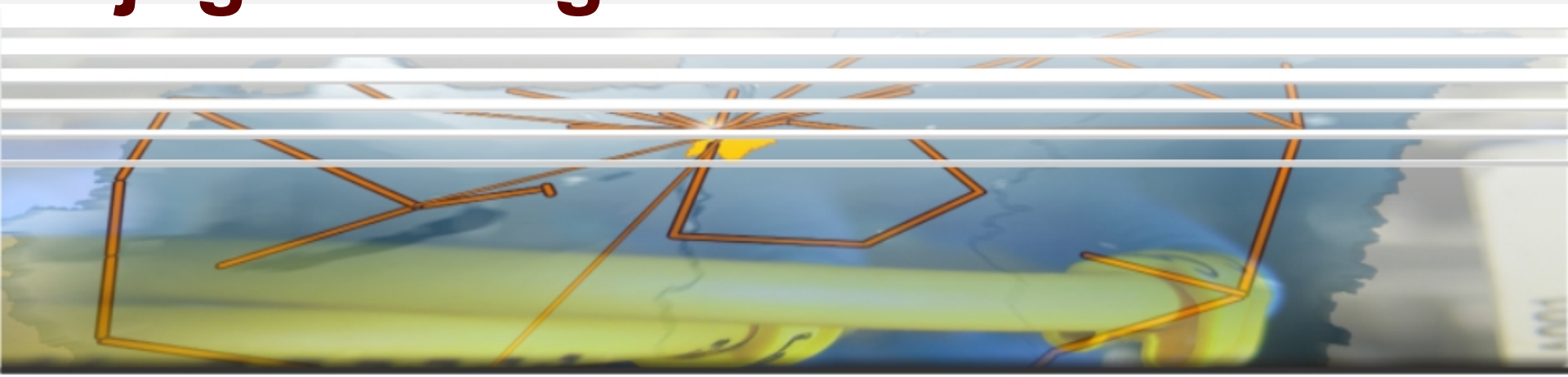
Szövetségi (föderatív) jogosultságkezelés



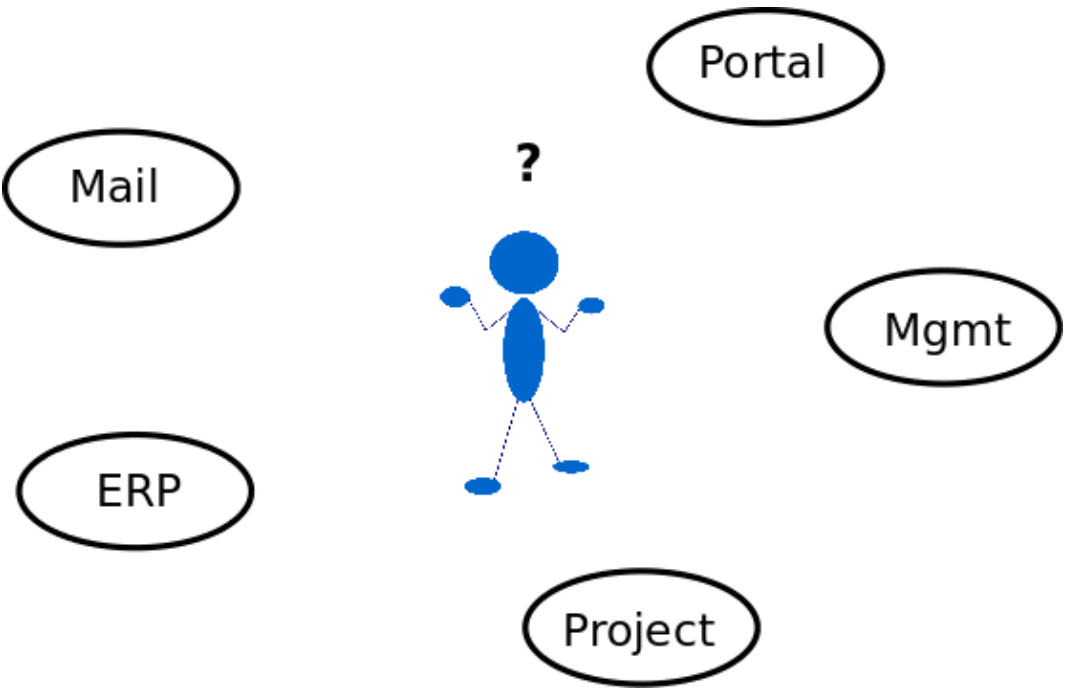
2010. április 8.
Networkshop, Debrecen

Bajnok Kristóf
NIIF Intézet

HBONE+

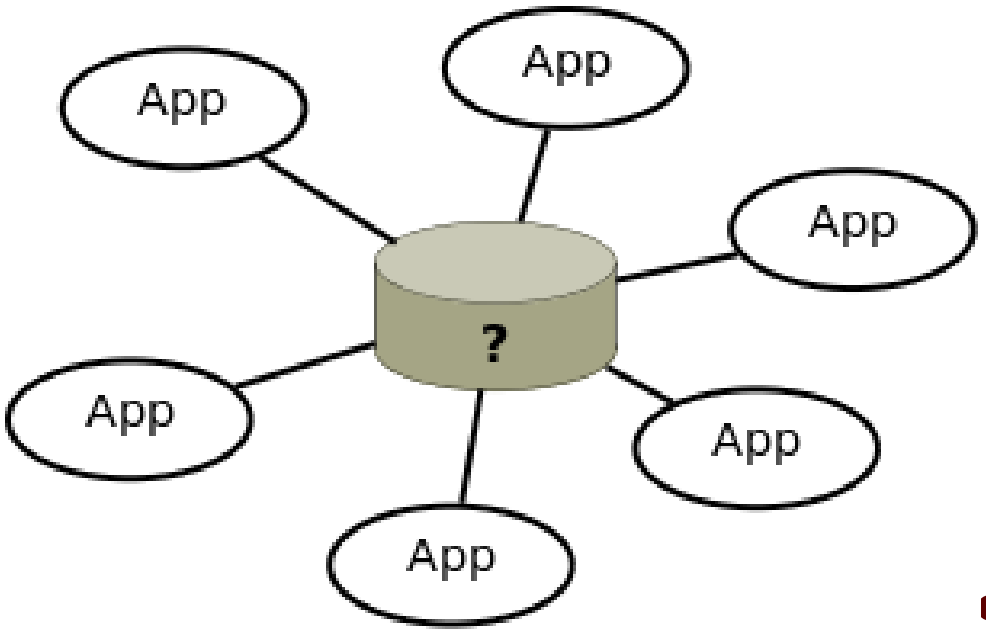
Befektetés a jövőbe
Új Magyarország
FEJLESZTÉSI TERV

Jelszavak, jelszavak, ...



- Alkalmazásonként külön felhasználó-nyilvántartás
  - nehezen használható
    - jelszó változtatás
    - sok jelszó
  - nem menedzselhető
    - új felhasználó hozzáadása
    - kilépett felhasználó törlése

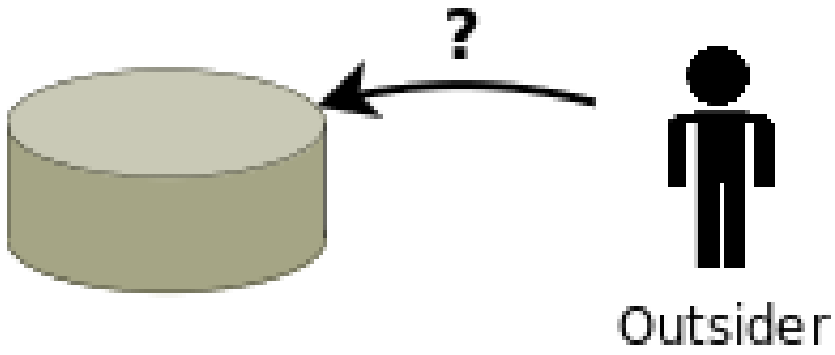
Központi adatbázis kell, ámde...



- Biztonság
  - ha minden alkalmazás hozzáfér a központi adatbázishoz
    - access control nehéz
    - egy alkalmazás jogaival az összes felhasználóhoz hozzáférhetünk
- Bonyolult schema

… nem elég

- Külsős hozzáférés biztosítása
  - biztonság
    - nem adunk-e több jogosultságot, mint szeretnénk
      - eduroam, VPN?
  - menedzsment
    - support, jelszóváltoztatás
  - felhasználó
    - még egy jelszó…



Föderatív azonosítás

- Az intézmények fogadják el egymás felhasználóit azonosítottnak
  - bizalmi szövetség = **föderáció**
- Intézményen belül legyen elegendő egyetlen azonosítási pont
  - belső és külső szolgáltatások számára

Föderatív azonosítás

- Az intézmények fogadják el egymás felhasználóit azonosítottnak
  - bizalmi szövetség = **föderáció**
- Intézményen belül legyen elegendő egyetlen azonosítási pont
  - belső és külső szolgáltatások számára

felhasználóknak:

eduID

Szerepek

- **Identity Provider (IdP)**
  - azonosítja a felhasználót
  - megadja az azonosítás körülményeit és a felhasználó tulajdonságait (attribútumok)
- **Service Provider (SP)**
  - feldolgozza az IdP-től kapott információt
  - jogosultság-ellenőrzést végez az attribútumok alapján
  - az attribútumokat továbbadja az alkalmazás számára

Előnyök

IdP

- átláthatóvá teszi az adatkezelést
- növeli a biztonságot
  - push modell
  - egységes bejelentkező felület
- belső szolgáltatások könnyen integrálhatók

SP

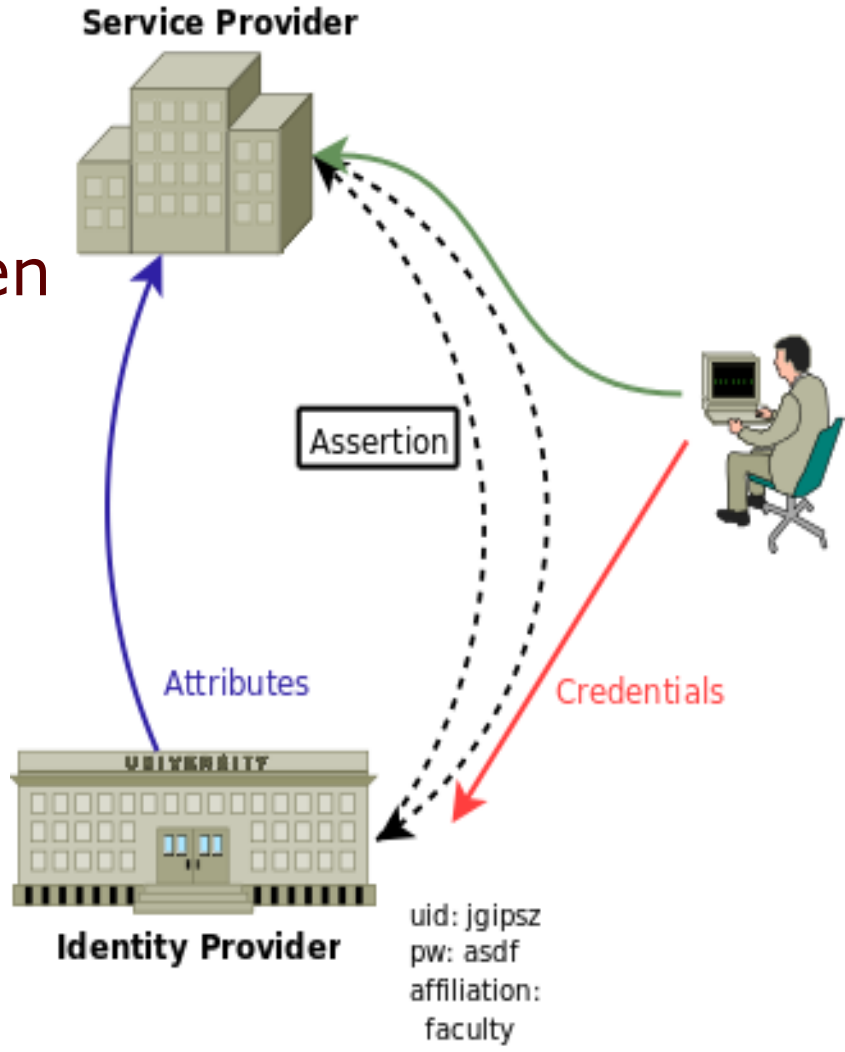
- csökkenti a felhasználó-adminisztrációval kapcsolatos költségeket
- nagy számú potenciális felhasználó

Felhasználó

- single sign-on
- sok szolgáltatás egyszerűen elérhető

Felhasználási területek (példák)

- Belső alkalmazások
- E-learning
  - egyetemek között közösen indított kurzusok
- Online könyvtári szolgáltatások
  - adatbázis-hozzáférések
  - intézményi előfizetés
- Projekt együttműködés
- Kereskedelmi és non-profit szolgáltatók



Infrastruktúra

- A jól megvalósított, szabványosan elérhető felhasználói azonosítási szolgáltatás ***az IT infrastruktúra része*** (middleware)
  - a szövetségi személyazonosság kezelés (Federated Identity Management) hasonló az Internethez
    - autonóm rendszerek szabványos összekapcsolása
- Nyílt szabvánnyal, szabad szoftverekkel megvalósítható

Jelen

- Hungarian Research & Education Federation (HREF)
  - pilot státusz
    - technikailag kész
    - 100% SAML2
  - 10 azonosító intézmény
    - BME, Debreceni Egyetem, Dunaújvárosi Főiskola, ELTE, KFKI Csillebérc, MTA Sztaki, NIIFI, Georgikon, PPKE, ZMNE
    - néhány intézmény csak részleges adatokkal
    - Virtual Home Organization vendégek számára
  - csatlakozás jelenleg nem szabályozott

Közelmúlt

- Fejlesztések
  - Resource Registry
    - föderáció résztvevőit tartalmazó metadata szerkesztésére
    - Shibboleth, SimpleSAMLphp konfigurációjának támogatására
    - felhasználói attribútumok kiadása
  - K+F
    - Shibboleth Single Logout, SimpleSAMLphp attribute filter, metadata signer, X.509 autentikációs modul, webmail integráció, Drupal Shibboleth modul, …
  - Neptun szinkronizáció

Folyamatban lévő munka

- Elkészült (véglegesítésre váró) dokumentumok
  - attribútum specifikáció

    https://wiki.aai.niif.hu/index.php/HREFAttributeSpec
  - metadata specifikáció

    https://wiki.aai.niif.hu/index.php/HREFMetadataSpec
  - adatvédelmi állásfoglalás

    http://www.hboneplus.hu/node/46
- Kidolgozás alatt
  - csatlakozási szerződés
  - IdM és üzemeltetési policy
  - struktúra

Bővülés

- Tyúk-tojás probléma
  - inflexiós ponthoz értünk
- IdP
  - felsőoktatási intézmények, kutatóintézmények
  - egyéb intézmények a saját dolgozóik részére
  - (iskolák)
- SP
  - **Könyvtárak**
  - **EISZ**, tudományos adattárak, kiadók
  - Kutatási, felsőoktatási alkalmazások
  - Kereskedelmi / non-profit szolgáltatók
  - Nemzetközi kutatási projektek
    - CLARIN, VICAJOP, ...

Köszönöm a figyelmet

aai@niif.hu
https://wiki.aai.niif.hu
(készülőben): http://eduid.hu