Bezpečnosť v EGEE – autentifikácia a autorizácia
(Grid security infrastructure)

Miroslav Dobrucký
Ústav informatiky
Slovenská akadémia vied
Bratislava

www.eu-egee.org

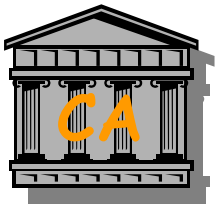
Information Society

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 (proxy certifikáty)
- **Dva základné koncepty:**
- **Autentifikácia: Kto som?**
  - Ekvivalent ku OP, cestovnému pasu, ...
  - Certifikáty
- **Autorizácia: Čo mám dovolené robiť?**
  - Určené povolenia, povinnosti, atď.
  - Virtuálne organizácie

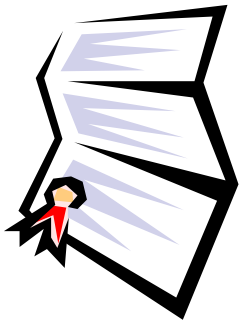
Zúčastnené entity

Certifikačná Autorita

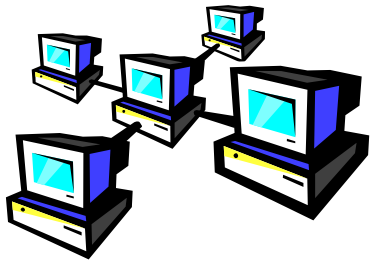


Používateľ

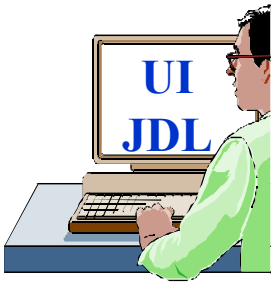
Privátny kľúč
Verejný kľúč
Certifikát



Zdroje
(strediská ponúkajúce služby)



Autentifikácia a Autorizácia



Používateľ

CA

1

Autentifikácia

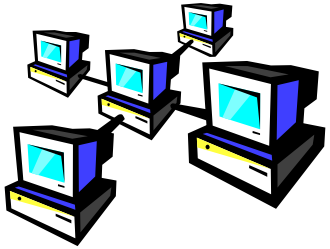
Účty

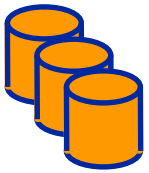
2

VO

3

Autorizácia





Služba

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 znova zadávať heslo (pass phrase) zakryptovaného privátneho kľúča

Ako vytvorím pár kľúč/žiadosť

grid-cert-request príkaz

```
[miro@cluster2 miro]$ 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:************
```

Ako získam certifikát

Doručím žiadosť relevantnej dôveryhodnej CA

```
[miro@cluster2 miro]$ 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.

RA následne doručí jej/jeho žiadosť certifikačnej autorite (CA), ktorá žiadosť podpíše a pošle naspäť ako certifikát. Obvykle má platnosť 1 rok a pred vypršaním platnosti môže byť využitý na podpísanie novej žiadosti, čo znamená, že sa už potom žiadateľ nemusí chodiť osobne preukazovať.

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

Nainštalovanie certifikátu

na UI stroj do adresára ~/.globus

```
[miro@cluster2 .globus]$ ls -l
-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
```

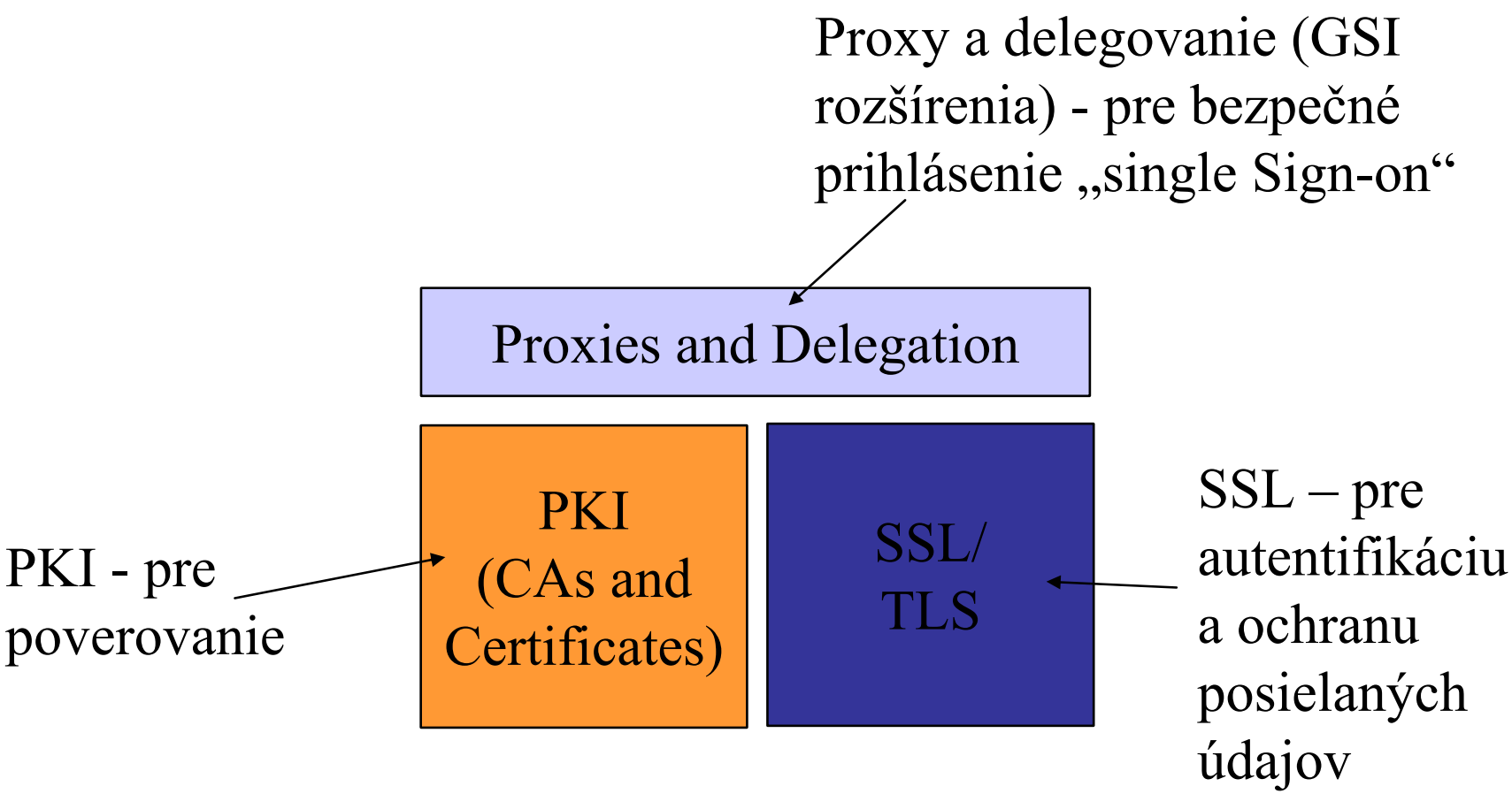
Revokácia, CRL

- **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

GSI - prehľad



Based on Slide from Globus Tutorial

Delegované certifikáty

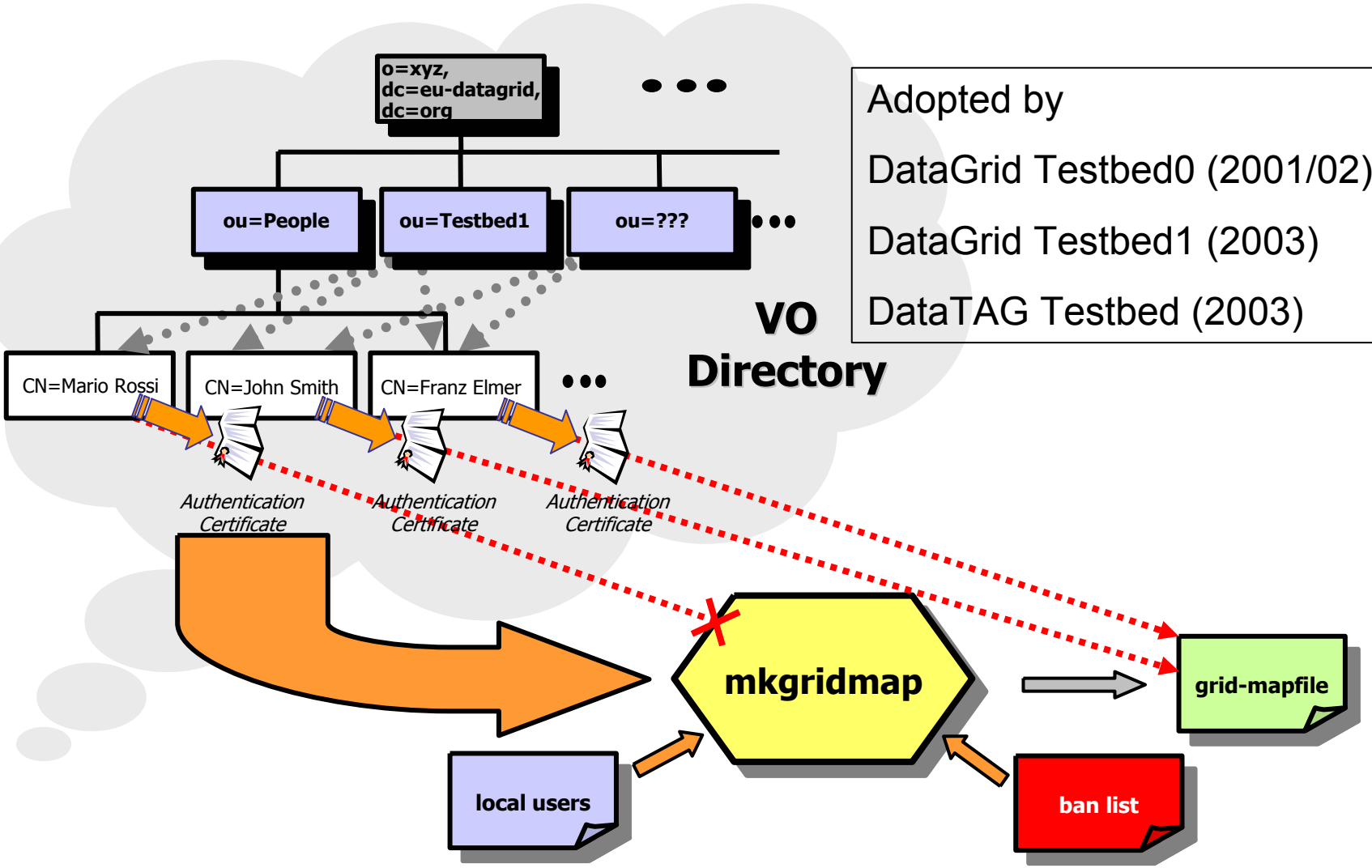
- **Proxy certifikát**
  - Krátko-dobý (12 hodín), s obmedzenými právomocami, odvodený z dlhodobého (1 rok) X.509 certifikátu
  - Podpísaný používateľovým certifikátom alebo iným proxy
  - Umožňuje procesu pôsobiť v mene používateľa
  - Je nezakryptovaný - preto musí byť uložený a dopravovaný bezpečnými 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

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)

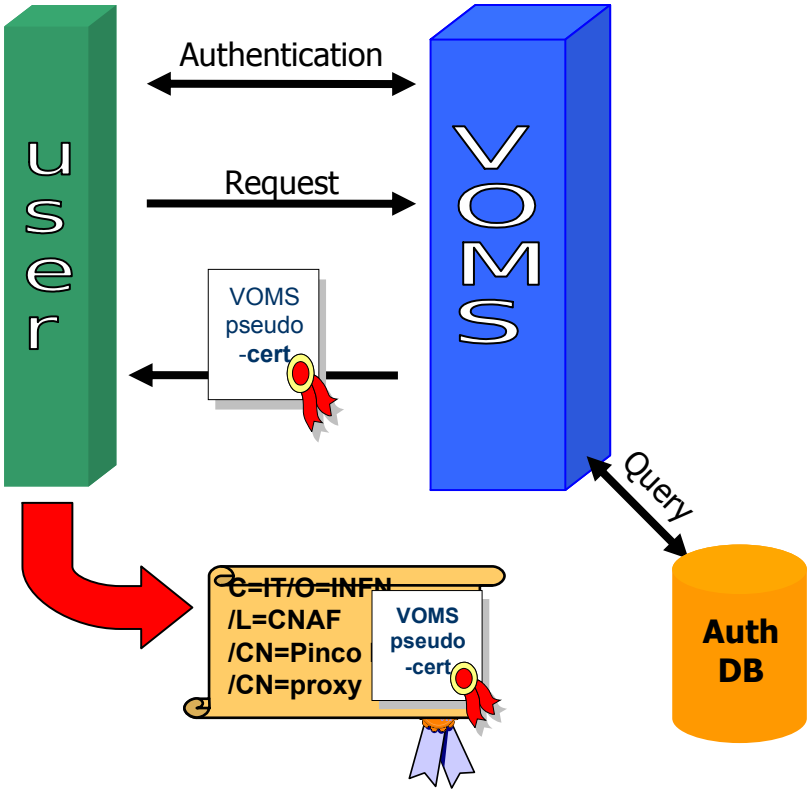
DataGrid Testbed1 (2003)

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 and DataTAG projektov

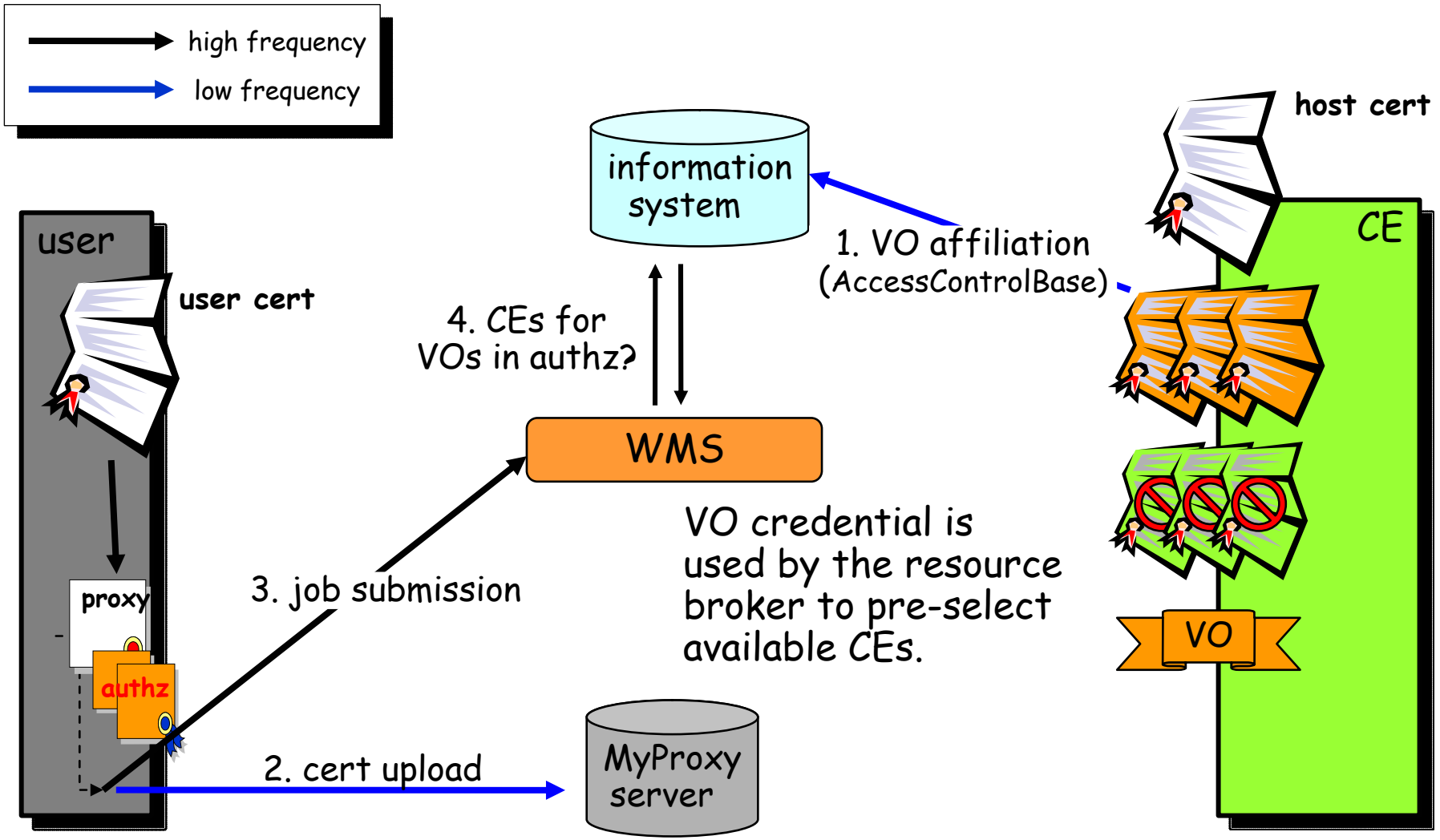
VOMS



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

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

Spúšťanie úloh s VOMS



Ďakujem za pozornosť

egee.ui@sav.sk

Miroslav Dobrucký

Ústav informatiky

Slovenská akadémia vied

Bratislava

www.eu-egee.org