Hogyan tovább eduroam?

HBONE workshop 2022

Mohácsi János - T&I szolgáltatás felelős nemzetközi kapcsolatok vezető

2022 május 26

KIFÜ

Áttekintés

- Múlt
- WiFi6E – lehetséges problémak – eduroam szempontok
- Eduroam CAT hiányok - Menedzselt eduroam IdP – geteduroam
- Publikus vagy Privát tanúsítvány
- Openssl 3.0
- Openroaming
- Kérdőív
- Összefoglalás

Előző eduroam előadások

- 2007 Networkshop – Tutamen et simplicitas – eduroam bevezető
- 2009 Hbone Workshop – eduroam konfigurációs workshop
- 2015 Hbone workshop - Eduroam változások - fejlesztések, fejlődések
- 2016 Networkshop -Hogyan lett NIIFI Magyarország egyik legnagyobb Wifi szolgáltatója - Menedzselt eduroam IdP bevezetése az iskolákban
- 2019 Diákháló menedzselt eduroam IdP
- Networkshop tutorialok 2007-2009 – Jákó Andrással közösen

KIFÜ WiFi 6 is simply WiFi 6 at 6GHz (almost)

- WiFi6E is legal on the UNII-5 band in EU since 2021 (only 500 Mhz)
- WiFi at 6GHz is only for WiFi6E (until WiFi7 comes)
- Pros:
  - No legacy (no 802.11n / ac)
  - WiFi6 requires WPA3 support
  - No hassle with DFS as at 5GHz
  - E.I.R.P per MHz instead of full channel width
  - And above all 24 new channels to run on
- "Disadvantages"
  - Still few clients that support WiFi6E (Apple)
  - "Only" 24 channels instead of the 59 in the US
  - Where are the WiFi tools?

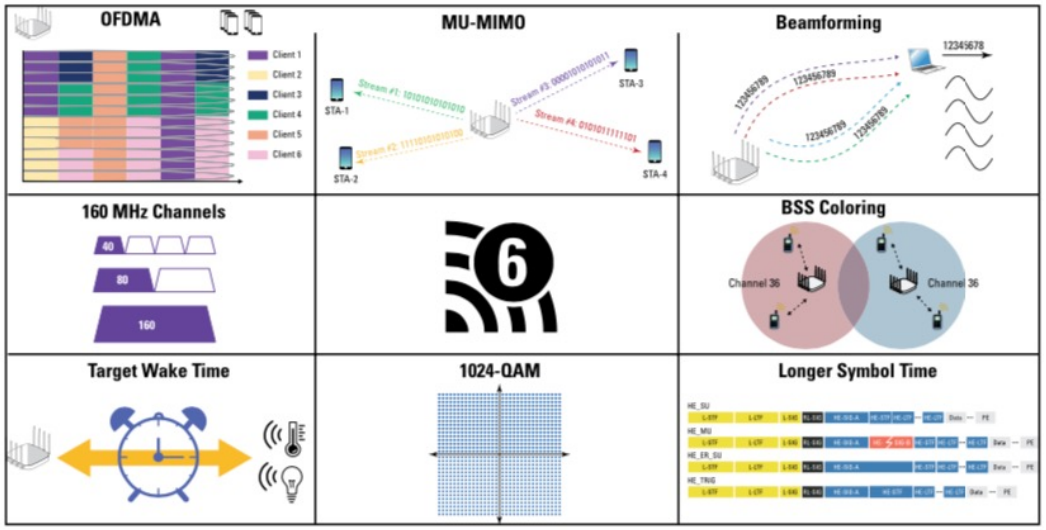
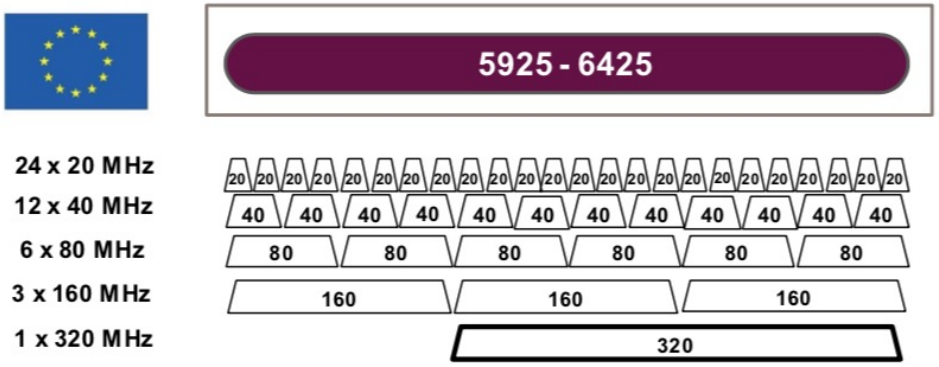
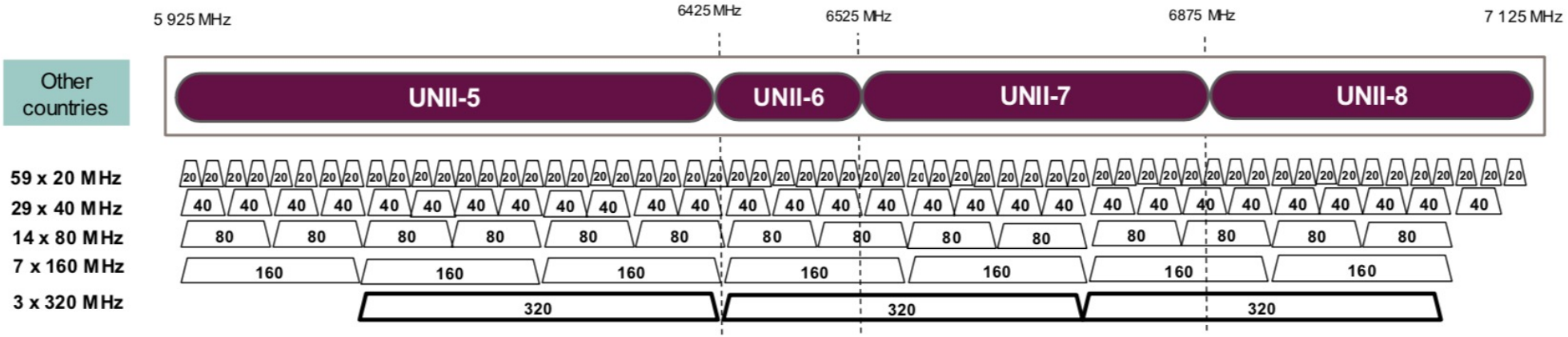


FIGURE 1-4: Wi-Fi 6 capabilities overview.

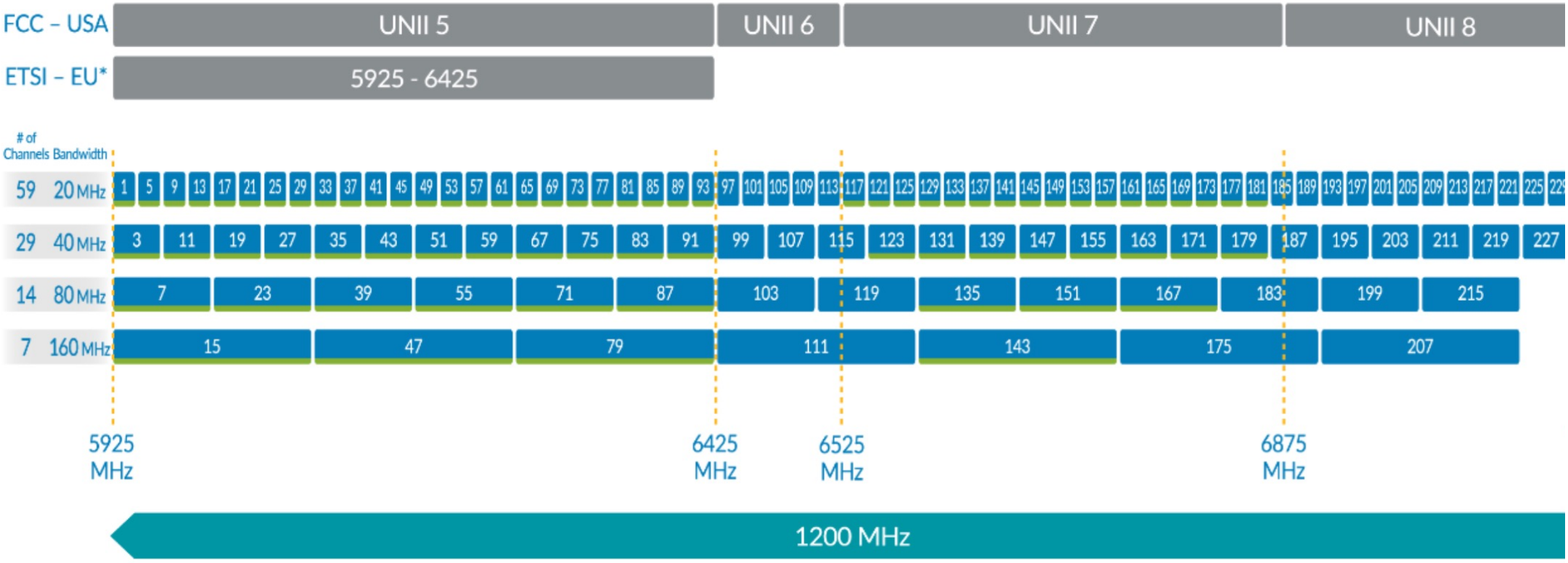
6 GHz spectrum access approaches



- Dynamic random spectrum access and contention-based protocols require access to **multiple channels** to maintain acceptable performance
- **IEEE 802.11be** designed for Extremely High Throughput: channel bandwidth of up to 320 MHz



6 GHz Channel Allocations



Regulatory framework for protecting 6 GHz incumbents

- **Regulators converging on regulatory framework:** based on three regulatory-classifications for 6 GHz RLAN devices:

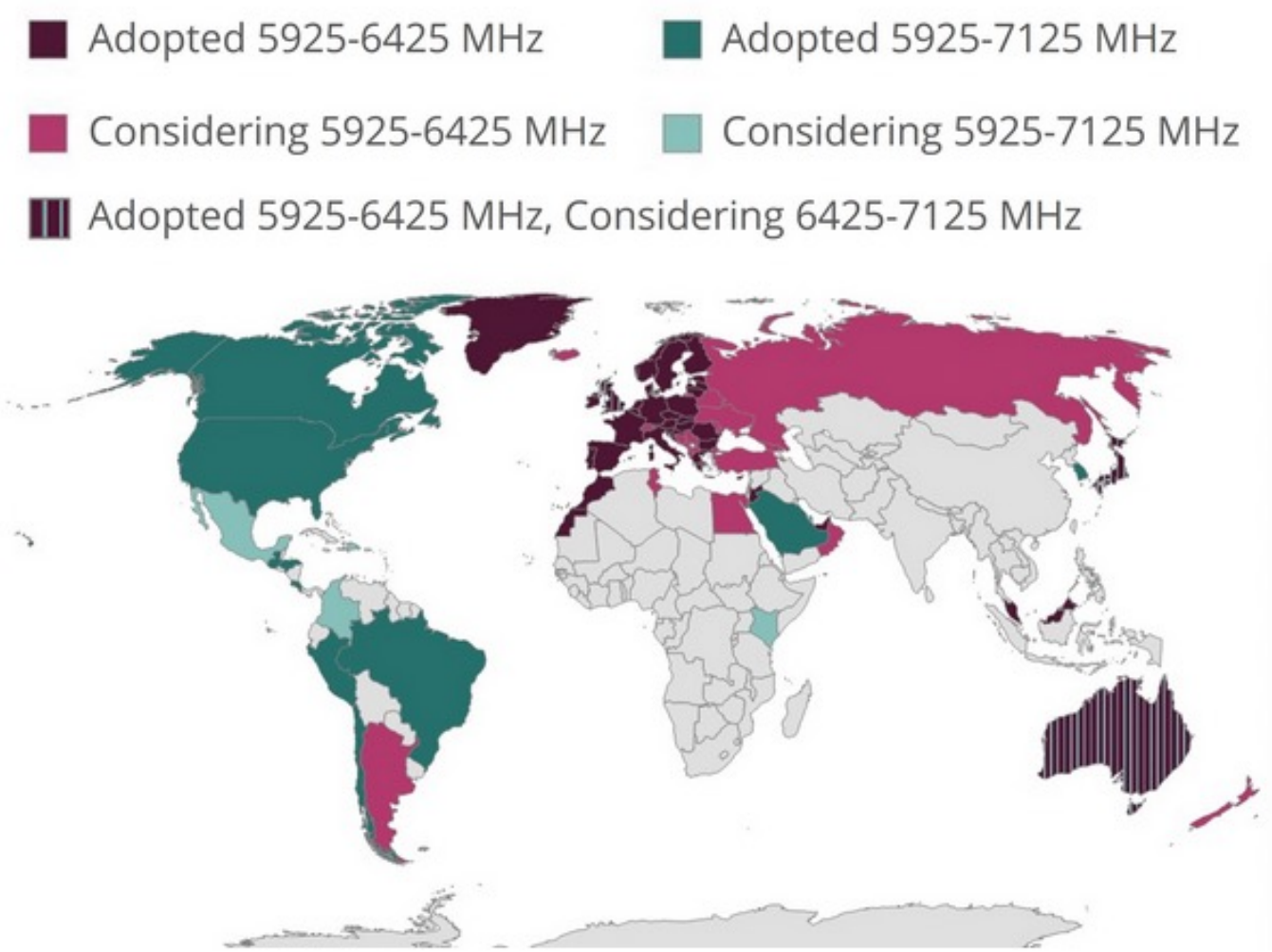
1. **Very Low Power (VLP) devices**: minimal signal power

2. **Low Power Indoor-only (LPI) devices**: low-power and building structure attenuation

3. **Standard Power devices**:
   - To protect Fixed Service: require automated frequency coordination, RLANs avoid frequency overlap with fixed service; implementation requires open access to FS licensing database
   - To protect FSS (on-orbit receivers): limit transmit power at 30 deg. elevation angle

What does this mean in EU?

- VLP on the entire approved frequency band (in and out)
- LPI only inside and only built-in antennas
- Standard Power requires so-called AFC and is not visible on the horizon within the EU, although Czech Republic has announced that they want to allow the entire 6GHz band and Standard Power



Technical condition for 6 GHz Very Low Power (VLP) device

	US (proposed)	Europe (adopted)	South Korea (adopted)	Brazil (adopted)
Frequency band	5.925-7.125 GHz	5.945-6.425 GHz	5.925-6.425 GHz	5.925-7.125 GHz
Channel access and occupation rules	contention-based	contention-based	contention-based	contention-based
Maximum AP e.i.r.p.	14 dBm	14 dBm	14 dBm	17 dBm
Maximum AP e.i.r.p. density	-8 dBm/MHz Industry ask: 1 dBm/MHz	1 dBm/MHz 10 dBm/MHz for narrowband	<20 MHz: 1 dBm/MHz <40 MHz: -2 dBm/MHz <80 MHz: -5 dBm/MHz <160 MHz: -8 dBm/MHz	-8 dBm/MHz
OOBE limit	-27 dBm/MHz below 5925 MHz	-45 dBm/MHz (-37 dBm/MHz in 2025) below 5935 MHz	-27 dBm/MHz below 5925 MHz	-27 dBm/MHz below 5925 MHz

Technical condition for 6 GHz Low Power Indoor-only (LPI) device

	US (adopted)	Europe (adopted)	South Korea (adopted)	Brazil (adopted)
Frequency band	5.925-7.125 GHz	5.945-6.425 GHz	5.925-7.125 GHz	5.925-7.125 GHz
Channel access and occupation rules	contention-based	contention-based	contention-based	contention-based
Maximum AP e.i.r.p.	30 dBm	23 dBm		30 dBm
Maximum AP e.i.r.p. density	5 dBm/MHz proposed 8 dBm/MHz	10 dBm/MHz	2 dBm/MHz	5 dBm/MHz
Maximum Client e.i.r.p.	24 dBm/MHz			24 dBm/MHz
Maximum Client e.i.r.p. density	-1 dBm/MHz			-1 dBm/MHz
OOBE limit	-27 dBm/MHz below 5925 MHz	-22 dBm/MHz below 5935 MHz	-27 dBm/MHz below 5925 MHz	-27 dBm/MHz below 5925 MHz

How to switch to 6Ghz?

- Only 6 GHz on access points?
- Well maybe not - How to find my 6GHz AP?
- 802.11v Reduced Neighbor report reports on 5GHz back which 6GHz channels are available.
- Active "Probe" on 6GHz will only be possible on every 4th channel. Channels 5, 21, 37, 53, 69, 85, (101, 117, 133, 149, 165, 181, 197, 213 and 229).
- To passively wait and listen to info from AP via so-called FLIS frames (Fast Initial Link Setup) or so-called "unsolicited probe response frames" (probe response without question from client). About 20ms per channel

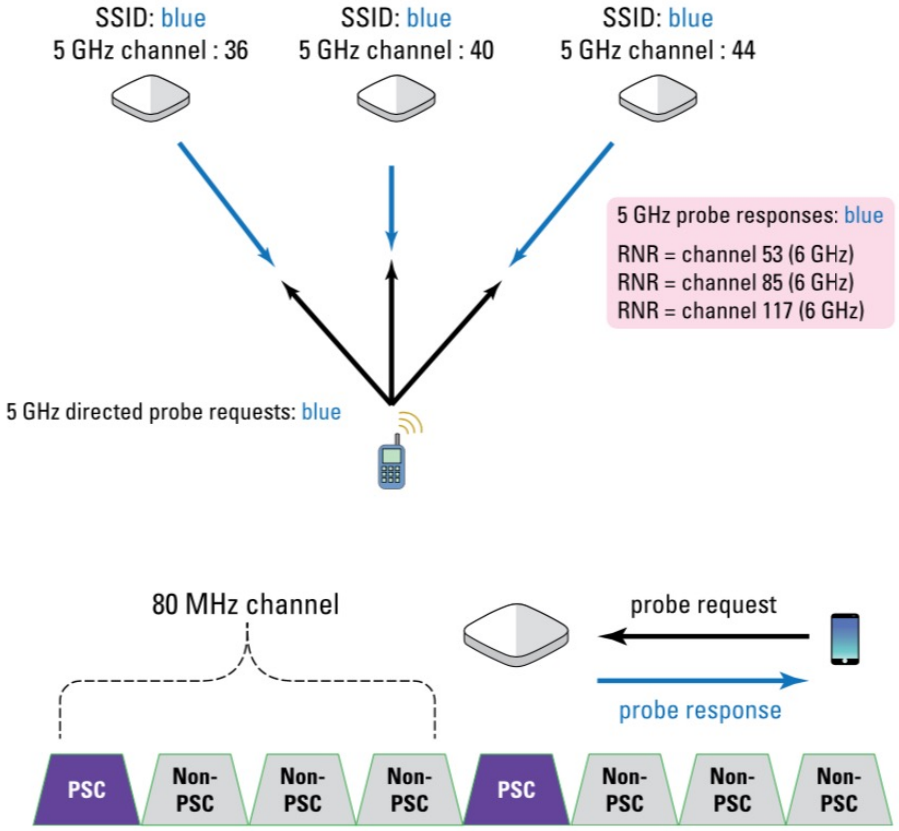


FIGURE 6-7: PSC and 80 MHz channels.

6GHz Channel layout for the EU until further notice…

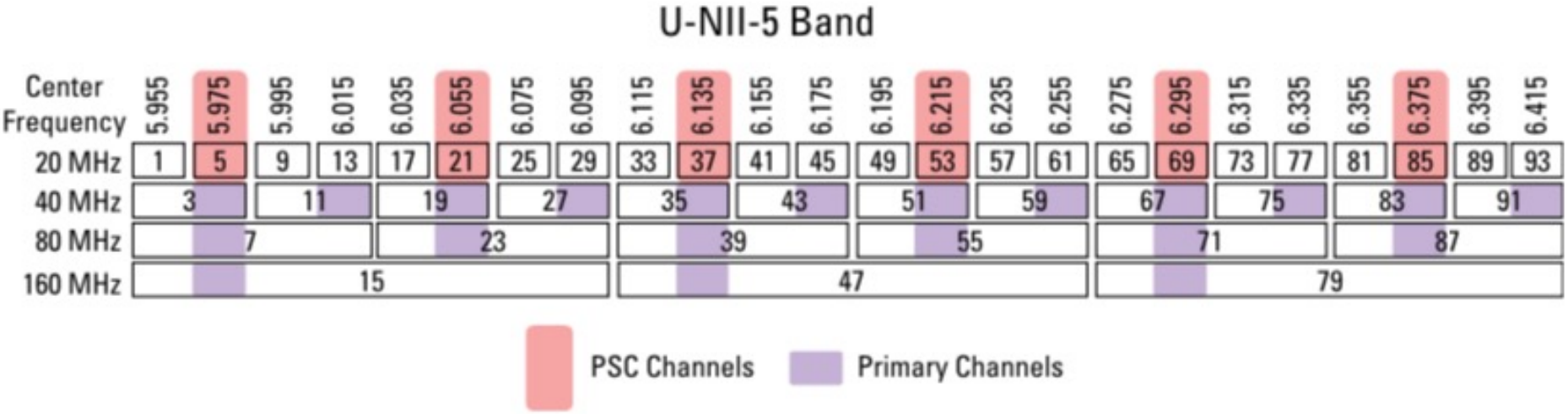


FIGURE 6-9: Preferred scanning channels and primary channels.

The filter problem with WiFi6E and how the current manufacturer solved it

- Difficult to run on the same AP one radio on a high 5GHz channel and another on a low 6GHz channel
- Some manufacturers will not use the first 6GHz channels to solve this.
- Others run with flex radio on high 5GHz or 6GHz and a dedicated 5GHz radio that only works on the low 5GHz band. (e.g. Arista C360)
- Dedicated 6Ghz radio with filter

OOBE limit	-27 dBm/MHz below 5925 MHz	-45 dBm/MHz (-37 dBm/MHz in 2025) below 5935 MHz	-27 dBm/MHz below 5925 MHz	-27 dBm/MHz below 5925 MHz

The issue of mGig and 60W PoE

- A fully equipped 3-band AP with 4x4 on 5 and 6GHz band will draw more than 30W.
- At the moment, only Arista has a WiFi6E AP that draws more than 30W. Aruba and Extreme solve the problem through a simpler 2x2 MIMO AP. But more APs that draw more than 30W are on G from several manufacturers.
- If you run a 20 / 40MHz channel plane, it is doubtful whether you can fill a 1Gb / s pipe.
- Maybe future access points can be made to draw less than 30W but in 3-4 years WiFi7 (802.11be) will come and then….
- If you have no plans to introduce WiFi6E, you can safely continue driving with 1 Gig and 30W PoE switches.

Do I need WiFi6E?

- It depends. ☺
- Is there enough capacity in the current infrastructure?
- Is there a need for very high priority clients / users?
- Do you share premises with others who "pollute” "your" spectrum?

KIFÜ Spectrum issues (Only UNII-5 in the EU ??) ☹

802.11be (WiFi7) will come in just 3-4 years and then in principle the entire 6GHz band will be a requirement for it to work.

http://dynamicspectrumalliance.org

World Radiocommunication Conference is the congress where the spectrum is distributed. GSMA wants to see that the band 5925-7125 MHz is reserved for 5G.

Today, only China has allocated all 1200 MHz in the proposed frequency band for 5G.

In Europe, the upper part is intended for 5G, while 500 MHz in the lower part can be used by wifi. The situation in Africa and the Middle East is similar.

In the US and Latin America, as it stands right now, the entire band will be unlicensed and primarily intended for wifi and other technologies that do not require a license.

NMHH érdemben nem foglalkozott vele – vs 5G lobbi.

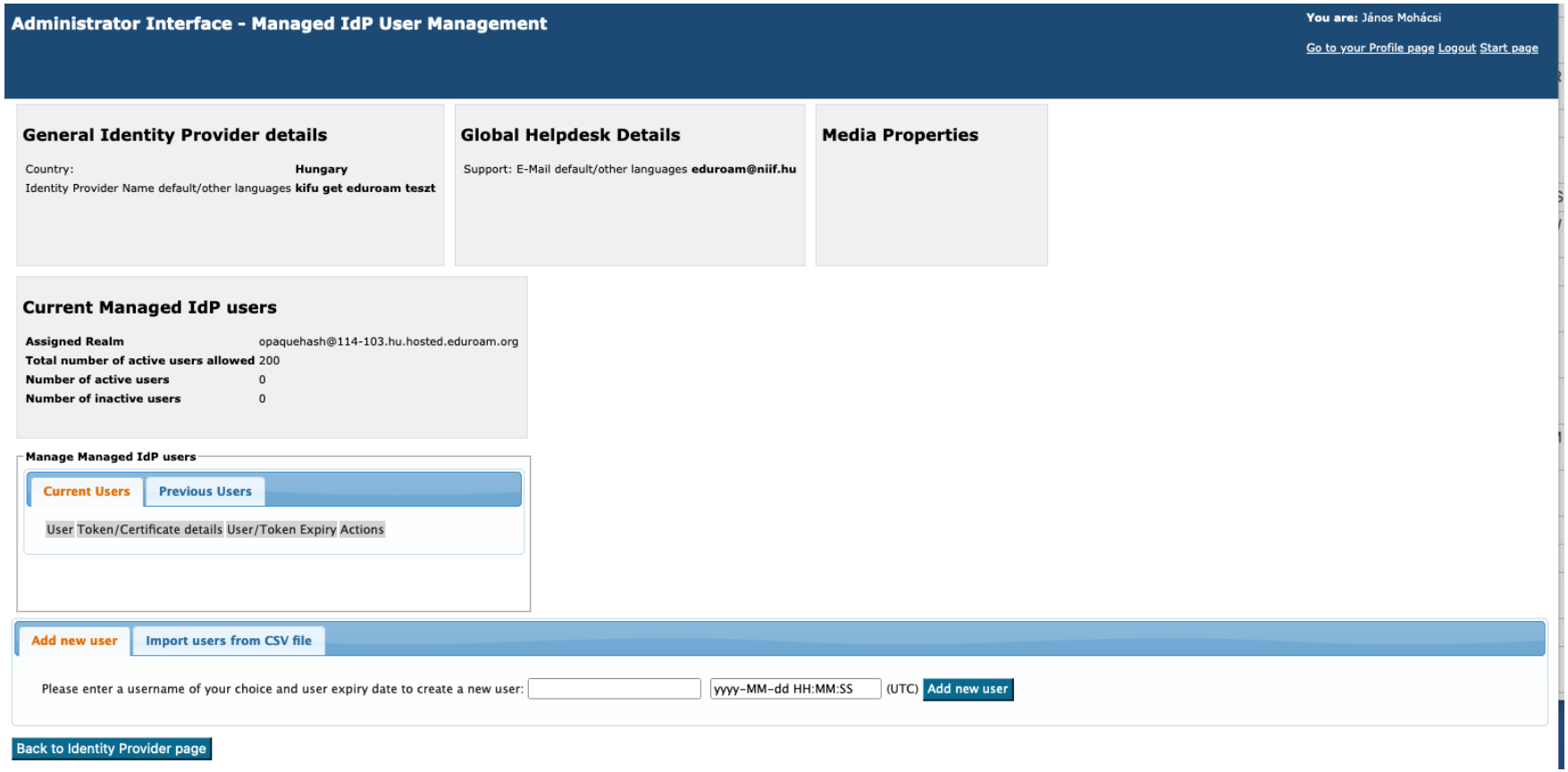
WiFi6E and eduroam

- Eduroam advisory – 19/05/2022
  1. Continue using “eduroam” BSSID – against recommendation to use different BSSID
     - Different BSSID might be valid for lower security mode networks: WiFi6 requires WPA3! –might cause disruption on ”no authentication” -> OWE/WiFi CEO or PSK -> SAE
  2. Protected Management Frames – keep PMF WPA3 transition mode (Access Points that announce PMFs as supported, but optional)– as for 2.4 and 5 Ghz Bands.
  3. Do not link Wi-Fi 6E with Optional PMFs/WPA3-Enterprise Transition mode

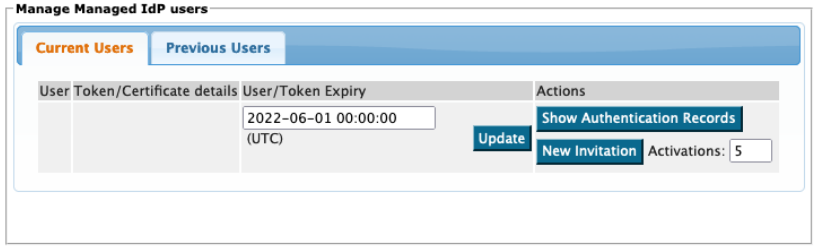
eduroam CAT – useful with few shortcomings

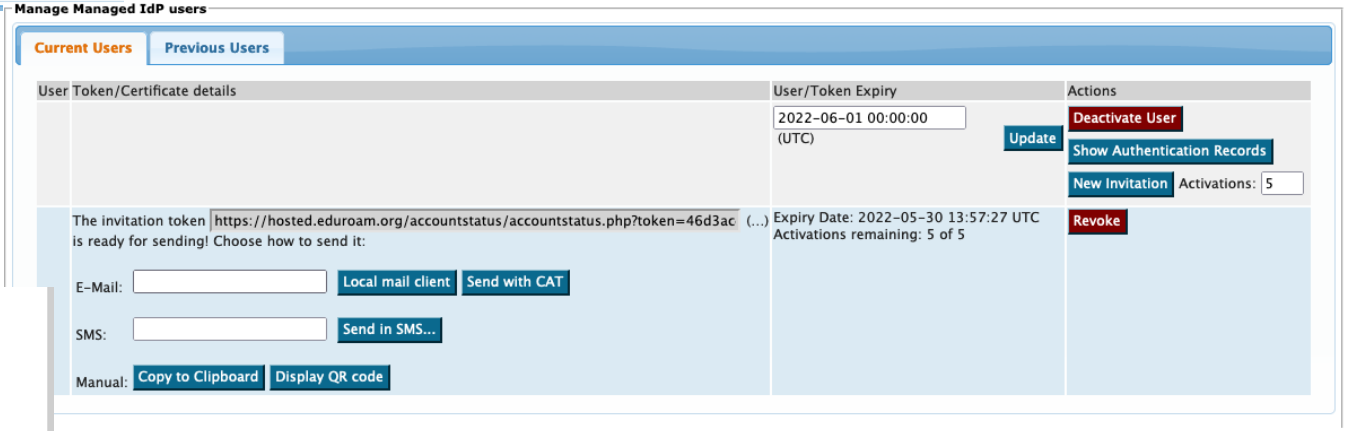
- Android app: some problems with Android 11 and no longer maintained
- No easy way to onboard for EAP-TLS (client certificate loaded separately)
- Lifecycle management of client certificates is missing (renew and when?)

Managed eduroam IdP /1



Managed eduroam IdP /2





Your invitation token is valid for 5 more device activations (0 have already been used).

You can now download a personalised eduroam® installation program.The installation program is **strictly personal**, to be used **only on this device (Linux)**, and it is **not permitted to share** this information with anyone.

When the system detects abuse such as sharing login data with others, all access rights for you will be revoked and you may be sanctioned by your local eduroam® administrator.

During the installation process, you will be asked for the following import PIN. This only happens once during the installation. You do not have to write down this PIN.

Import PIN: 4203

Click here to download your eduroam® installer!

geteduroam status at KIFÜ

- Managed eduroam IdP tested and evaluated
  - It works!
  - There are a number of things that need to be fixed
  - Admin portal is missing to find connection PseudoID -> User.
  - Certificates and keys are stored in a common database along with other (security?)
- Plan to deploy in more widespread
  - Current solution for smaller IdPs (connect with eduID) who just want to make eduroam work (admin portal missing) – contact us
  - Development: Connecting geteduroam PseudoID to User to correct administration
  - Guest access with educational institution management

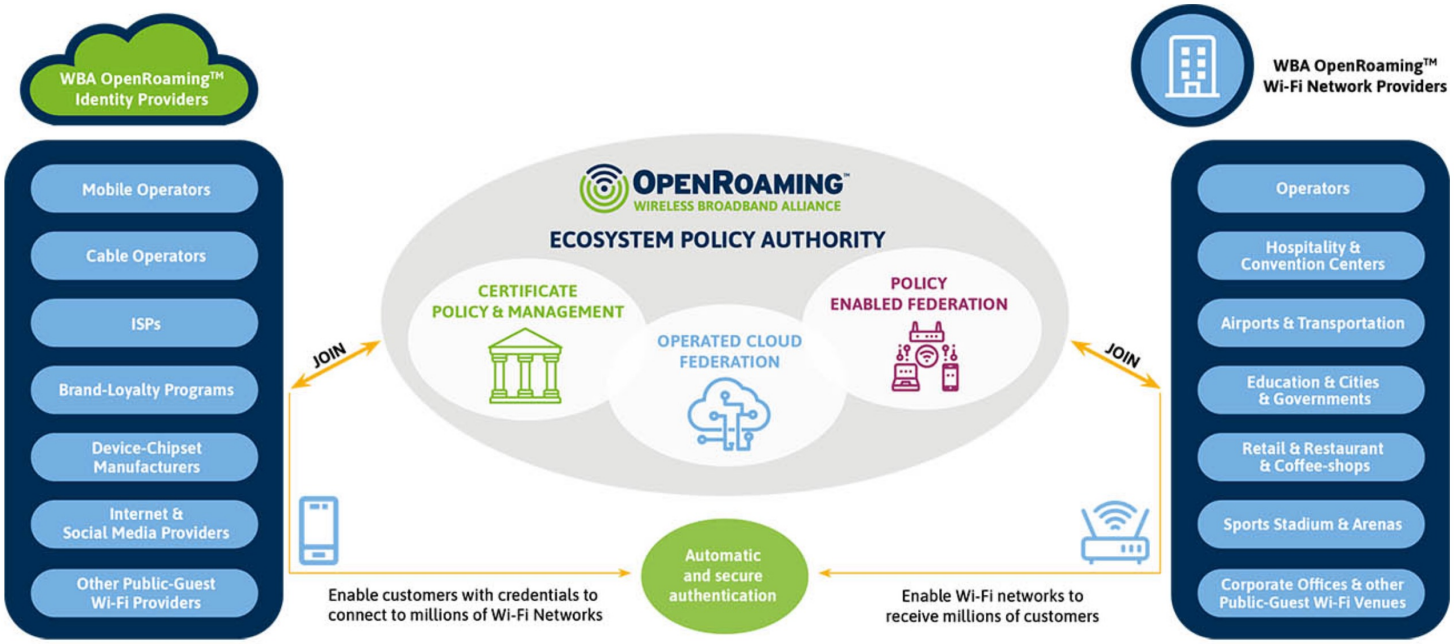
KIFÜ openssl 3.0

- TLS versions / insecure renegotiation
  - by default, no insecure renegotiations
  - these typically only occur in TLS 1.0 / 1.1
  - wpa_supplicant and NetworkManager will fail horribly in face of an EAP server needing this
  - strangely enough, wpa_supplicant is patched to exceptionally allow this and override the insecurity
  - It shouldn't be that way. Everyone should support TLS 1.2+ these days.
  - NPS up until Windows Server 2016 seems to be hit by this by default (but has gone end of Mainstream Support October 2023!) – more info
  - Bug reports suggest some Aruba built-in EAP server does the same (based on Freeradius 1.1.4)
- TLS client certs
  - openssl 1 uses by default an RC4- cipher to encrypt the private key with the password
  - openssl 3 refuses to decrypt this, because of "legacy”
  - when generating a client cert on openssl 1, use the "-descert" option
  - when decrypting a "legacy" client cert on openssl 3, use the "-legacy" option

Radius-Server certificate (public vs private)

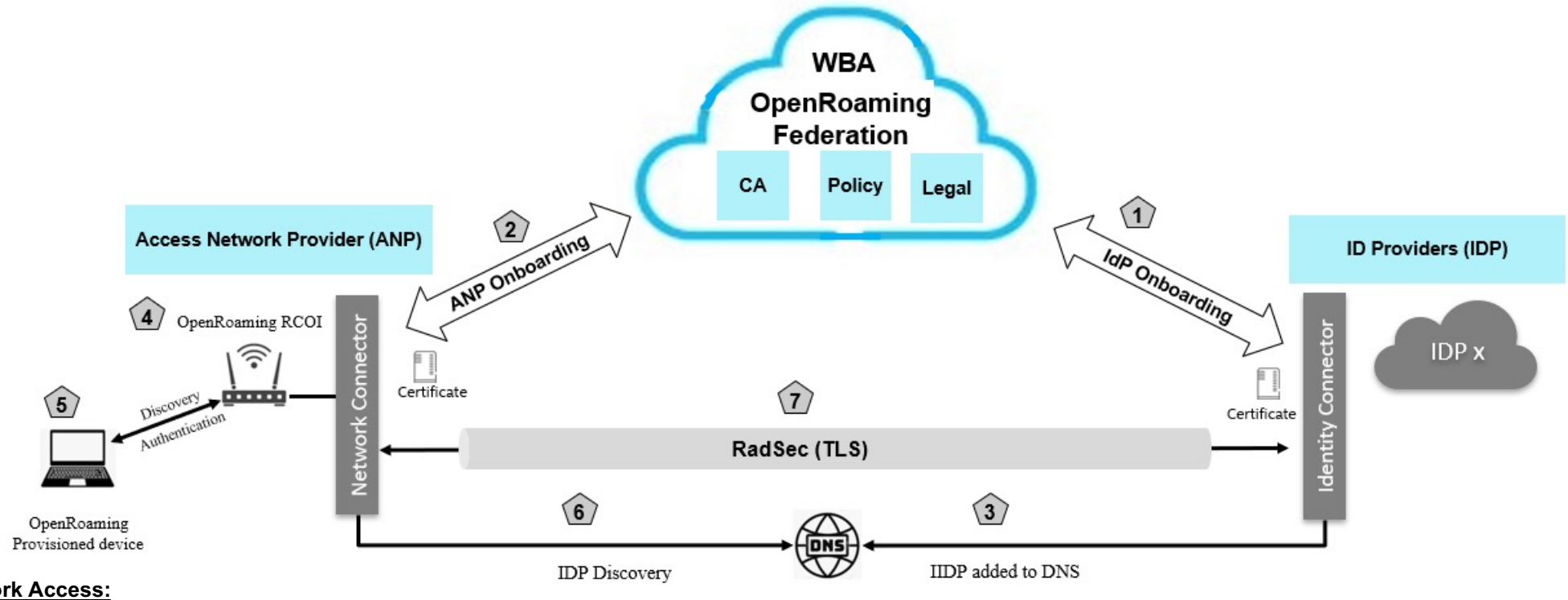
- Public
  - Already in machine (maybe)
  - PEAP or EAP/TTLS out of the box
  - Security
  - Replace certificate? Problem
  - Replace root CA? Problem
  - Do all clients support so-called pinning?
- Private
  - Secure (you have full control)
  - Long certificate life.
  - CA-root must be installed (CAT, geteduroam)
  - Future risk that suppliers lock down devices.

Openroaming



www.openroaming.org

KIFÜ OpenRoaming – How it works?



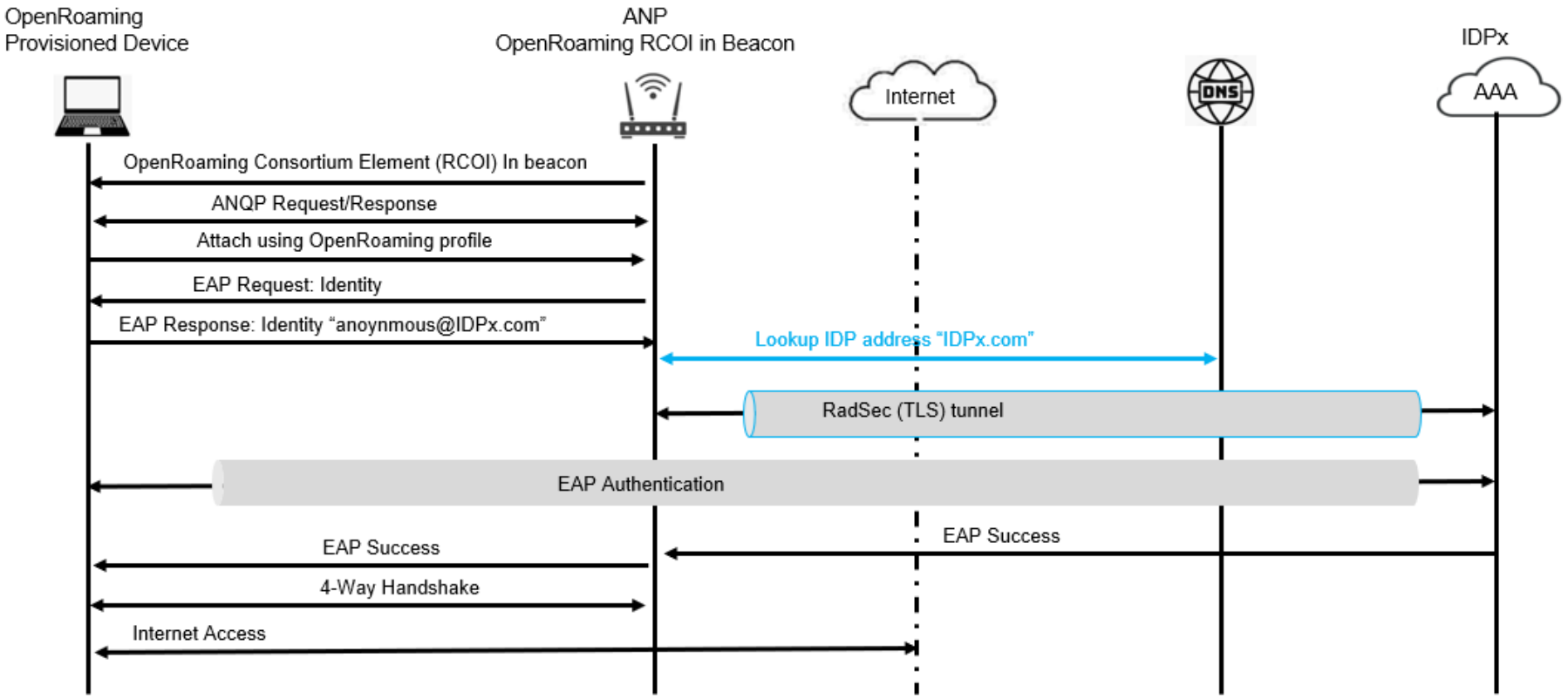
Network Access:

- Device is provisioned with OpenRoaming profile
- ANP AP advertises "Federated Roaming RCOI in the beacon.
- Device discovers OpenRoaming network
- Device attaches ANP AP using OpenRoaming profile.
- ANP finds IDP in DNS
- Secure and authenticated tunnel establishment

Onboarding ANPs and IDPs:

- ANPs and IDPs registers with OpenRoaming Federation
- OpenRoaming Federation verifies them and issues certificates and WBAID
- IDPs are added to OpenRoaming DNS

OpenRoaming Discovery and Authentication Flow



Openroaming – How?

- Do not set up anything of your own without checking with us at KIFÜ
- NAPTR record requires DNSSEC!
- Still not (to my knowledge) any OpenRoaming SP in Hungary but one soon

Some furhter readmin

- WiFi6E for Dummies guide: https://www.extremenetworks.com/resources/ebook/wi-fi-6-6e-for-dummies/
- https://wiki.geant.org/display/H2eduroam
- www.openroaming.org
- www.wi-fi.org

Kérdőív

Kérdések?

Köszönet

Mohacsi.Janos@kifu.gov.hu

aai@kifu.hu