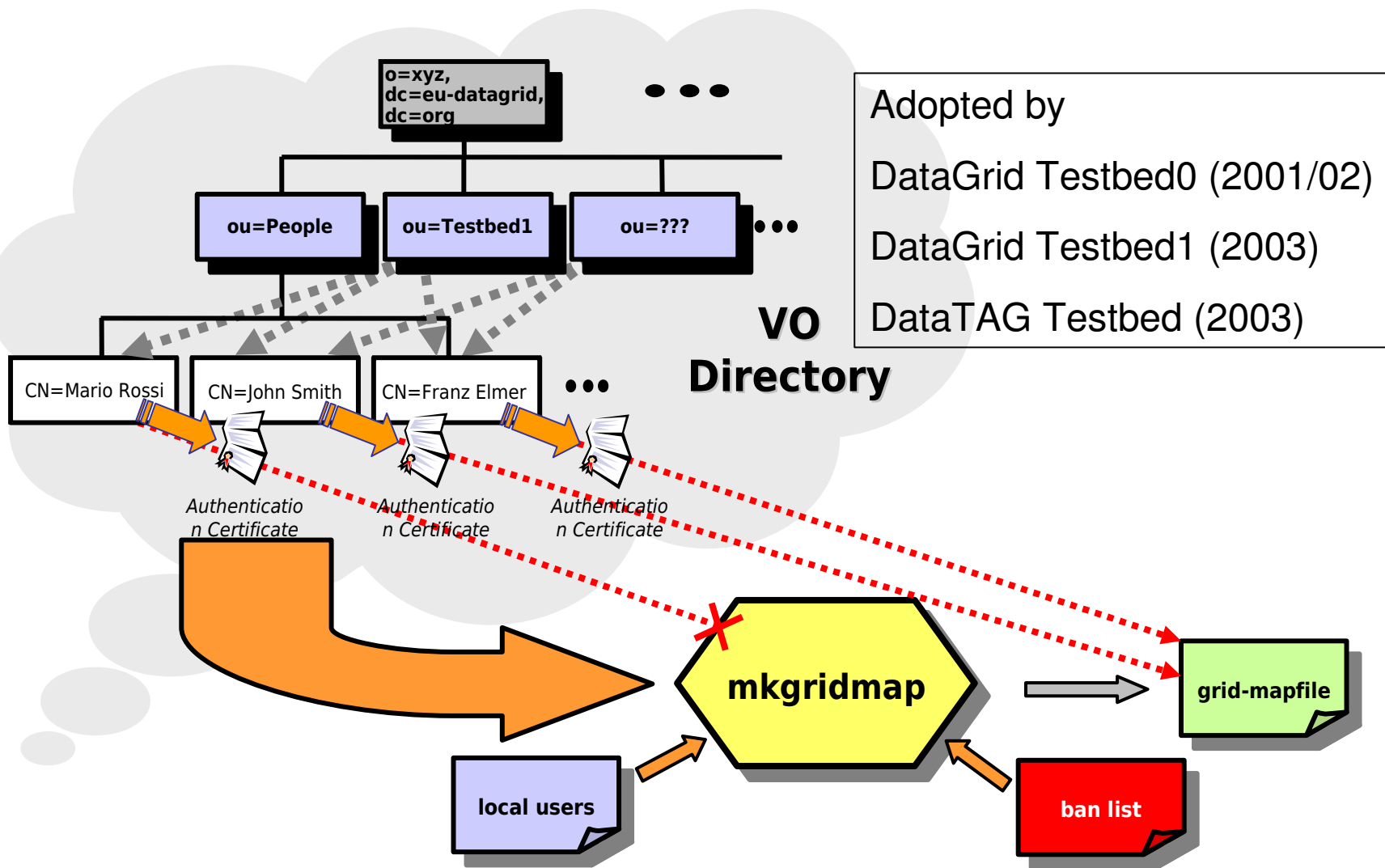
## VOMS

- Používateľ môže byť členom **viacerých** VO
  - Hromadné oprávnenia
- VO môže mať skupiny
  - Rôzne práva pre každú
    - Rôzne skupiny experimentátorov
    - ...
  - Vnorené skupiny
- VO prideluje roly
  - Na zvláštne účely
    - Napr. systémový administrátor
    - Keď predpokladá túto rolu
- Proxy certifikát nesie prídavné atribúty
- voms-proxy-init

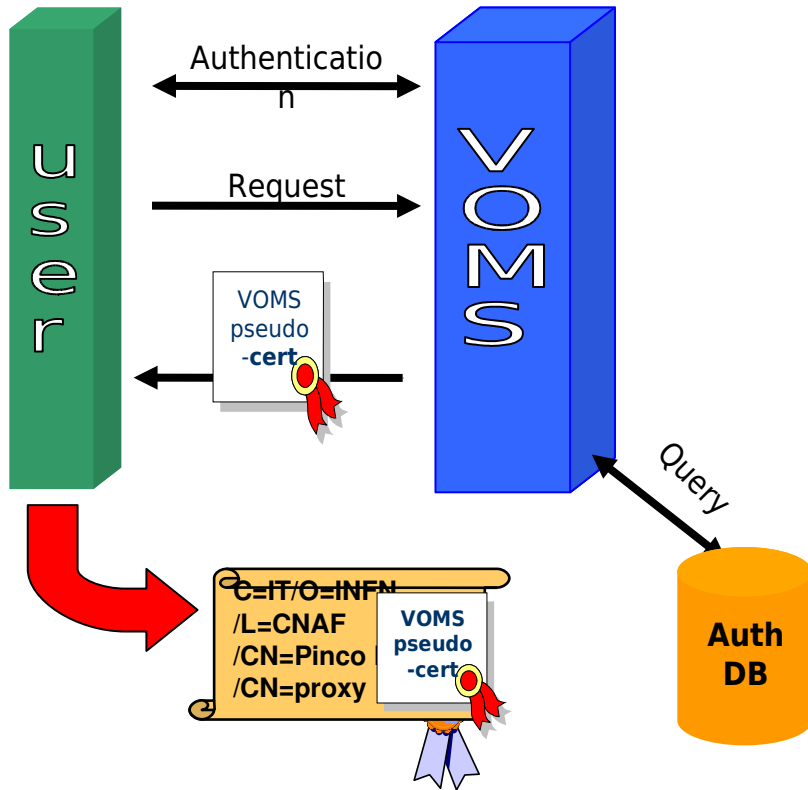
- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- Rekapitulácia

## LDAP server

- Udržiava 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



- **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



- **Vzájomná autentifikácia klient-server**
  - Bezpečný komunikačný kanál pomocou štandardného Globus API
- Klient pošle žiadosť VOMS serveru
- Server **preverí správnosť** žiadosti
- **Server pošle** naspäť vyžiadajú info (podpíše ju) v “**Pseudo-Certifikáte**”
- Klient preverí platnosť prijatej info
- Voliteľne: [Klient zopakuje proces pre iné VOMS’y]
- Klient **vytvorí proxy certifikát** obsahujúci všetku prijatú info v (**nie-kritickom**) rozšírení
- Klient môže pridať ďalšiu autentifikačnú info (kerberos tikety, atď...)



- 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/>

- Ako sa prihlásim do Gridu?
- Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- Rekapitulácia

- **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 **nezakrytovaný** - preto musí byť uložený a dopravovaný **bezpečnými** spôsobmi

- **MyProxy server**

- Udržiava 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 (keď bežný proxy expiruje)
  - Proxy certifikát je automaticky obnovovaný počas celého behu úlohy

## 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: Tue Mar 11 22:37:05 2008
```

grid-proxy-info

grid-proxy-destroy

## 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: Tue Mar 11 22:43:03 2008
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.
```

Poznámka: na MyProxy v LCG (alebo gLite pod GT2) sa ukladá len štandardný proxy; nedá sa tam vložiť rozšírený VOMS proxy.

GT4 implementácia používa prepínač „-o“ nasledovaný menom VO

## 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

## 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 Tue Mar 11 22:59:27 2008
```

**voms-proxy-info**

**voms-proxy-destroy**

```
[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-\*



**[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 WMPProxy:

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

with the delegation identifier: `mojprvy`

=====

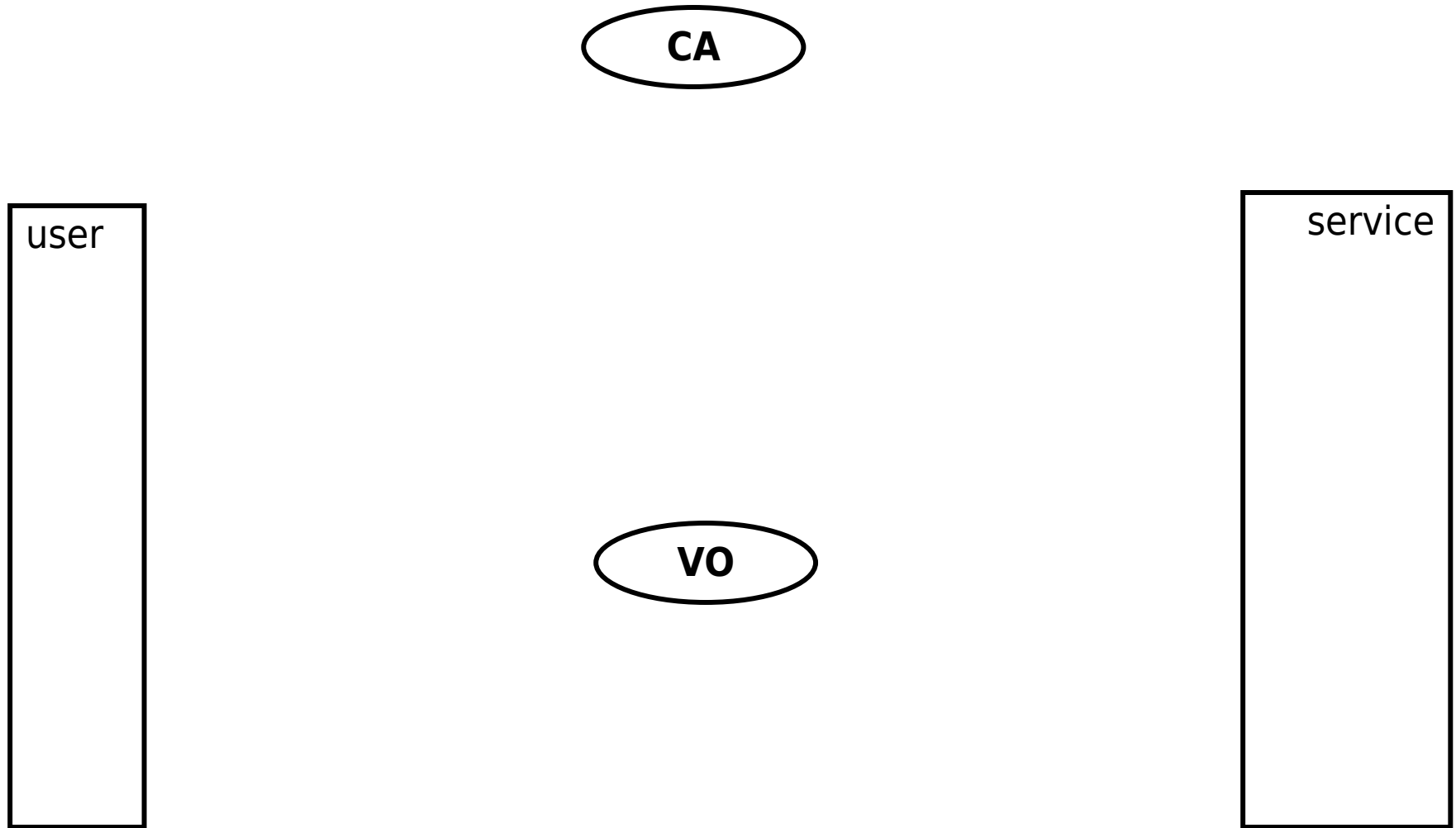
**Alebo sa dá delegovať až pri spustení úlohy (jobu).**

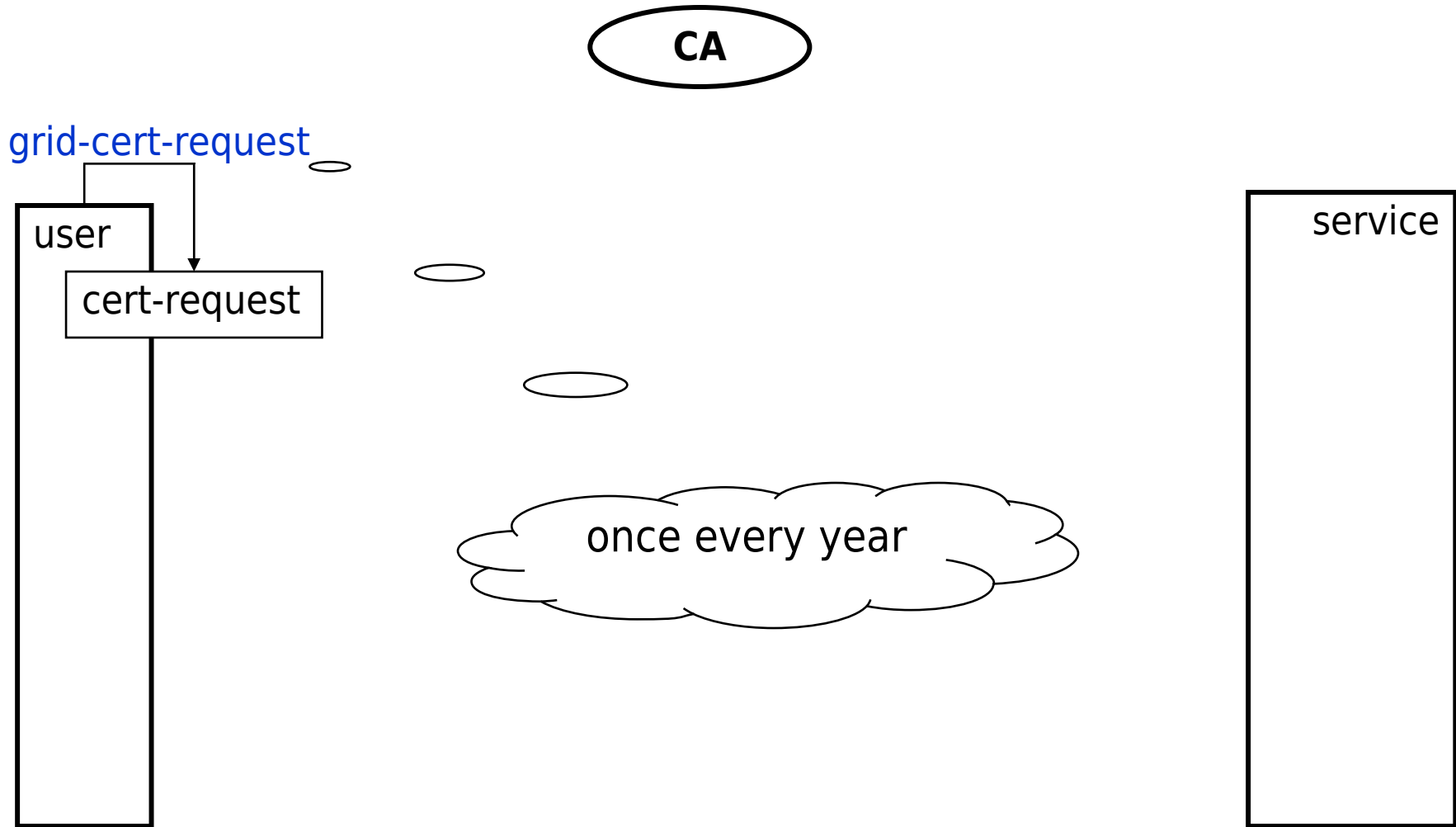
**Informácia o stave delegáta (proxy) sa v gLite 3.1 dá zistiť príkazom:**

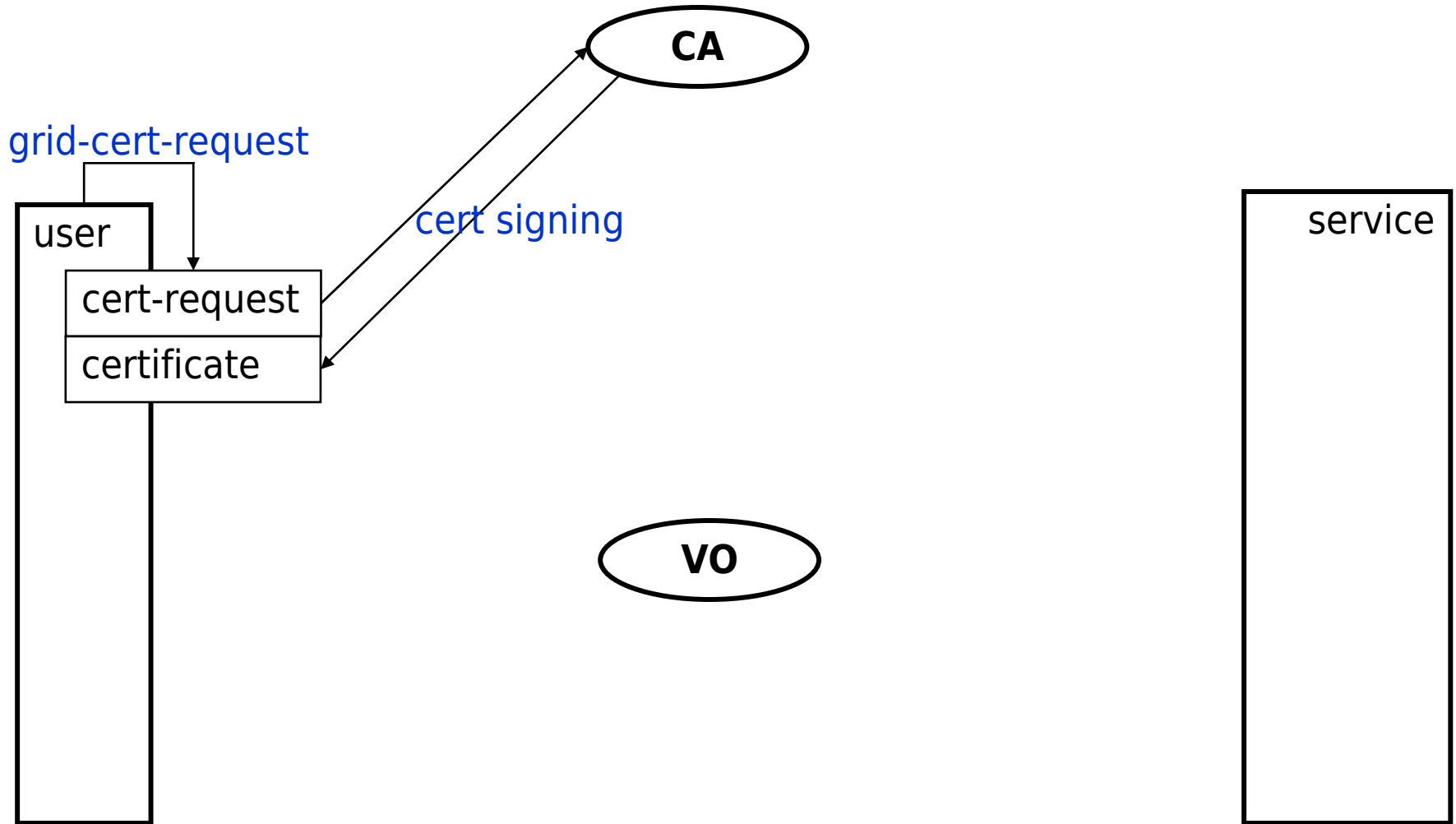
**glite-wms-job-info -d mojprvy**

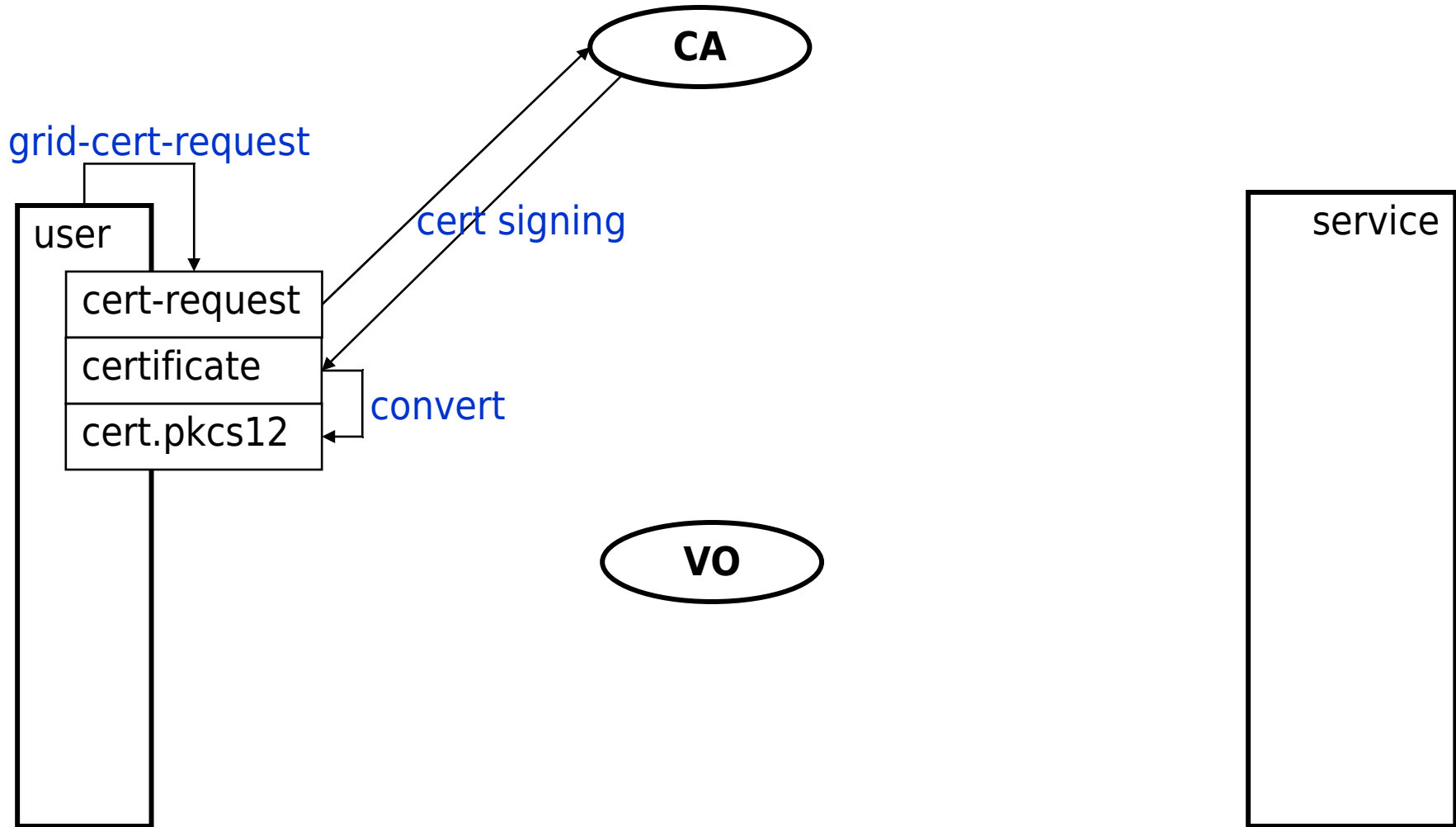
**Ako sa dá delegát zmazať? Asi len delegovaním 1-hodinového proxy.**

- Ako sa prihlásim do Gridu?
  - Certifikáty - Autentifikácia
- GSI
  - Autorizácia
  - Delegované certifikáty
- **Rekapitulácia (A walk-through)**









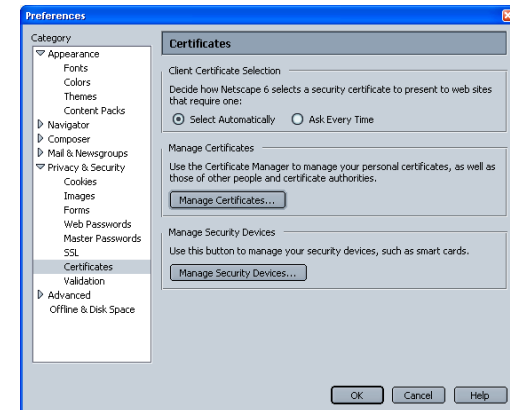
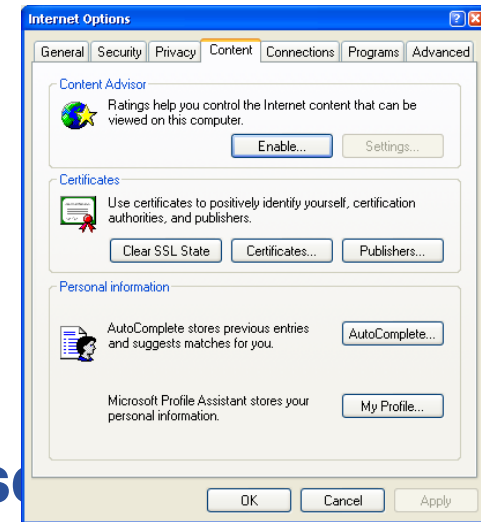
- Your certificate must be in **PKCS#12** format

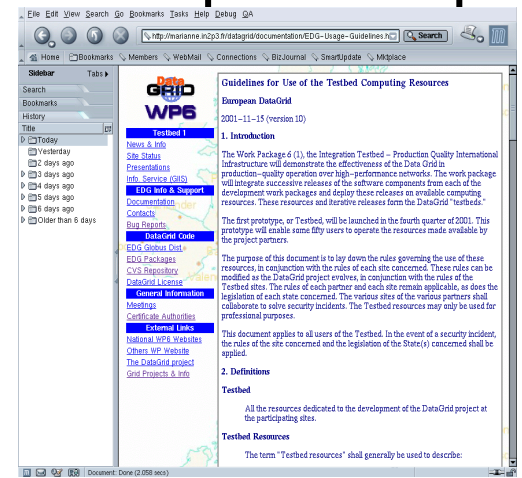
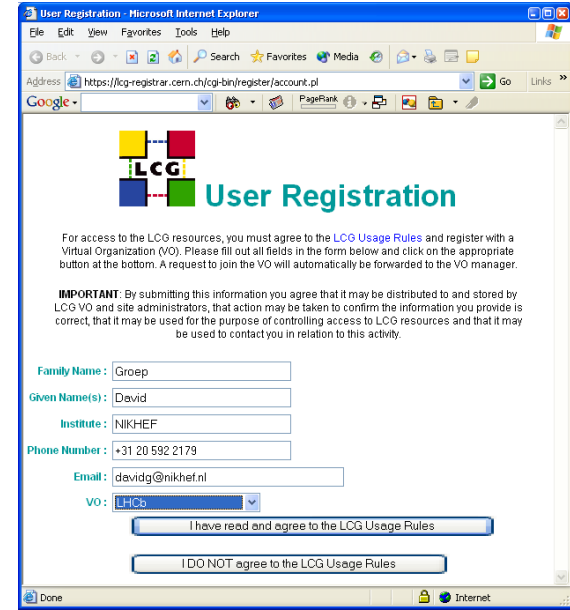
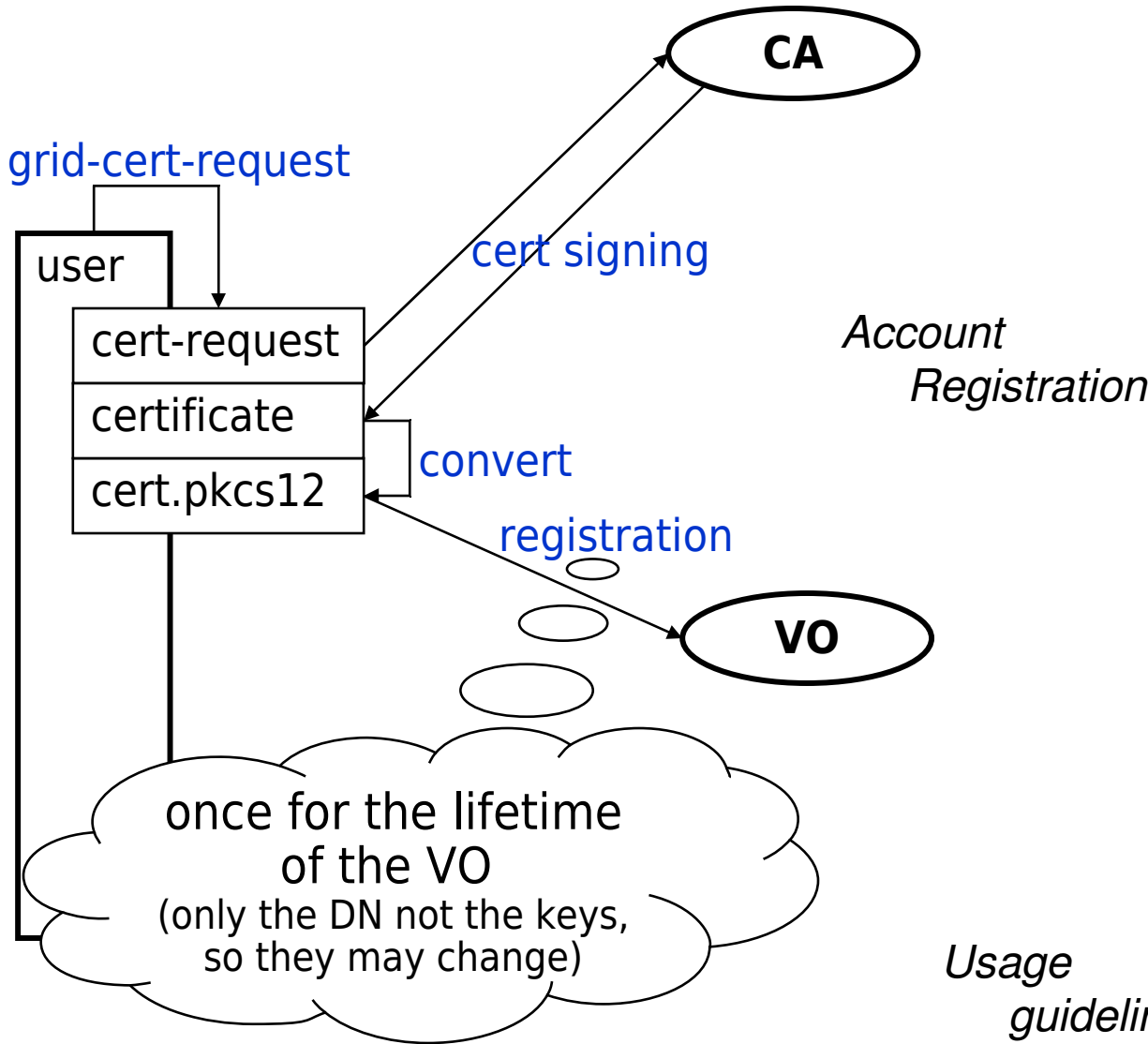
```
openssl pkcs12 -export \
-in ~/.globus/usercert.pem \
-inkey ~/.globus/userkey.pem \
-out user.p12 \
-name 'Joe Smith'
```

- Use the “certificate store” of your browser

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

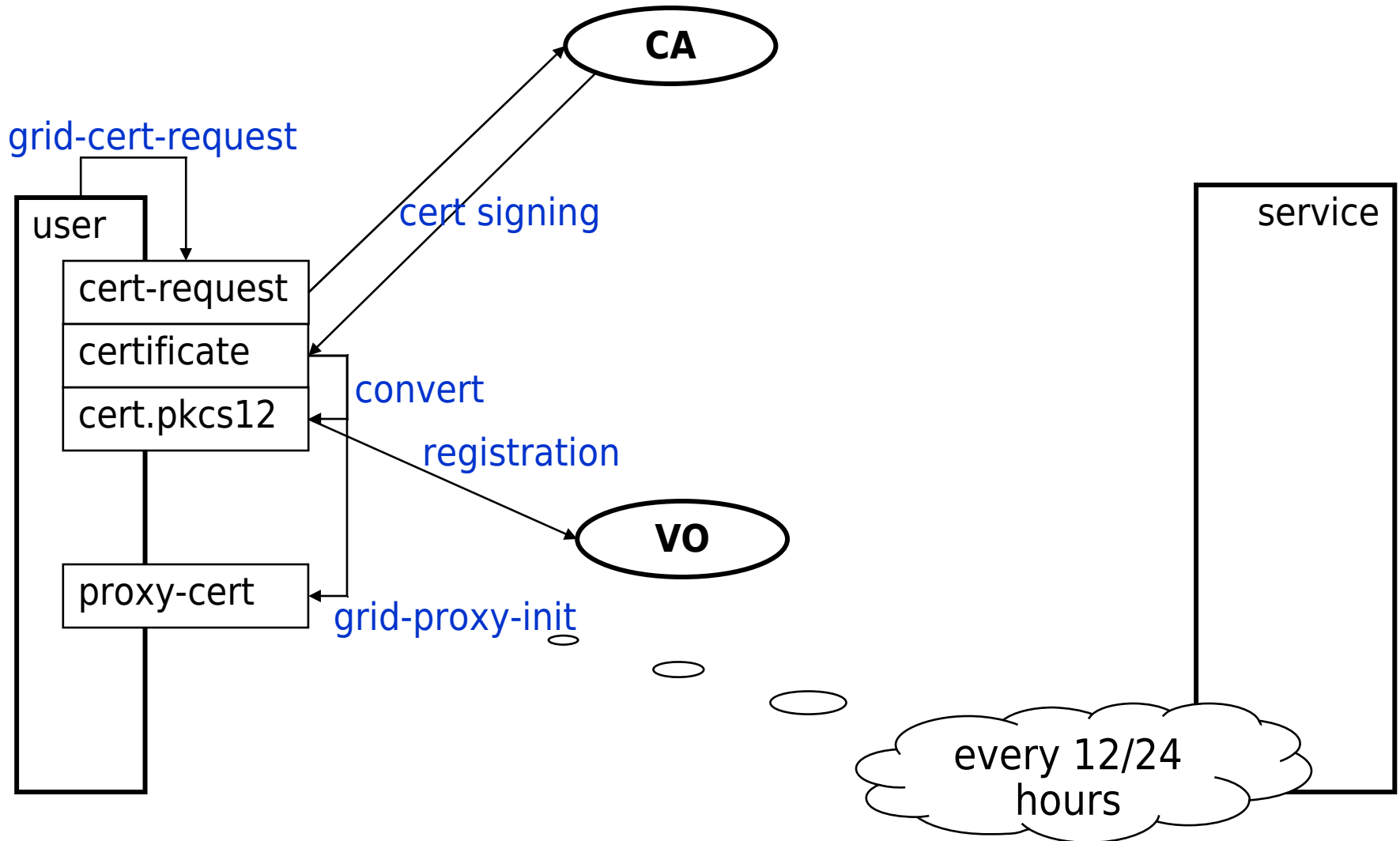
- And **SET THE MASTER PASSWORD**

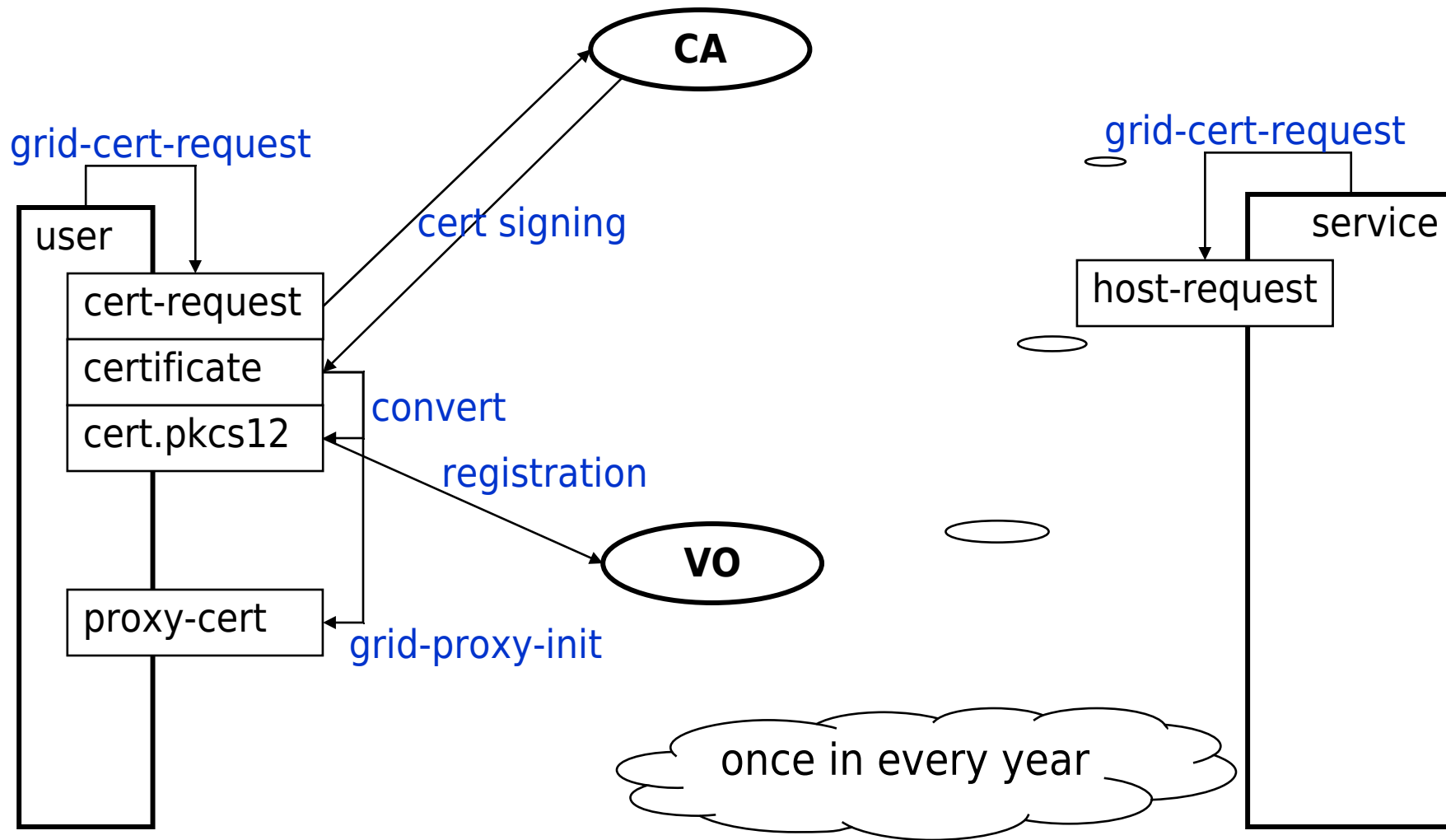


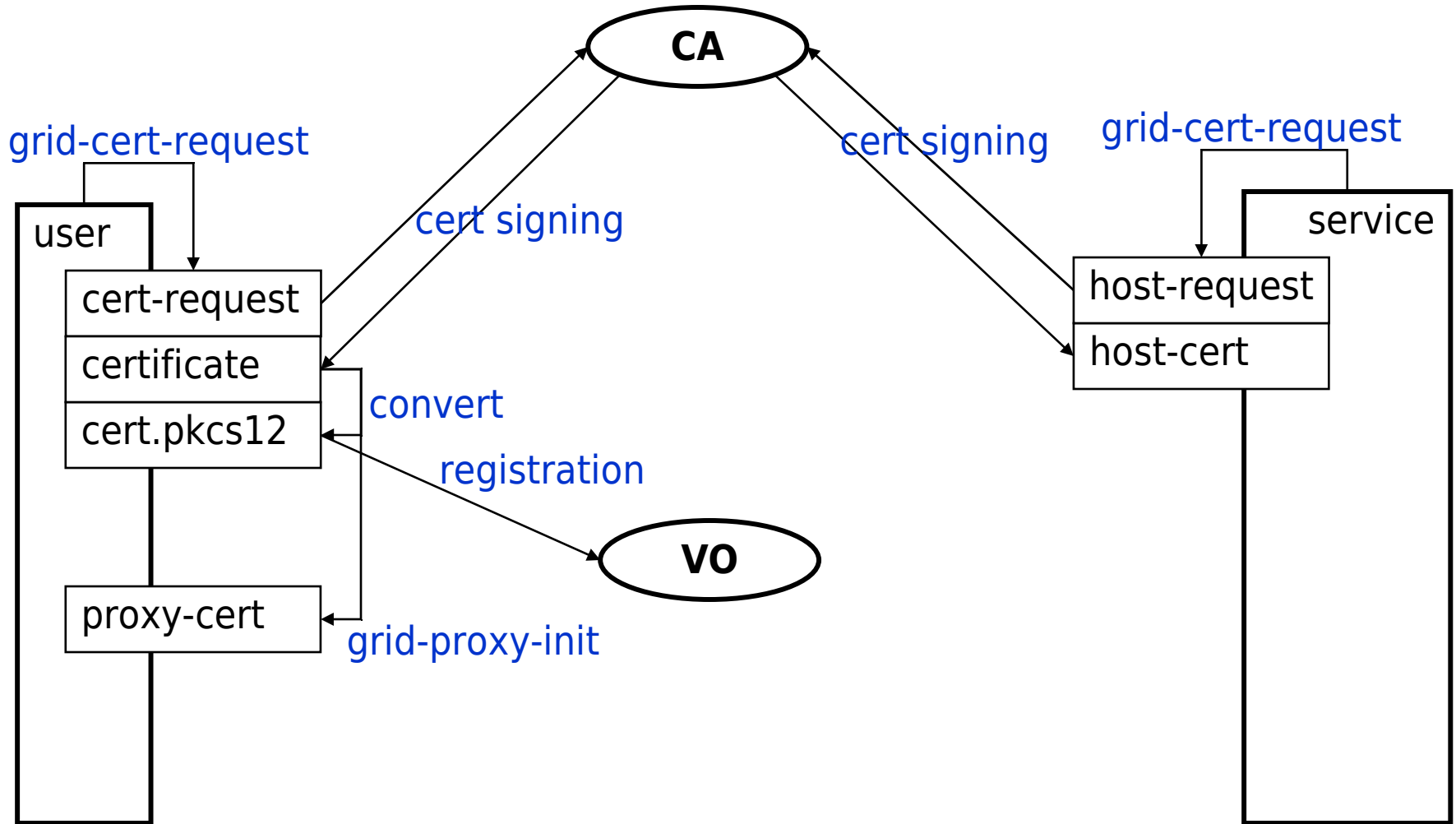


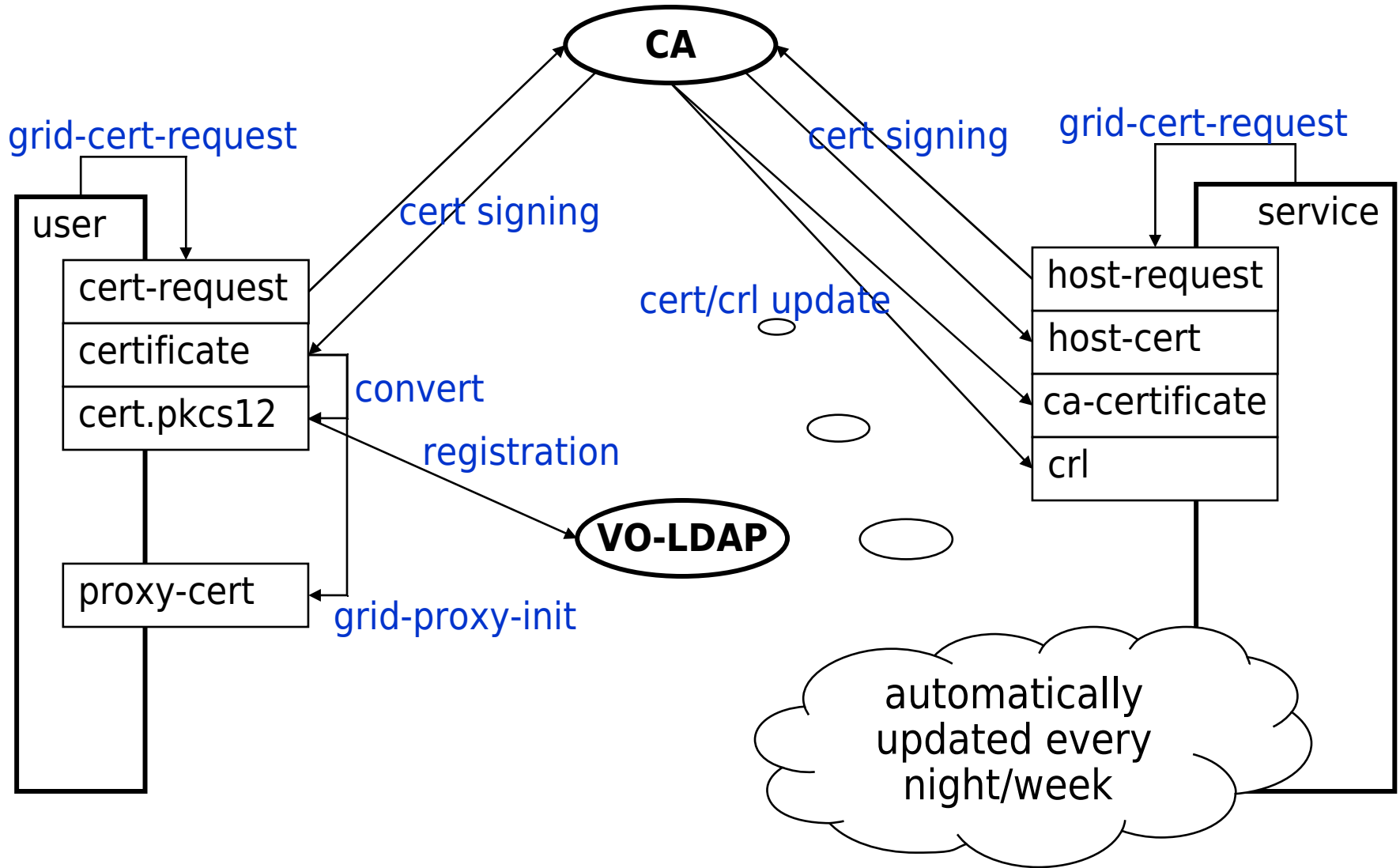
Usage guidelines

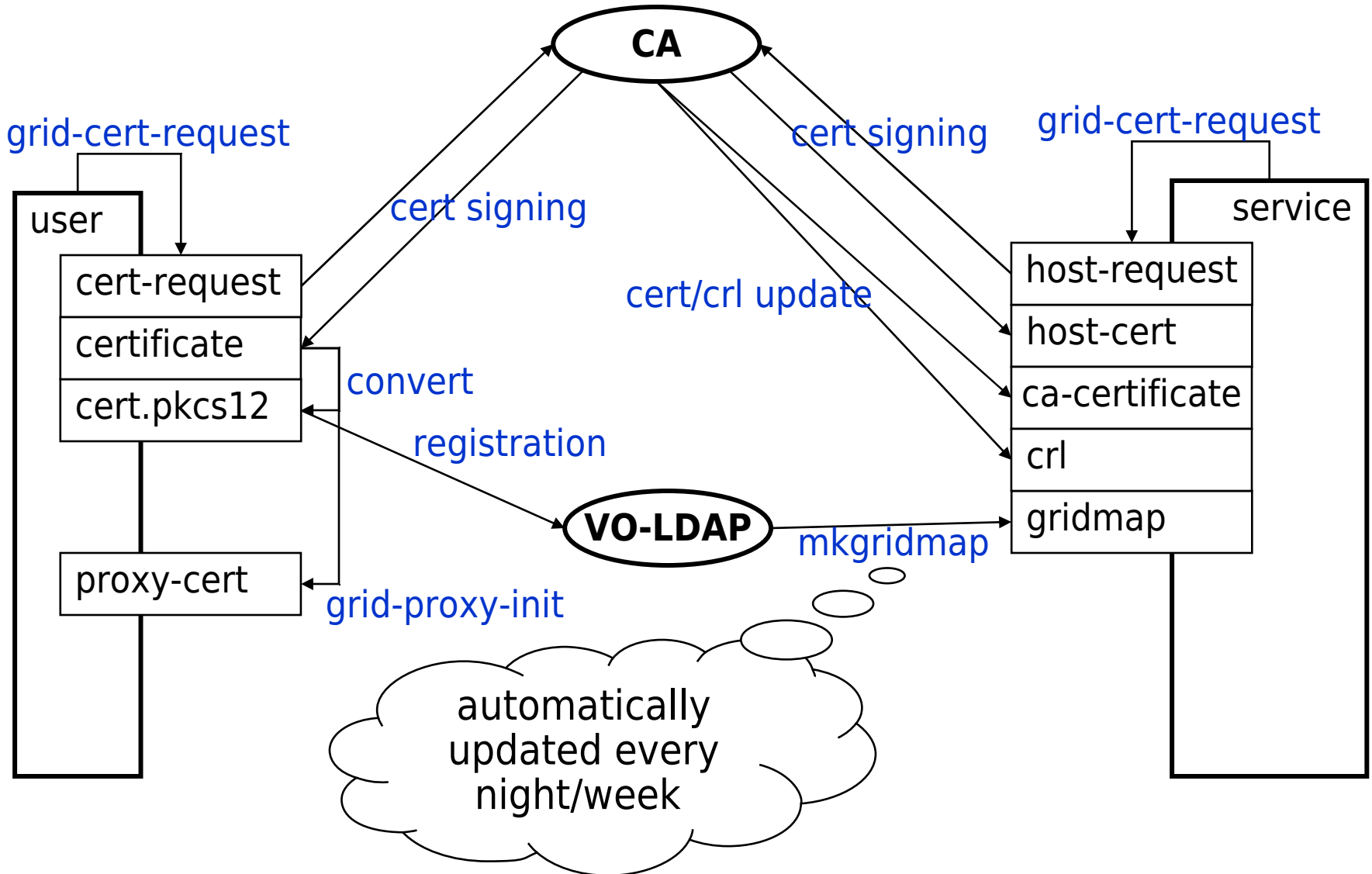


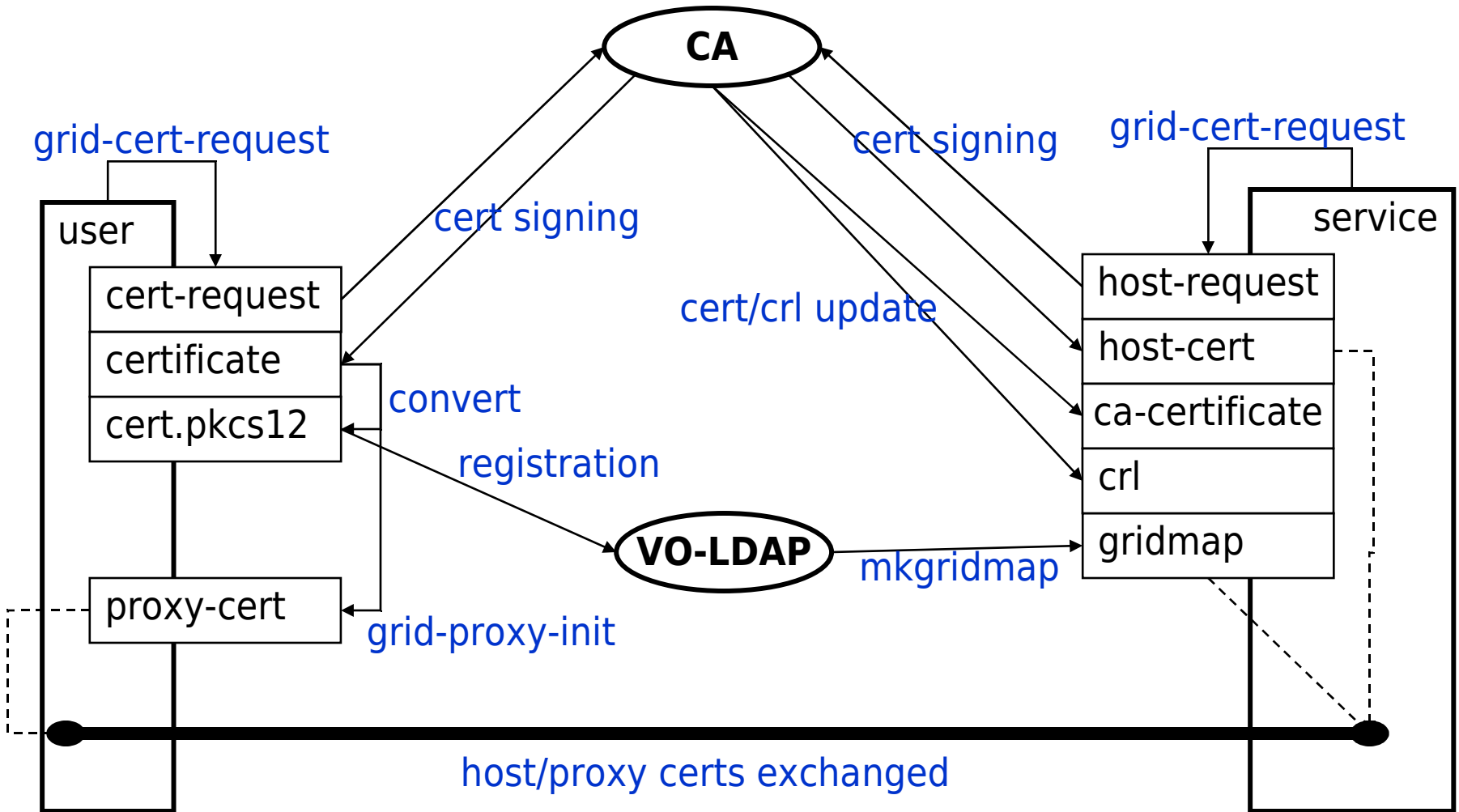












**Ďakujem za pozornosť**

**egee.ui{AT}sav.sk**

**<http://www.ui.sav.sk/egee>**

*Miroslav Dobrucký*

*Ústav informatiky*

*Slovenská akadémia vied*

*Bratislava*