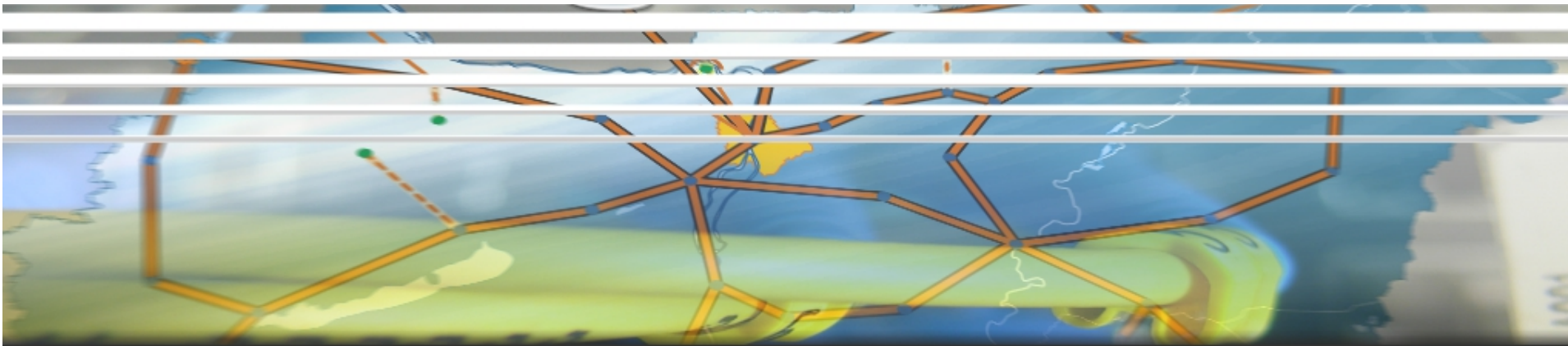


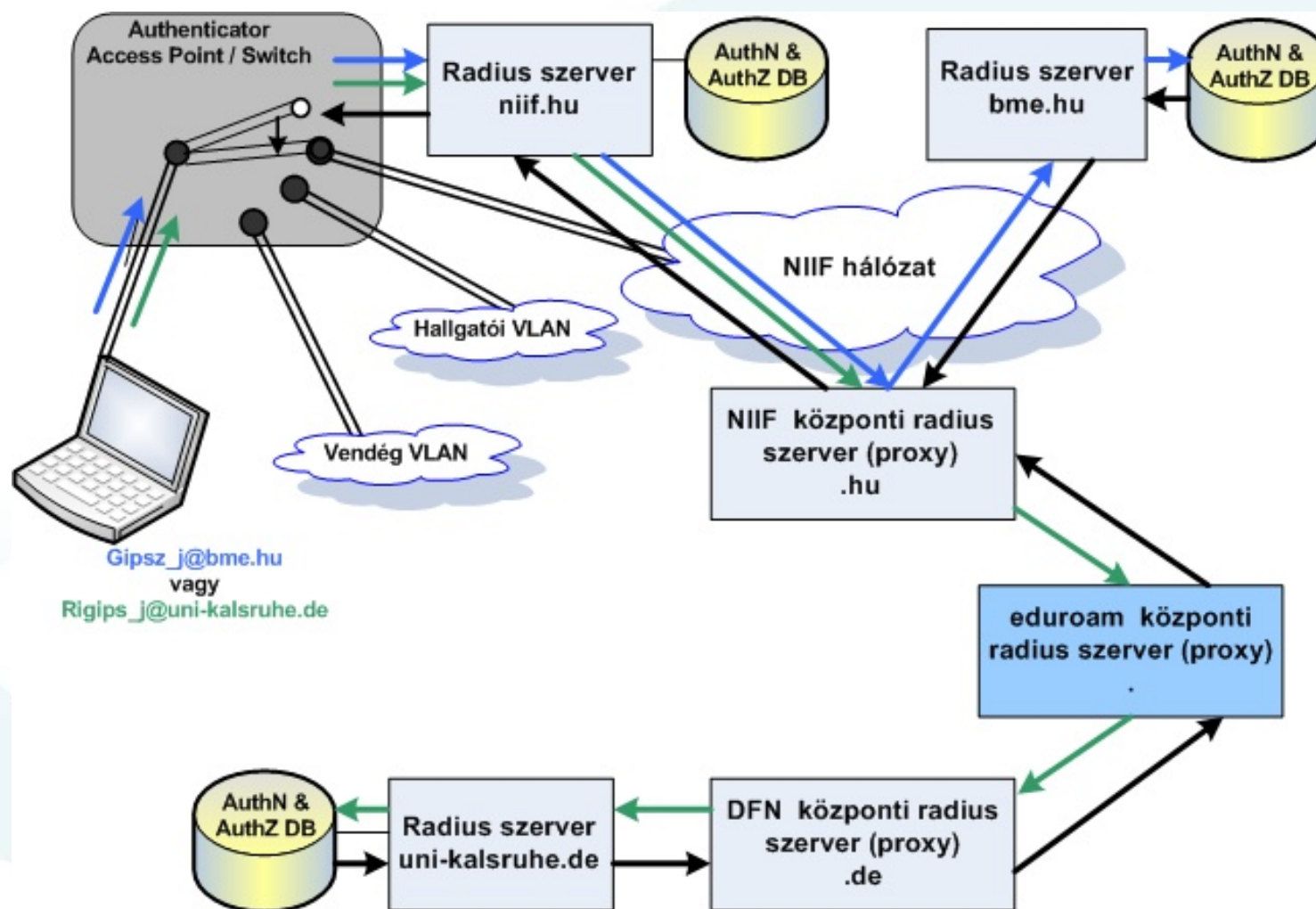
Eduroam változások **- fejlesztések, fejlődések**



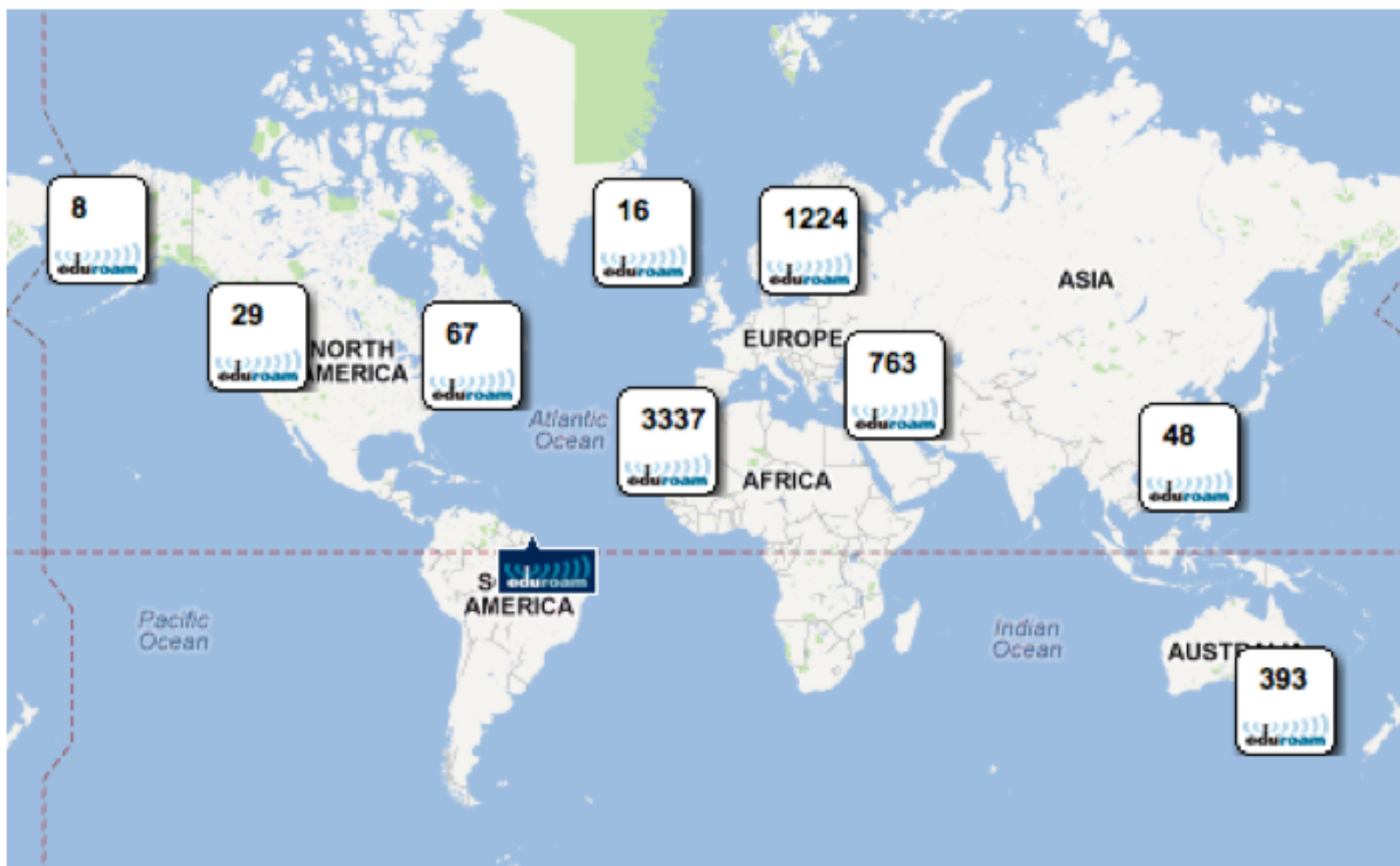
Mohácsi János NIIF Intézet
HBONE Workshop 2015



eduroam modell



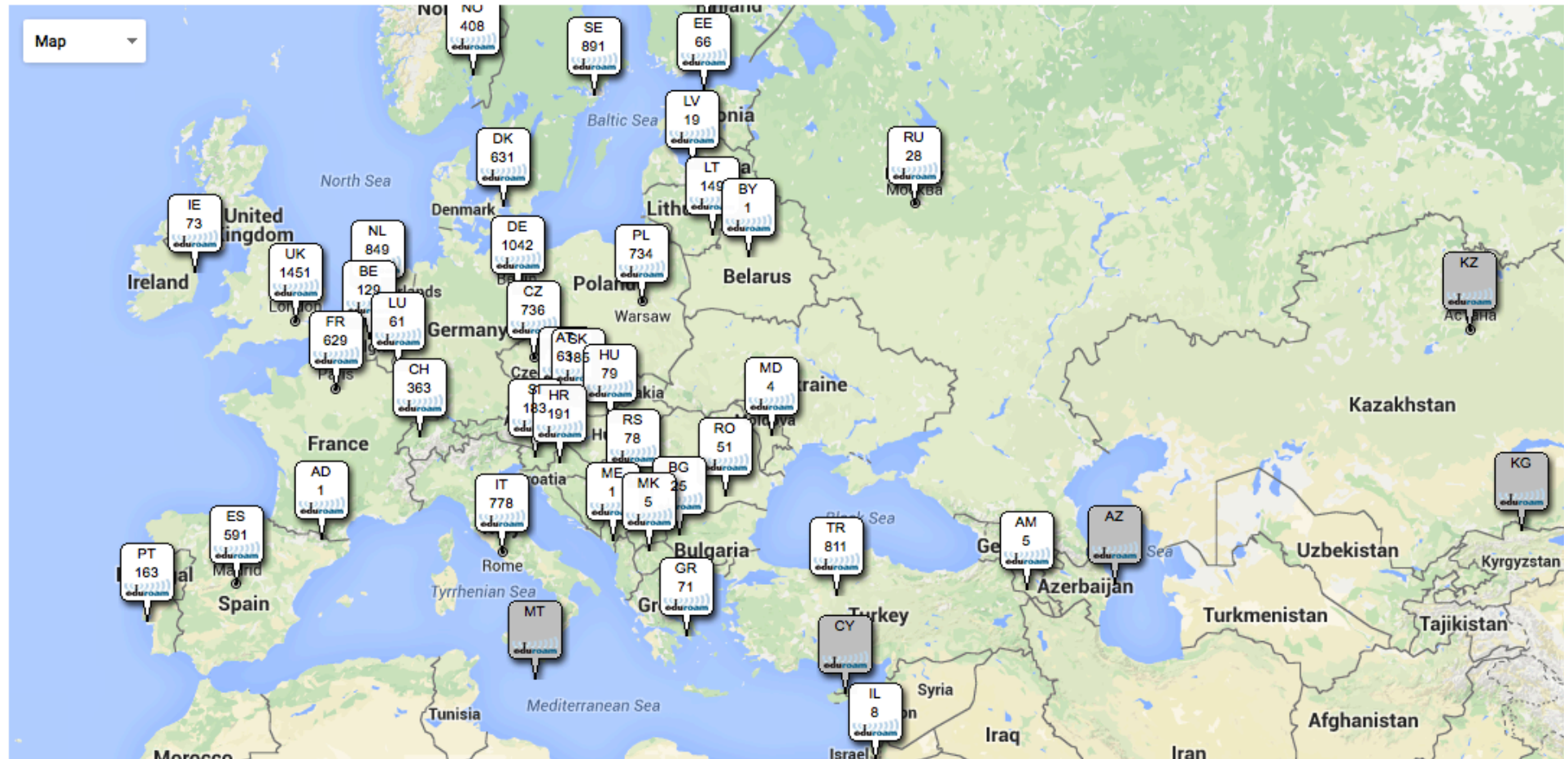
Eduroam elterjedtség -2013



Eduroam elterjedtség – csak Európa-2015

Maps

Global < Europe eduroam map



Forrás: monitor.eduroam.org

eduroam változások HBONE WS2015

Eduroam elterjedtség – csak Magyarország-2015

- Hamarosan több mint 300 eduroam SP helyszín – kész csak nincsen az eduroam adatbázisba felvéve
 - ~ 300 Sulinetes iskola
 - NIIF által menedzselte 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 mint 1000 helyszín – kész csak az adatbázisba felvéve
 - ~ 300 Sulinetes iskola
 - NIIF által menedzselte IdP (Radius+felhasználó)
 - Intézmény felelős a felújításért – felújítás 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

CAT was recently upgraded to version 1.1.1. Please report any issues to the mailing list cat-users@geant.net

Welcome to eduroam CAT

eduroam Configuration Assistant Tool



View this page in [Български](#) [Català](#) [Čeština](#) [Deutsch](#) [English\(GB\)](#) [Español](#) [Français](#) [Galego](#) [Hrvatski](#) [Italiano](#) [Norsk](#) [Polski](#) [Slovenščina](#) [Srpski](#) [Suomi](#) [Ελληνικό](#) [Magyar](#) [Português](#) [Slovenčina](#)

[Start page](#)

[About eduroam](#)

[About eduroam
CAT](#)

[Terms of use](#)

[FAQ](#)

[Report a problem](#)

[Become a CAT
developer](#)

[eduroam admin:
manage your IdP](#)

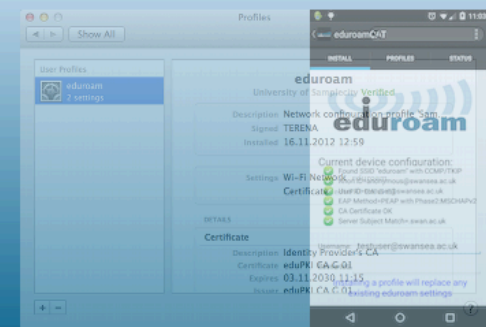
eduroam installation made easy:

Apple OS X

10.7+

Custom built for your home institution

Digitally signed by the organisation that
coordinates eduroam: TERENA



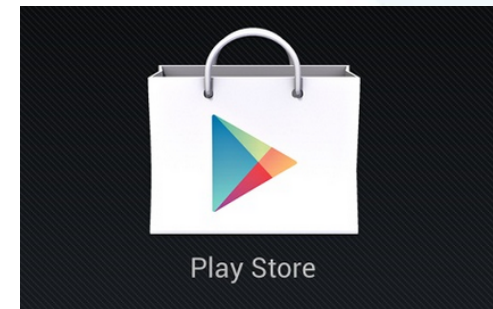
eduroam user:
download your eduroam installer

eduroam változások HBONE WS2015

eduroamCAT – Android támogatás

eduroam CAT: Configuration Assistance Tool

- Felhasználó letölti az IdP-re jellemző speciális konfiguráló eszközt

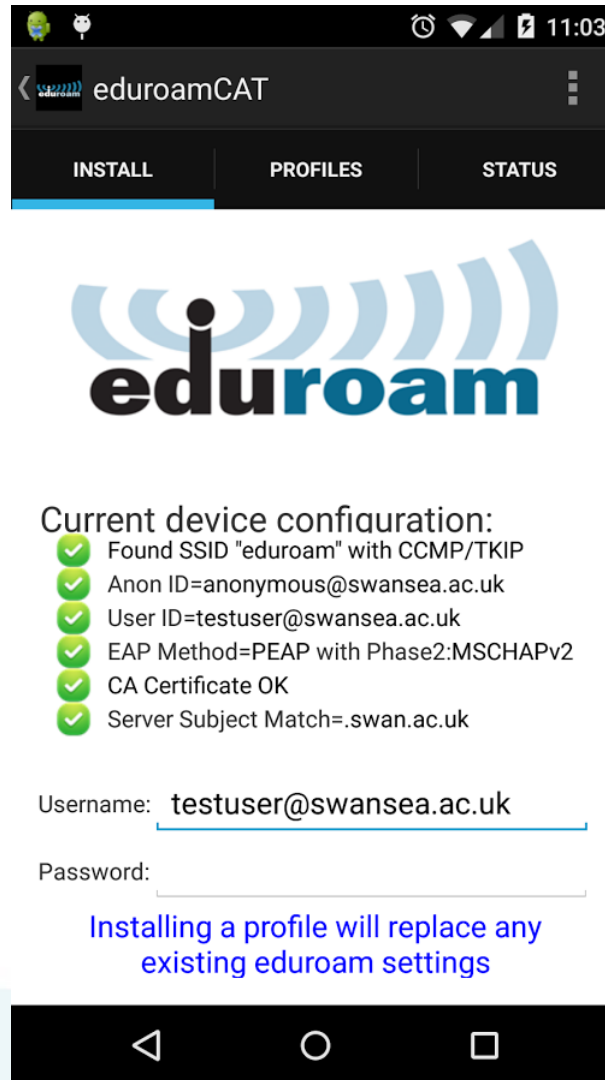


- **Probléma:** Android Play Store alkalmazás modell
 - Android alkalmazásokat csak valamilyen alkalmazás boltból lehet egyszerűen telepíteni
 - Alkalmazás bolt (Play Store), de nem volna célszerű ezernyi hasonló alkalmazás
 - Egy eduroam CAT app amely testre szabható minden IdP-re

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 – Android 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

Ellenőrző eszközök

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

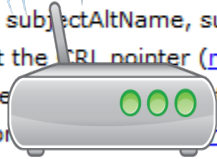
- eduroam CAT (1.1) RADIUS tesztek
 - eduroam CAT adminisztrációs interfészének része
 - Alapvető radius szerver konfigurációs hibákat képes jelezni



Configuration variants:

These variants will allow you to test the supplicant behaviour when something unexpected or badly configured happens.

- default configuration ([more info](#)) ([device test comments](#))
- immediate Access-Reject ([more info](#)) ([device test comments](#))
- Access-Reject after EAP conversation (default CA) ([more info](#)) ([device test comments](#))
- No reply ([more info](#)) ([device test comments](#))
- No EAP match ([more info](#)) ([device test comments](#))
- default CA, correct name in the subject, no subjectAltName ([more info](#)) ([device test comments](#))
- default CA, different name in the subject, no subjectAltName ([more info](#)) ([device test comments](#))
- default CA, different name in the subject, correct name in subjectAltName ([more info](#)) ([device test comments](#))
- default CA, correct name in the subject, different name in subjectAltName ([more info](#)) ([device test comments](#))
- default CA, correct name in subjectAltName, subject empty ([more info](#)) ([device test comments](#))
- default CA, different name in subjectAltName, subject empty ([more info](#)) ([device test comments](#))
- default CA, certificate without the URL pointer ([more info](#)) ([device test comments](#))
- default CA, no CA-FALSE in server extensions ([more info](#)) ([device test comments](#))
- default CA, certificate listed on server ([more info](#)) ([device test comments](#))
- default CA, expired certificate ([more info](#)) ([device test comments](#))
- Server sending root CA cert ([more info](#)) ([device test comments](#))
- Server cert signed with SHA-1 ([more info](#)) ([device test comments](#))
- certificate from another CA ([more info](#)) ([device test comments](#))



- 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

Realm testing for: umk.pl

DNS checks **Static connectivity tests** Dynamic connectivity tests Live login tests

[Repeat static connectivity tests](#)

STATIC connectivity tests

This check sends a request for the realm through various entry points of the eduroam infrastructure. The request will contain the 'Operator-Name' attribute, and will be larger than 1500 Bytes to catch two common configuration problems. Since we don't have actual credentials for the realm, we can't authenticate successfully - so the expected outcome is to get an Access-Reject after having gone through an EAP conversation.

Testing from: eduroamTL dk

i Connected to radius1.umk.pl.
elapsed time: 1356 ms.

Test partially successful: a bidirectional RADIUS conversation with multiple round-trips was carried out, and ended in an Access-Reject as planned. Some properties of the connection attempt were sub-optimal; the list is below.

i The certificate chain includes the root CA certificate. This does not serve any useful purpose but inflates the packet exchange, possibly leading to more round-trips and thus slower authentication.
[show server certificate details»](#)

Testing from: eduroamTL nl

i Connected to radius1.umk.pl.
elapsed time: 1585 ms.

Test partially successful: a bidirectional RADIUS conversation with multiple round-trips was carried out, and ended in an Access-Reject as planned. Some properties of the connection attempt were sub-optimal; the list is below.

i The certificate chain includes the root CA certificate. This does not serve any useful purpose but inflates the packet exchange, possibly leading to more round-trips and thus slower authentication.
[show server certificate details»](#)

[Return to dashboard](#)

Eduroam, TLS 1.2 és egyéb

- 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

