



---

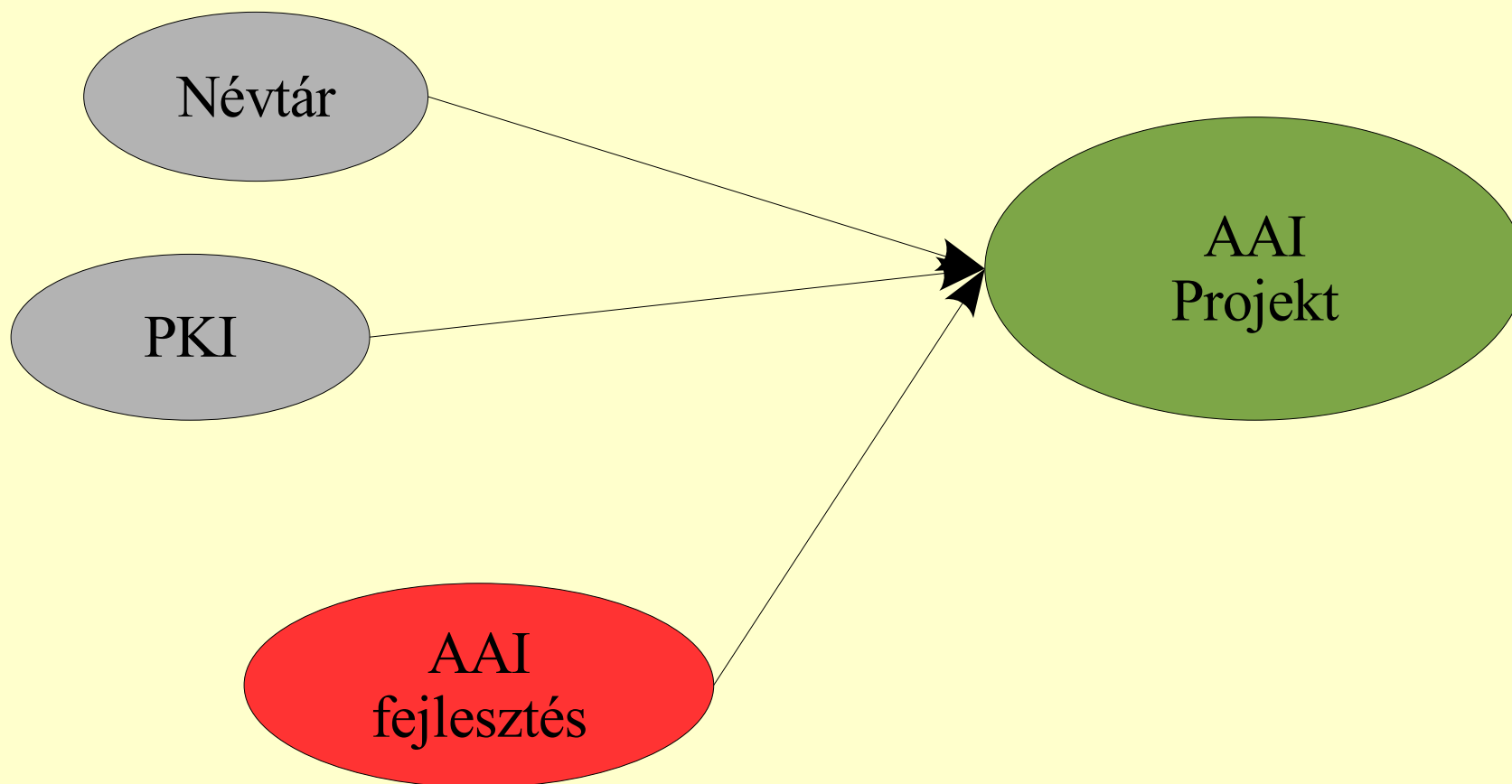
# AAI Projekt

Bajnok Kristóf

*NIIF Intézet*

[bajnokk@niif.hu](mailto:bajnokk@niif.hu)

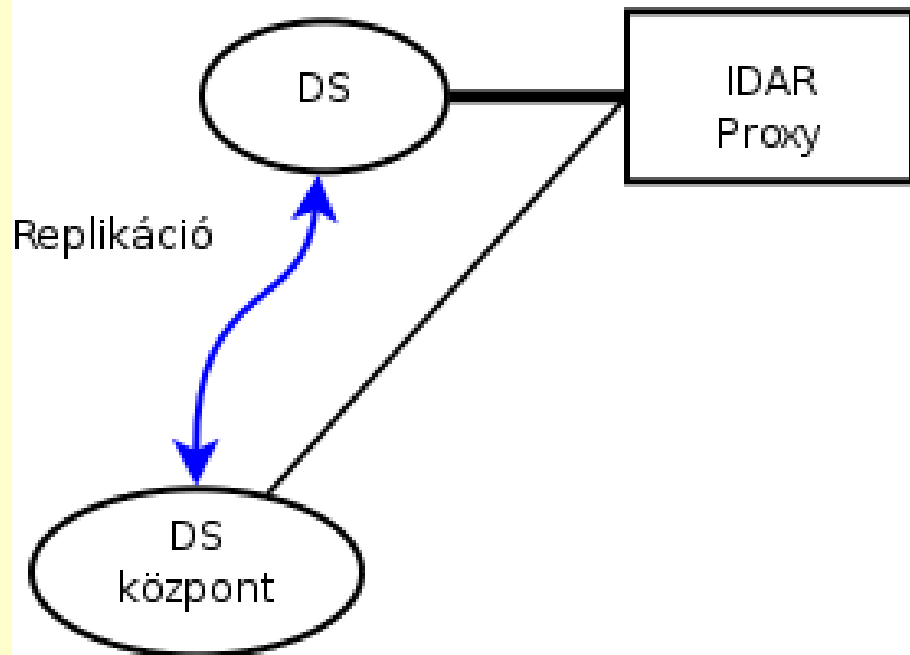
# Pozicionálás



# Névtár ma

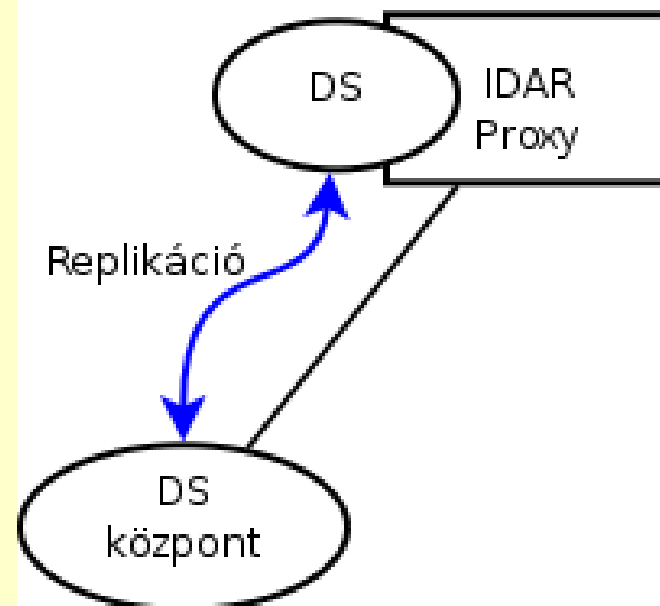
## Fázis 1 (Solaris)

directory.XXX.hbone.hu



## Fázis 2 (Linux)

directory.XXX.hbone.hu





# Névtár problémák

- ---
- Műszaki
  - A Proxy egyszeres hibapontot jelent
  - SUN-ok elavultak, drága a javíttatásuk
  - Régi operációs rendszerek
    - de az „egyszeres hibapont”-ság miatt nehéz hozzányúlni
- Jogi
  - Az NIIF **adatkezelő**, ált. *felhatalmazás nélkül*
    - tisztelet a kivételnek



# Névtár problémák

- ---
- Elvi
  - „Nem erőszak a disznótor”
    - Olyan intézményekhez kerültek gépek, akik egyelőre nem gondolkoznak névtár-fejlesztésben
  - „Az én házam az én váram”
    - Mit keres az NIIF az intézményi adatoknál?
  - Alternatív megoldások nem integrálhatók
    - pl. van olyan, hogy valahová alkalmasabb más felhasználói adattárolási módszer



# Névtár új stratégia

- ---
- Nem használt gépeket lekapcsoljuk, visszahozzuk
- Használatban levő csomópontokat lecseréljük
  - **„LDAP Box”**
    - 2xDell 2650
    - Linux LVS hibatűrés
    - Directory Proxy + Directory Server
- Replikációt leállítjuk
- **Igény szerint!**
  - Akár intézményi rendszerfelügyelet
    - „root jog”
  - Akár teljes körű névtár jogok
    - pl. új adatbázisok, replikációk, **séma**



# NIIF névtár szolgáltatásai

- ---
- Központi „White-pages” LDAP szerver
  - referral
- „LDAP Box”
  - Nem alanyi jogon!
  - Nem kötelező!
  - telepítés, rendszerfelügyelet
- LDAP támogatás
  - Wiki
  - Oktatás, előadások
- NIIFPerson schema



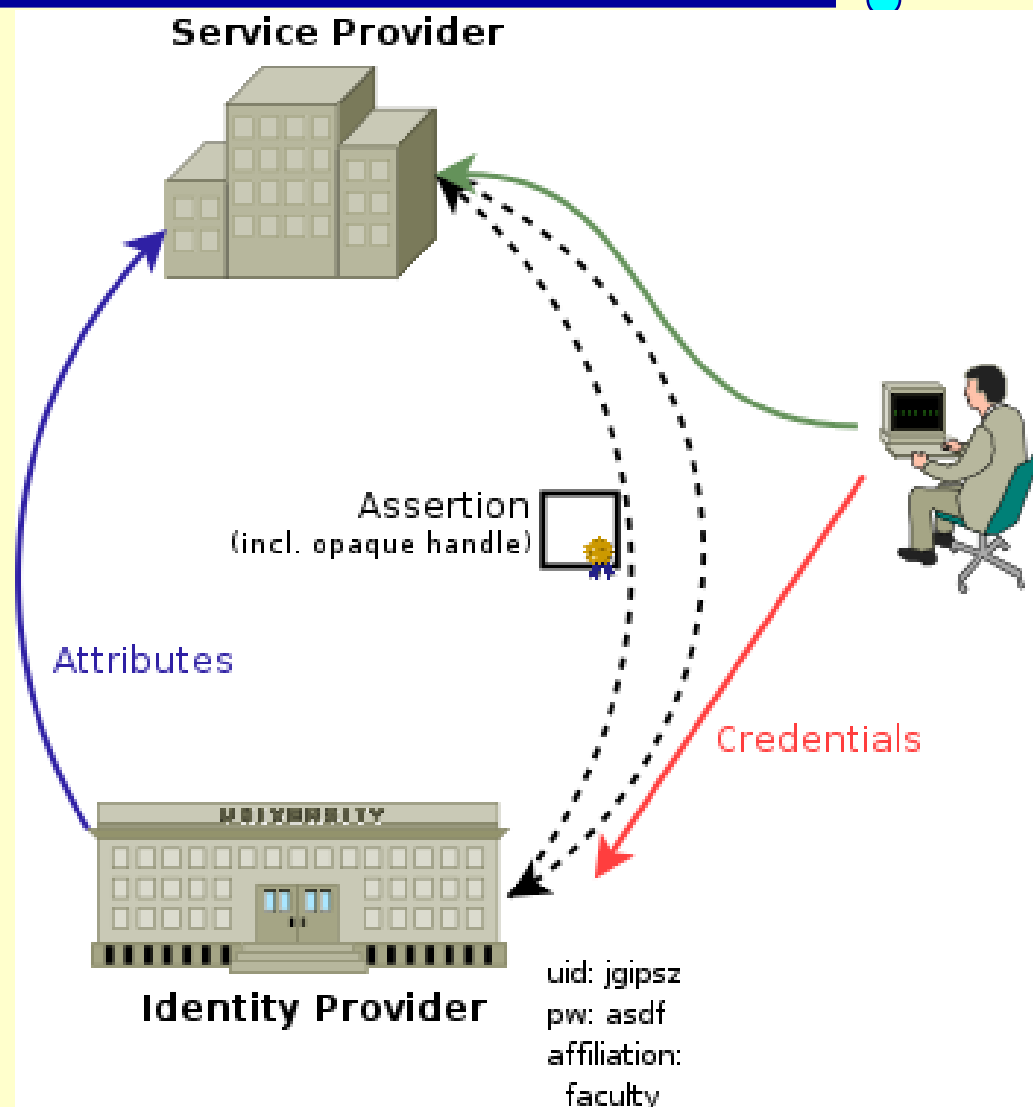
# AAI

- 
- Webes Single Sign-On
  - Elosztott felhasználó-kezelés



# Shibboleth

- Internet2
  - Akadémiai (+kereskedelmi) szféra
- Identity Federation
  - egy felhasználó egy IdP-nél „van otthon”
  - IdP attribútumokat ad át az SP-nek
- SP **autorizál**
  - attribútumok alapján





# AAI előnyei az intézmények számára

- ---
- Belső Single Sign-on
- Egységes felhasználó-azonosítás
  - Akár „biztonságosabban” is
- Együttműködési lehetőség intézmények között
  - belső: **HREF**
    - *Hungarian Research and Education Federation*
  - külső:
    - részvétel akármilyen más föderációban
    - kétoldalú megállapodások partner intézményekkel
    - Inter-Federation: föderációk közötti együttműködés
      - Géant2 JRA5: EduGAIN



# NIIF AAI

- ---
- **Technikai pilot fázis**
  - NIIFI-n belül
- **Föderációs pilot fázis**
  - néhány partner intézménnyel
  - intézményi belső AAI bevezetés támogatása
  - **HREF** szabályzatok kidolgozása az intézményekkel együtt
- **Éles üzem**
  - támogatás
  - audit



# AAI Fejlesztések

- ---
- AAI Box = LDAP Box +
  - Shibboleth IdP (Identity Provider)
  - EduROAM Radius szerver
- Fejlesztések
  - Shibboleth webes konfigurációs lehetőségek
  - Opt-in IdP
    - a felhasználót tájékoztatni kell, hogy milyen adatait kívánjuk átadni másoknak
    - Single Sign-On biztosítása mellett