AAI

Networkshop,
2006. április 22.

Bajnok Kristóf

bajnokk@sztaki.hu
MTA-SZTAKI
ITAK

Authentication and Authorization Infrastructure

- Autentikáció
  - A felhasználó digitális személyazonosságának hiteles megállapítása
- Autorizáció
  - Az azonosított felhasználó jogosultságainak ellenőrzése, betartatása
- **Infrastruktúra**
  - Mindezt egységesen, szabványosan, elosztottan, könnyen kezelhetően

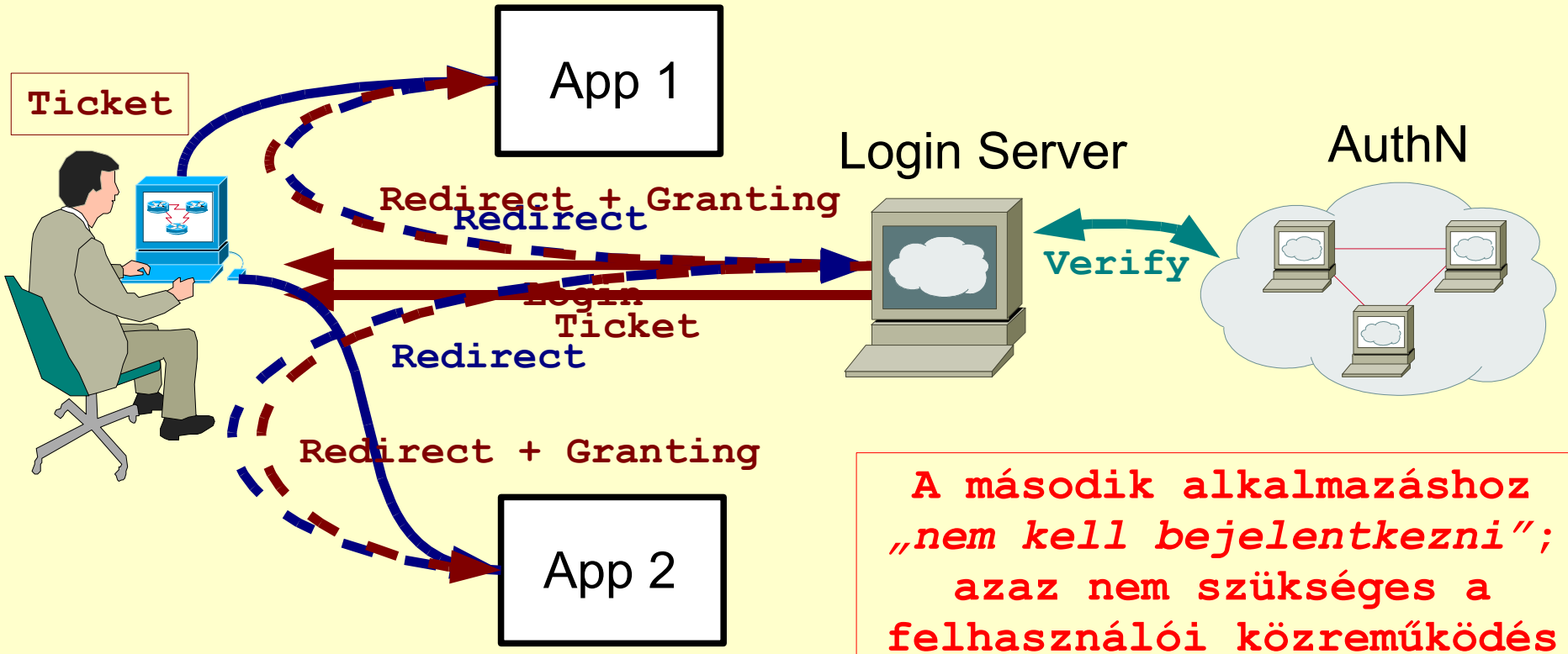
Mit várunk az autentikációtól?

- Legyen biztonságos
  - ne lehessen ellopni a személyazonosságunkat
- Legyen egységes, egyszerű
  - mert csak így lehet biztonságos
- Legyen naprakész
    - új kollégának ne kelljen hetekig várnia; vice versa
- Ne legyen idegesítő
  - ne kérdezzen rá ugyanarra állandóan

Identity Management

- Kezdetben felhasználói információk konszolidált tárolása
  - X.500, LDAP
- Alkalmazások kezdtek ráépülni
  - Egyre több webes alkalmazás
  - Sokféle bejelentkezési eljárás
    - Minden alkalmazásba külön-külön be kell jelentkeznie a felhasználónak
- Jogosultságok nyilvántartása

Single Sign-On



A második alkalmazáshoz *„nem kell bejelentkezni”*; azaz nem szükséges a felhasználói közreműködés

Federation

- Több intézmény közösen dolgozik
  - A közösen használt erőforrásokhoz szabályozott keretek között kell hozzáférni
  - **Legyen elég egyetlen identitás!**
- Az intézmények **megbíznak** egymás *Identity Managementjében*
  - eljárások
  - attribútumok használata

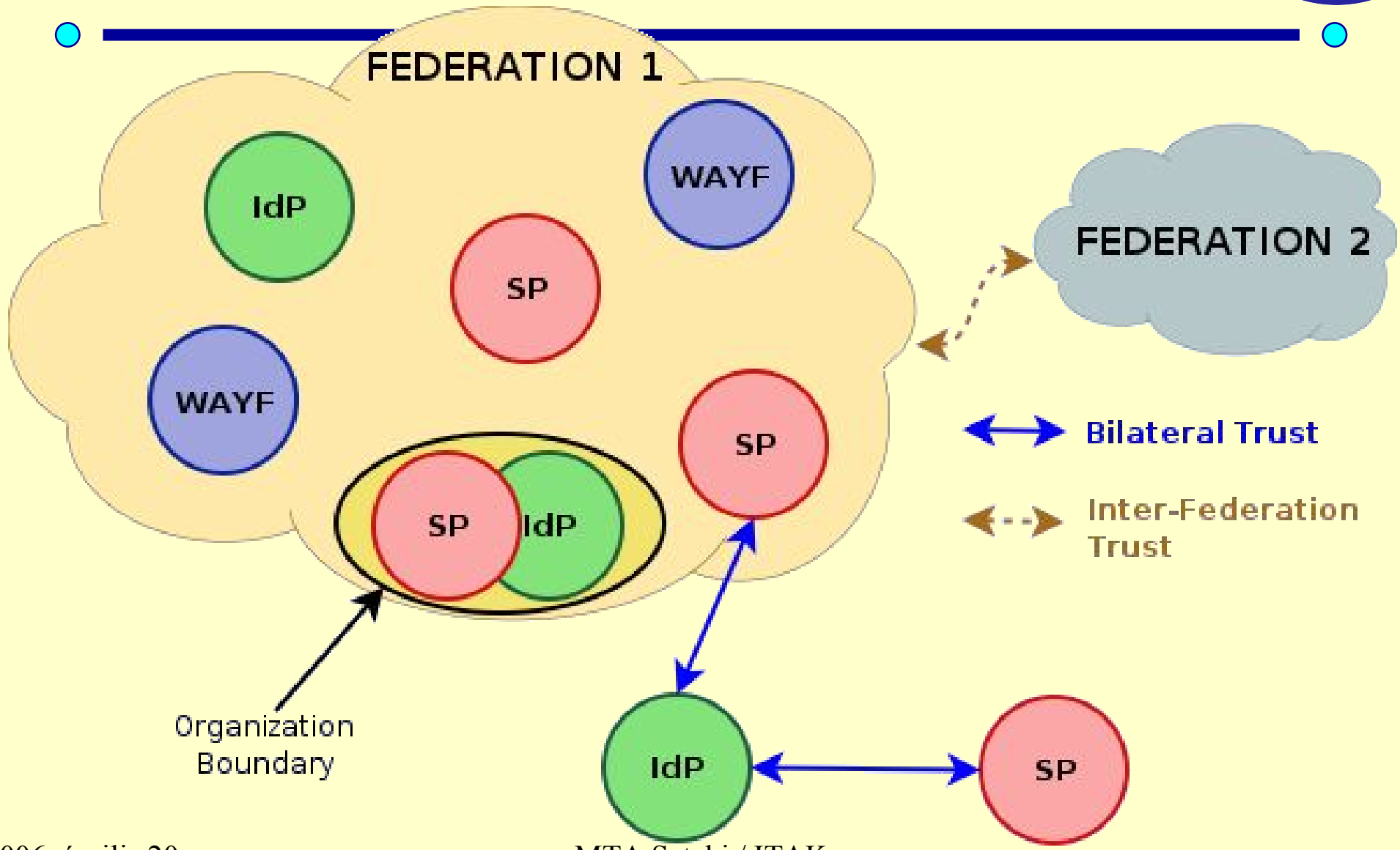
Federation elemek

- **Identity Provider (IdP)**: „anyaintézmény”
  - azonosítást végez (SSO domainek között is)
  - felügyeli az identitásokat
  - felhasználói adatokat szolgáltat
- **Service Provider (SP)**: tartalomszolgáltató
  - megbízik az IdP-ben
    - nincsenek saját felhasználói
- Federation management
  - Home location (WAYF), metadata, stb

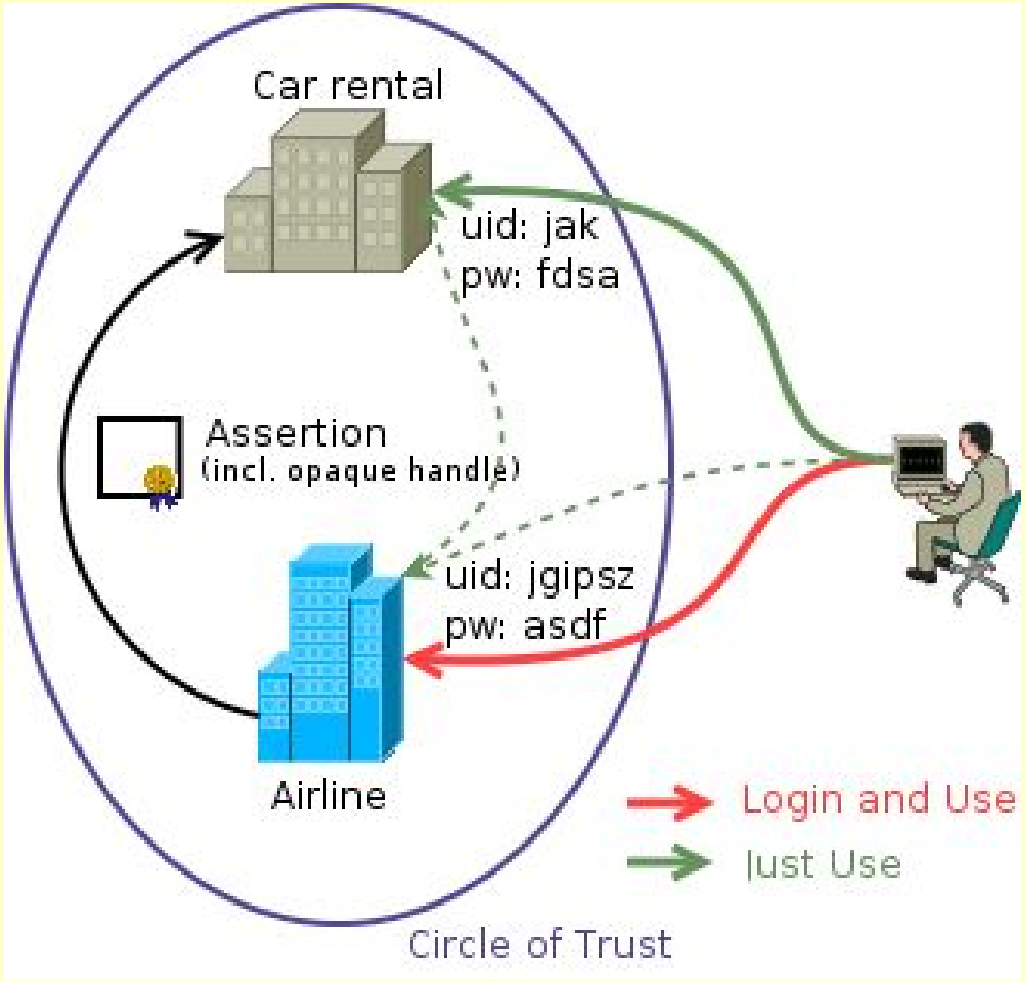
Kommunikáció az AAI-n belül

- **SAML** (Security Assertion Markup Language)
  - OASIS nyílt szabvány, XML alapú
  - **Assertion**: állítás + paraméterek
    - autentikációs esemény
    - attribútumok (+ egyéb...)
  - XML Signature (W3C) hitelesítés
  - Profilok:
    - Browser profilok: az üzenetek továbbítása a böngészőn keresztül (POST)
    - SOAP-alapú profilok: közvetlen

Federation Topológia



Federation modellek
Liberty

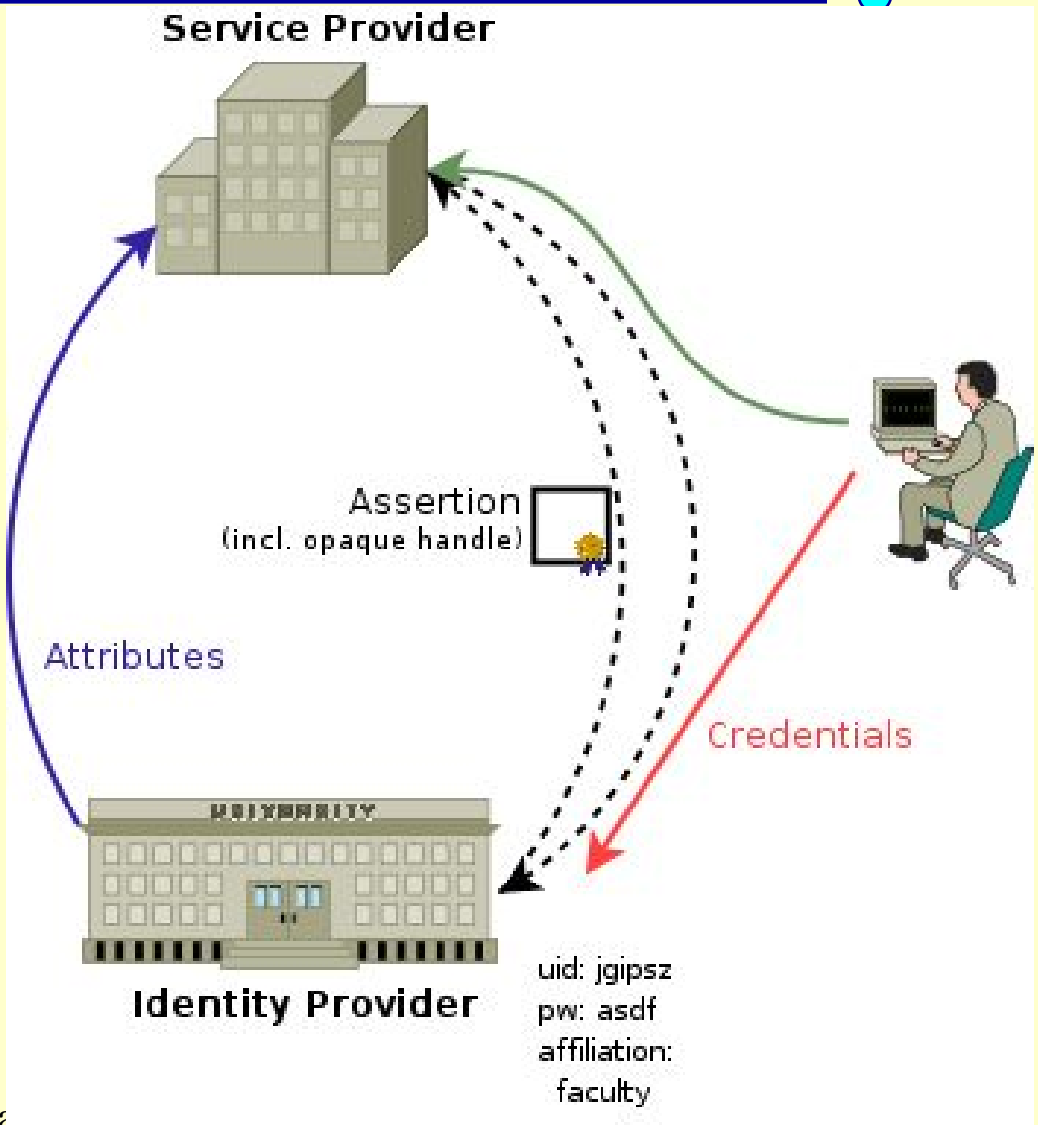


- Liberty Alliance
  - Kereskedelmi szféra
- Account linking
  - A felhasználónak több szolgáltatónál van (lehet) identitása
  - Az identitások összekapcsolhatók a **felhasználó által**
- Single Sign-on

Federation modellek: **Ügyfélkapu**

Federation modellek: **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



Összefoglalás

- Az AAI lényege, hogy az autentikációs és autorizációs kérdéseket az alkalmazásoktól ***elkülönítve kezeljük***
- Közös erőforrások használatának általánossá válásával szükséges lesz az intézményeknek ***Föderációkat*** alkotni

Erre van az előre!