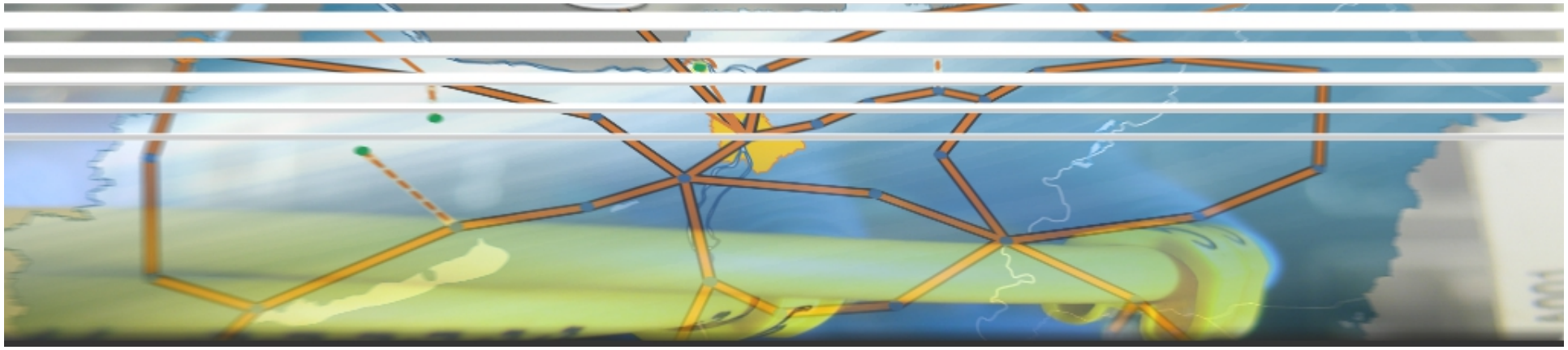
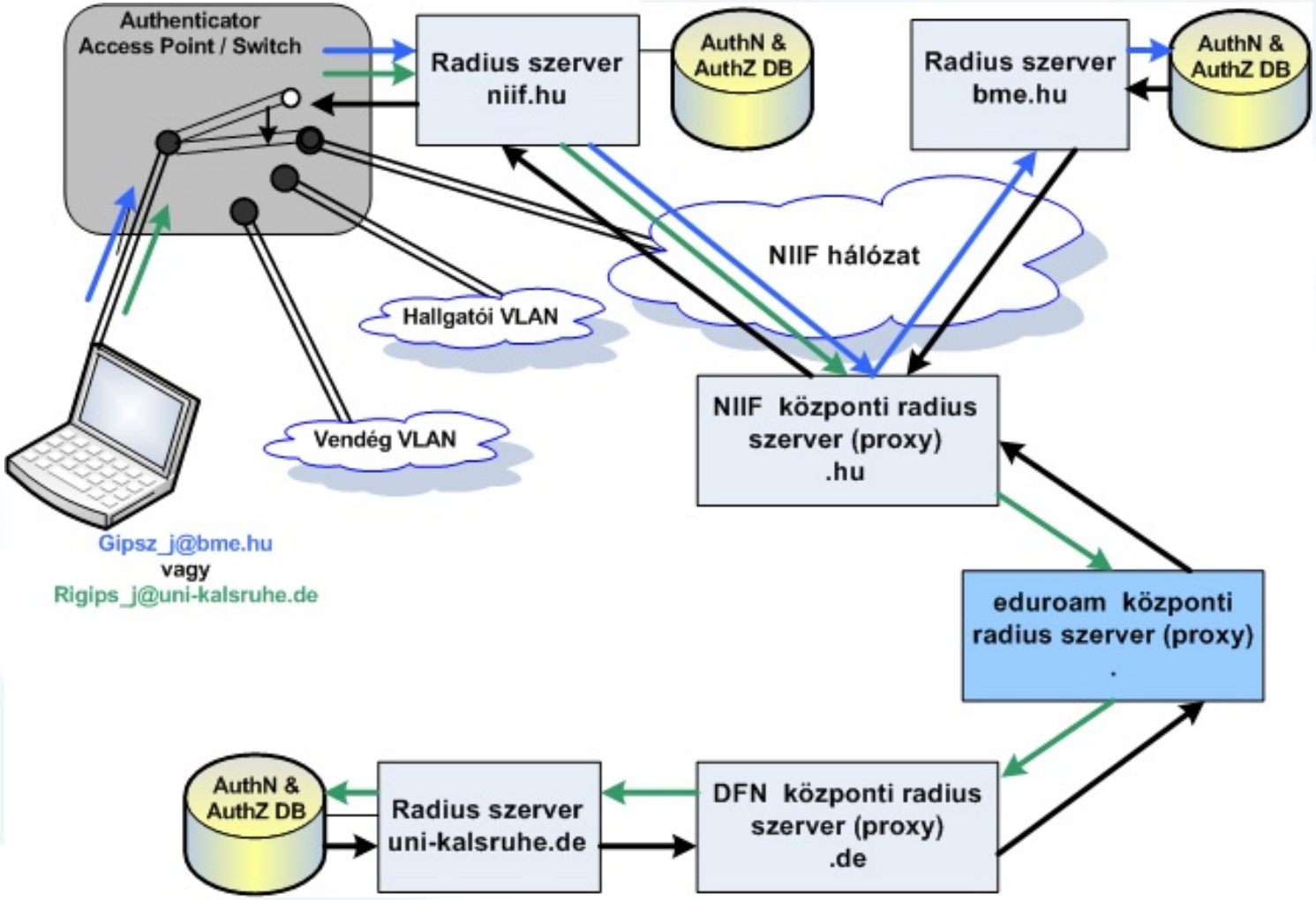
Eduroam változások
- fejlesztések, fejlődések



Mohácsi János NIIF Intézet

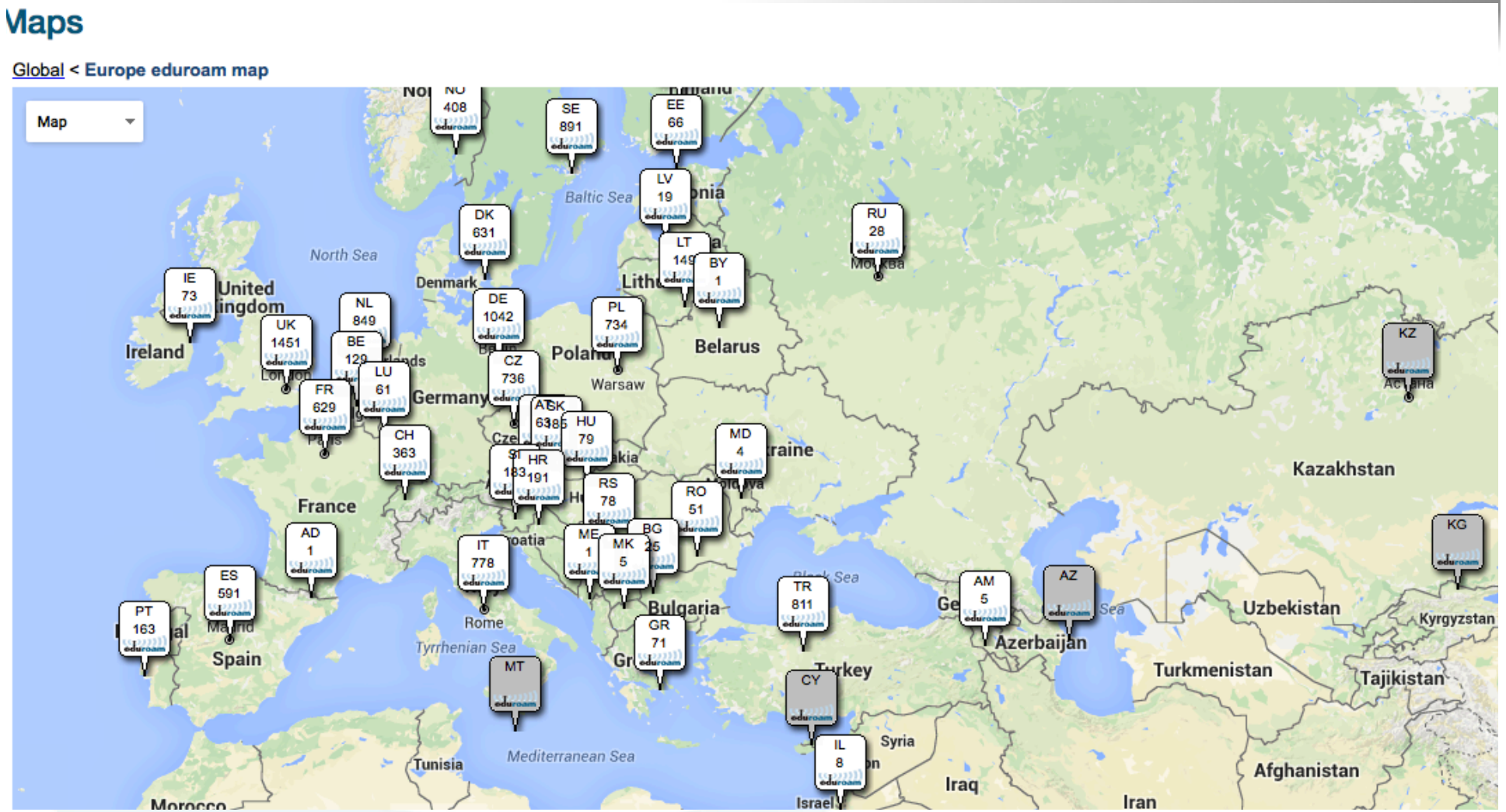
HBONE Workshop 2015

eduroam modell



Eduroam elterjedtség -2013

Eduroam elterjedtség – csak Európa-2015



Forrás: monitor.eduroam.org

Eduroam elterjedtség – csak Magyarország-2015

- Hamarosan több mint 300 eduroam SP helyszín – kész csak nincsen az eduroam adatbázisba felvéve
  - ~ 300 Sulinetes iskola
    - NIIF által menedzselt eduroam SP (AP) és eduroam IdP (Radius+felhasználói adatbázis)
    - Intézmény felelős a felhasználói adatbázis frissentartásáért – felhasználó menedzsment a dashboardba integrálva – tömeges felhasználó kezeléssel -> eduID - (FeaaS)
    - Felügyelt Wifi + eduID szolgáltatás
- Hamarosan további ~ 1000 helyszín

Eduroam elterjedtség – csak Magyarország-2015

- Hamarosan több mi
  helyszín – kész csak
  adatbázisba felvéve
  - ~ 300 Sulinetes iskol
    - NIIF által menedzselt
      IdP (Radius+felhaszná
    - Intézmény felelős a fe
      frissentartásáért – felh
      dashboardba integrálva – tömeges felhasználó kezeléssel -> eduID - (FeaaS)
    - Felügyelt Wifi + eduID szolgáltatás

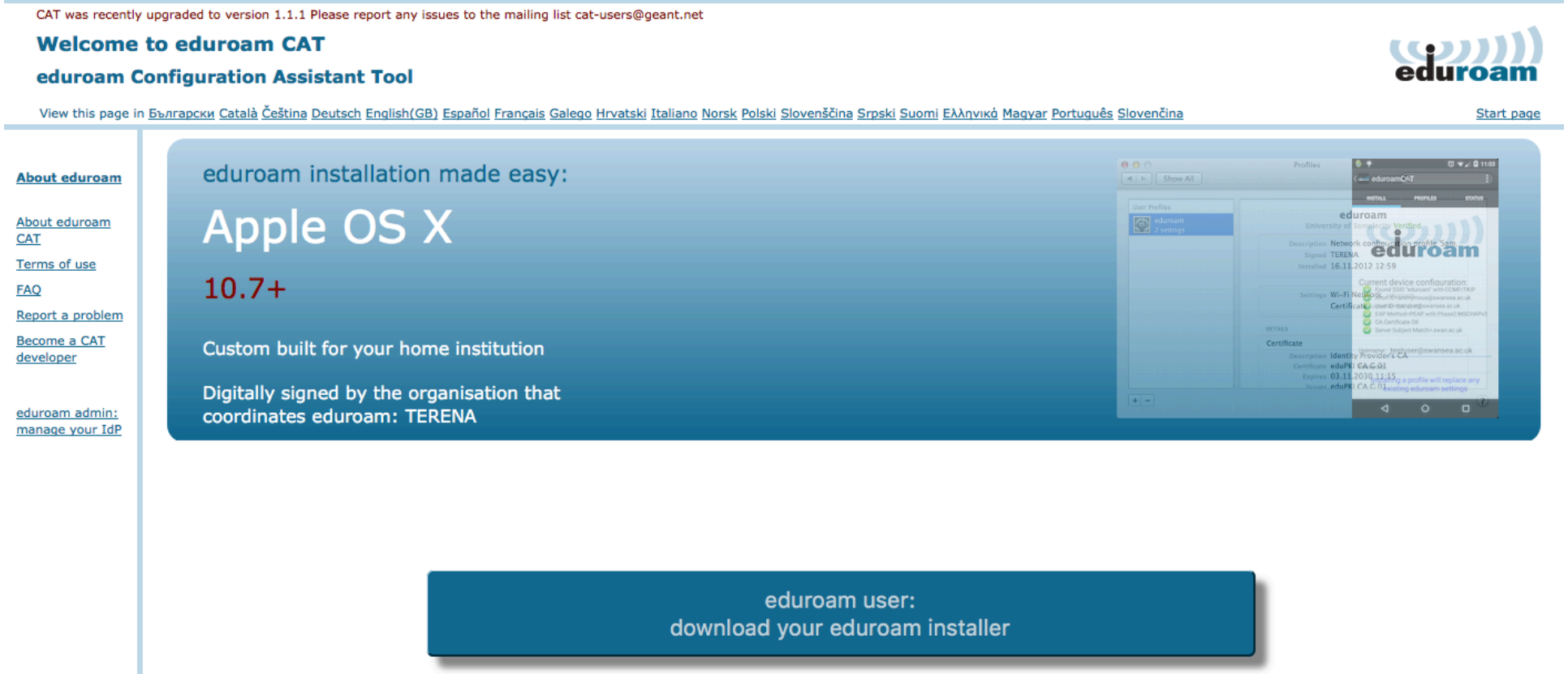
- Hamarosan további ~ 1000 helyszín

Eduroam fejlesztések – eduroam CAT

- 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 kliens oldalon kész
- 13 intézmény a 34 eduroam tagból

Eduroam fejlesztések – eduroam CAT

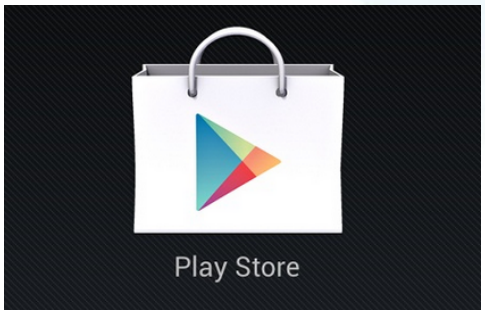
- Egyszer jól be kell állítani, utána működik



eduroamCAT – Android támogatás

eduroam CAT: Configuration Assistance Tool

- Felhasználó letölti az IdP-re jellemző speciális konfiguráló eszközt



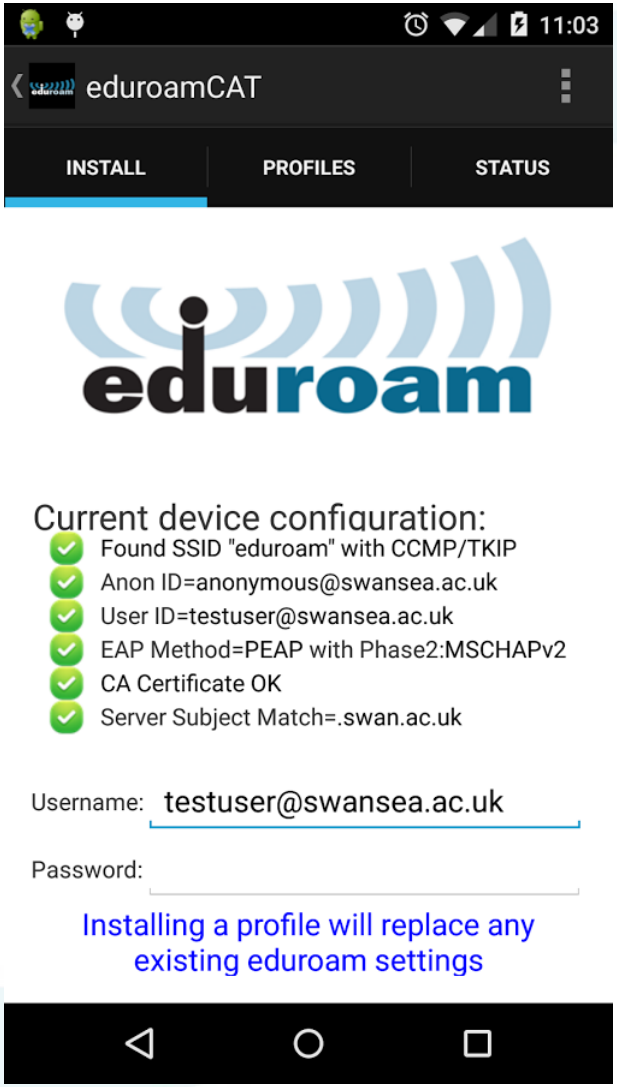
- Probléma: Android Play Store alkalmazás modell
  - Android alkalmazásokat csak valamilyen alkalmazás boltból lehet egyszerűen telepíteni
  - Alkalmazás bolt (Play Store), de nem volna célszerű ezernyi hasonló alkalmazás
  - Egy eduroam CAT app amely testre szabható minden IdP-re

Eduroam CAT – Android támogatás /2

- Megoldás: **EAPConfig file**
  - Szabványosított formátum EAP konfigurációs információk terítésére
  - IETF Internet Draft, GEANT SENSE OpenCall
  - XML formátum, amelyet az app detektál és feldolgoz
- EAPConfig tartalmazza:
  - IdP információk (tanúsítvány etc)
  - EAP metódus információk
  - Helpdesk / támogatási információk
- App – Andorid 4.3+

  https://play.google.com/store/apps/details?id=uk.ac.swansea.eduroamcat
- Android – csak akkor biztonságos, ha privát CA-t használ az IdP

Eduroam CAT – Android támogatás /3



eduroamCAT – Windows támogatás

- Windows XP – kikerült!
- Windows Vista és Windows 7 nem támogatja az EAP/TTLS-t
  - Korábban a CAT-ben SecureW2 – GPL változat
    - Jogi problémák
  - Arneslink – GPL
    - Jelenleg sajnos tartalmaz SecureW2 kódot (<20%)
    - Következő változat – mikor?
- Windows Phone 8.x – csak akkor biztonságos, ha privát CA-t használ az IdP

Ellenörző eszközök

- EAPlab – https://eaplab.supplicants.net
  - GEANT projekt SENSE OpenCall eredménye
  - EAP teszt környezet eszközök, supplicant tesztelésére

- eduroam CAT (1.1) RADIUS tesztek
  - eduroam CAT adminisztrációs interfészének része
  - Alapvető radius szerver konfigurációs hibákat képes jelezni

EAPlab

- one proxy server at the front
- server routes packets to back-end servers
- routing is realm-based and is directed by the UI and the EAPlab database

CAT RADIUS tests – test through the eduroam infrastructure

- connection tests are run from the eduroam root servers
- fake user credentials are used
- server-provided information, mainly certificate information is studied and compared against the CAT profile settings
- many certificate imperfections can be spotted

Eduroam, TLS 1.2 és egyebek

- Mi az a TLS 1.2?
  - RFC5246
    - TLS 1.1 + MD5/SHA1 -> SHA256
    - Jobb hash és aláírási algoritmus választás
    - AES GCM és CCM mód titkosítás és javított CBC mód
- Kliensek haladnak a korral – megkövetelik a TLS 1.2-őt
  - wpa_supplicant2.4 - default beállítás - Linux
  - Android 6.0 (Marshmallow)
  - IOS 9 beta és OS X El Captain beta – a végleges már nem
  - Windows 10 phone?
- IOS 9 megköveteli a >1024 DH kulcsot

Eduroam és TLS 1.2

- Miért baj, ha erős a biztonság?
  - A radius IdP-nek is támogatnia kell a TLS 1.2-őt!
    - FreeRADIUS2
      - <2.2.6 - nincsen TLS1.2 egyeztetés -> támogatás
      - 2.2.6 and 2.2.7 – van TLS1.2 egyeztetés de nincsen támogatás
      - 2.2.9 vagy 2.2.10 (openssl 1.0.2) – jól működő
    - FreeRADIUS3
      - <3.0.6 - nincsen TLS1.2 egyeztetés -> támogatás
      - 3.0.6 – 3.0.9 – van TLS1.2 egyeztetés de nincsen támogatás
      - 3.0.10 vagy 3.0.10 (openssl 1.0.2) – jól működő
    - Microsoft NPS
      - https://technet.microsoft.com/en-us/library/security/2977292.aspx and https://support.microsoft.com/en-us/kb/2977292

Köszönöm a figyelmet!

Kérdések? eduroam@niif.hu