Föderatív authentikációs rendszerek

Mohácsi János, Polákovics István, Wágner Ferenc, Lajber Zoltán, Szalay Ferenc

Névtár ?

Föderatív Névtár?

Eduroam – Radius ?

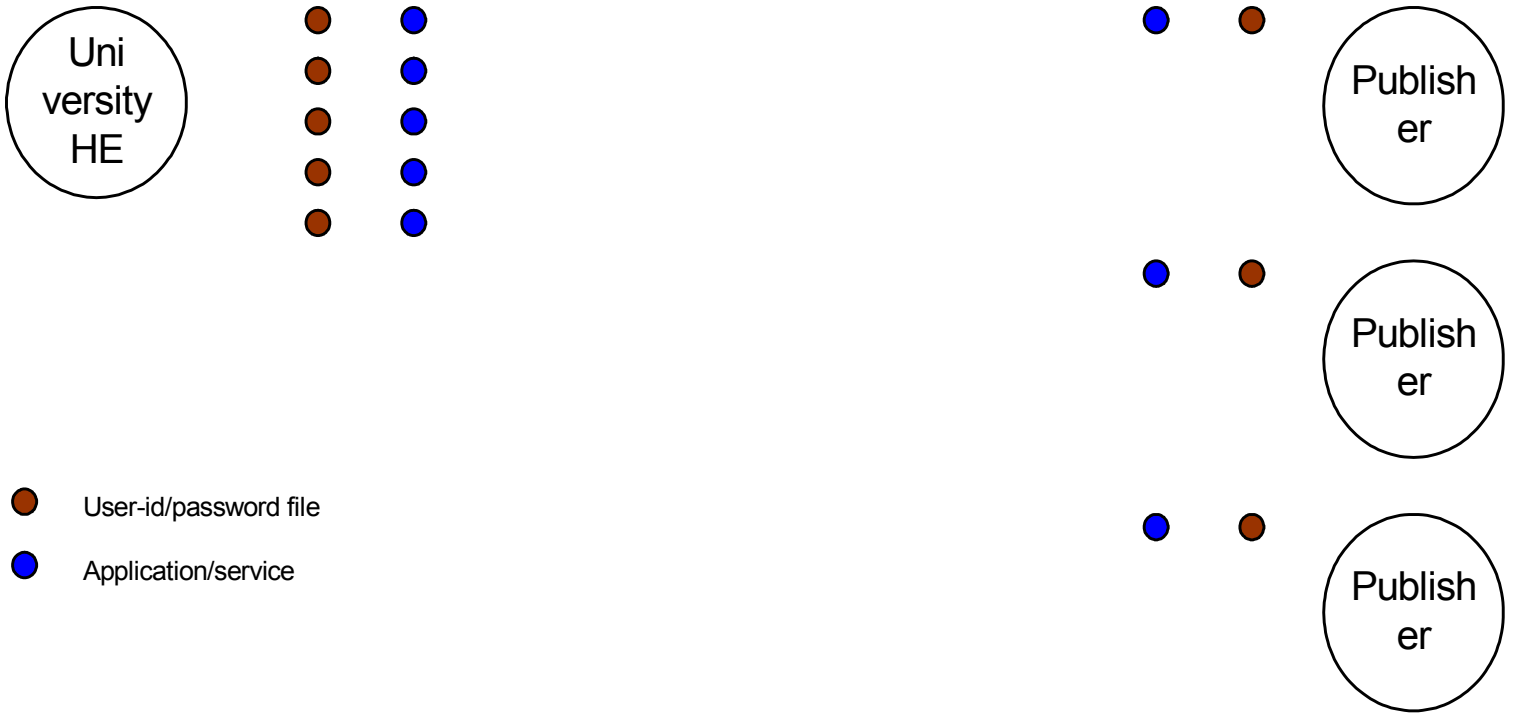
EduGain (Shibboleth) – AAI ?

PKI ?

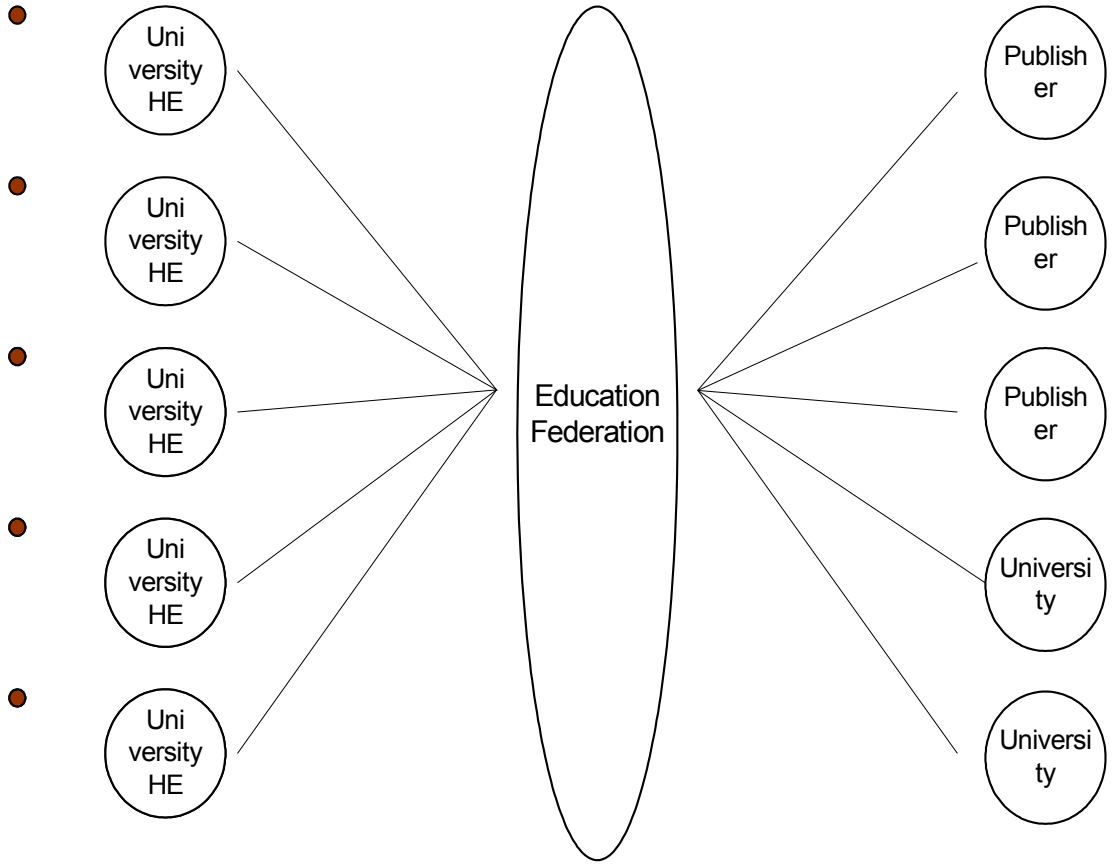
AAI rendszerek

- Célok:
  - Authentikáció – id management
  - Authorizáció -
  - Elosztott
  - Szervezett
  - Felügyelt
  - Szabványos
- Szolgáltatás!

Jelenlegi helyzet



Föderáció


Uni versity HE
Uni versity HE
Uni versity HE
Uni versity HE
Uni versity HE
Education Federation
Publish er
Publish er
Publish er
Universi ty
Universi ty

Föderáció

- Föderáció lehetővé teszi az erőforrások megosztását
- Föderáció alapja egy megállapodás a résztvevők között
- Föderáció közös nyelvet beszél
- Föderáció lehet része egy nagyobb füderációnak
- Föderációk együtt müködése: konföderáció

Föderációs elemek

- Szabványok: 802.1X, Radius, SAML, ID-FF, WS-FD
- Policy
  - Szabályok
  - résztvevők (IdP)
  - szolgáltatók (SP)
  - Föderáció müködtetője (NREN)
- Sémák
  - EduPerson
    - privacy
- Bizalom

Eduroam - esettanulmány
Univerzális IPv4 és IPv6 hozzáférés biztosítása wireless technológiával

Mohácsi János
NIIF/HUNGARNET

Követelmények egy modern wireless hozzáféréssel szemben

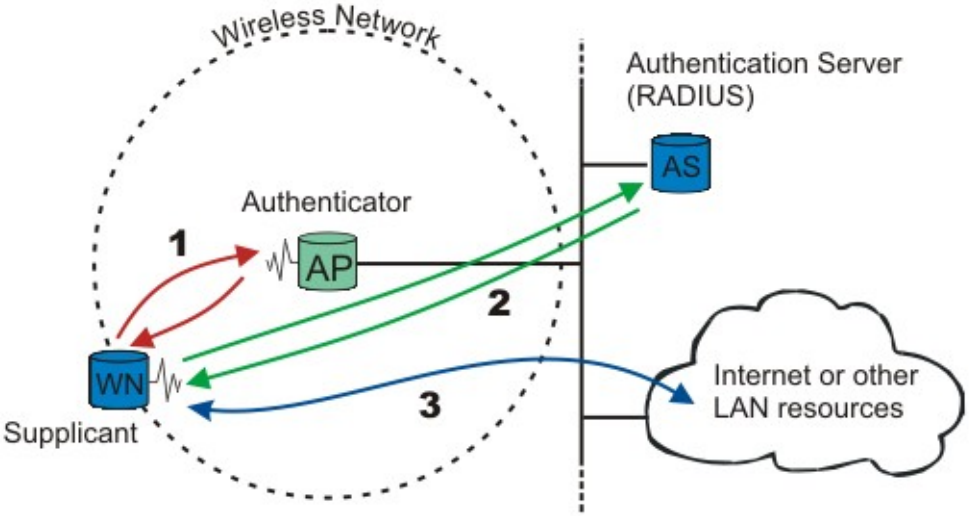
- A felhasználók egyértelmű azonosítása a hálózat szélén
  - Nem lehet a wireless kapcsolatot “ellopni”
- Lehetőség látogatók fogadására
- Skálázható
  - Anya intézményi felhasználói administráció és authentikáció – nincs központi adatkezelő!!!
  - Jó, ha tudjuk használni a már létező Radius infrastruktúrát
- Könnyen használható
- Nyitott
  - Minden operációs rendszerben támogatott
  - Szállító független
- Biztonságos
- IPv6 támogatás
- Eduroam kompatibilis

IEEE 802.1x

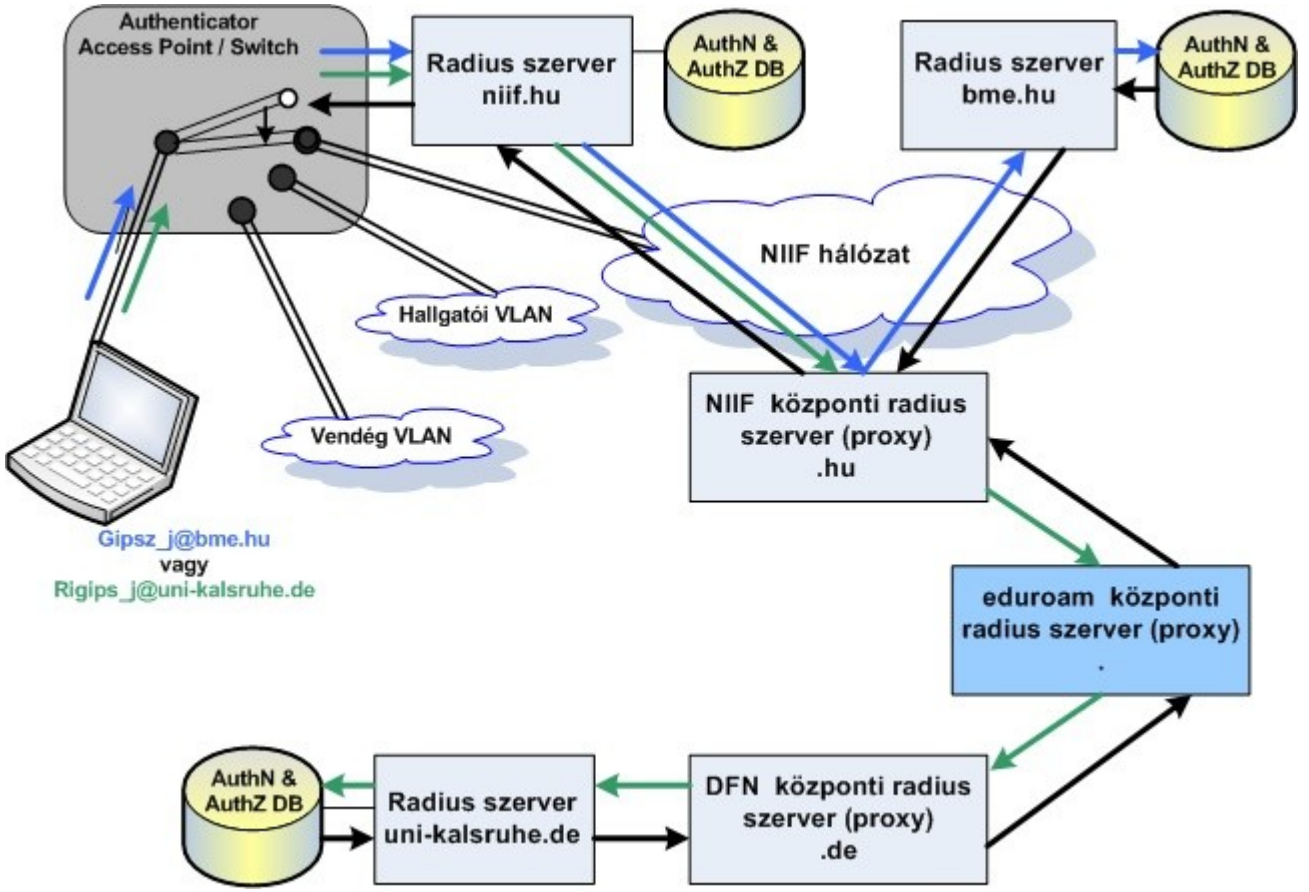
- Igazi port alapú Layer 2 azonosítás a kliens és a AP/switch között
- Többféle authentikáció lehetséges (EAP-MD5, MS-CHAPv2, EAP-SIM, EAP-TLS, EAP-TTLS, PEAP)
- Szabványos
- Titkosítja a kommunikációt dinamikus kulcsokkal
- RADIUS támogatás
  - Skálázható
- Dinamikus VLAN hozzárendelés támogatott
- Kliens szoftver szükséges (OS vagy 3rd -party)
- Vezeték nélküli és vezetékes hálózat is támogatott

802.1x és Wireless

- WPA és 802.11i ún. Enterprise módja implementálja a 802.1x-et



Roaming?


Authenticator
Access Point / Switch
Radius szerver
niif.hu
AuthN &
AuthZ DB
Radius szerver
bme.hu
AuthN &
AuthZ DB
NIIF hálózat
Hallgatói VLAN
Vendég VLAN
NIIF központi radius
szerver (proxy)
.hu
Gipsz_j@bme.hu
vagy
Rigips_j@uni-kalsruhe.de
eduroam központi
radius szerver (proxy)
.
AuthN &
AuthZ DB
Radius szerver
uni-kalsruhe.de
DFN központi radius
szerver (proxy)
.de