Eduroam

Az NIIF tervei

Fehér Ede

HBONE Workshop
Mátraháza, 2005. november 9-11.

Tartalomjegyzék

- Mi az Eduroam?
- Tagok, felhasználók
- Működési modell
- Bizalmi szövetségek
- Felhasznált technológiák
- Továbbfejlesztési irányok
- NIIF pilot és csatlakozás

Mi az Eduroam?

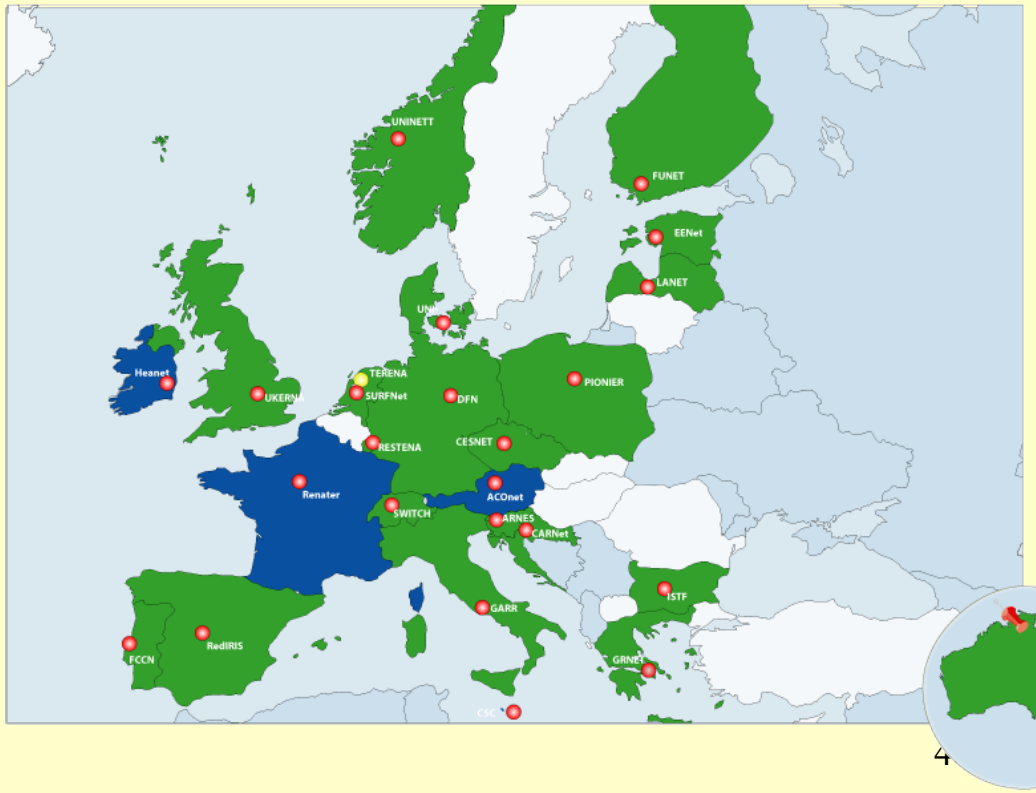
Az Eduroam (Education Roaming):

- **szolgáltatás a mobilitás és virtuális kutatói környezet megvalósításához**;
- **AutN infrastruktúra-** meglévő eszközökre, megoldásokra épül
- **vezetéknélküli hálózati hozzáférés**;
- **bizalmi szövetségen** alapuló autentikációs keretrendszer, amely a kutató hálózathoz hasonlóan hierarchikusan épül fel;
- **fejlesztési aktivitás** a GEANT2-ben (JRA5)
- Terena trademark:

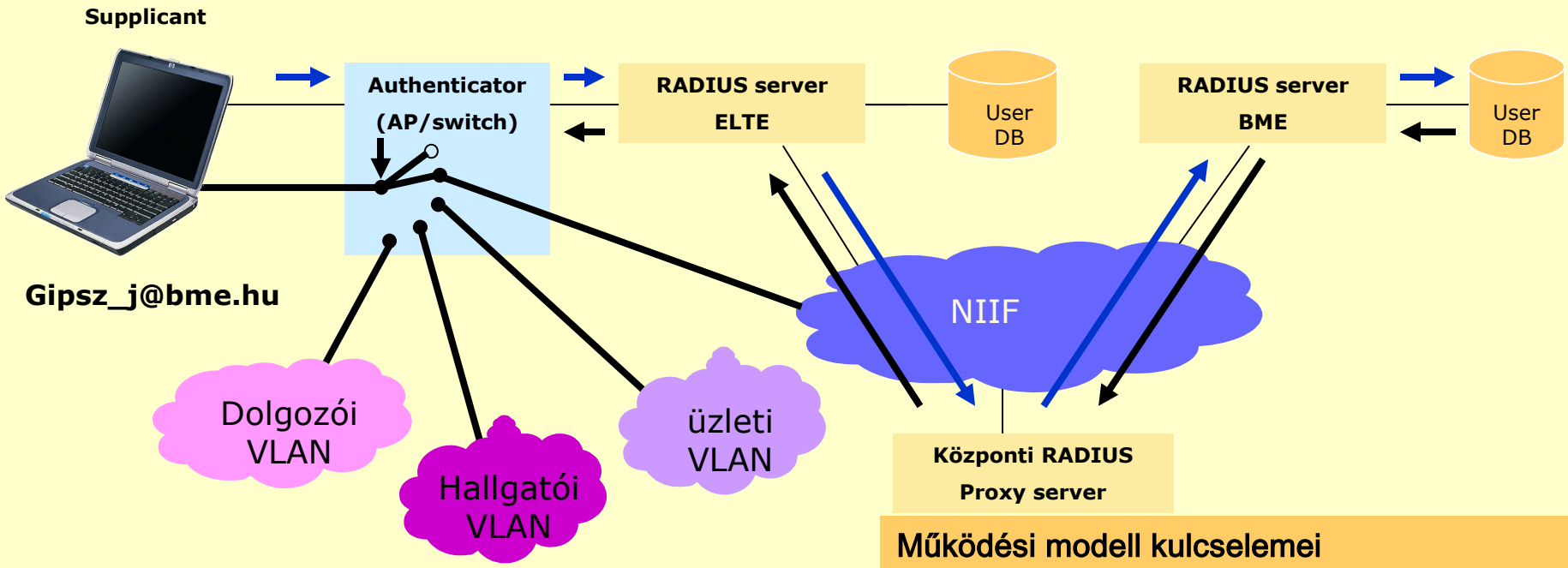
eduroam
Network roaming for higher education and research

Tagok, felhasználók

- Kutatói hálózati kezdeményezés (TF-Mobility), tagok kutatói hálózati intézmények. ~20 ország, ~400 intézmény
- Felhasználói a csatlakozó intézmények dolgozói, hallgatói
- Dinamikus bővülés
- Hierarchikus felépítés:
  - TERENA
  - Nemzeti kutatói szervezet
  - Tagintézmények
- Cél a globális lefedettség



Működési modell

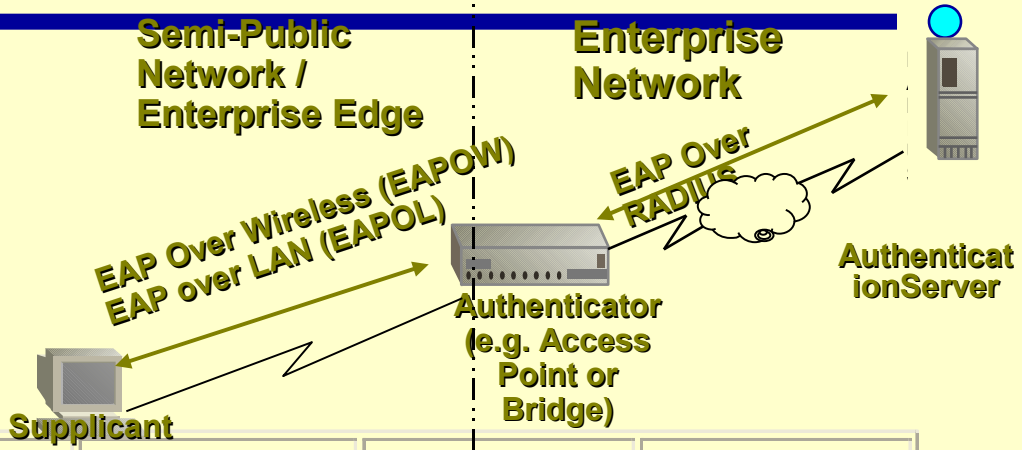


Működési modell kulcselemei

- 802.1x
- RADIUS hierarchia
- Bizalmi szövetség az intézmények között (megállapodások)
- Megfelelő azonosítók (SSID, uid)
- (VLAN kezelés)

Felhasznált technológiák

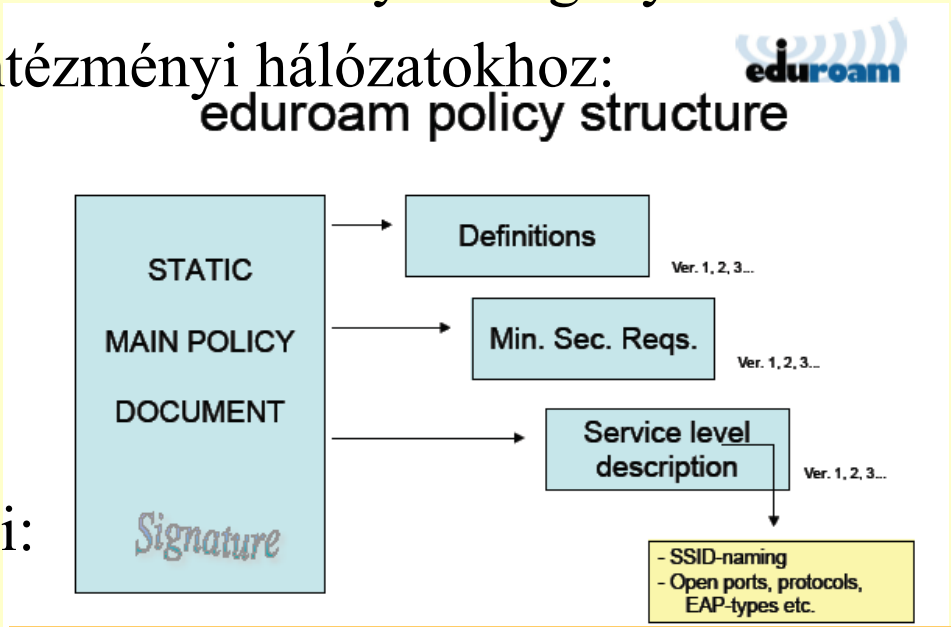
- 802.1x
- EAP (RFC 2284) – link layer
- RADIUS (proxy funkciók)
- WPA-TKIP/MIC,
- WPA2-/EAS-CCMP



	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Server Authentication	None	Password Hash	Public Key (Certificate)	Public Key (Certificate)	Public Key (Certificate)
Supplicant Authentication	Password Hash	Password Hash	Public Key (Certificate or Smart Card)	CHAP, PAP, MS-CHAP(v2), EAP	Any EAP, like EAP-MS-CHAPv2 or Public Key
Dynamic Key Delivery	No	Yes	Yes	Yes	Yes

Bizalmi szövetség

- Eduroam egy bizalmi szövetség a hálózati hozzáféréshez érdekében → megállapodásokat és szabályokat igényel
- Kölcsönös hozzáférés az intézményi hálózatokhoz:
  - rugalmasság
  - könnyű kezelhetőség
  - biztonság
  - nyomon követhetőség
- Eduroam federation szintjei:
  - Eduroam Secretariat
  - NREN
  - intézmény



Csatlakozáshoz szükséges:

- Minimum biztonsági követelmények teljesítése
- SLA követelmények teljesítése
- eduroam policy authority elfogadása
- Lehetséges szankciók elfogadása

Főbb követelmények

1. Megállapodás az NREN és az Eduroam szövetség között
2. Az NREN és a csatlakozó intézmények között aláírt megállapodás!

Főbb kitételek mindkét megállapodásban:

- Fogadó intézmény AUP-jének betartása
- Authentikációs szerver működtetése
- Biztonságos authentikáció (titkosított csatorna)
- Információ biztosítása a szolgáltatásról
- Tájékoztatás a biztonsági szintről
- Oktatást és szupportot az anyaintézmény nyújtja
- Authentikációs folyamat és hálózatelérés loggolása
- Biztonsági események jelentése

Egyéb bizalmi szövetségen alapuló AAI megoldások

- shibboleth.internet2.edu, www.a-select.org, www.igtf.org www.projectliberty.org, stb.
- Főbb kategorizálási attribútumok:
  - Mit fed le az AAA-ból: AuthN - AuthZ
  - Milyen erőforráshoz történő hozzáférést kezel: Hálózathoz - webes alkalmazásokhoz – alkalmazáshoz
- Két leginkább terjedő, bizalmi szövetségen alapúló megoldás összehasonlítása

Eduroam	**Shibbolet**
AuthN	AuthZ
Hálózati hozzáférés (wireless)	Alkalmazás hozzáférés
802.1x, Radius	SAML

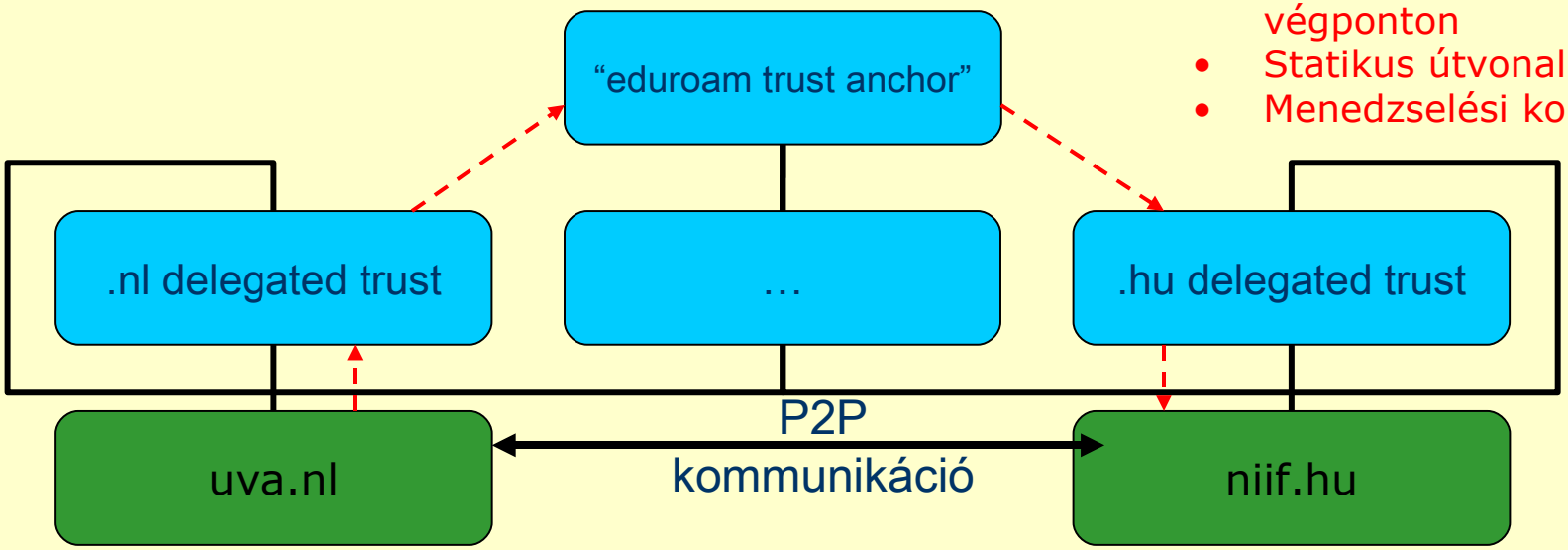
- Mindkét megoldást magába foglaló rendszerek megjelenése várható

Továbbfejlesztési irányok

- Az infrastruktúra menedzselése és monitorozása
- XML séma és adatbázis az eduroam hotspot-okról
- Azonosítók egységesítése (pl. SSID, ciphers):
  - **eduroam -**
  - **eduroam-wep -** dinamikus WEP kulcs
  - **eduroam-wpa -** WPA+TKIP,
  - **eduroam-wpa2 -** WPA2 (WPA+AES).
- Kis intézményeknek: eduroam-in-a-box
- eduroam kliens:
  - szabad forráskódú
  - több platformon elérhető
  - könnyen kezelhető

Továbbfejlesztési irányok

- az autentikációs folyamat függetlenítése bizalmi kapcsolatoktól



- AA forgalom átmegy valamennyi közbülső végponton
- Statikus útvonal
- Menedzselési korlátok

- Lehetséges megoldások: (Diameter, DNSsec, Radsec/DNSroam)

NIIF pilot és csatlakozás

- Cél: az NIIF és a hazai intézmények csatlakozása az Eduroam-hoz
- A csatlakozáshoz szükséges fejlesztések és adminisztratív feladok végrehajtása
- Pilot rendszer kiépítése az elkövetkező 3 hónapban pár intézmény bevonásával (BME, ELTE, NIIFI, SzTAKI), a minimális követelmények teljesítése.
- Weboldal elindítása - műszaki segédletek, policy dokumentumok, hot-spot információk