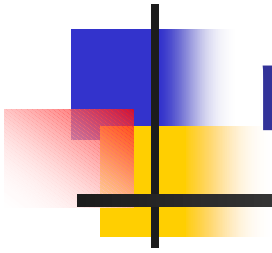
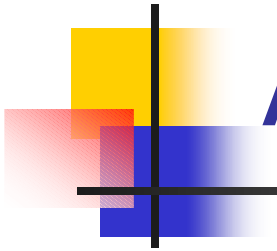


Kerberos, LDAP és OpenAFS alapú osztott fájlrendszer megoldások

Turi Péter
ELTE Információtechnológiai Központ
turip@elte.hu



Amiről szó lesz

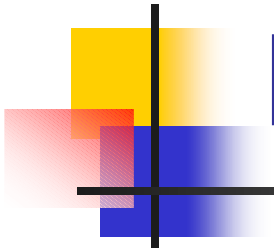
- Kerberos 5
  - Terminológia
  - Protokoll
  - Mi a kerberos és mi nem?
- LDAP
  - Hogyan illik bele a képbe?
- OpenAFS
  - Felépítés (részleges)
  - Hogyan illik bele a képbe?

Feltételezések a Kerberos protokoll kialakításában

- A Kerberos szerverek és a kliensek biztonságosak
- A hálózat viszont nem feltétlenül

Következmények:

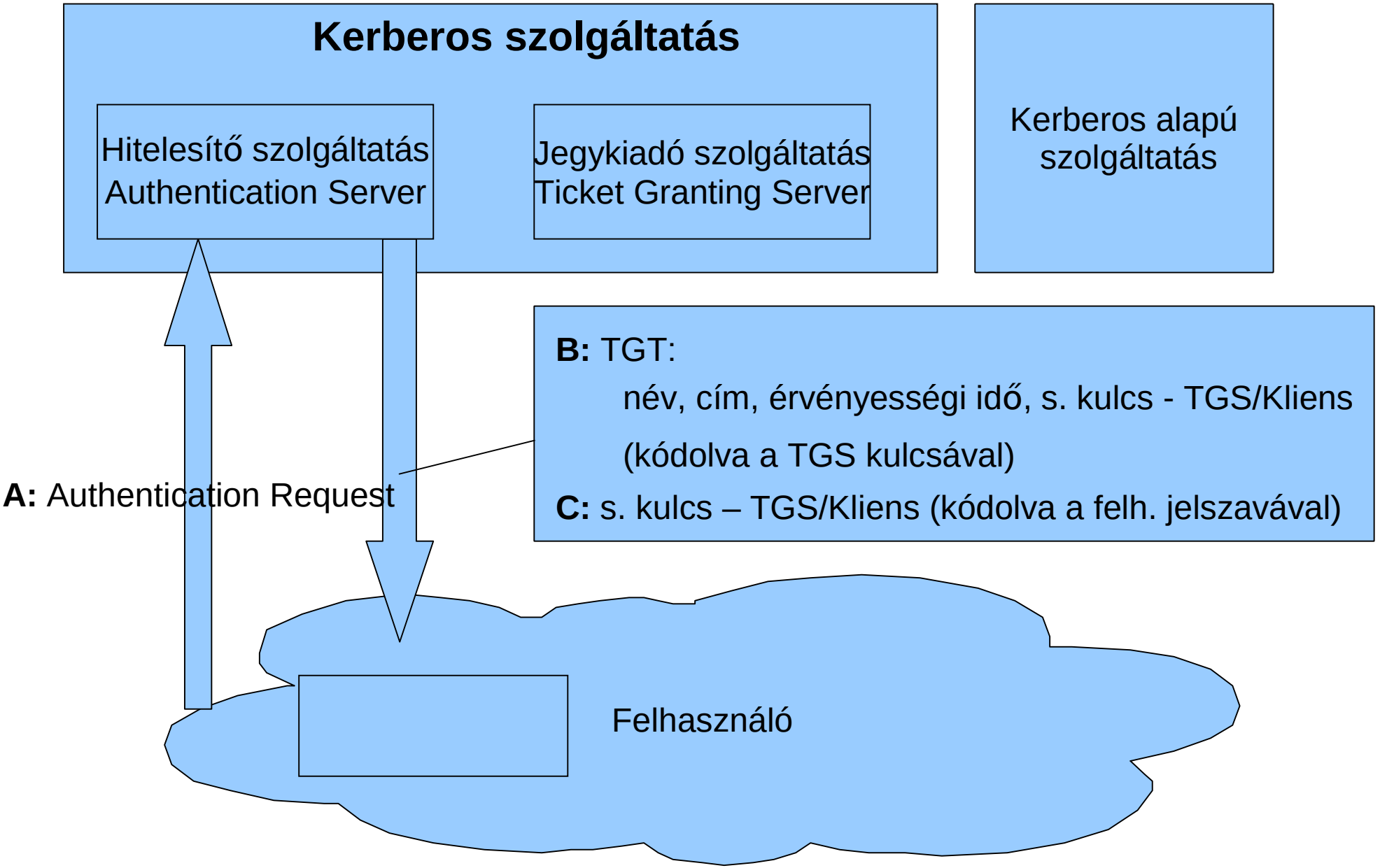
- A jelszó csak a kerberos szervereken tárolódik
- A jelszó sem hash-elve, sem kódolatlanul nem küldhető át a hálózaton



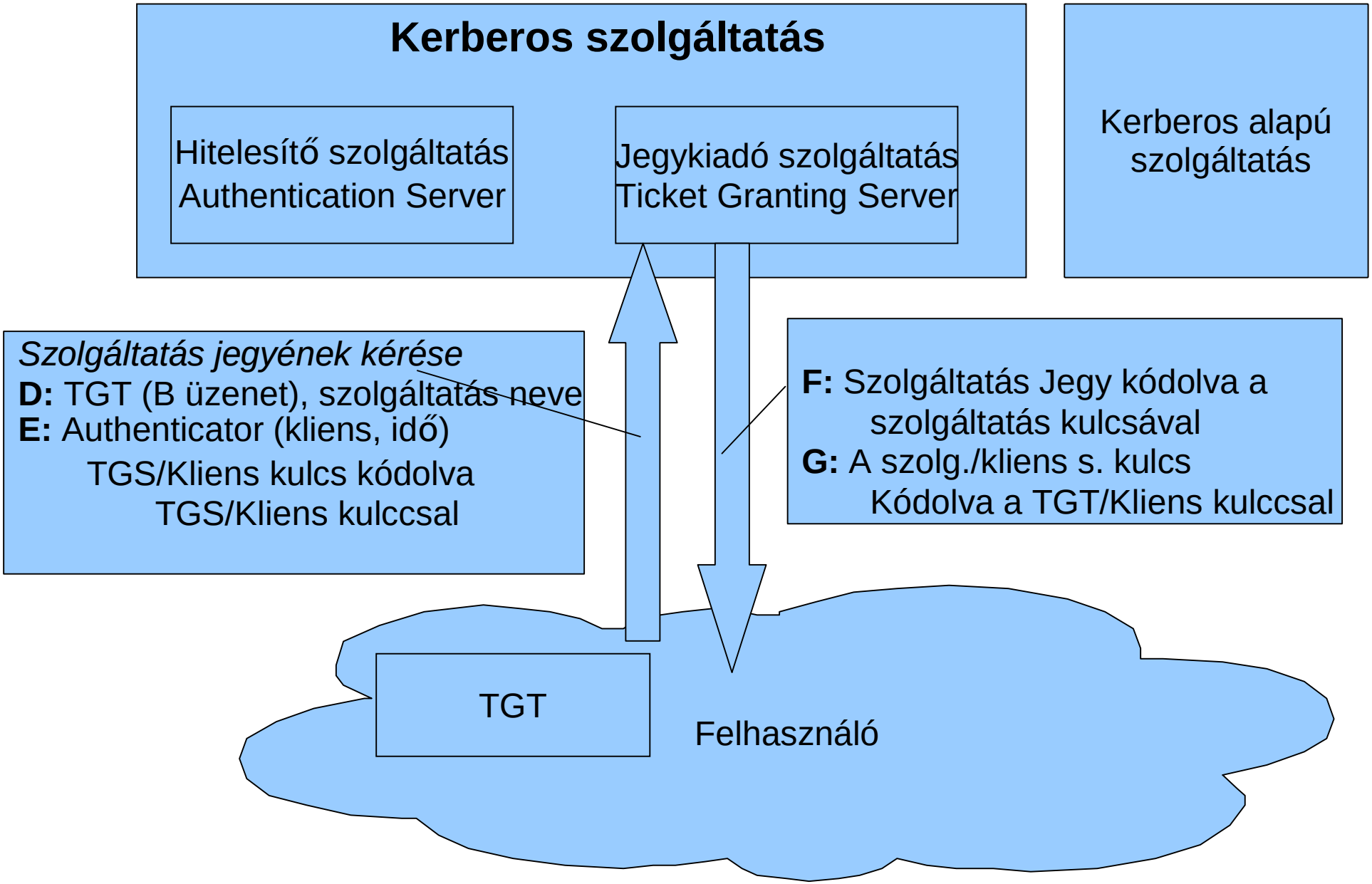
Kerberos terminológia

- Realm
- Principal,
- Jegy (név, élettartam, forráscím, kulcs)
- KVNO (Key Version Number) és szerepe
- KDC, Auth. Server, Ticket Granting Server
- Session
- Keytab
- GSSAPI

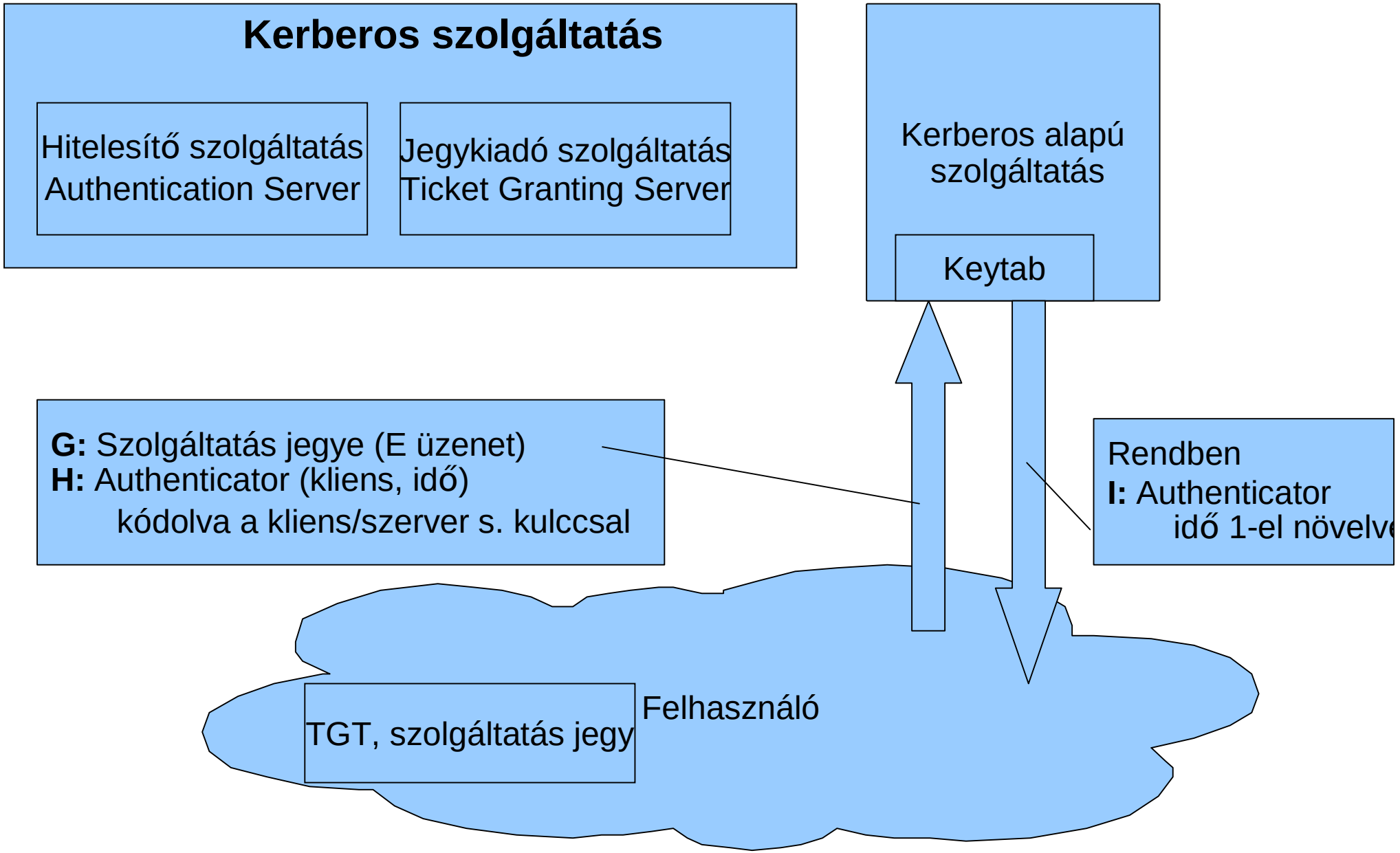
Hitelesítés – felhasználó azonosítása

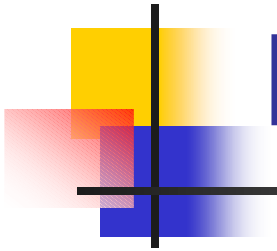


Hitelestés – szolgáltatás jegyének kérése



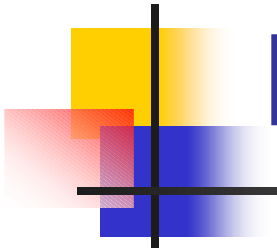
Hitelesítés – azonosítás a szolgáltatásnál





Előnyök

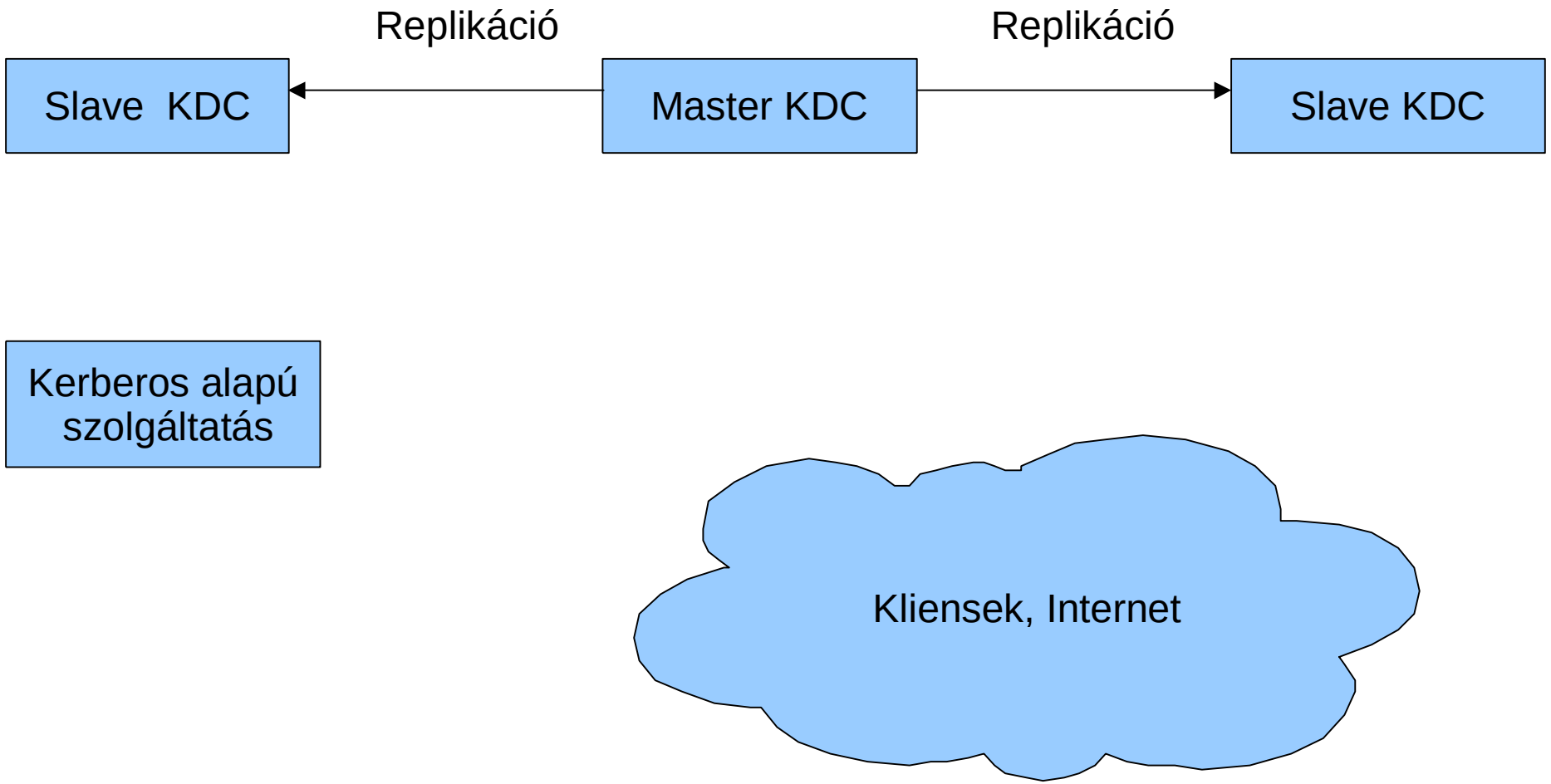
- Bárhol (ahol van kerberos kliens telepítve használható), nem csak az általunk karbantartott szervereken
- Kvázi automatikus kliens konfiguráció (implementációfüggő)
- Lehetséges windows integráció
- Single sign on (az otthoni klienseken is)

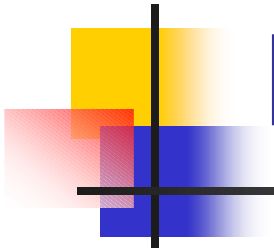


Problémák

- A rendszer nem véd a kliens oldali jelszó lopás ellen.
- Keytab „ellopása”
- Single master replikáció és jelszóváltoztatás
- Egységes fájlrendszer elérés kellene
- Kerberos támogatás hiánya (GSSAPI)

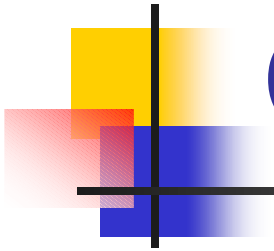
Hálózati topológia





Kerberos és LDAP

- Kerberos
  - entitások hitelesítése
- LDAP
  - entitások hitelesítése
  - felhasználói adatok kiadása (uid, teljes név, stb).
- Teljesen LDAP alapú megoldás vs. Kerberos és LDAP
  - GSSAPI szerepe



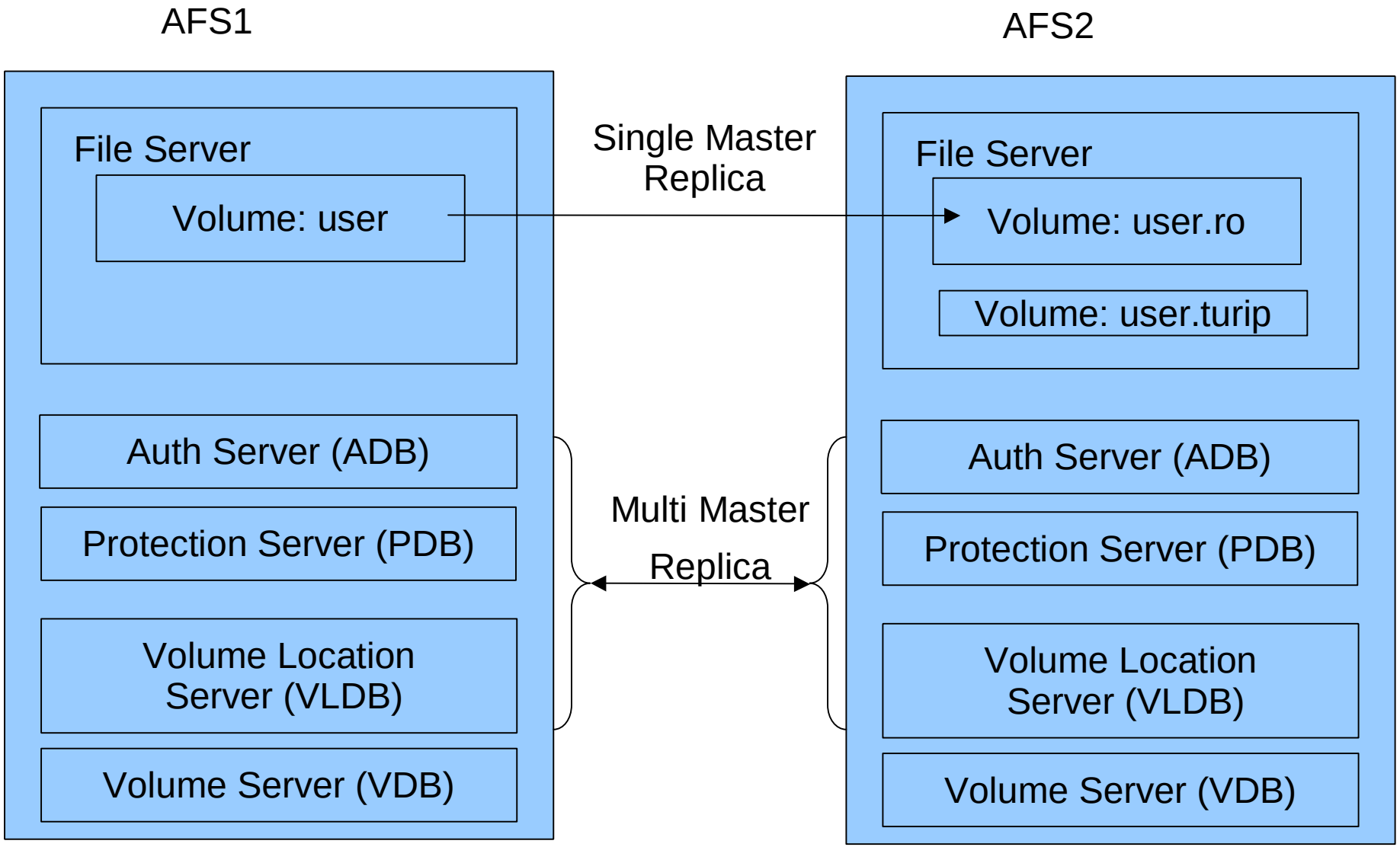
OpenAFS

- Osztott fájlrendszer, Kerberos hitelesítési megoldással.
- Cellák, kötetek (volume) használata és kvóta kezelés
- Saját felhasználói adatbázis
- Jogkezelés: ACL, Könyvtárakra
- Replikáció
- Kódolt RPC, saját kötet formátum

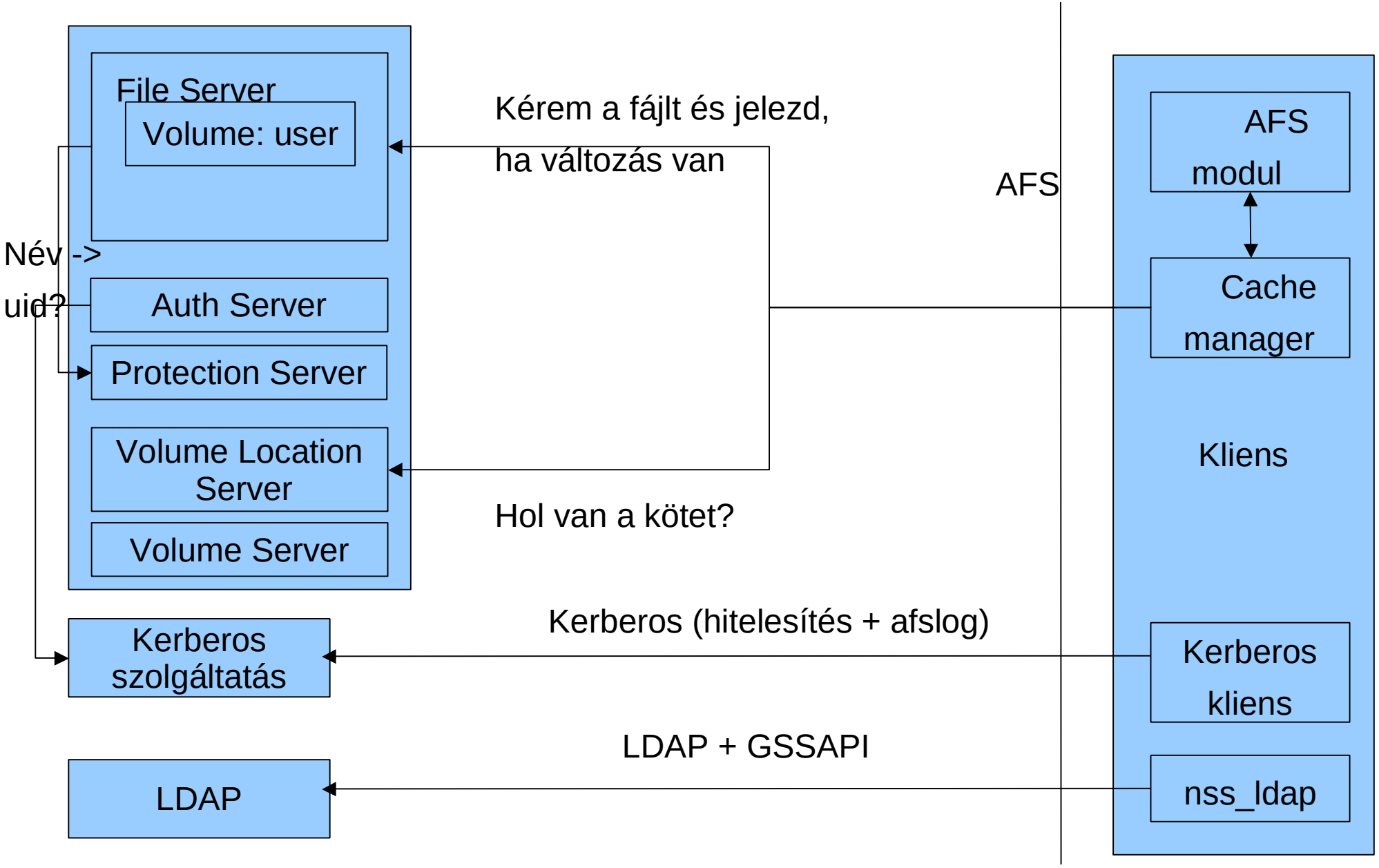
OpenAFS - komponensek

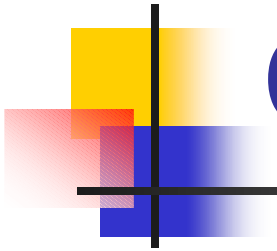
- Authentication Server: hitelesítés
- Protection Server: felhasználói csoportok
- File Server
- Volume Location Server: hol található az adott kötet?
- Volume Server: Kötet műveletek.
- BOS Server: „felvigyázó” folyamat
- Cache Manager: kliensen felelős a fájlszerverrel való kommunikációért

AFS Fileszerverek



Mindez működés közben





Összefoglalás

OpenAFS és Kerberos:

- HA megoldás (replikáció)
- Tetszőleges helyről elérhető (otthonról, stb.)
- Jól skálázható (több szerver)
- 3 éve működő implementáció az ELTE-n (caesar klaszter, http://caesar.elte.hu/)

OpenAFS

- Samba alternatíva lehet
- Előző napi állapot