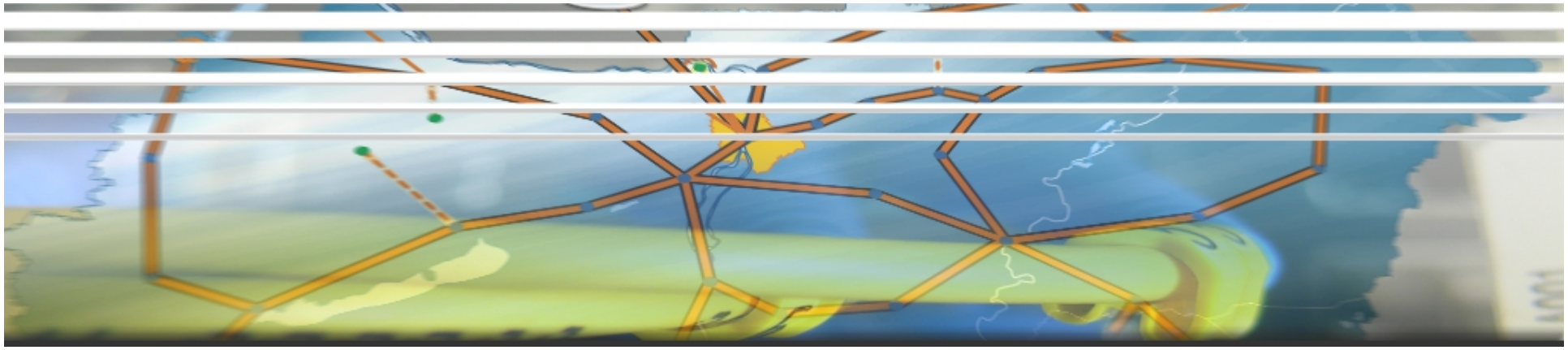
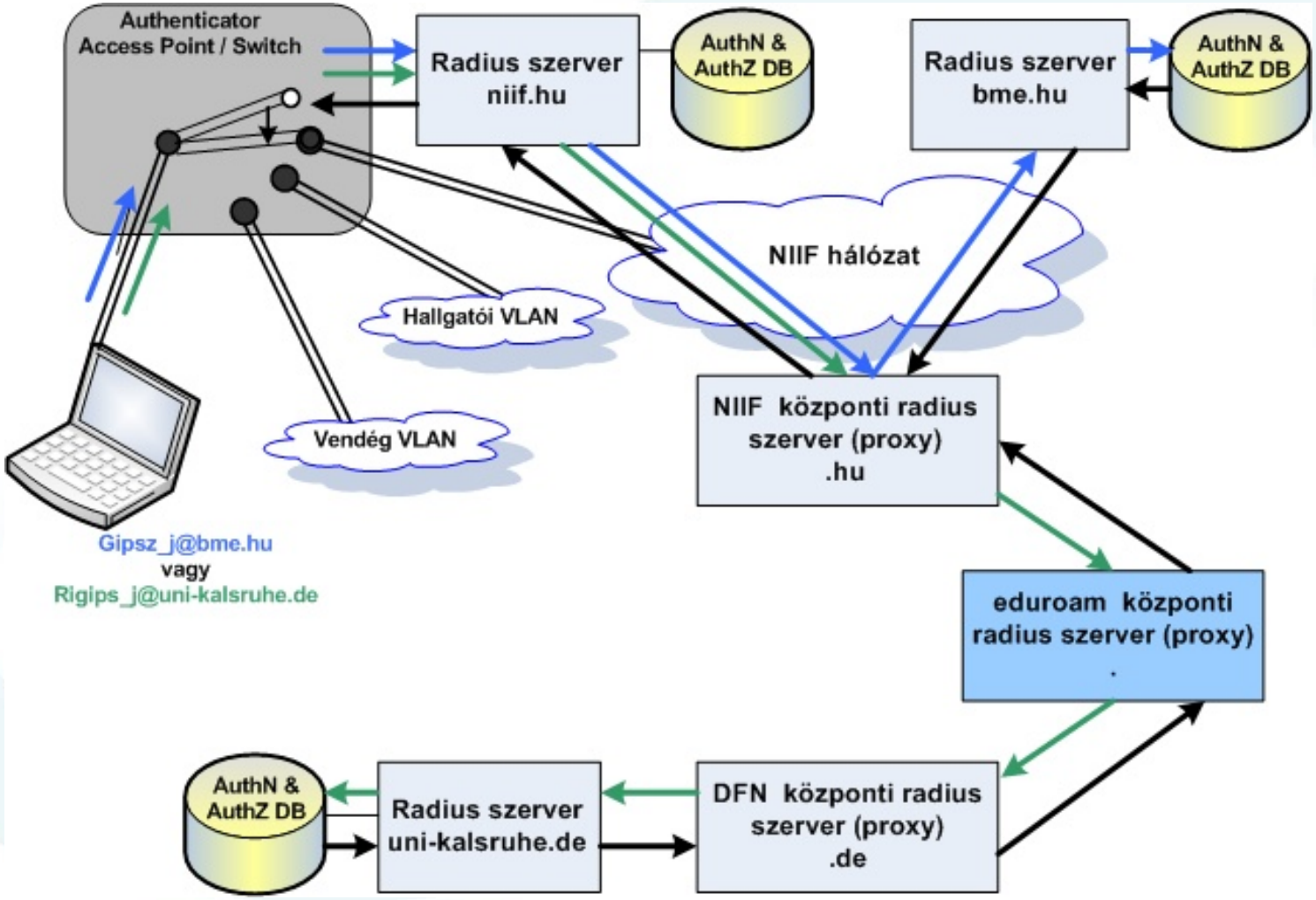
# Hogyan tovább eduroam?



Mohácsi János NIIF Intézet

HBONE Workshop 2013

# eduroam modell



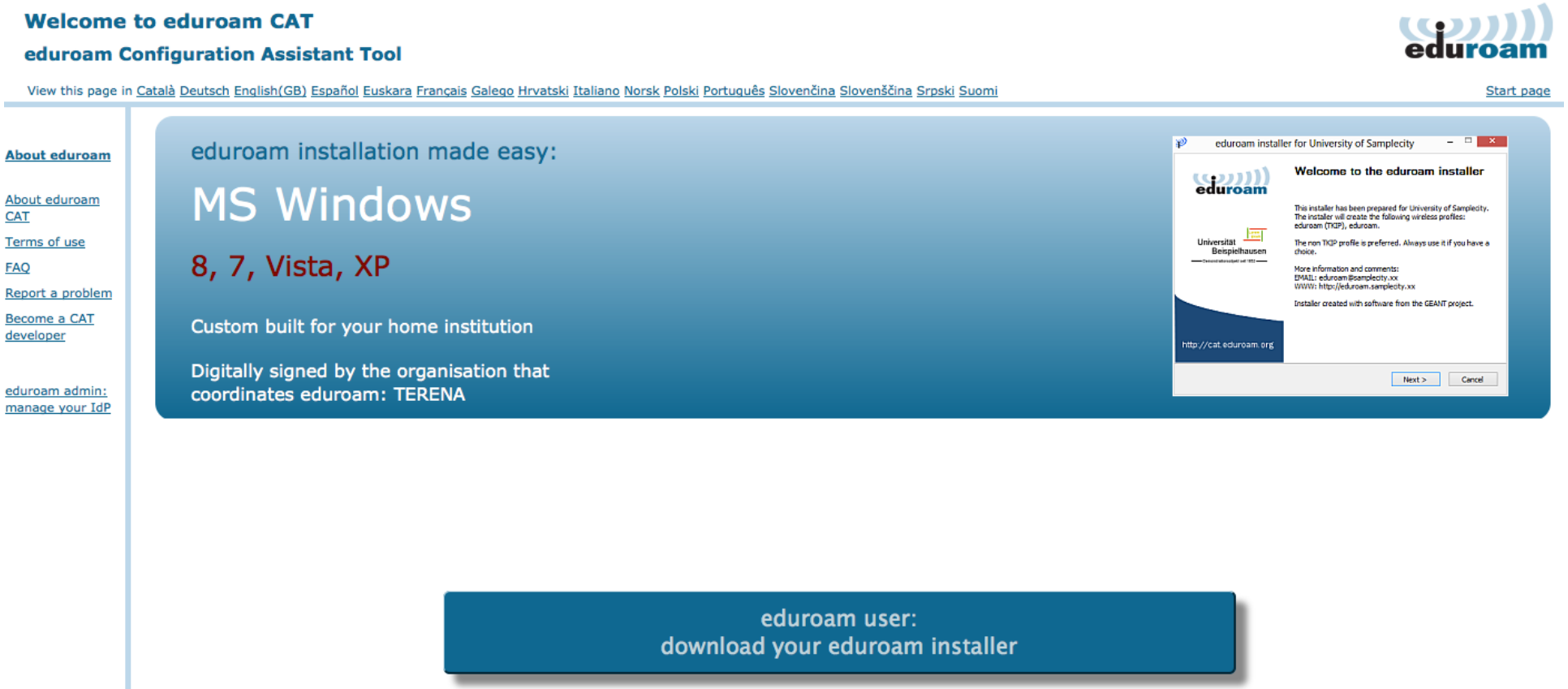
# Eduroam elterjedtség

# eduroam problémák- konfiguráció

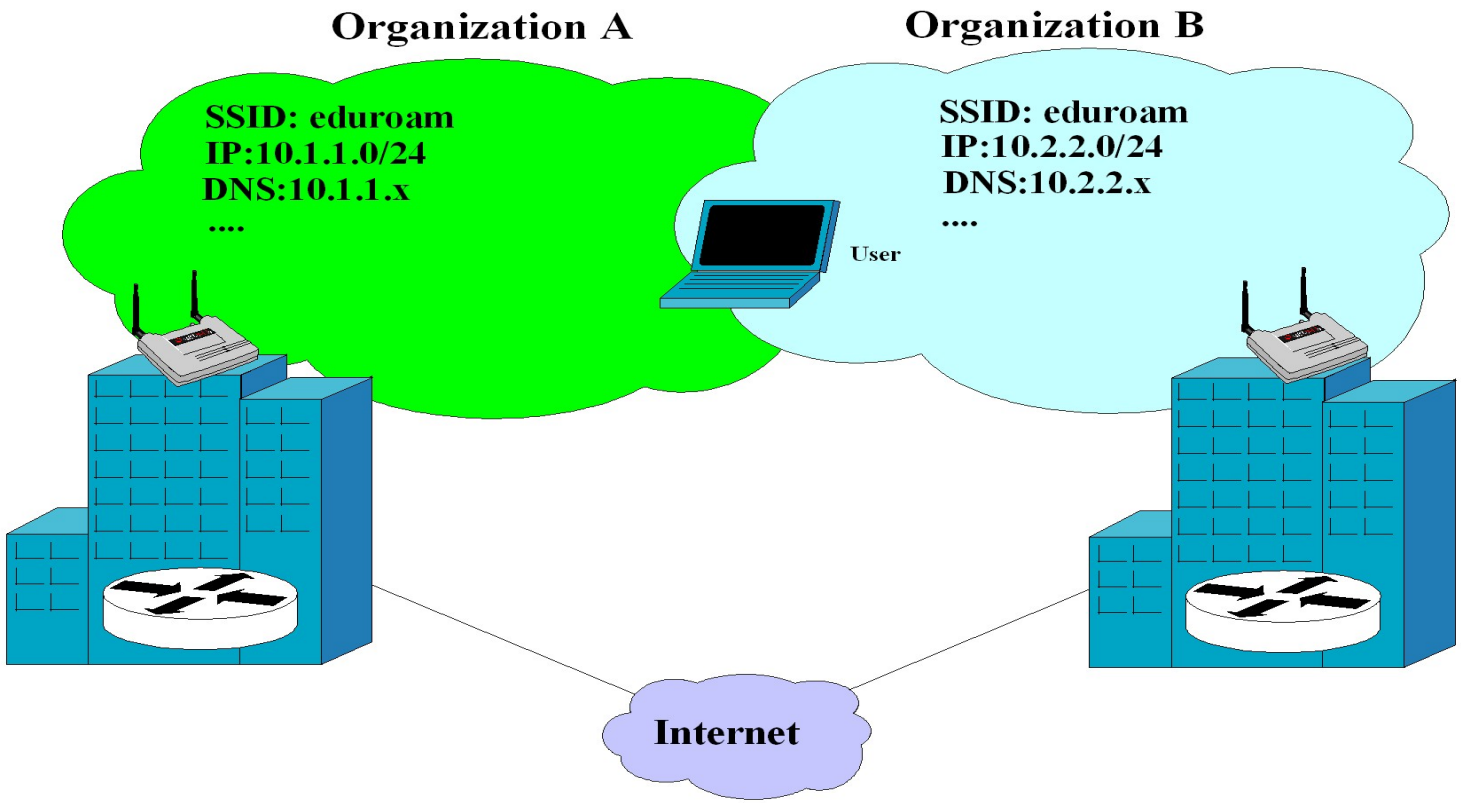
- Egyszer jól be kell állítani, utána működik
  - Milyen CA? EAP? szervertanúsítvány?
- Megoldás: eduroam CAT
  - Egyszerűsített automatikus kliens installáció
  - Intézmény specifikus információk elérhetők (logó, AUP, stb.)
  - Aláírt installer
- http://cat.eduroam.org
- Magyarítás hamarosan

# eduroam problémák- konfiguráció

- Egyszer jól be kell állítani, utána működik



# eduroam problémák – átlapolódó WIFI



# eduroam problémák – átlapolódó WIFI /2

- 1. Szabályzat:

"Overlapping IP-subnets with same SSID is known to be a problem. If this situation occurs the SSIDs of those institutions involved can be changed to 'eduroam-[inst]' (where [inst] is an easily understandable indication of institutions name). If this solution is applied the SSIDs MUST be broadcasted." -> NIIF eduroam ERSZ változtatás 3.2.6.8. pont

+ könnyű implementálni
+ le/fel csatlakozó kliens problémáját megoldja
- Transzparens roaming eltűnik, de van eduroam CAT támogatás

- 2. 802.11u – HS 2.0

# eduroam problémák – RC4 gyengeség

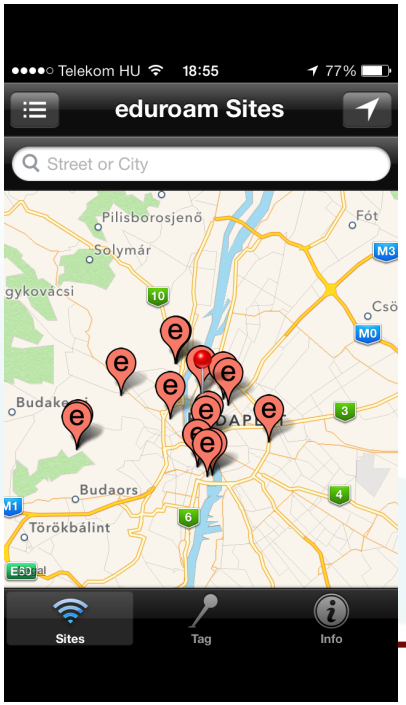
- RC4 és TKIP sebezhető
- Hacktivity 2012 konferencia:
  - Cracking WPA/WPA2 Personal + Enterprise for Fun and Profit
    - WEP broken – "WPA is an intermediate solution by Wi-Fi Alliance"
    - "WPA cracking – precalculation based SSID, passphrase for dicts" – then brute force
    - Catch-all honey pot for wireless clients, Hole 196 …
    - WPA Enterprise? – crackable
- AES és CCMP használandó ->WPA2-Enterprise
  - eduroam advisory 003 - nem lesz engedélyezett a TKIP!
  - -> NIIF eduroam ERSZ változtatás 3.2.6.5. és 3.2.6.6. pont
  - eduroam CAT nem fogja engedni a TKIP-et!

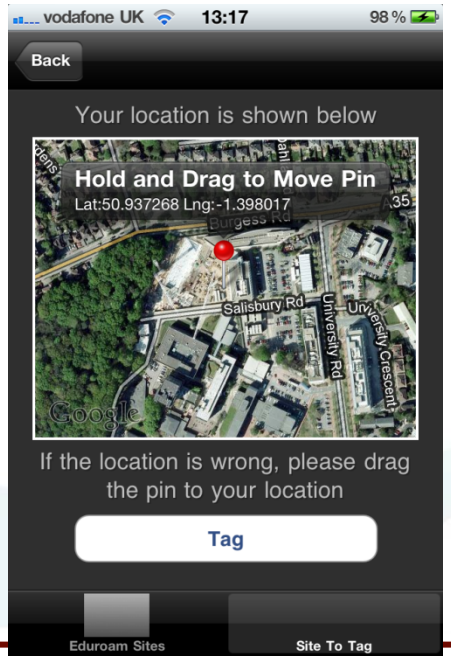
# eduroam problémák – esetleges beékelődés megelőzése

- Nem biztonságos, ha a supplicant-ek/kliensek úgy lettek konfigurálva, hogy minden tanúsítványt elfogadjanak:
  1. Szükséges az elfogadott gyökértanusítvány telepítése
  2. Szükséges a tanusított szervernév ellenőrzése
- Ha a fenti KÉT pont nem teljesül  a supplicant/kliens mindenféle jött-ment, hamisított szervernek megadja a hozzáférési kódjait….
- Szabályzat:
- “"6.3.2 Specifications and Operational Requirements: Identity Providers Adherence to the following specifications is REQUIRED [...] The server-side EAP credentials MUST be communicated to the user base, and end-user documentation needs to be precise enough to allow users the unique identification of their EAP server”
- -> NIIF eduroam ERSZ változtatás 3.1.1 pont kiegészítése

# Eduroam problémák – hol tudom használni?

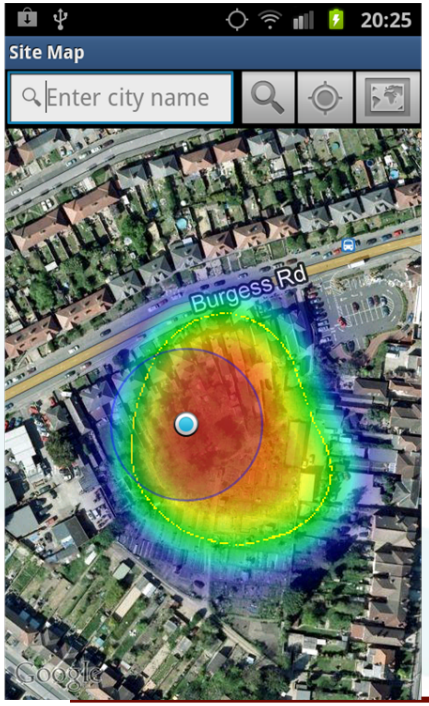
- iOS eduroam companion 2011 Decembere óta elérhető:
- https://itunes.apple.com/hu/app/eduroam-companion/id480611749

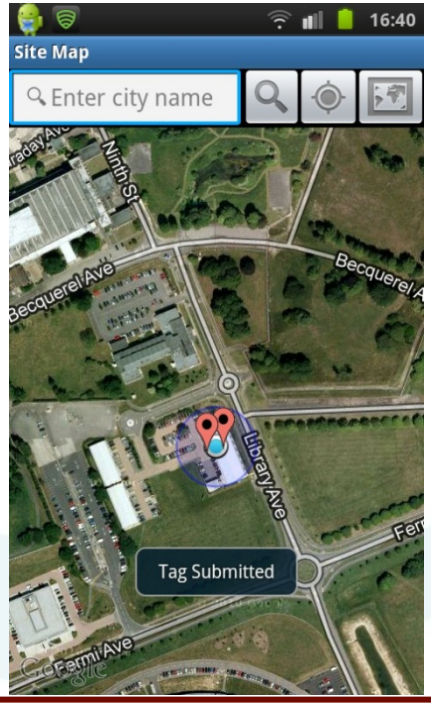



# eduroam problémák – hol tudom használni? /2

- Android verziója az eduroam companion –nak is elérhető Google app store 2012 május óta:
- https://play.google.com/store/apps/details?id=net.ja.android.eduroamcompanion



# eduroam szabályzat hiányosságok

- 802.11ac/ad/? nincsen benne – kell?
- AP-k GPS koordinátájának kötelező megadása legalább épület szintjén.
- A probléma esetén a kommunikációs útvonalak definiálása
- Radius attributum előírások a konföderációs szabályzatnak megfelelően
- Nyitandó portok/protokollok: IPSec, TCP/3128, TCP/8080
- eduroam “brand” kérdések
- RadSec lehetőségek

# Mi az a RadSec?

- Radius (EAP) protokoll tartalmának becsomagolása TCP-ben (SCTP-be)
- TCP transzport ? - megbízhatóság
  - UDP jó megoldás volt, amíg 1-2 csomag váltás volt szükséges a felhasználó azonosításhoz – EAP-nál több 10 csomag!
  - A Radius szomszéd "elérhetősége" nem egy becslésen alapulhat
- A RadSec peer-ek kölcsönössen azonosítják egymást és titkosítják a forgalmat egymás között TLS-el - biztonság
  - Nincsen szükség a gyenge shared secretre és statikus IP összerendelésre
- A shared secret-től és IP cím összerendelés hiénya lehetőv; teszi a RadSec peer dinamikus felfedezését – eduroam skálazható működtető hierarchiával

# RadSec kölcsönös azonosítás

- Az adott realm-hez tartozó authentikációs szerver IP címe (@niif.hu -> radius.ki.iif.hu)

  megoldás: NAPTR records DNS –ben “x-eduroam” szolgáltatásra
- Ellenőrzés, hogy a felderített host-ban meg lehet bízni – valós eduroam IdP

  megoldások:

  PKI – jelenleg ez működik -

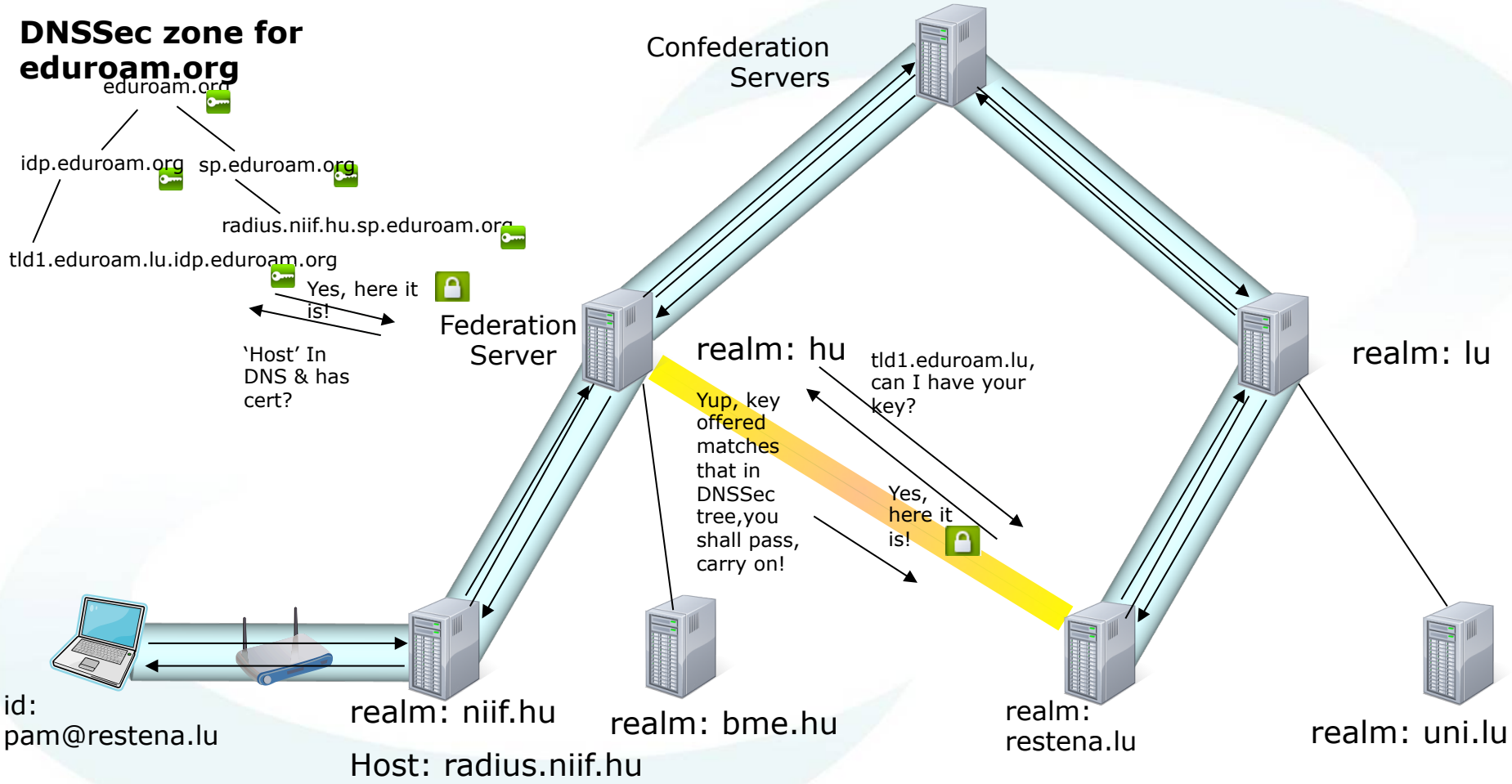
  PKI – nehéz üzemeltetni – egy CA?, több CA?, visszavonás?

  DANE?: RFC 6698 - DNS-based Authentication of Named Entities

  problémák az implementációval
- Kölcsönözös ellenőrzés

  megoldás: RFC6614 (RADIUS over TLS)

# eduroam DANE-el



# RadSec implementációk

- OSC's “Radiator”
- Stig Venaas (UNINETT) radsecproxy
- FreeRADIUS 3.0
- LanCOM AP

- Semmelyik nem implementálja a DANE-t

- NIIF pilot indítása hamarosan…

# Köszönöm!

Kérdések? eduroam@niif.hu