eduroam

evoluzione a livello globale

Paul Dekkers

eduroam, SURF

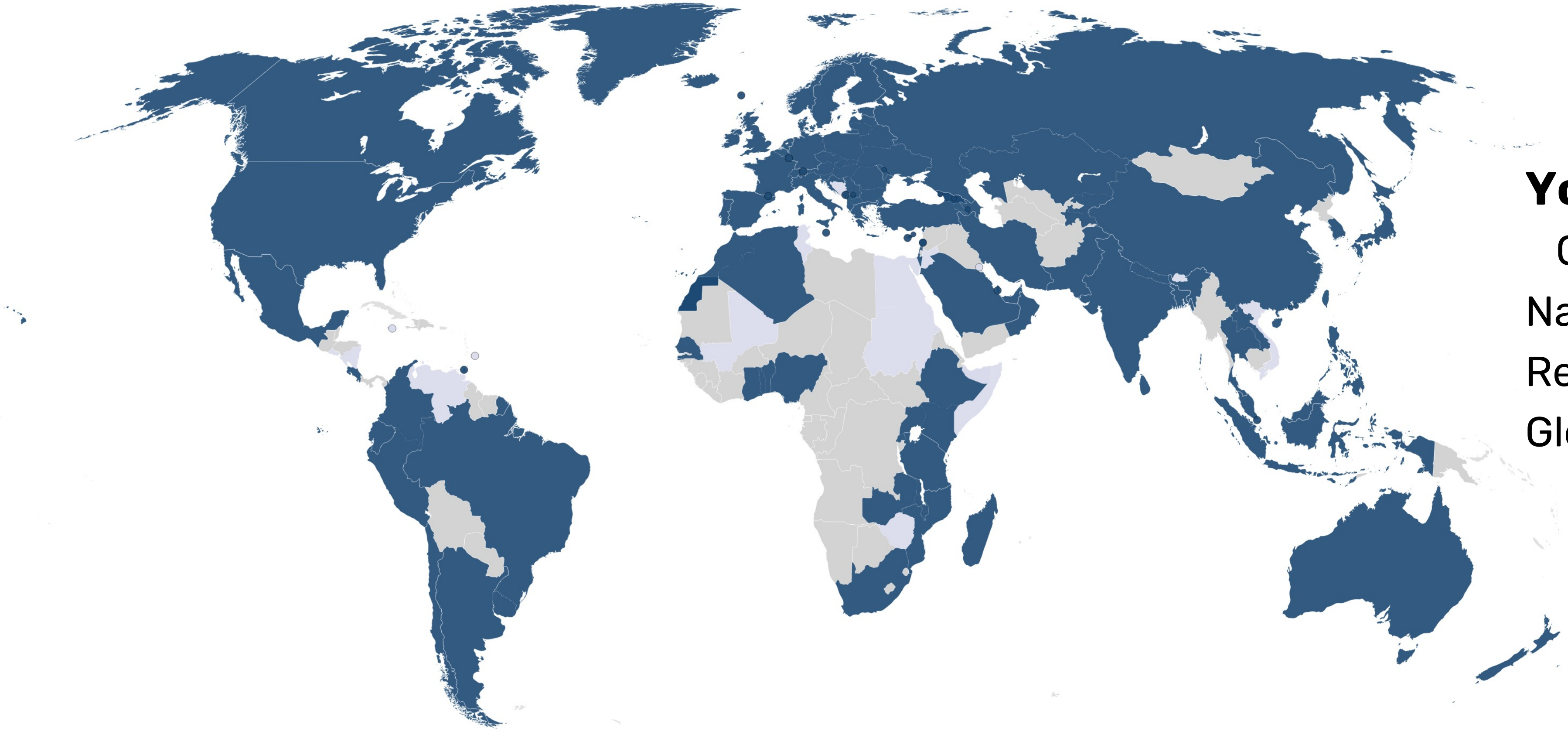
WORKSHOP GARR 2021

NET MAKERS

eduroam

Global eduroam

- eduroam, a service we all build together



You !

Campuses, IdPs, SPs

National roaming operators

Regions

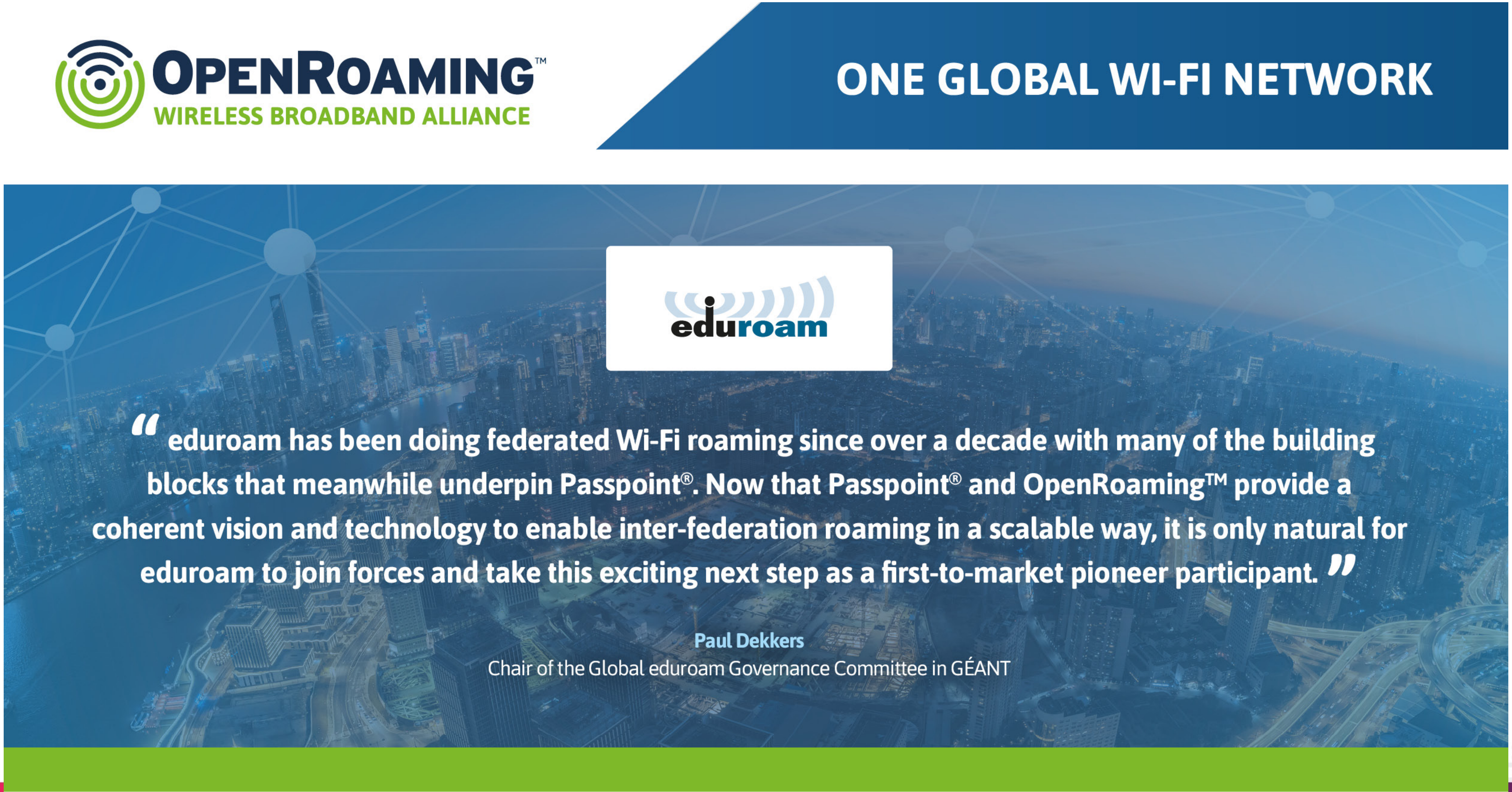
Global eduroam

Global developments, hightlight today

- Operations, development
  - International proxies
  - Supporting services, like eduroam CAT
  - Monitoring, data exchange
- Liason different organizations
  - Wi-Fi-Alliance
  - WBA
  - …
- **OpenRoaming**
- **geteduroam**

eduroam is WBA member (so you benefit)

Participation, similarities, what does it mean…



OPENROAMING™

WIRELESS BROADBAND ALLIANCE

ONE GLOBAL WI-FI NETWORK

eduroam

> “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

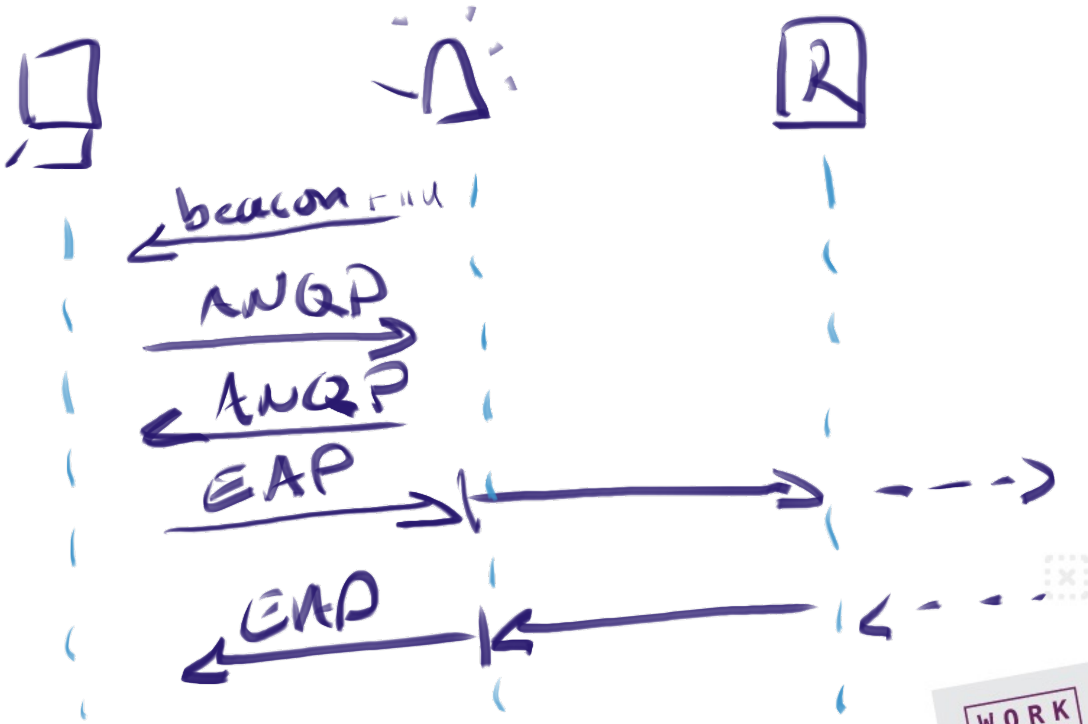
eduroam, (inter fed) roaming, …

- **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

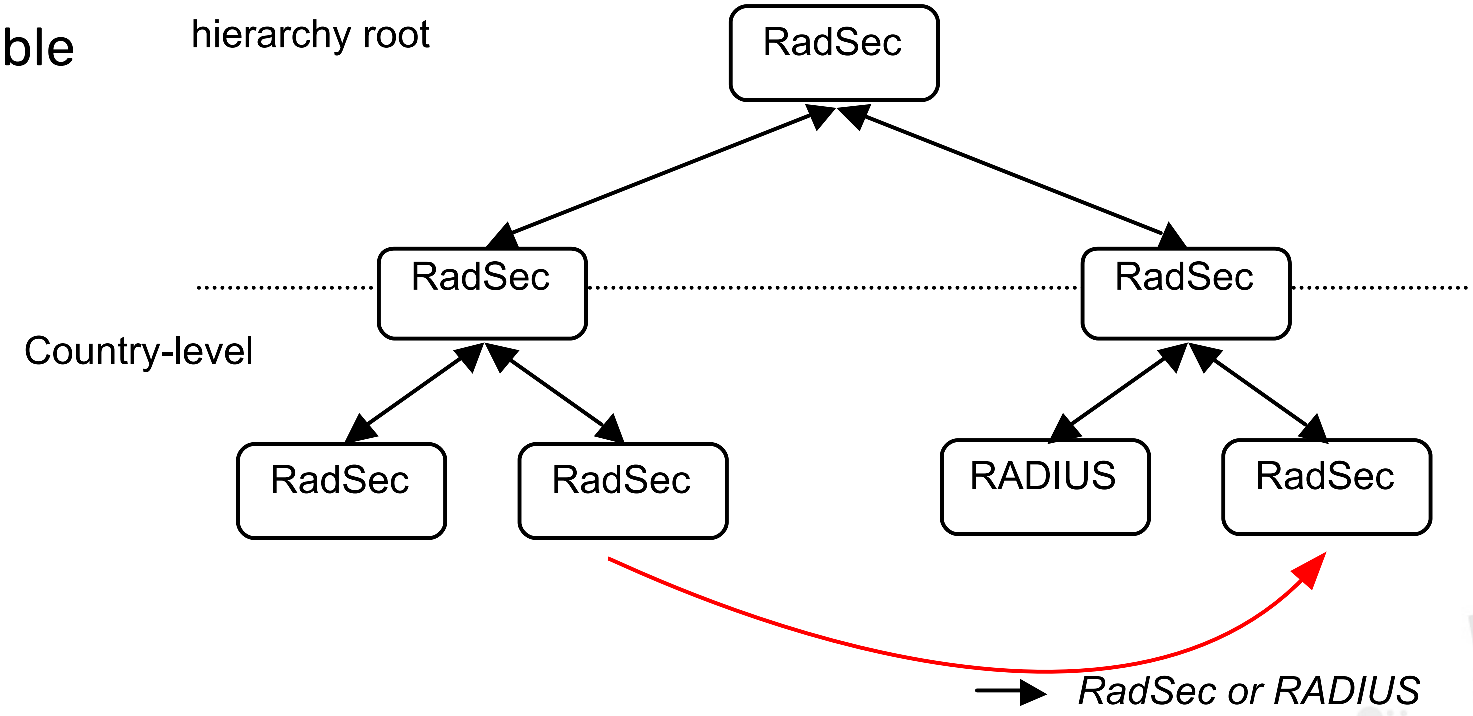
Hotspot 2.0, HS20, Passpoint®, 802.11u

- More than just SSIDs:
  - **RCOI** (Roaming Consortium Organization Identifier),
  - NAIrealm, domain, 3GPP (MNC/MCC, offloading)
- ANQP (Access Network Query Protocol) for discovery of netwerks (home, roaming, EAP-types)
- Afterwards: WPA(2)-Enterprise, EAP
- Multiple releases, limited support
  R1: Basics, 802.11u
  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



Passpoint, dynamic peer discovery, … OpenRoaming™

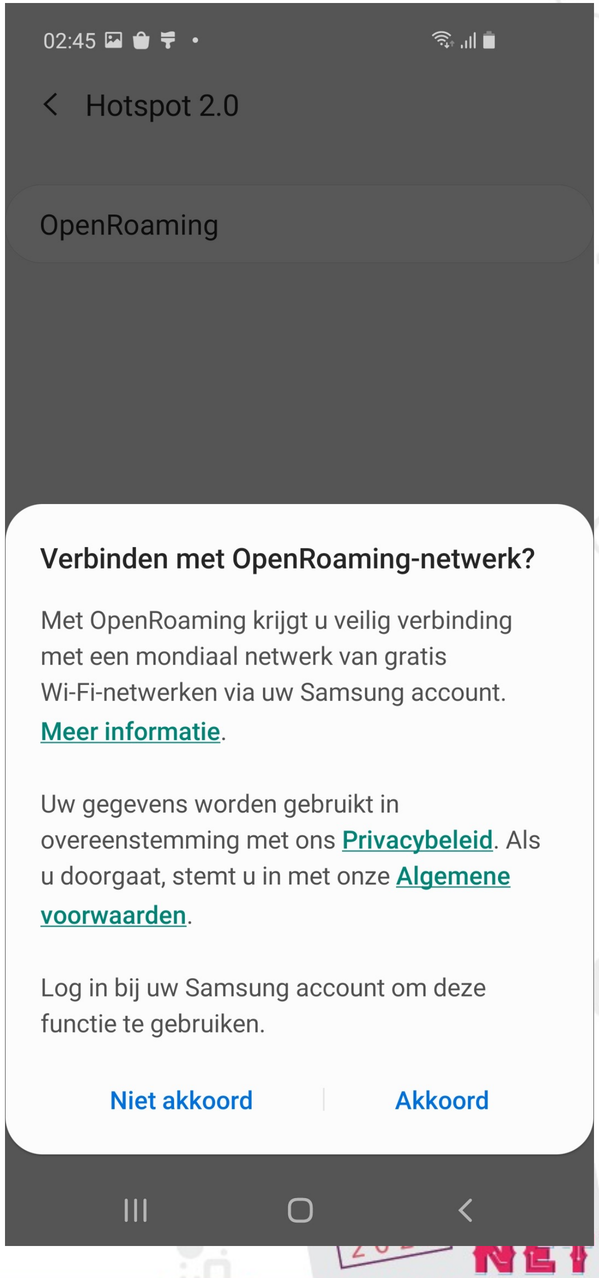
- Previous slides showed technology behind Passpoint and dynamic peer discovery
- We do this (in part) in eduroam

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)



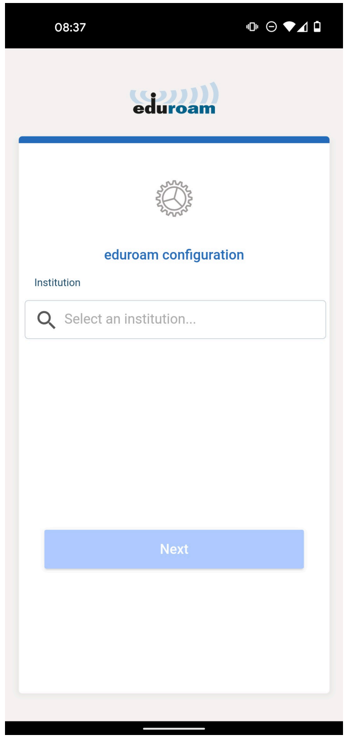
Verbinden met OpenRoaming-netwerk?

Met OpenRoaming krijgt u veilig verbinding met een mondiaal netwerk van gratis Wi-Fi-netwerken via uw Samsung account. Meer informatie.

Uw gegevens worden gebruikt in overeenstemming met ons Privacybeleid. Als u doorgaat, stemt u in met onze Algemene voorwaarden.

Log in bij uw Samsung account om deze functie te gebruiken.

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

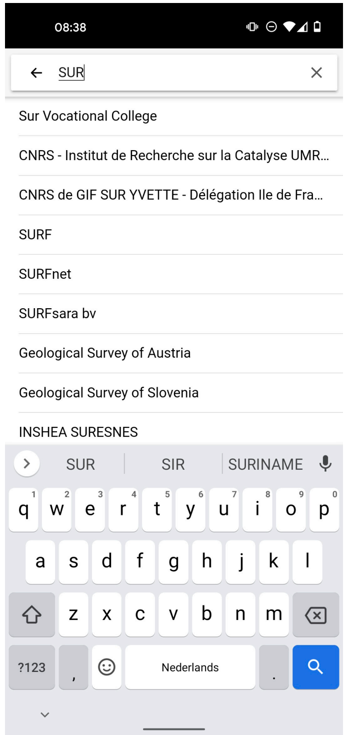

08:37

eduroam configuration

Institution

Select an institution...

Next


08:38

SUR

Sur Vocational College

CNRS - Institut de Recherche sur la Catalyse UMR...

CNRS de GIF SUR YVETTE - Délégation Ile de Fra...

SURF

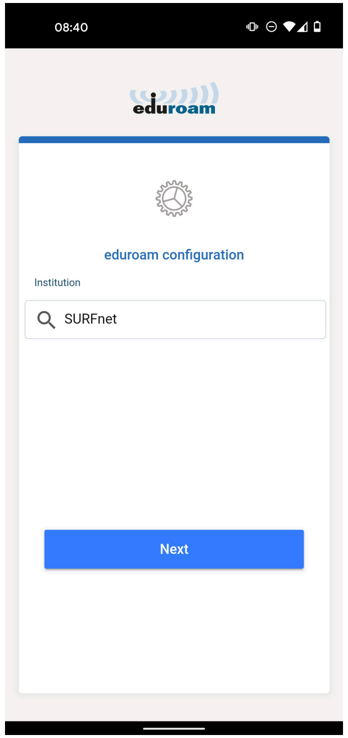
SURFnet

SURFsara bv

Geological Survey of Austria

Geological Survey of Slovenia

INSHEA SURESNES

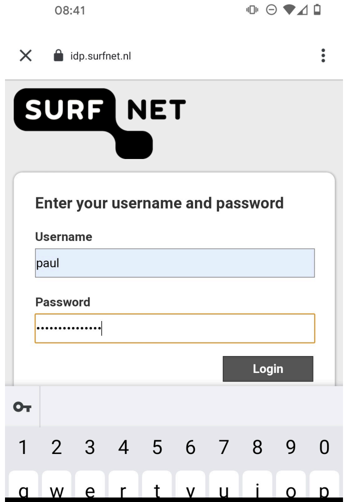

08:40

eduroam configuration

Institution

SURFnet

Next


08:41

idp.surfnet.nl

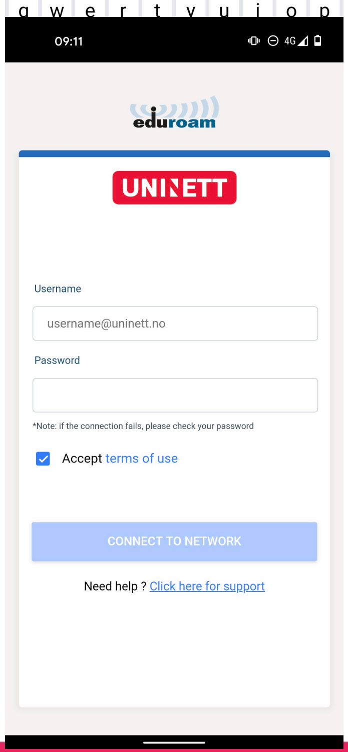
SURF NET

Enter your username and password

Username: paul

Password: ················

Login


09:11

UNINETT

Username

username@uninett.no

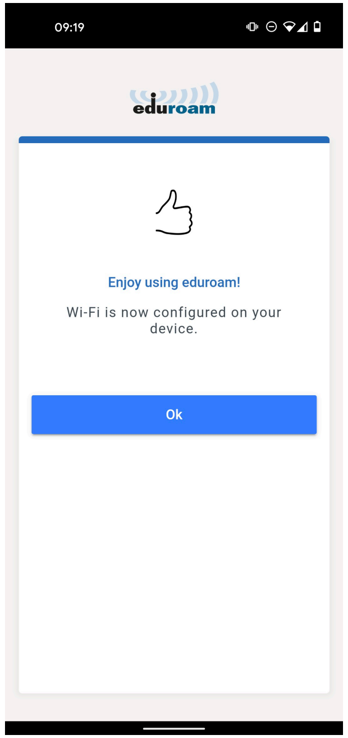
Password

*Note: if the connection fails, please check your password

☑ Accept terms of use

CONNECT TO NETWORK

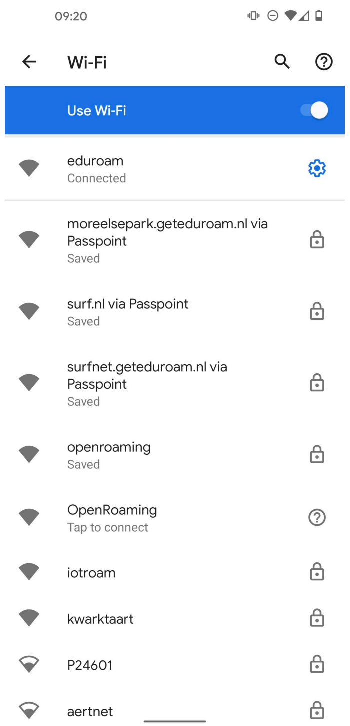
Need help ? Click here for support


09:19

Enjoy using eduroam!

Wi-Fi is now configured on your device.

Ok


09:20

Wi-Fi

Use Wi-Fi

eduroam
Connected

moreelsepark.geteduroam.nl via Passpoint
Saved

surf.nl via Passpoint
Saved

surfnet.geteduroam.nl via Passpoint
Saved

openroaming
Saved

OpenRoaming
Tap to connect

iotroam

kwarktaart

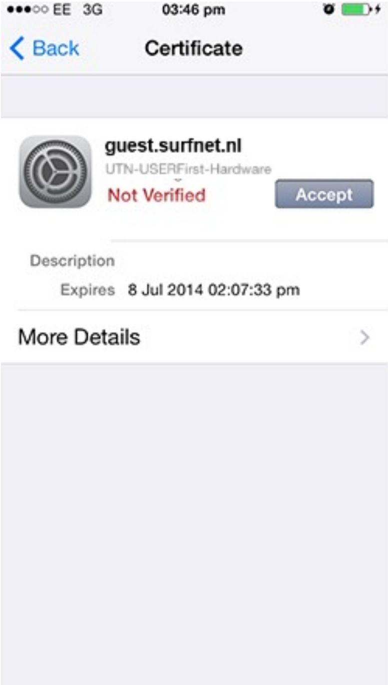
P24601

aertnet

Also, for: security, privacy

- Mutual authentication easiest attack-vector (EAPHammer)
  - -PAP < -MSCHAPv2 < EAP-TLS
- User is the weakest link
  - Trust-on-first-use (TOFU)
- https://eduroam.org/eduroam-advisory-mutualauth/
- 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)



guest.surfnet.nl

UTN-USERFirst-Hardware

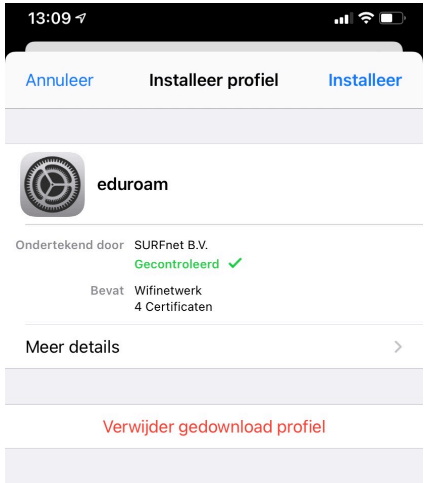
Not Verified

Accept

Description

Expires 8 Jul 2014 02:07:33 pm

More Details



eduroam

Ondertekend door SURFnet B.V.

Gecontroleerd ✓

Bevat Wifinetwerk

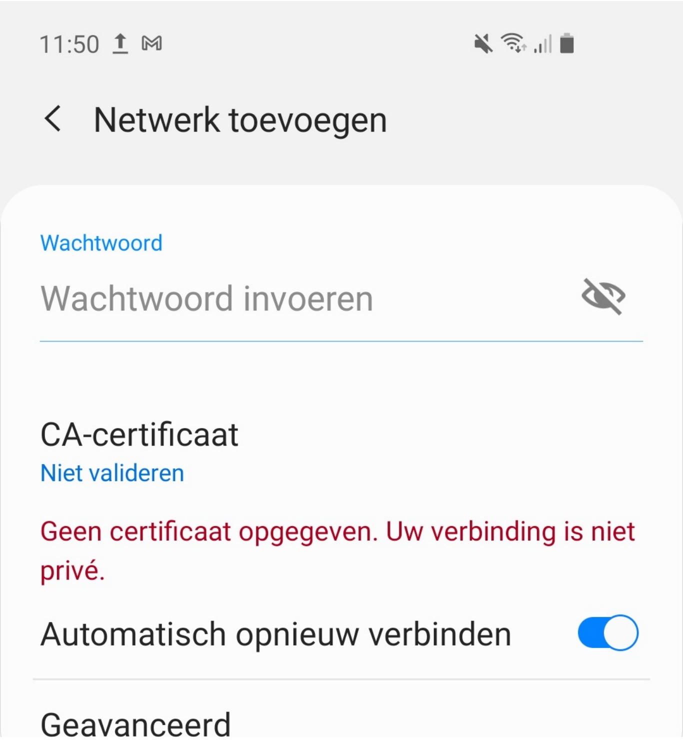
4 Certificaten

Meer details

Verwijder gedownload profiel

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.)



11:50

Netwerk toevoegen

Wachtwoord

Wachtwoord invoeren

CA-certificaat

Niet valideren

Geen certificaat opgegeven. Uw verbinding is niet privé.

Automatisch opnieuw verbinden

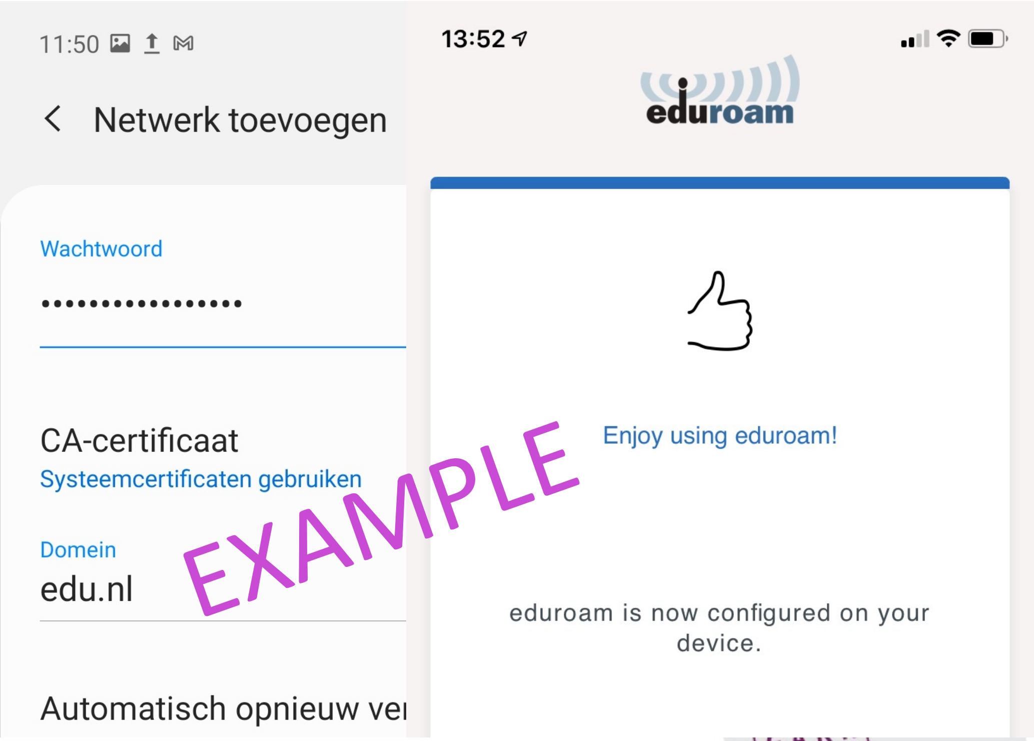
Geavanceerd

Still not OK? Options:

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

Easier and better:

- Installer, eduroam CAT / geteduroam



11:50

Netwerk toevoegen

Wachtwoord

••••••••••••••••

CA-certificaat

Systeemcertificaten gebruiken

Domein

edu.nl

Automatisch opnieuw ver

13:52

eduroam

Enjoy using eduroam!

eduroam is now configured on your device.

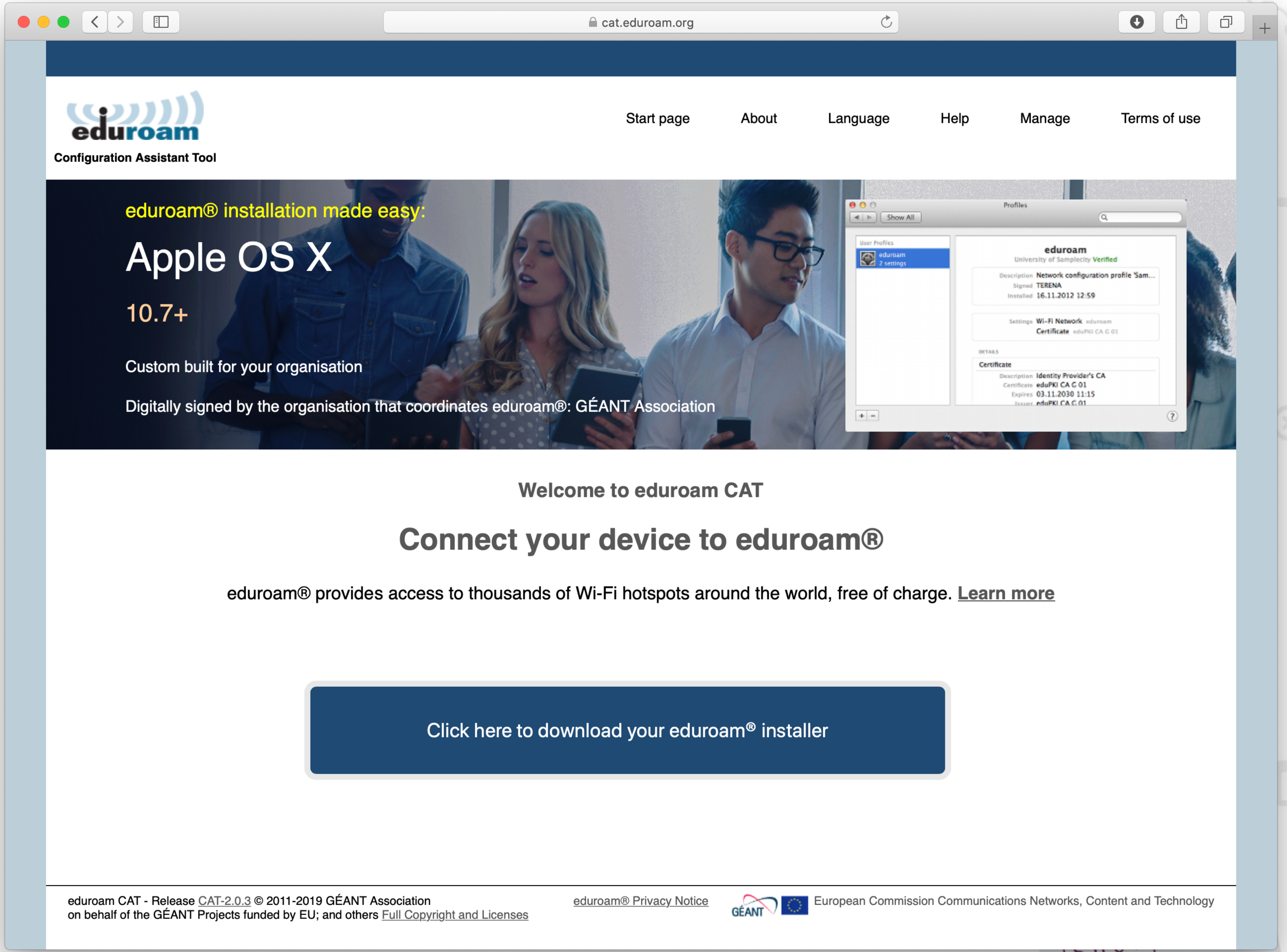
eduroam CAT

👍

- 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



Configuration Assistant Tool

eduroam® installation made easy:

Apple OS X

10.7+

Custom built for your organisation

Digitally signed by the organisation that coordinates eduroam®: GÉANT Association

eduroam
University of Samplecity Verified

Description Network configuration profile 'Sam...
Signed TERENA
Installed 16.11.2012 12:59

Settings Wi-Fi Network eduroam
Certificate eduPKI CA G 01

DETAILS

Certificate
Description Identity Provider's CA
Certificate eduPKI CA G 01
Expires 03.11.2030 11:15
Issuer eduPKI CA G 01

Welcome to eduroam CAT

Connect your device to eduroam®

eduroam® provides access to thousands of Wi-Fi hotspots around the world, free of charge. Learn more

eduroam CAT - Release CAT-2.0.3 © 2011-2019 GÉANT Association
on behalf of the GÉANT Projects funded by EU; and others Full Copyright and Licenses

eduroam® Privacy Notice

European Commission Communications Networks, Content and Technology

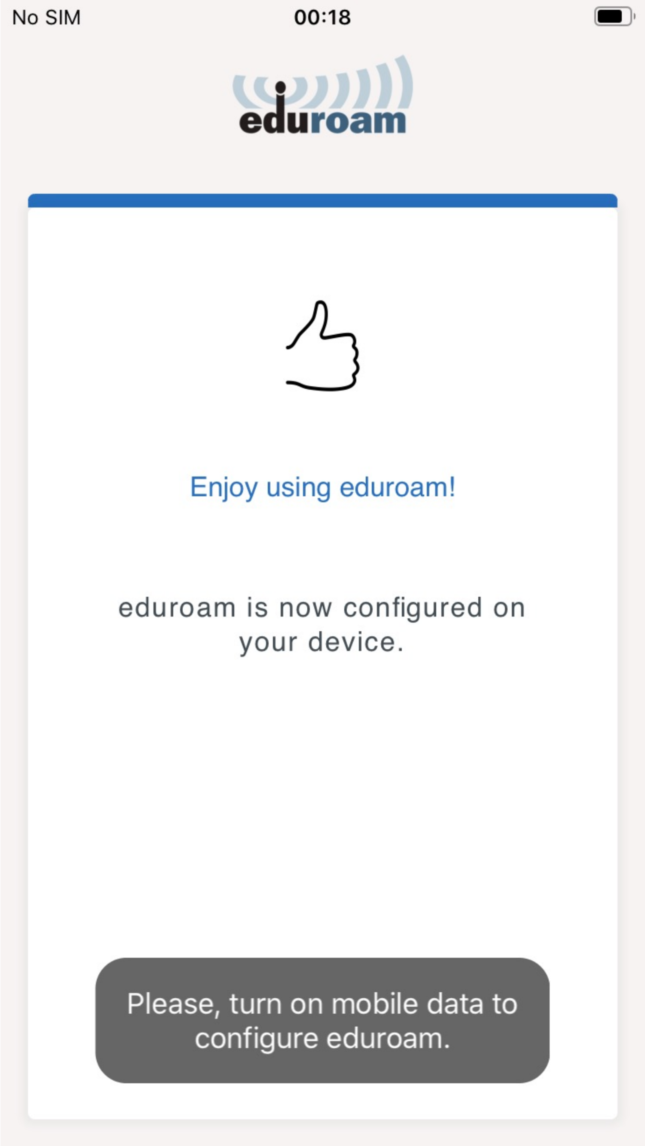
geteduroam

👍

- Good client for all platforms
- Contains CAT profiles: works for all organizations!
- Passpoint, Hotspot 2.0 settings (OpenRoaming!)
- Alternative workflow to provision TLS 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



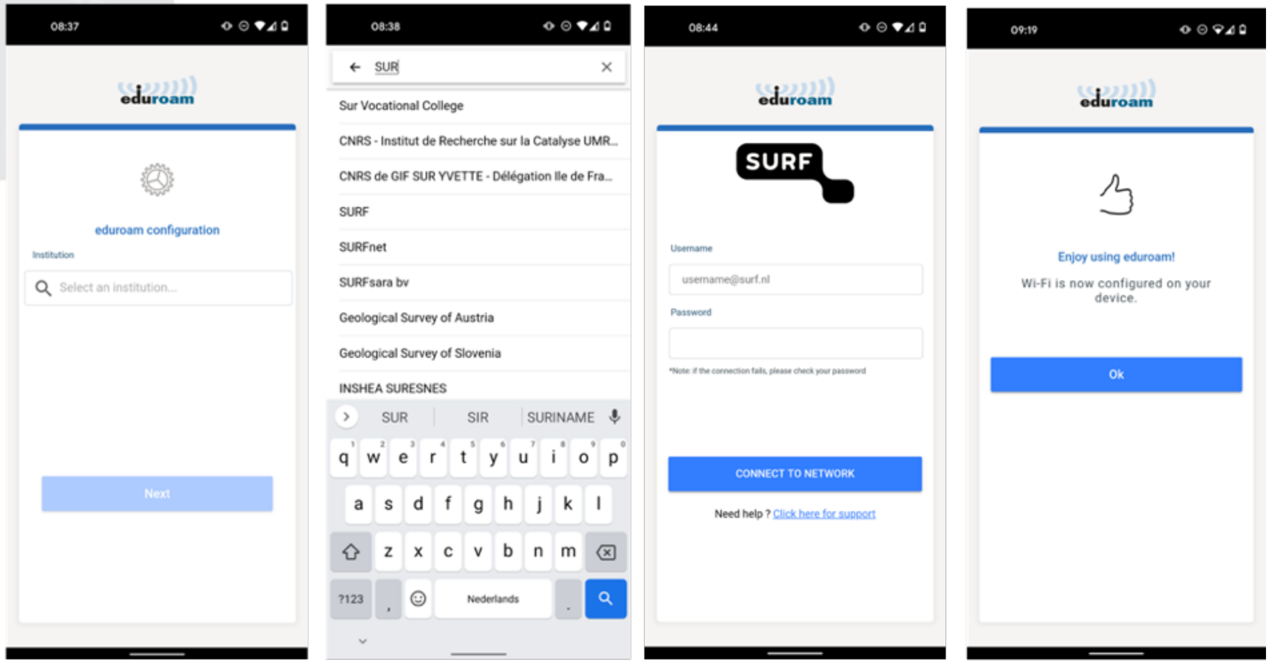
Enjoy using eduroam!

eduroam is now configured on your device.

Please, turn on mobile data to configure eduroam.

geteduroam scenarios

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



08:37

eduroam

eduroam configuration

Institution

Select an institution...

Next

08:38

SUR

Sur Vocational College

CNRS - Institut de Recherche sur la Catalyse UMR...

CNRS de GIF SUR YVETTE - Délégation Ile de Fra...

SURF

SURFnet

SURFsara bv

Geological Survey of Austria

Geological Survey of Slovenia

INSHEA SURESNES

08:44

eduroam

SURF

Username

username@surf.nl

Password

*Note: if the connection fails, please check your password

CONNECT TO NETWORK

Need help ? Click here for support

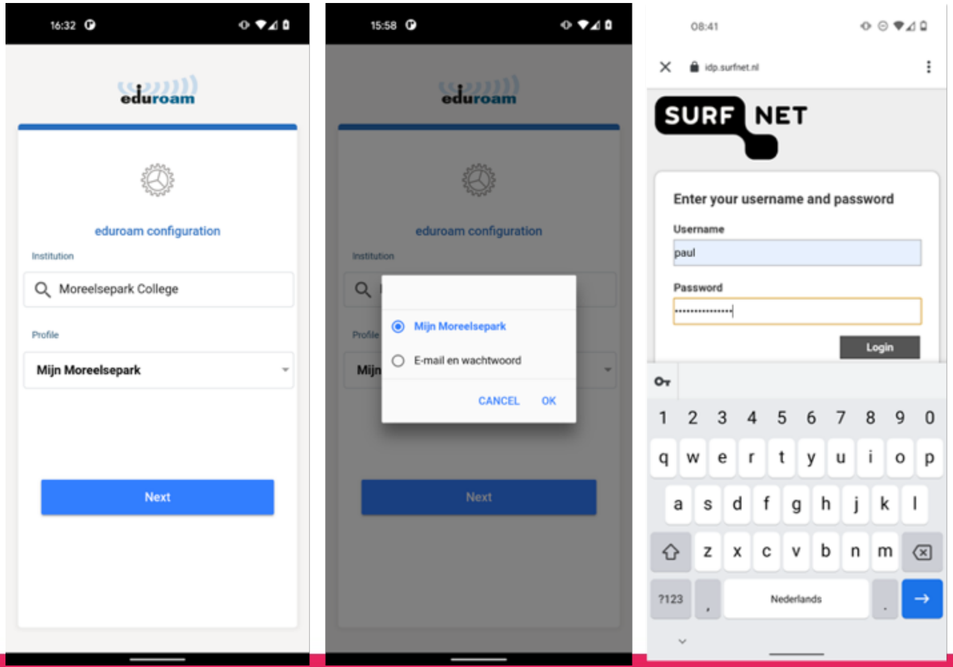
09:19

eduroam

Enjoy using eduroam!

Wi-Fi is now configured on your device.

Ok



16:32

eduroam

eduroam configuration

Institution

Moreelsepark College

Profile

Mijn Moreelsepark

Next

15:58

eduroam configuration

● Mijn Moreelsepark

○ E-mail en wachtwoord

CANCEL OK

Next

08:41

idp.surfnet.nl

SURF NET

Enter your username and password

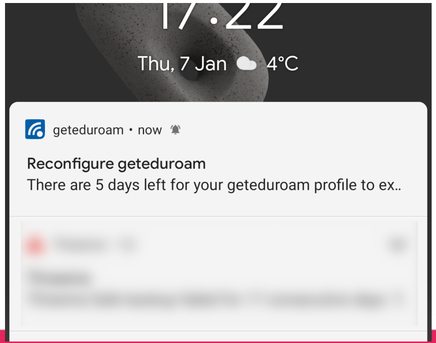
Username

paul

Password

Login

Mobiele browser voor pseudo-accounts



17:22

Thu, 7 Jan 4°C

geteduroam • now

Reconfigure geteduroam

There are 5 days left for your geteduroam profile to ex..

geteduroam, OpenRoaming

- User-friendly Apps to properly onboard devices
    - Replaces old eduroam CAT app for Android
- Increased security and flexibility with certificates and (Cloud) IdPs
- Comes at the right time for onboarding Passpoint/OpenRoaming, and WPA3 R3
- eduroam users may benefit from future OpenRoaming sites