Biztonság a gLite-ban

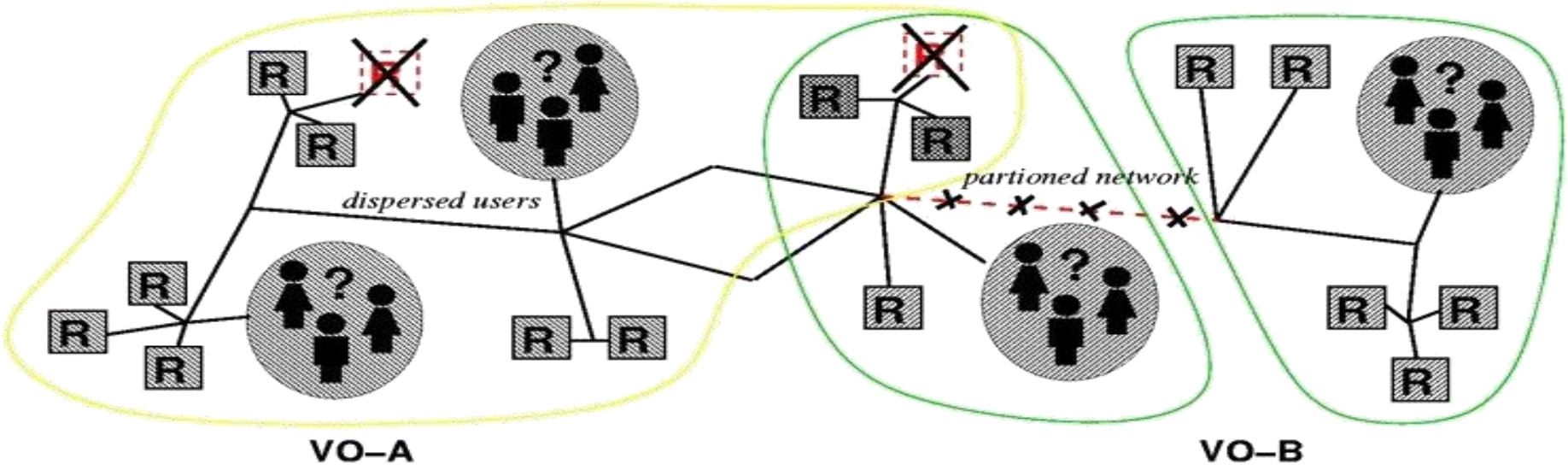
Mi a Grid biztonság?

A Grid probléma lehetővé tenni „koordinált erőforrás megosztást és probléma megoldást dinamikus több szervezeti egységből álló virtuális szervezetekben.”

”A Grid anatómiája”
Ian Foster, Carl Kesselman, Steven Tuecke

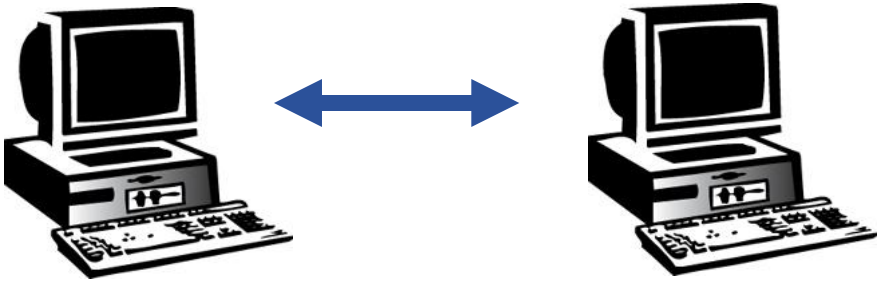
- A Grid-nek lehetővé kell tenni a VO koncepciót
- Milyen biztonság kell VO szinten?

A virtuális szervezet koncepciója



- VO minden alkalmazás, terhelés vagy közösség száméra
- Egy bizonyos erőforrás rész kijelölése egy vagy egy csoport felhasználónak
- Dinamikus rész kifejezése …

Problémák hálózati szinten



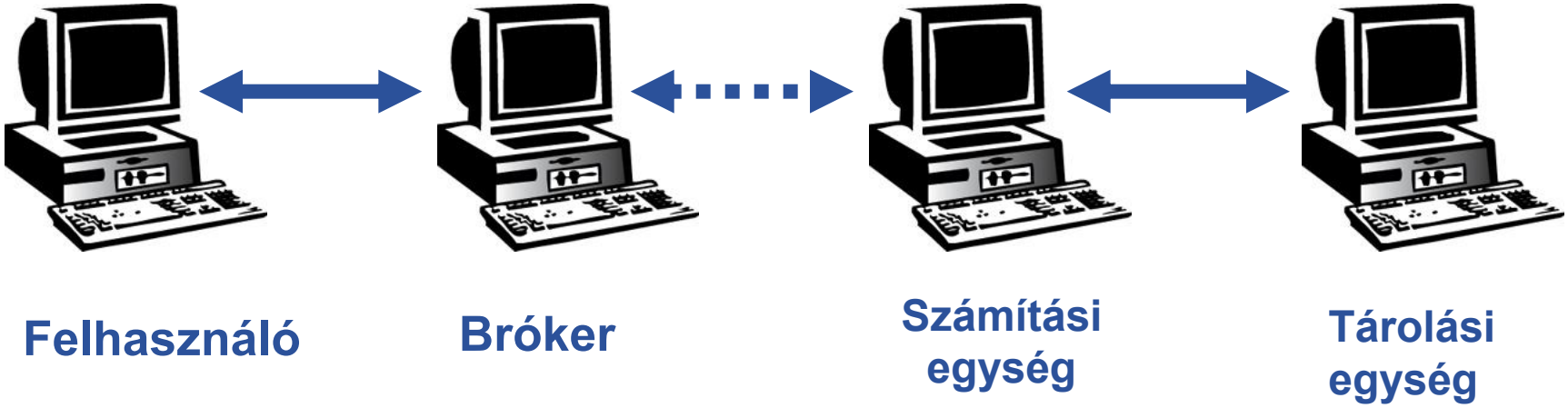
Felhasználó

Grid szolgáltatás

A Grid résztvevői az Interneten kommunikálnak

- **Hogyan lehet a kommunikációs végpontokat azonosítani?**
  - Authentication
- **Hogyan lehet egy biztonságos csatornát felépíteni két végpont között?**
  - Titkosítás
  - Letagadhatatlanság
  - Integritás

Problémák VO szinten



- **Melyik hálózati entitás tartozik hozzá a VO-hoz? Melyik nem?**
- **Mit szabad egy VO tagnak tenni?**
  - Hozzáférés engedélyezés
- **Hogyan tud egy szolgáltatás a felhasználó nevében fellépni?**
  - Hogyan tud a bróker hozzáférni a „felhasználó site-jához”?
  - Hogyan tud egy bróker által indított feladat hozzáférni a felhasználó privát adataihoz?

Biztonsági infrastruktúra

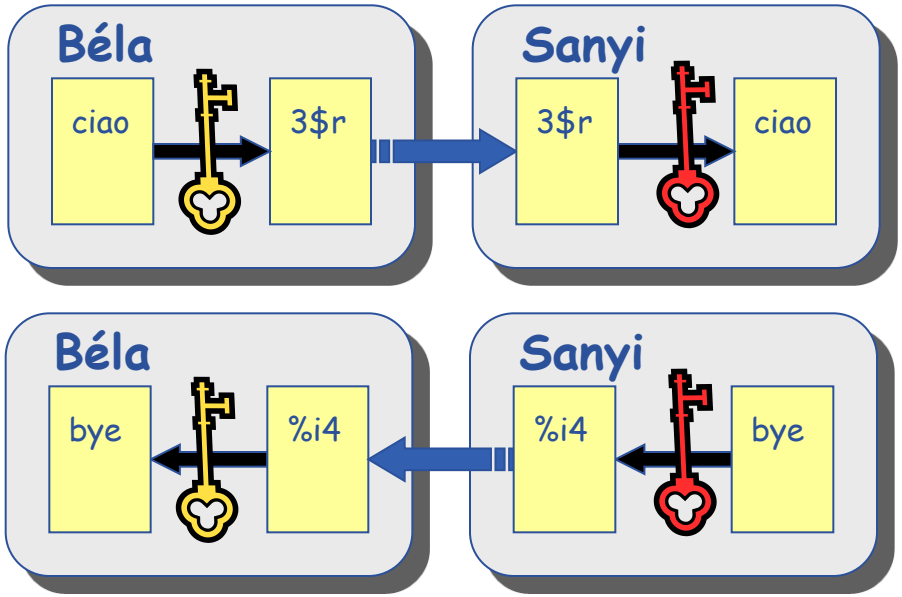
Biztonság hálózati szinten:

Nyilvános kulcsú infrastuktúra (PKI)

A nyilvános kulcsú infrastruktúra alapjai

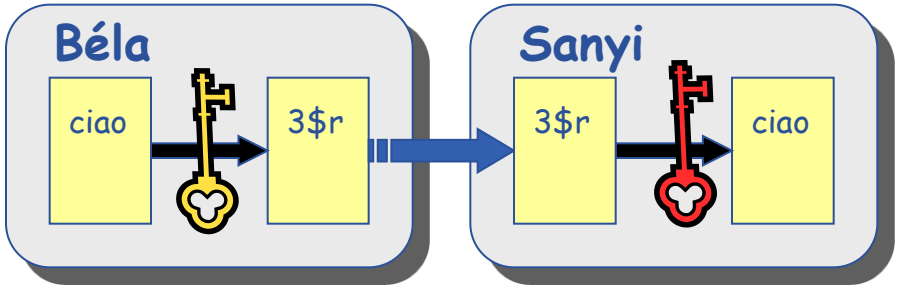
- **Minden hálózati entitás (felhasználó/gép/software) rendelkezik két kulccsal: egy *privát* és *nyilvános* kulccsal**
  - Lehetetlen megszerezni a privát kulcsot a nyilvánosból
  - Egy kulcs által titkosított üzenetet csak a **másik** kulccsal lehet visszafejteni.

- **Koncepció:**
  - A nyilvános kulcsokat kicseréljük
  - A küldő a fogadó nyilvános kulcsával titkosít
  - A fogadó a saját titkos kulcsával fejti vissza az üzenetet



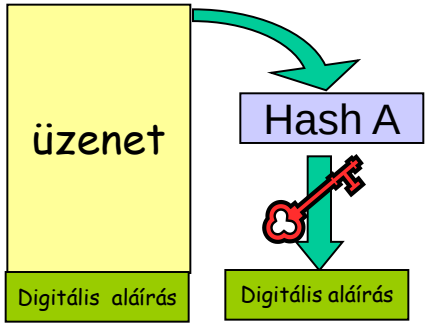
PKI működése

- **Titkosítás**
  - Titkosítás a fogadó nyilvános kulcsával
  - Csak egy fogadó tudja megfejteni az üzenetet



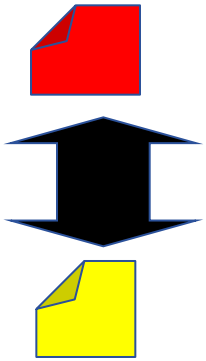
- **Letagadhatatlanság**
  - **Naiv megközelítés:** az üzenet titkosítása a küldő privát kulcsával
    - Hosszú üzeneteknél túl költséges
  - **Megoldás:**
    - Az üzenet ellenőrző összegének előállítása
    - Az ellenőrző összeg titkosítása a küldő privát kulcsával
    - Titkosított ellenőrző összeg hozzáfűzése az üzenthez

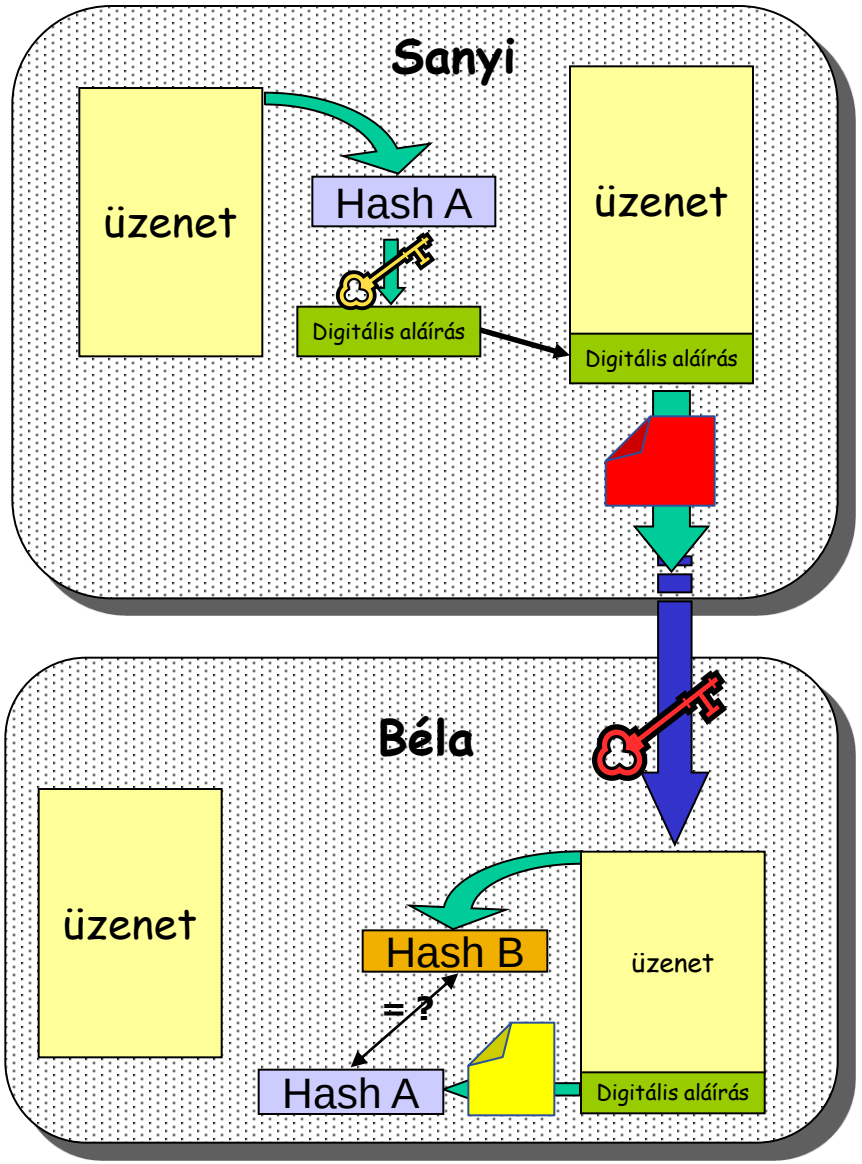
      → **Digitális aláírás**
  - Járulékos haszon: Integritás



PKI működés közben

Kölcsönös hitelesítés és nyilvános kulcscsere: SSL protokoll

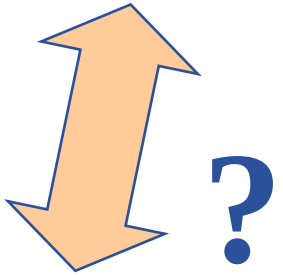




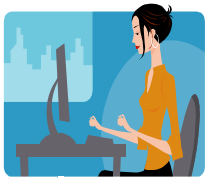
Entitás identitás

- Mivel csak nekem van hozzáférésem a privát kulcsomhoz biztos lehetsz benne, hogy én írtam alá a dokumentumot
- De honnan tudod, hogy a jó nyilvános kulcsom van nálad?





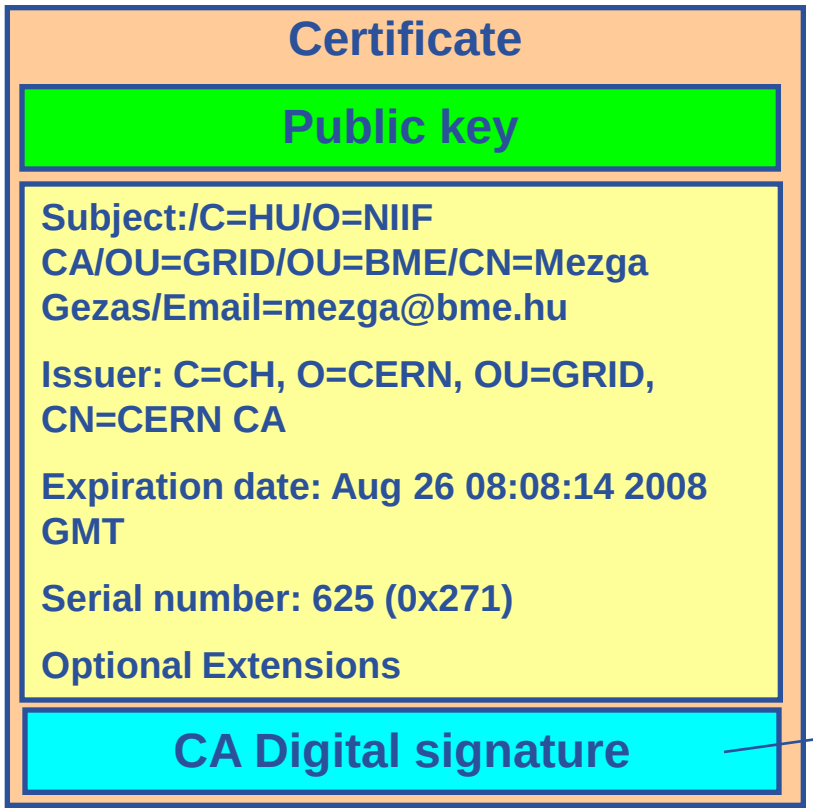


Nyilvános és titkos kulcsok

- A nyilvános kulcsot egy tanúsítvány tartalmazza
- A tanúsítványokat egy mindenki által megbízott harmadik fél készíti (CA)

- A titkos kulcsot egy jelszóval védett fájl tartalmazza
- A privát kulcsot a felhasználó hozza létre



1. A nyilvános kulcs és meta információk ellenőrző összege,
2. Titkosítva a CA titkos kulcsával

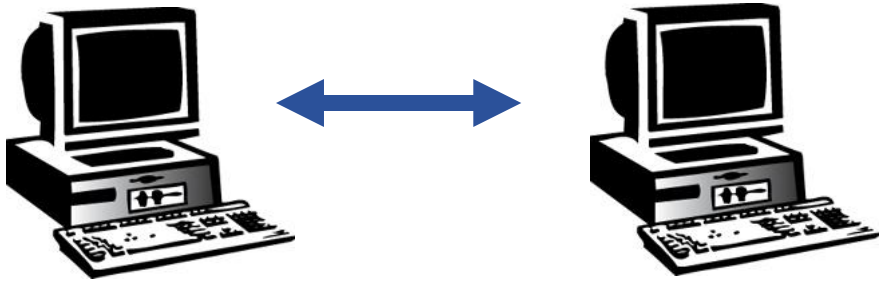
Privát kulcs és tanúsítvány

- **A titkos kulcs és a tanúsítvány helyei:**
  - Böngészőben tárolva
  - Fájlokban tárolva különböző formátumokban (PEM, P12, …)

```
[test@glite-tutor test]$ ls -l .globus/
total 8
-rw-r--r--   1 test   users   1761 Oct 25  2006 usercert.pem
-r--------   1 test   users   951  Oct 24  2006 userkey.pem
```

Ha valaki használja a te tanúsítványodat, akkor nem lehet letagadni, hogy nem te voltál.

Problémák hálózati szinten



Felhasználó Grid szolgáltatás

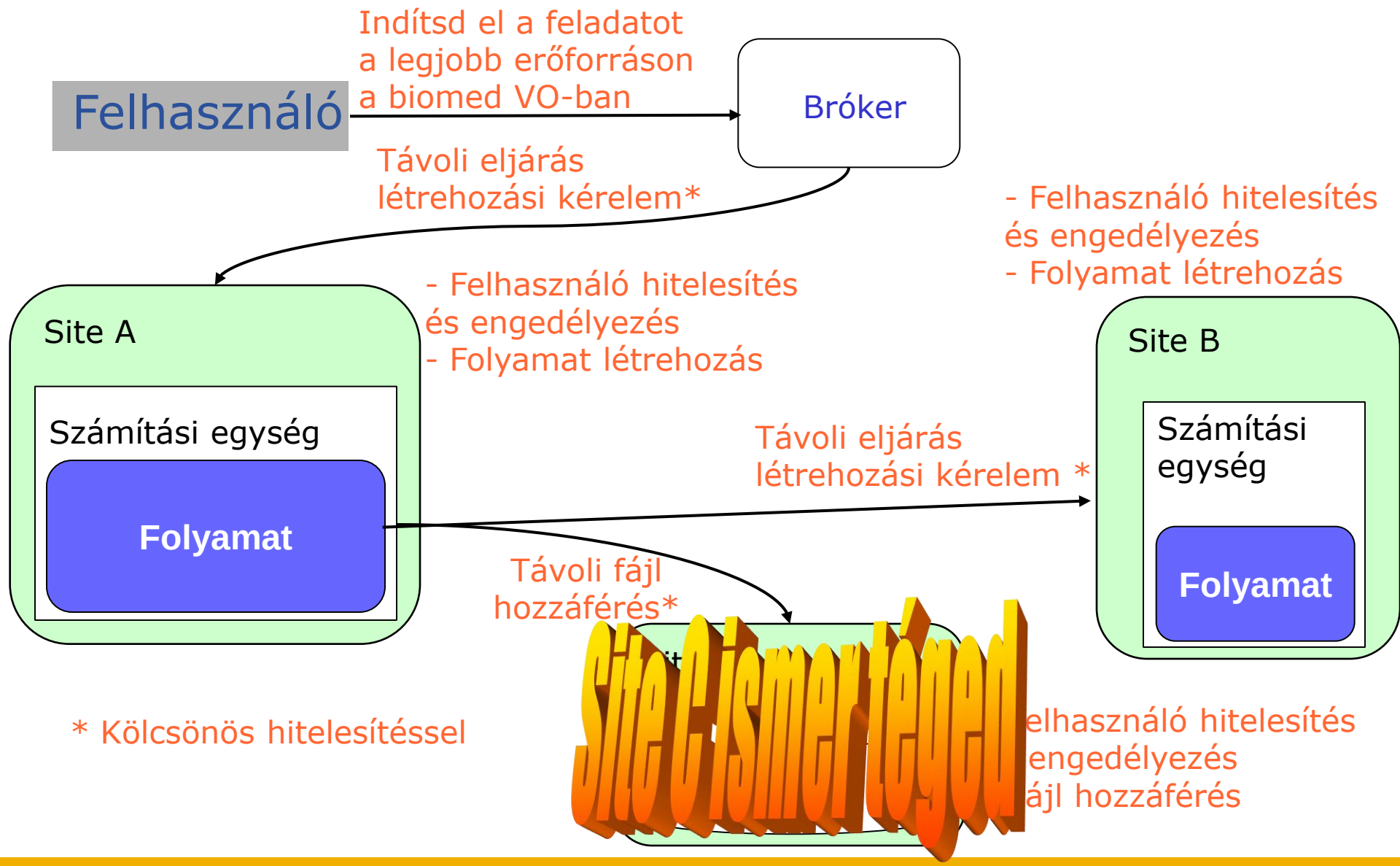
A VO tagjai az Interneten kommunikálnak

- **Hogyan lehet a kommunikációs végpontokat azonosítani?** ✓
  - Hitelesítés
- **Hogyan lehet egy biztonságos csatornát létrehozni a két fél között?**
  - Titkosítás ✓
  - Letagadhatatlanság ✓
  - Integritás ✓

Biztonsági infrastruktúra/2

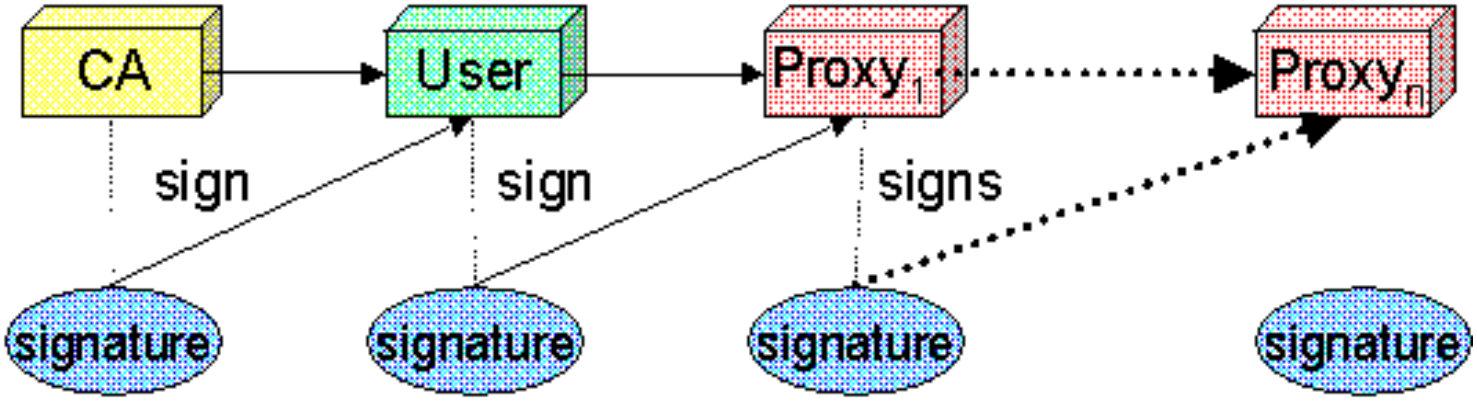
Biztonság VO szinten

Grid szolgáltatások ~ ágensek: Delegáció szükségessége

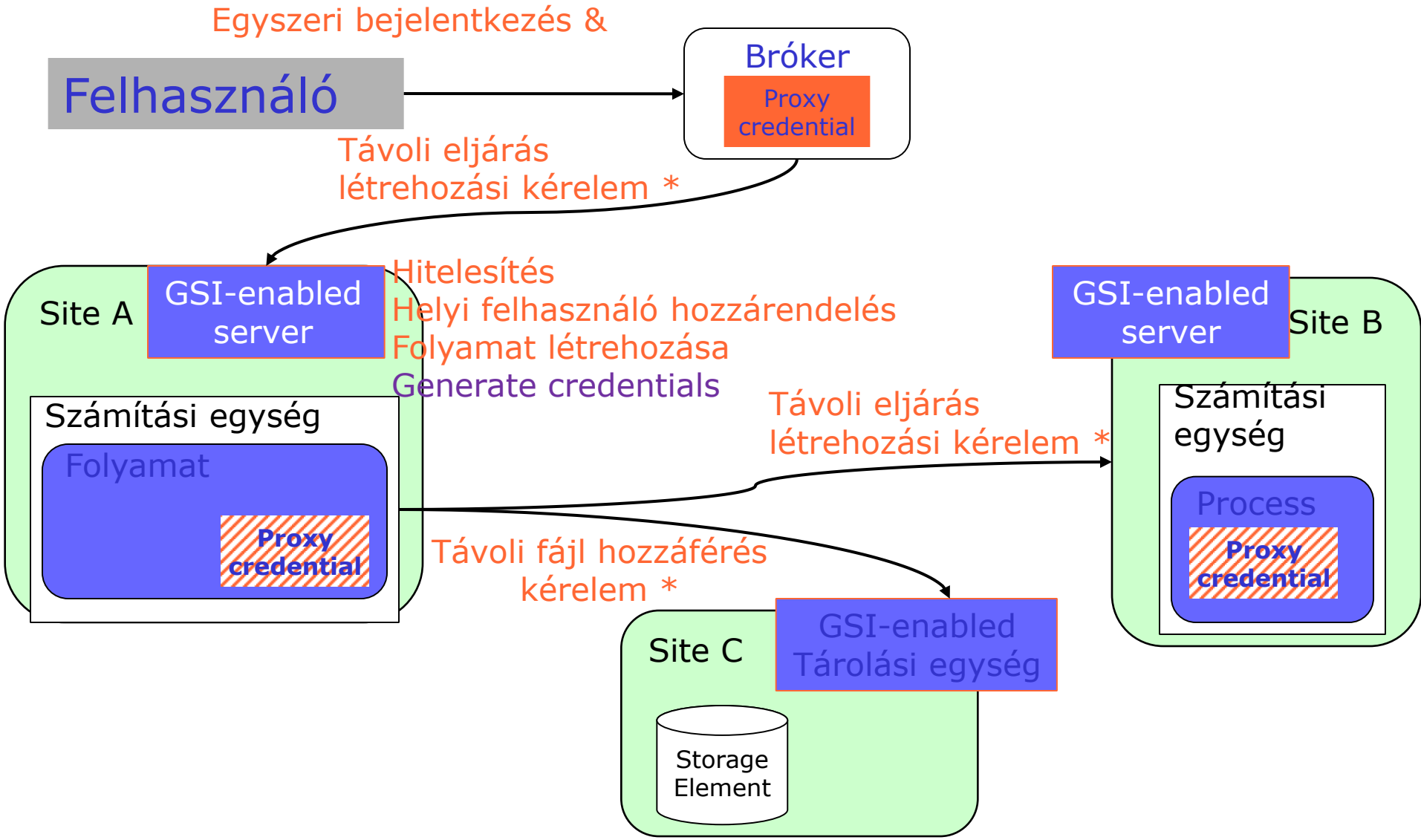


Delegáció korlátozott érv. proxival

- **Delegáció – lehetővé teszi, hogy távoli folyamat vagy szolgáltatás hitelesítse magát a felhasználó nevében**
- **Távoli folyamat/szolgáltatás „megszemélyesíti” a felhasználót**
- **Megoldás: Egy újabb szintű kulcs – tanúsítvány létrehozása a felhasználó tanúsítványából**
  - Az új kulcs-pár egy egyszerű fájl: Proxy credential
  - A proxy titkos kulcsát nem védi jelszó
  - A proxy korlátozható az elvégezető műveletek terén
  - A proxynak korlátozott az időbeli érvényessége



Proxy működés közben



Bejelentkezés a Gridbe: Proxy létrehozása

```
[denes@ui ~]$ voms-proxy-init --voms gilda
Your identity: /C=HU/O=NIIF CA/OU=GRID/OU=BME/CN=Nemeth
Denes/Email=nemeth.denes@iit.bme.hu
Creating temporary proxy ..................................................... Done
Contacting  voms.ct.infn.it:15001 [/C=IT/O=INFN/OU=Host/L=Catania/CN=voms.ct.infn.it]
"gilda" Done
Creating proxy ..................................... Done
Your proxy is valid until Mon Oct  6 22:39:09 2008
```

% voms-proxy-init → bejelentkezés a Gridbe

Enter PEM pass phrase: ****** → A titkos kulcsot egy jelszó védi

% voms-proxy-destroy → kijelentkezés a Gridből

A delegált credentialok nem kerülnek visszavonásra