

OPENROAMING GETEDUROAM

Paul Dekkers

April 19, 2021, SUNET

SURF

eduroam is WBA member – so you are!
participation in OpenRoaming, similarities eduroam, what does it mean



ONE GLOBAL WI-FI NETWORK



“ eduroam has been doing federated Wi-Fi roaming since over a decade with many of the building blocks that meanwhile underpin Passpoint®. Now that Passpoint® and OpenRoaming™ provide a coherent vision and technology to enable inter-federation roaming in a scalable way, it is only natural for eduroam to join forces and take this exciting next step as a first-to-market pioneer participant. ”

Paul Dekkers

Chair of the Global eduroam Governance Committee in GÉANT

eduroam, (inter fed) roaming, ...

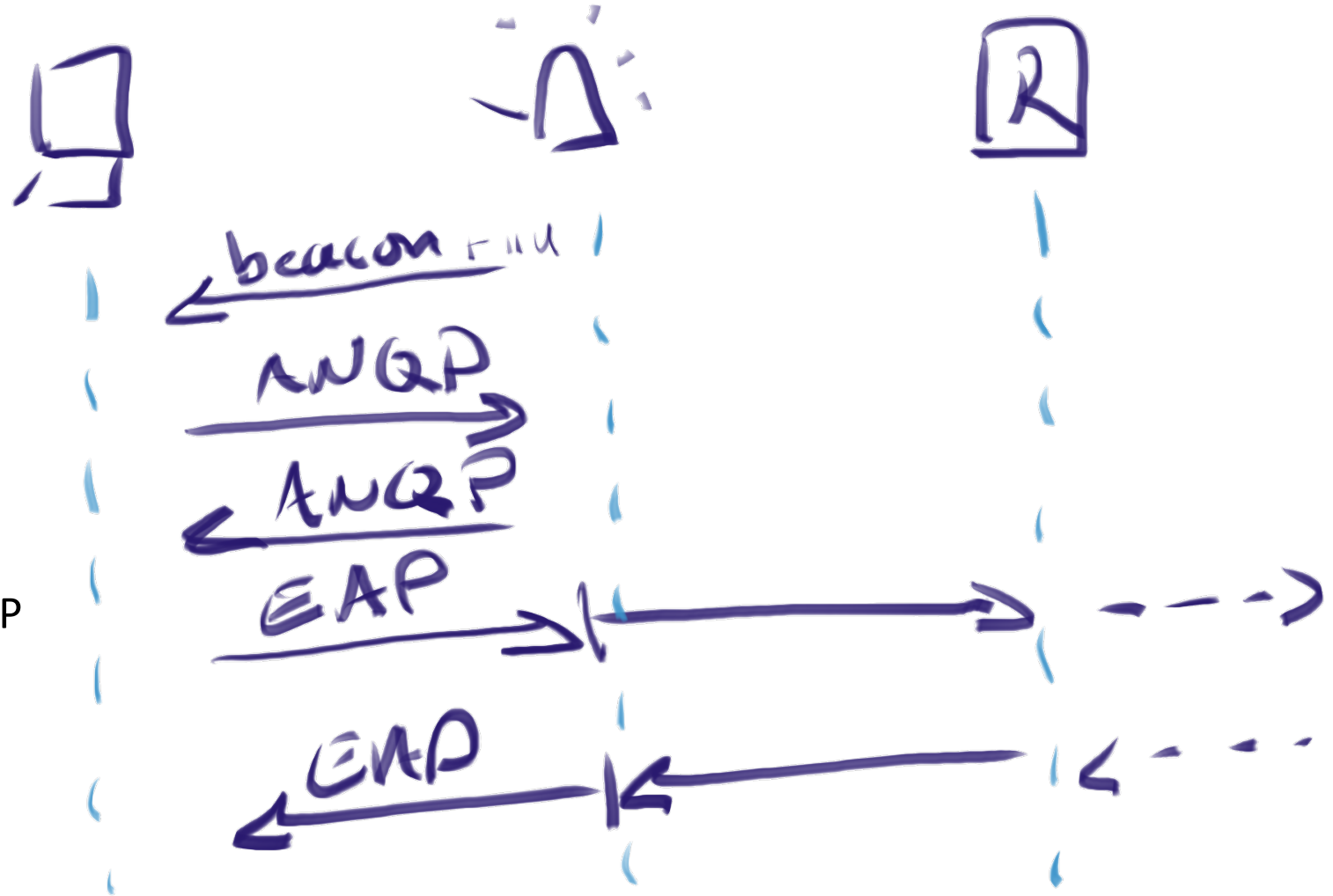
- eduroam is the biggest federated roaming-infrastructure
 - 7200 IdPs
 - 30000 locations
 - 106 countries
- Roaming by standardizing on SSID (1x, RADIUS, transparent EAP)
- Blueprint, authorisation, use-case, rules are simple (reused largely in eg. govroam)
- Global governance (GeGC), regions, NROs

- Hotspot 2.0/Passpoint,
We have an eduroam RCOI for venues that have no SSID available
Participated in NGH trials
WiFi4EU

- Dynamic peer discovery

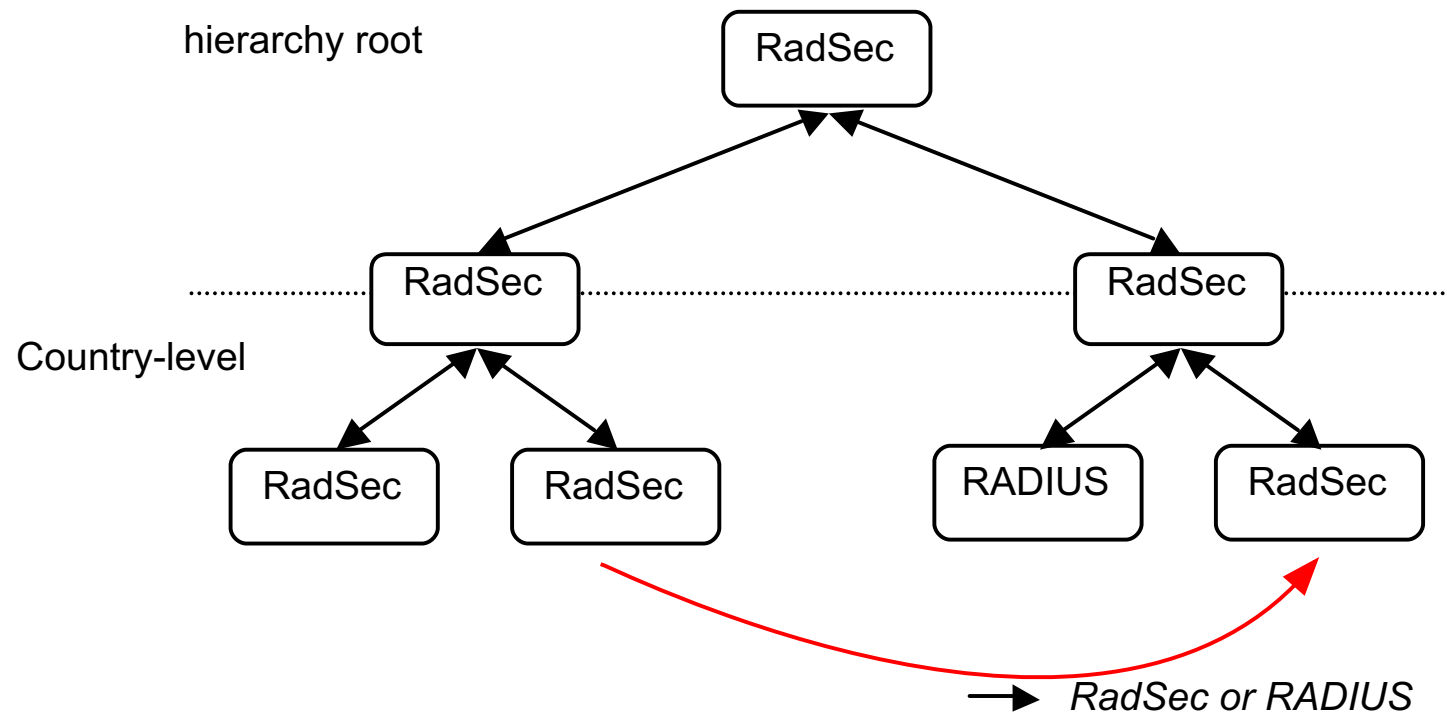
Hotspot 2.0, HS20, Passpoint[®], 802.11u

- More than just SSIDs:
 - RCOI** (Roaming Consortium Organization Identifier),
 - NAIrealm, domain, 3GPP (MNC/MCC, offloading)
- ANQP (Access Network Query Protocol) for discovery of networks (home, roaming, EAP-types)
- Afterwards: WPA(2)-Enterprise, EAP
- Multiple releases, limited support
 - R2: Online Sign-Up (OSU)
 - R3: safe "AUP/T&C portal", details in RADIUS req.'d for routing



RadSec, dynamic peer discovery (1)

- eduroam test RadSec since 2004
- RADIUS (UDP) trust is IP, shared secret
- RadSec (TCP, TLS) trust is PKI
direct connections possible



RadSec, dynamic peer discovery (2)

- Dynamic routing in use for exceptions, between countries:

```
% host -t naptr zone.college
zone.college has NAPTR record 50 50 "s" "x-eduroam:radius.tls" "" _radsec._tcp.surfnet.eduroam.nl.
```

- Delegation within NRO:

```
% host -t naptr kennisnet.nl
kennisnet.nl has NAPTR record 50 50 "s" "x-eduroam:radius.tls" "" _radsec._tcp.kennisnet.eduroam.nl.
```

- OpenRoaming:

```
% host -t naptr edu.nl
edu.nl has naptr record 50 50 "s" "x-eduroam:radius.tls" "" _radsec._tcp.edu.nl.
edu.nl has naptr record 50 50 "s" "aaa+auth:radius.tls.tcp" "" _radsec._tcp.openroaming.eduroam.org.
```

```
% host -t srv _radsec._tcp.openroaming.eduroam.org.
_radsec._tcp.openroaming.eduroam.org has SRV record 0 0 2083 openroaming1.eduroam.org.
```

Passpoint, dynamic peer discovery, ... OpenRoaming™

- Previous slides showed technology behind Passpoint and dynamic peer discovery
- We do this (in part) in eduroam



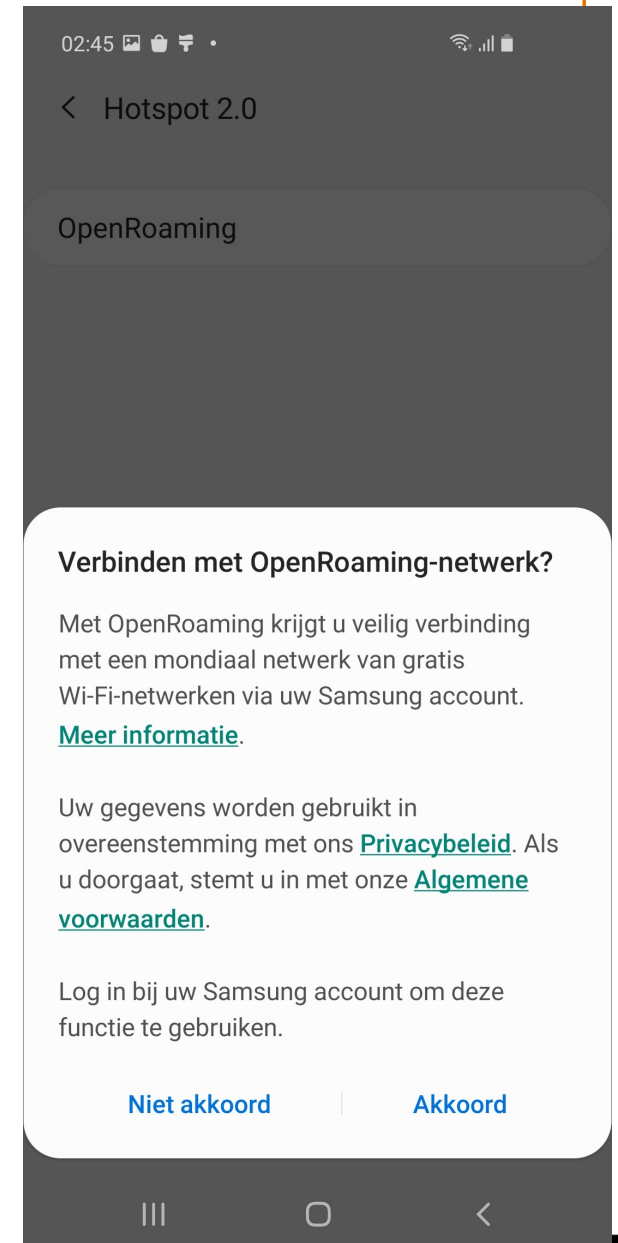
Insert: OpenRoaming™

- More roaming hubs, between mobile operators, vendors, providers, NGH trials
- Is not just secure Wi-Fi, but like eduroam accepts many (different) IdPs, SPs
- Complex matrix asks for complex technology?

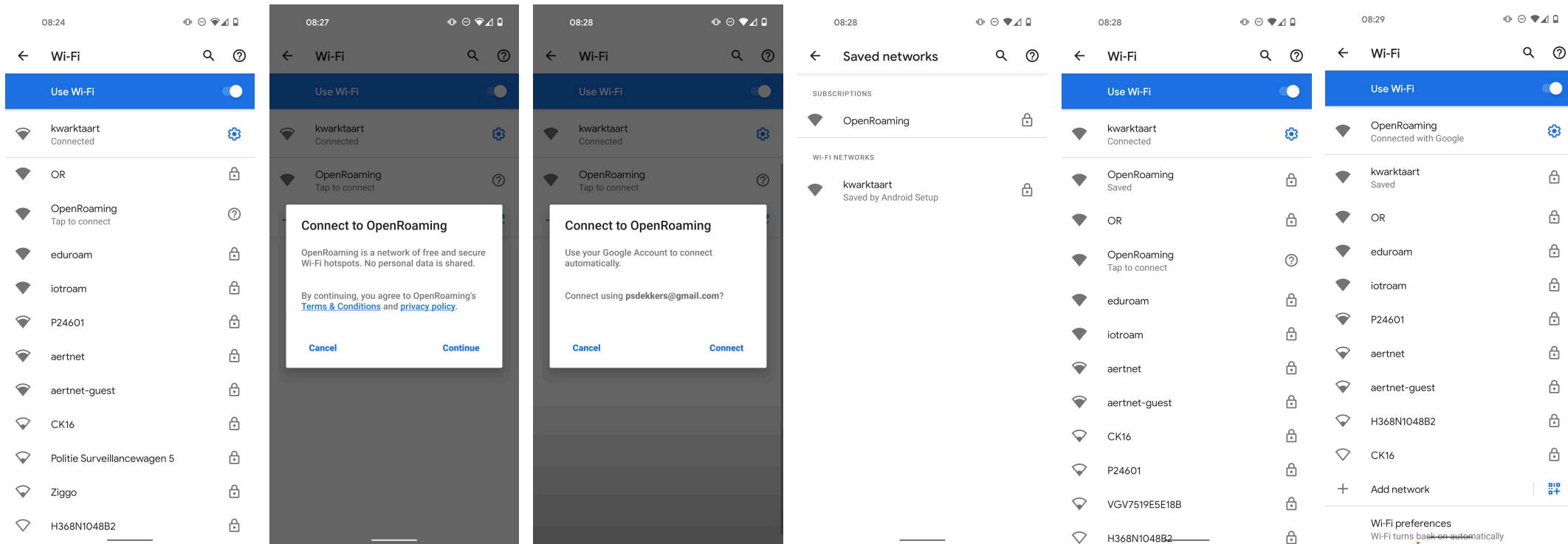


OpenRoaming™

- Developed by Cisco, transferred to WBA
- WBA's Wireless Roaming Intermediary eXchange (WRIX) Framework Interconnect, reporting/rating/data clearing, settlement
- Policies (what SPs, IdPs, privacy modes)
- Roaming based on different RCOIs
 - OpenRoaming education RCOI
 - OpenRoaming ALL (compatible T&C)
 - Settlement or settlement free
 - Privacy: true identity or anonymous, CUI
 - Type: Vendor, Service Provider, Hospitality, Enterprise, Government, ...
- WBAID (ours is “eduroam”, some suffixed by country ID)



Android 11 makes OpenRoaming onboarding easy



- <https://wballiance.com/openroaming/privacy-policy-2020/>
- <https://wballiance.com/openroaming/toc-2020/>
- The device adds a network subscription, OpenRoaming only connects “manually”

OpenRoaming™ and eduroam: status

- eduroam has become member of Wireless Broadband Alliance
- We are participating in the OpenRoaming workgroups
- We have our own identity (WBAID)
 - RADIUS
 - Certificates, I-CA
- Considered as one big SP for eduroam (without sacrificing SSIDs), eduroam acts as one big IdP
- Decided to use eduroam RCOI only for NON-OpenRoaming purposes (proper eduroam SPs unable to use SSID)
- Promote use of specific OpenRoaming RCOIs in profiles (opt-in)
- Provisioning will be important (geteduroam, CAT)
- Trials and Showcases

Evaluations for SPs (operators, venues) and IdPs

- With eduroam by SSID, all users get on the network without configuration change
- With eduroam RCOI, few users get on the network, since it's been in CAT and geteduroam (and is opt-out)
- With OpenRoaming edu RCOI, probably no users get on the network still, we use opt-in
- SPs, operators, venues, see immediate value of using eduroam SSID, less from Passpoint
- eduroam is very visual (SSID), Passpoint is less visible (also if it doesn't work)

- eduroam will cost an SSID, some sites may not have that available
- Adhere to the eduroam rules (not very complex)
- Work with local operators/NRO

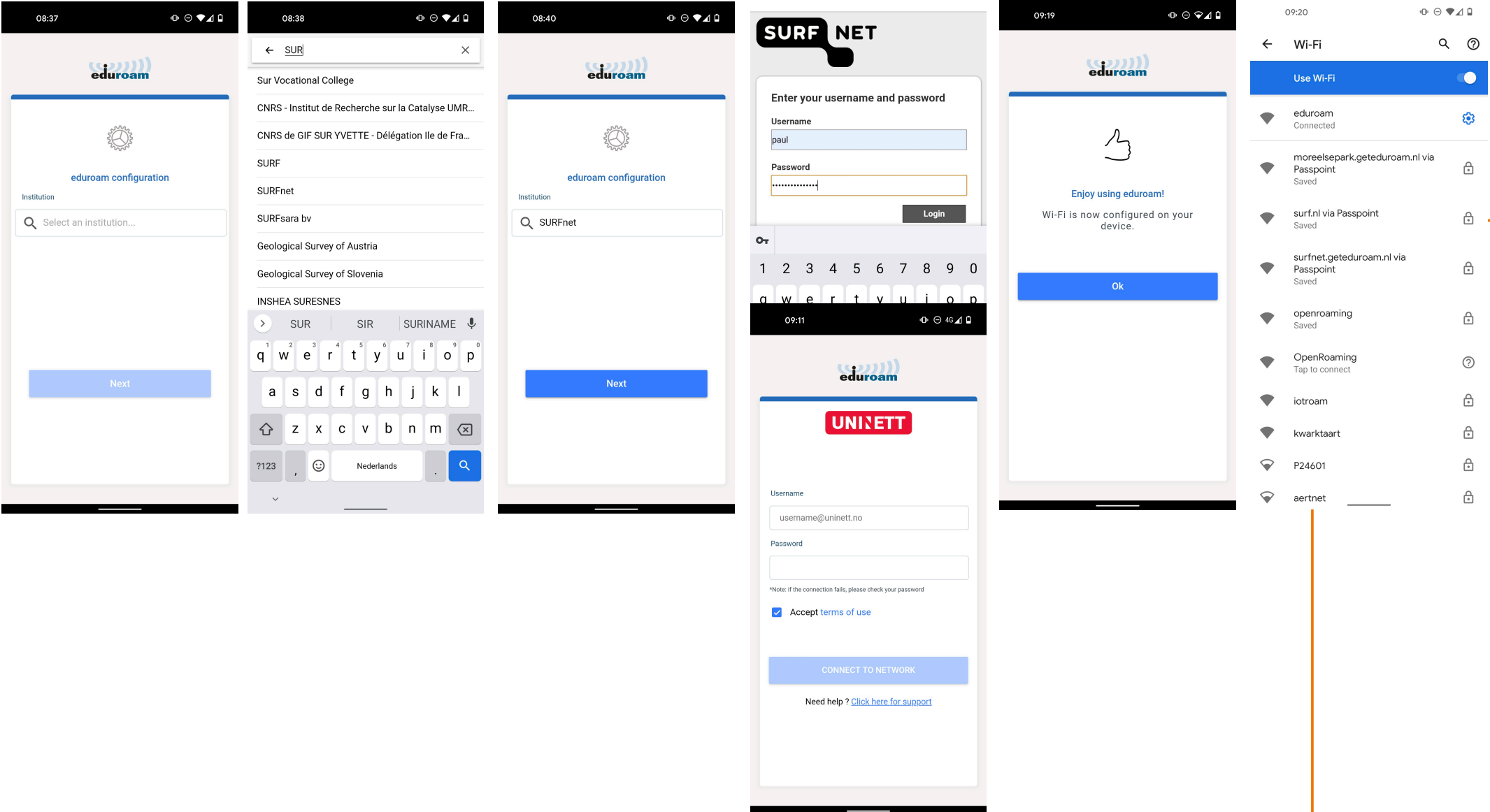
OpenRoaming™ and eduroam: trials!

- Easy to participate
- Connect IdP by adding NAPTR record
(why not add both while you're add it)

```
% host -t naptr uva.nl
uva.nl has naptr record 50 50 "s" "aaa+auth:radius.tls.tcp" "" _radsec._tcp.openroaming.eduroam.org.
uva.nl has naptr record 50 50 "s" "x-eduroam:radius.tls" "" _radsec._tcp.surfnet.eduroam.nl.
% host -t naptr hva.nl
hva.nl has naptr record 50 50 "s" "aaa+auth:radius.tls.tcp" "" _radsec._tcp.openroaming.eduroam.org.
hva.nl has naptr record 50 50 "s" "x-eduroam:radius.tls" "" _radsec._tcp.surfnet.eduroam.nl.
```

- More IdP obligations: proper onboarding, consent to OpenRoaming terms & conditions
- Connect SP via separate proxy, or by using Vendor equipment
 - Configure Hotspot 2.0
 - Compatible policies, scope
- Showcases, see visitors use the network

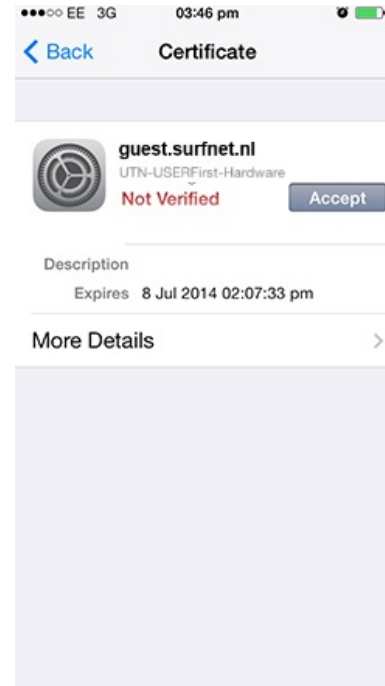
In eduroam we require an App for (proper) (Passpoint) onboarding



Also, for: security, privacy

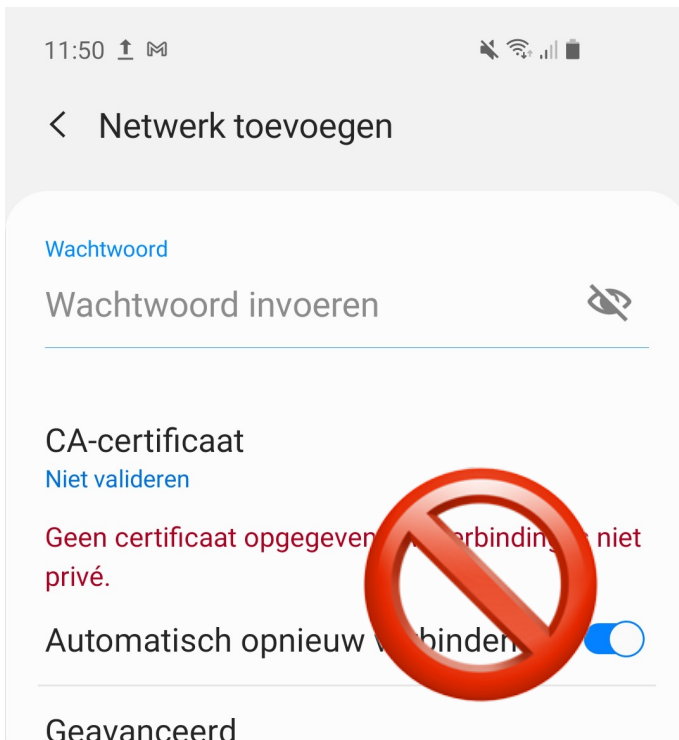
- Mutual authentication easiest attack-vector (EAPHammer)
 - -PAP < -MSCHAPv2 < EAP-TLS
- User is the weakest link
 - Trust-on-first-use (TOFU)
- Privacy wrt data “in the air”

- To configure everything right: use a profile
 - Outer username for privacy
 - Server mutual authentications (CAs (rollover!) and Common Names)
 - And why not: client-certificate (no passwords to steal)



Certificate validation Android, WPA3 R3 / Wi-Fi certification

- The Android december update removed the “Do not validate server certificate” option (complies with Wi-Fi alliance certification)
- Good, this was never a good idea! (But maybe users accidentally misconfigured.)



Still not OK? Options:

- Offer CA download
- "System certificates"
- Different EAP-type

Easier:

- Installer, eduroam CAT / geteduroam



eduroam CAT



- Single place for profiles
- All settings correctly!



- Android app
- No built-in credentials
- Certificate provisioning for users is hard
- HS20/Pp profiles hard
- Hosted IdP is not for a big userbase

Hosted IdP

- For small organizations without IdM
- Invite/installer via SMS or mail
- Like CAT, but with credentials: certificates
- Can compare with guest solutions

The screenshot displays the 'eduroam Managed IdP' Administrator Interface. The page title is 'Administrator Interface - Managed IdP User Management'. The user is identified as Paul Dekkers. The interface is divided into several sections:

- General Identity Provider details:** Country: Netherlands; Identity Provider Name: default/other languages eduroam NL.
- Global Helpdesk Details:** Support: E-Mail default/other languages eduroam-beheer@surfnet.nl.
- Media Properties:** (Empty section)
- Current Managed IdP users:** Assigned Realm: opaquehash@38-34.nl.hosted.eduroam.org; Total number of active users allowed: 200; Number of active users: 2; Number of inactive users: 0.

The main section is 'Manage Managed IdP users', which includes tabs for 'Current Users' and 'Previous Users'. It contains a table with the following data:

User	Token/Certificate details	User/Token Expiry	Actions
Florian Draisma	Device: Android 9.0 Pie Serial Number: 75ef817d8563f007 CN: exreyv8sxnj5ixkhfm7e06bemeaz0z6m5ia@... Expiry: 2021-01-01 12:58:00 Issued: 2019-04-11 14:58:00 Revoke	2020-12-31 23:59:59 (UTC) Update	Deactivate User Show Authentication Records New Invitation Activations: 5
Paul Dekkers	Device: Apple OS X El Capitan Serial Number: 161b2fdb60bb8749 CN: 6i5hx5omilf0nl7us6t30si13z607uhfahv u@... Expiry: 2025-01-01 07:27:42 Issued: 2019-04-09 09:27:42 Revoke	Device: Apple iOS mobile devices (iOS 7-11) Serial Number: 3d6e286e23c93999 CN: bx9u5guuhmmpar6c126lbsuxfs18kofot cub@... Expiry: 2035-01-01 07:29:57 Issued: 2019-04-09 09:29:57 Revoke	Device: Android 8.0 Oreo Serial Number: 61ac8677c16c508 CN: bfnvrx9f94kss4kk782jhyb7mr7oudunp njh@... Expiry: 2035-01-01 13:12:15 Issued: 2019-04-11 15:12:15 Revoke
	Device: Apple macOS Mojave Serial Number: 69687baea9c27188 CN: 8oqq3z4nw97yty1w6dh6vjkwx2zjp2yc dnn@... Expiry: 2035-01-01 14:13:19 Issued: 2019-09-17 16:13:19 Revoke	2034-12-31 23:59:59 (UTC) Update	Deactivate User Show Authentication Records New Invitation Activations: 5

At the bottom, there are buttons for 'Add new user' and 'Import users from CSV file'. A form below these buttons prompts the user to enter a username and an expiry date (YYYY-MM-DD HH:MM:SS UTC) to create a new user.

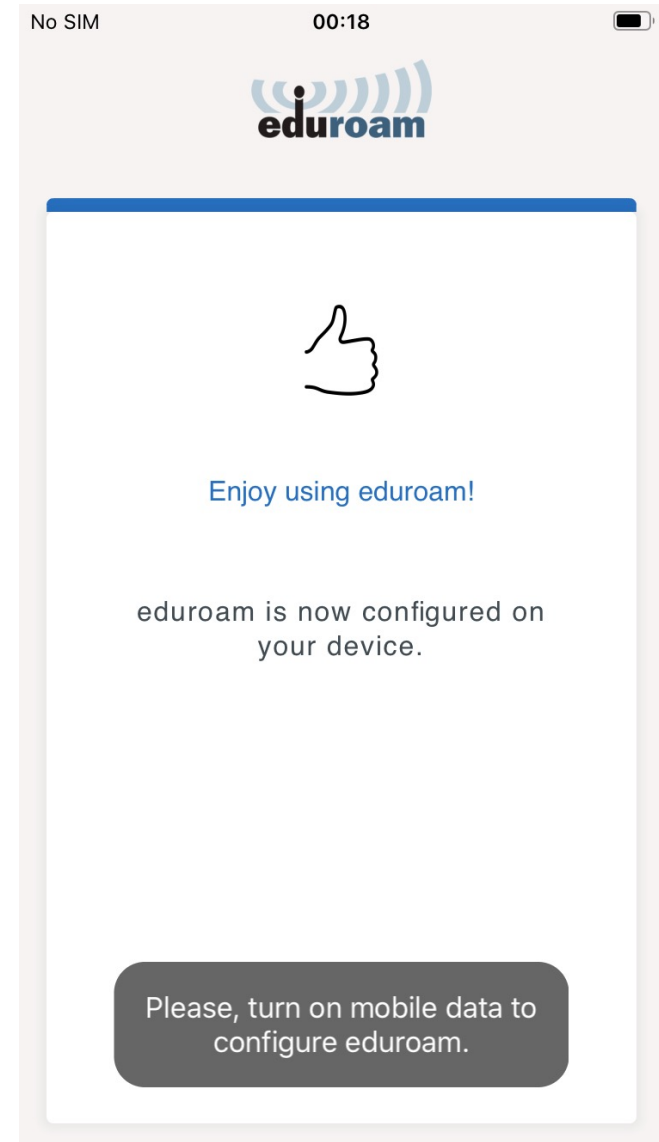
geteduroam



- Good client for all platforms
- Contains CAT profiles: works for all organizations!
- Passpoint, Hotspot 2.0 settings (OpenRoaming!)
- Alternative workflow to provision pseudo-credentials using federated authentication (OAUTH, SAML)
- With that flow: also a Hosted IdP
- Initiative from NORDUnet and SURF

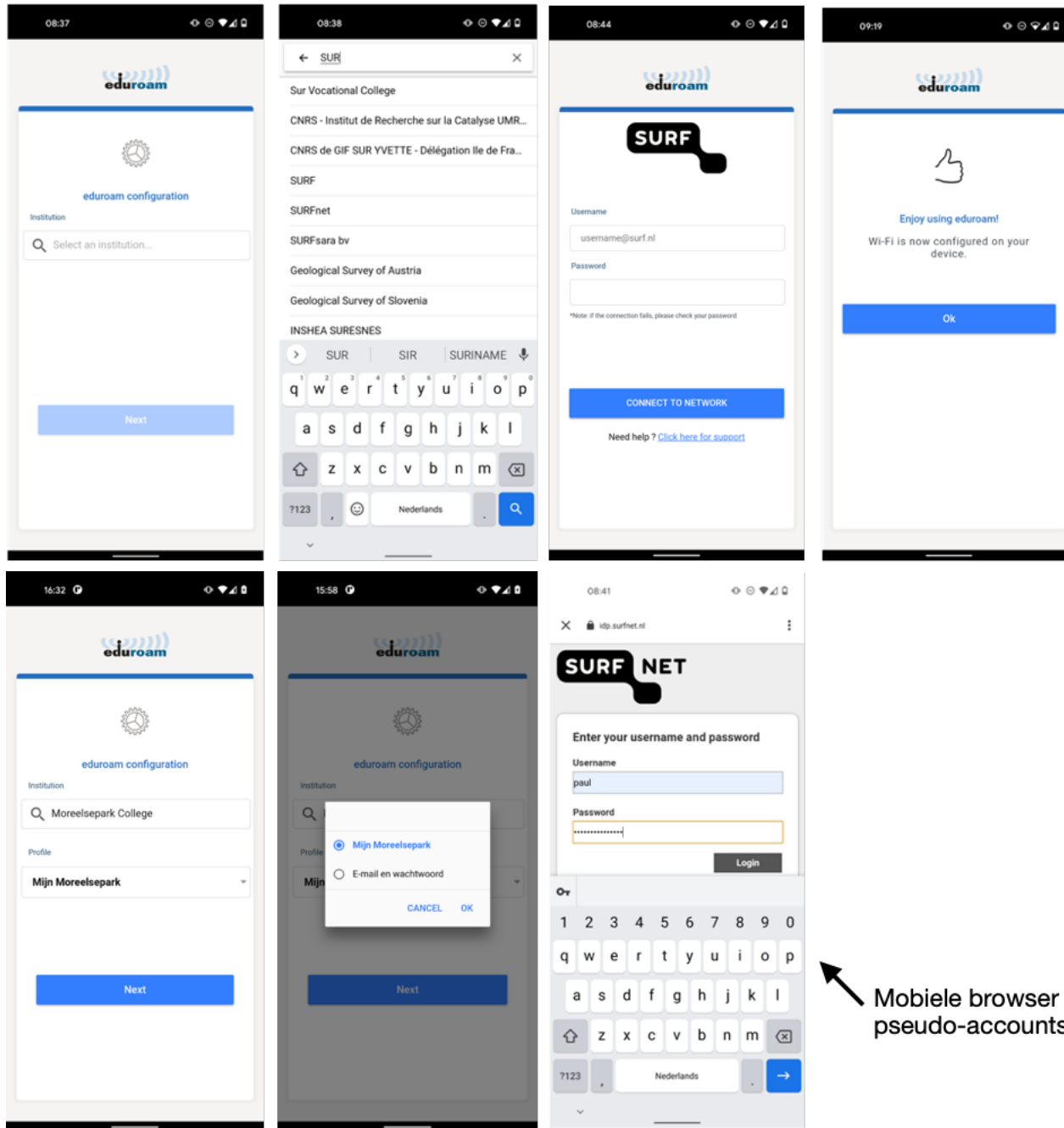


- Chicken-Egg: need connectivity for the app



geteduroam scenarios

- Use organization profile
- Hosted geteduroam, pseudo accounts via SAML



Mobile browser voor pseudo-accounts



geteduroam

- User-friendly Apps to properly onboard devices
 - Replaces old eduroam CAT app for Android
- Increased security and flexibility with certificates and (Cloud) IdPs
- OT Service connected to eduGAIN, ask SUNET for onboarding in trial
- Comes at the right time for onboarding Passpoint/OpenRoaming, and WPA3 R3


OpenRoaming

- If you are in eduroam, you can be in OpenRoaming
- eduroam OT provides global infrastructure to use OpenRoaming as IdP, or for SP trials
- Feel free to ask for more details/benefits of WBA membership



 Paul Dekkers

 paul.dekkers@surf.nl

 @pauldekkers

SURF