

OPENROAMING GETEDUROAM

Paul Dekkers

October 13, 2020, SUNET

SURF



“ 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

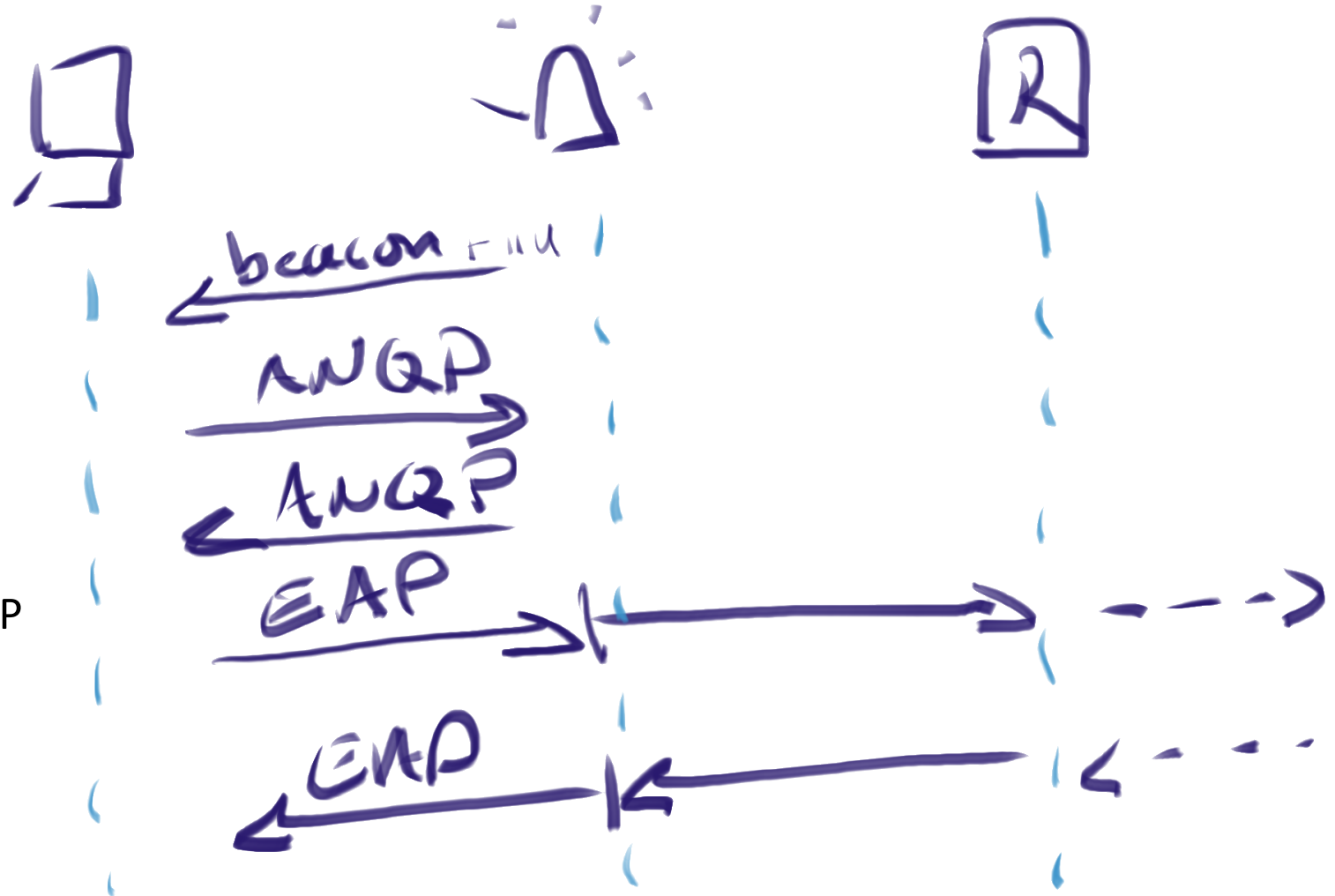
eduroam, (inter fed) roaming, ... OpenRoaming™

- eduroam is the biggest federated roaming-infrastructure
 - 7200 IdPs
 - 30000 locations
 - 106 countries
- Roaming by standardizing on SSID
- Blueprint, authorisation, use-case, rules are simple
- Global governance (GeGC), regions, NROs

- More roaming hubs, between mobile operators, vendors, providers, NGH trials
- Complex matrix asks for complex technology?
- Hotspot 2.0/Passpoint, Dynamic peer discovery

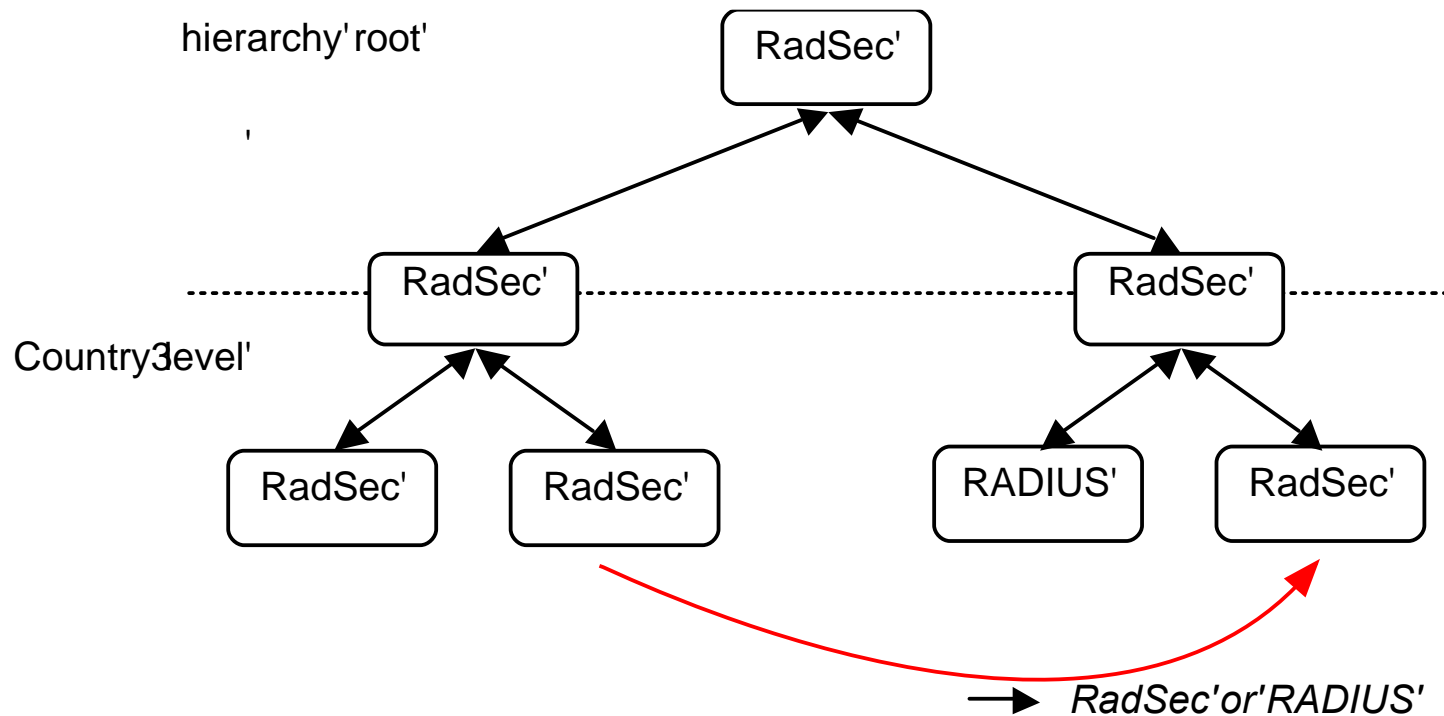
Hotspot 2.0, HS20, Passpoint®, 802.11u

- 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.
```

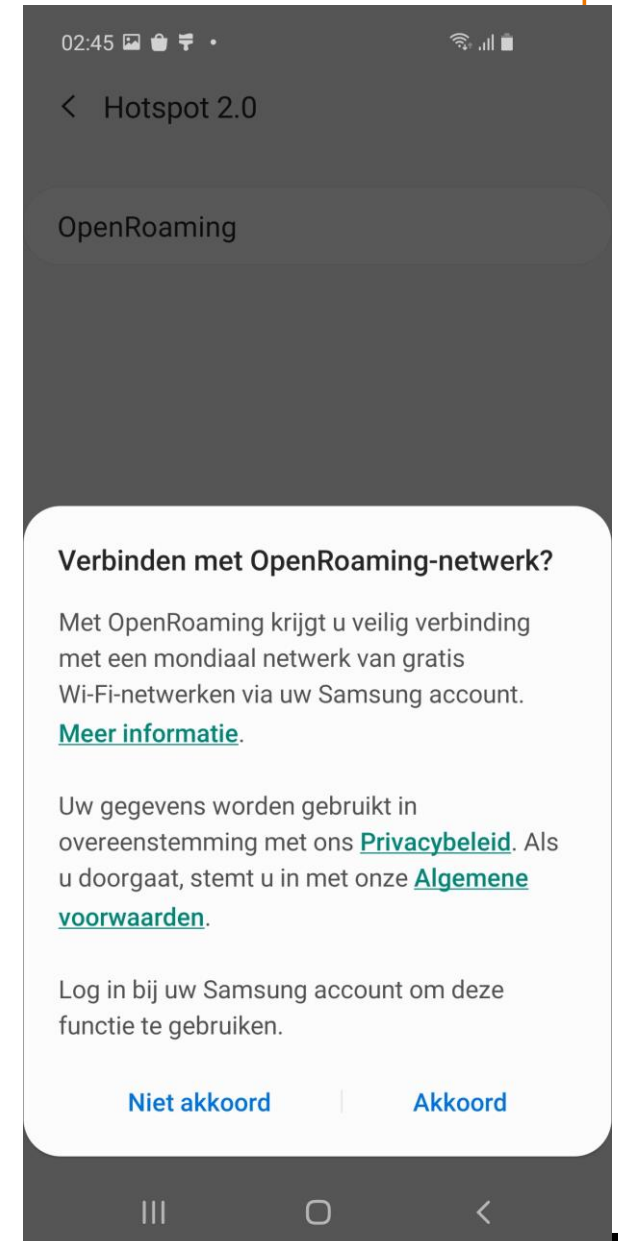
- OpenRoaming:

```
% 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.
```


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
 - eduroam 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)



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 one big SP for eduroam (without sacrificing SSIDs), eduroam as one big IdP
- Decided to use and promote the eduroam RCOIs (opt-out)
- Promote use of specific OpenRoaming RCOIs in profiles (opt-in)
- Provisioning will be important (geteduroam, CAT)
- Discussion about fallback mechanism, “superglue”
- Trials and Showcases

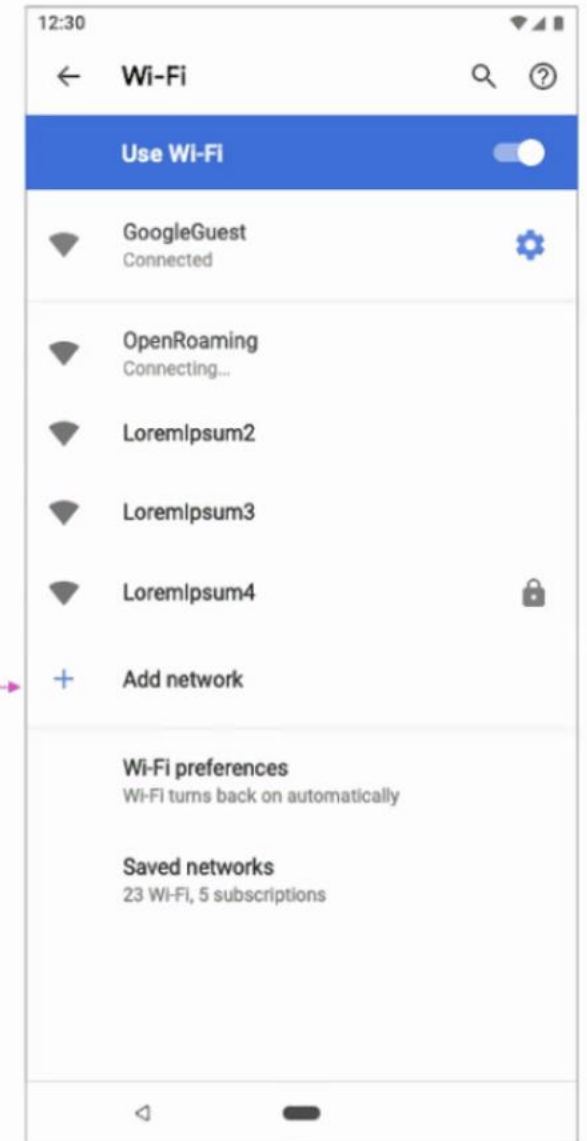
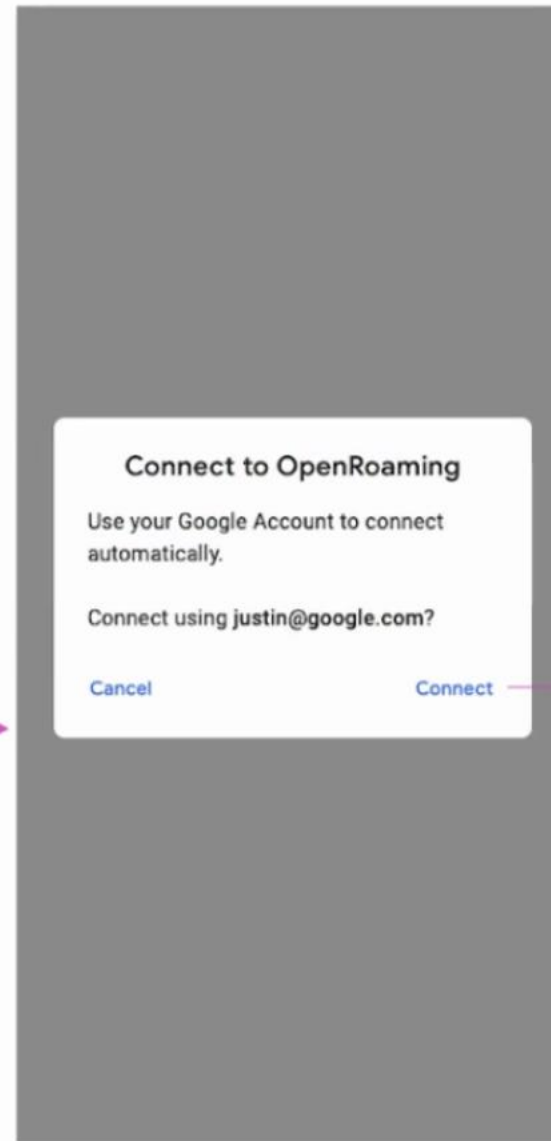
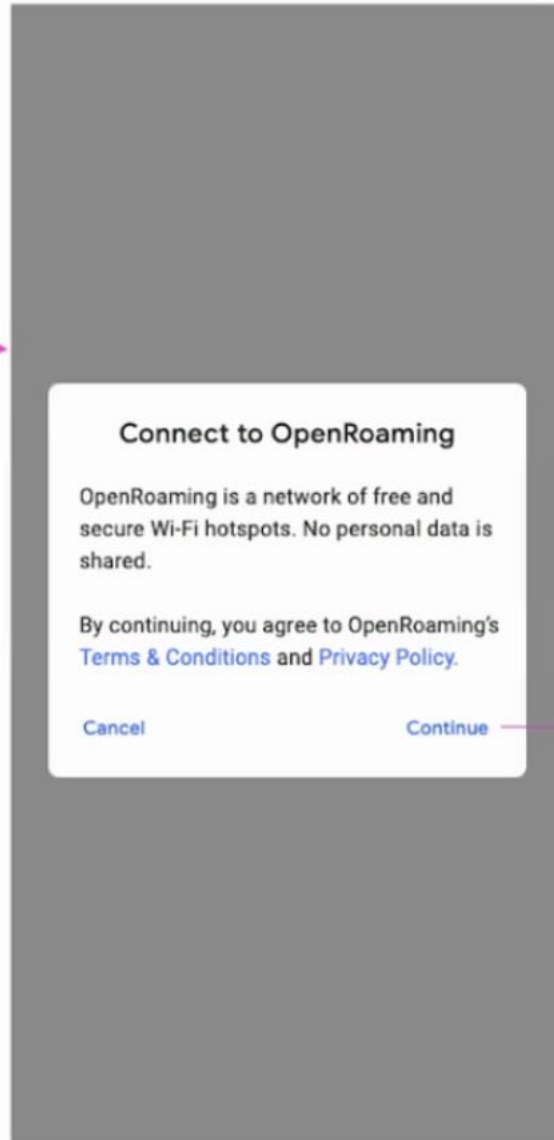
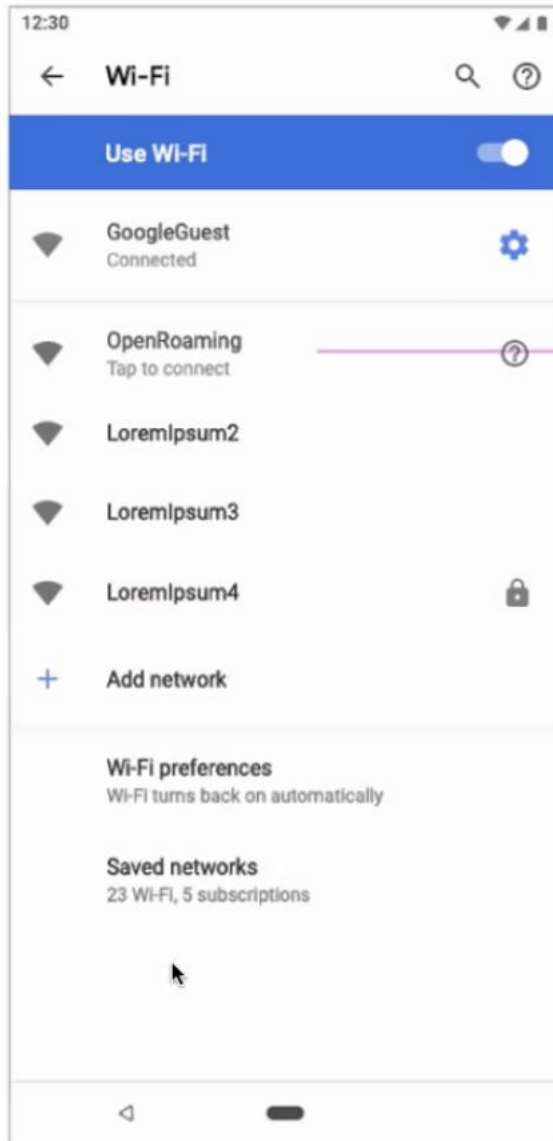
OpenRoaming™ and eduroam: trials!

- 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.
```

- Connect SP via separate proxy, or by using Vendor equipment
 - Configure Hotspot 2.0
 - Have visitors
 - Compatible policies, scope
- Showcases

Android 11 makes OpenRoaming so easy



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

eduroam
Configuration Assistant Tool

Start page About Language Help Manage Terms of use

eduroam® installation made easy:
Apple OS X
10.7+

Custom built for your organisation
Digitally signed by the organisation that coordinates eduroam®: GÉANT Association

Profiles

User Profiles
eduroam
2 settings

eduroam
University of Southampton Verified

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

Settings: Wi-Fi Network: eduroam
Certificate: eduPKI CA C 01

DETAILS

Certificate
Description: Identity Provider's CA
Certificate: eduPKI CA C 01
Expires: 03.11.2030 11:15
Issuer: eduPKI CA C 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](#)

Click here to download your eduroam® installer

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](#)

GÉANT European Commission Communications Networks, Content and Technology

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 has 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: 6i5hx5omilfonl7us6t30si13z607uhfahvu@... 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: bx9u5guuhmmpar6c126lbsuxfs18kofotcub@... Expiry: 2035-01-01 07:29:57 Issued: 2019-04-09 09:29:57 Revoke	Device: Android 8.0 Oreo Serial Number: 61ac8677c16c508 CN: bfvxr9f94kss4kk782jhyb7mr7oudunpnjh@... Expiry: 2035-01-01 13:12:15 Issued: 2019-04-11 15:12:15 Revoke	2034-12-31 23:59:59 (UTC) Update	Deactivate User Show Authentication Records New Invitation Activations: 5
	Device: Apple macOS Mojave Serial Number: 69687baea9c27188 CN: 8oqq3z4nw97yty1w6dh6vjkwx2zjp2ycdnn@... Expiry: 2035-01-01 14:13:19 Issued: 2019-09-17 16:13:19 Revoke				

At the bottom, there are buttons for 'Add new user' and 'Import users from CSV file'. A form for adding a new user is visible, with fields for 'Please enter a username of your choice and user expiry date to create a new user: [input] yyyy-MM-dd HH:MM:SS (UTC) [Add new user](#)'.

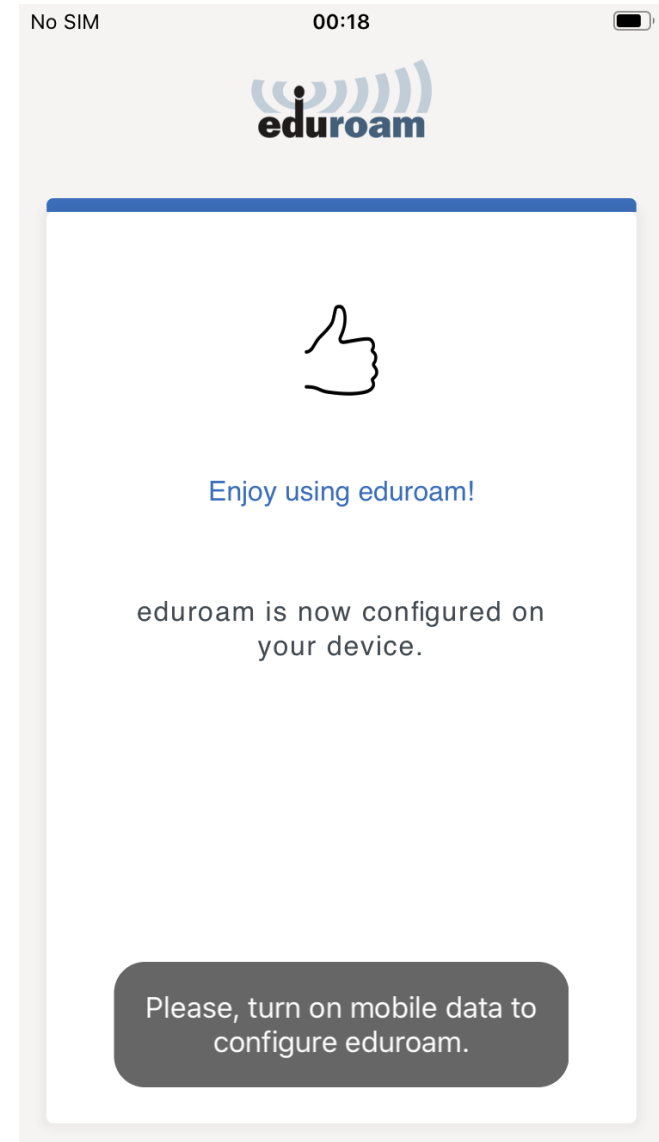
geteduroam



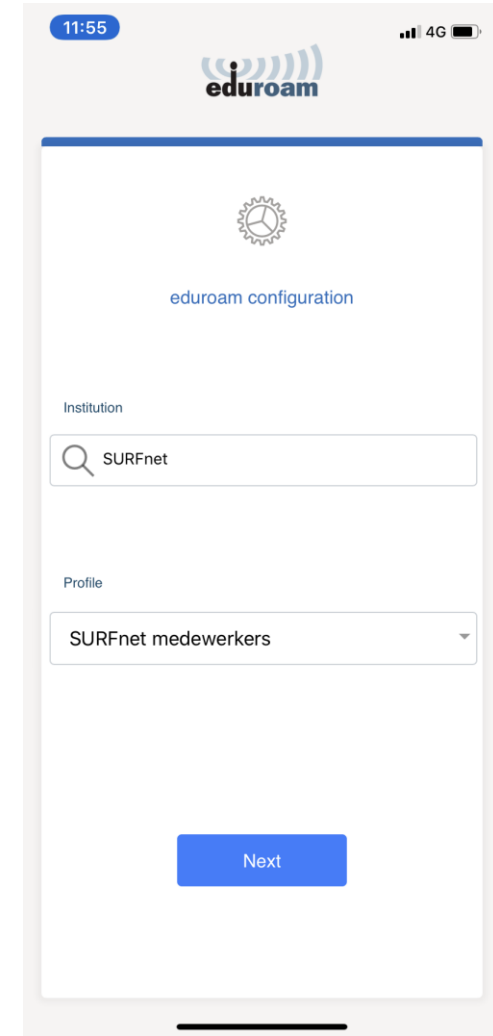
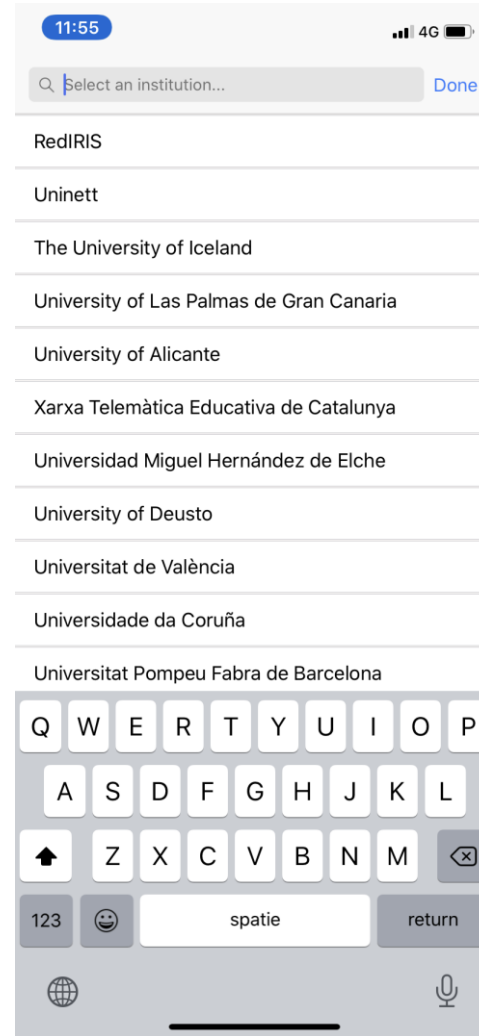
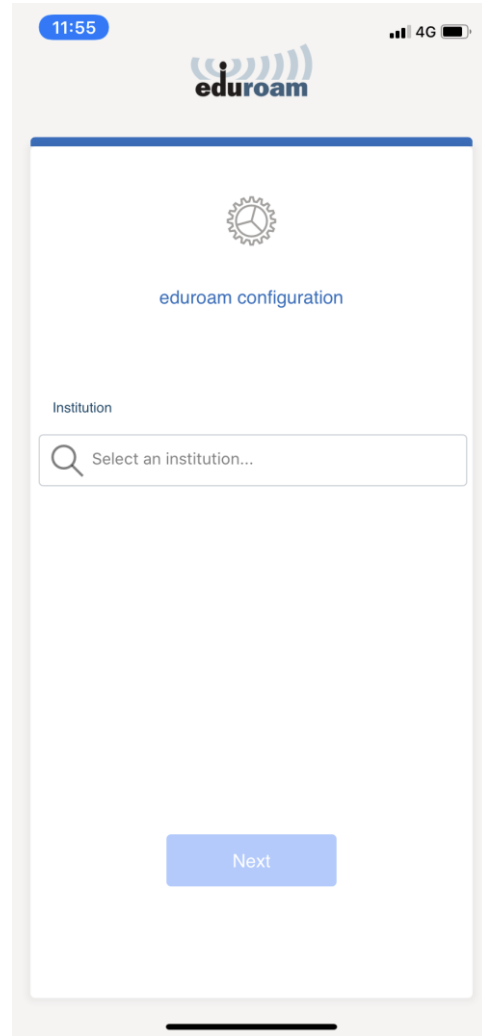
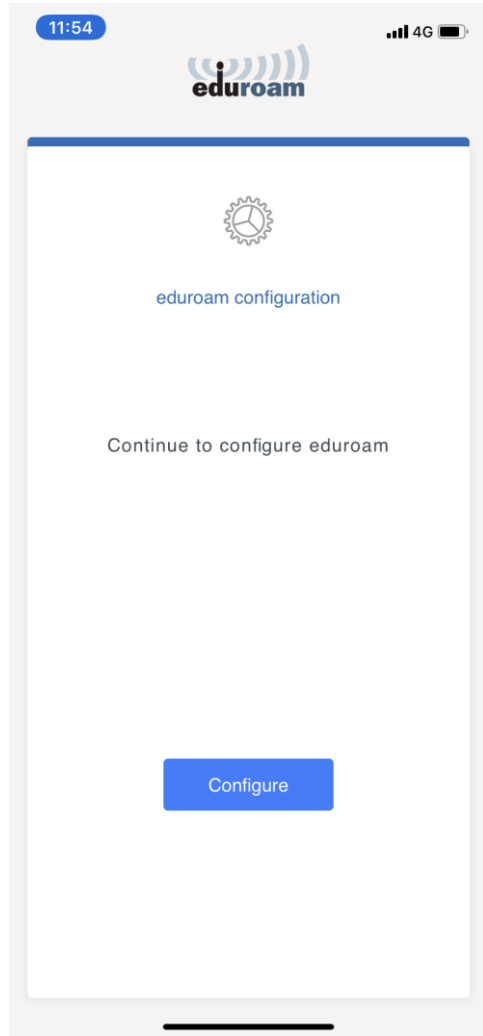
- Good client for all platforms
- Contains CAT profiles: works for all organizations!
- Passpoint, Hotspot 2.0 settings (OpenRoaming!)
- Alternative workflow to provision pseudo-credentials using federated authentication (OAUTH, SAML)
- With that flow: also a Hosted IdP
- Initiative from NORDUnet and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



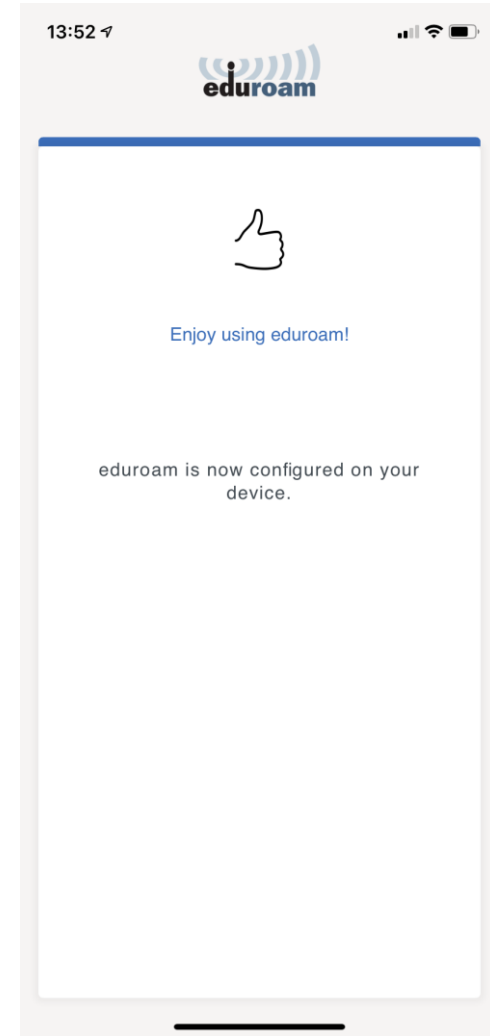
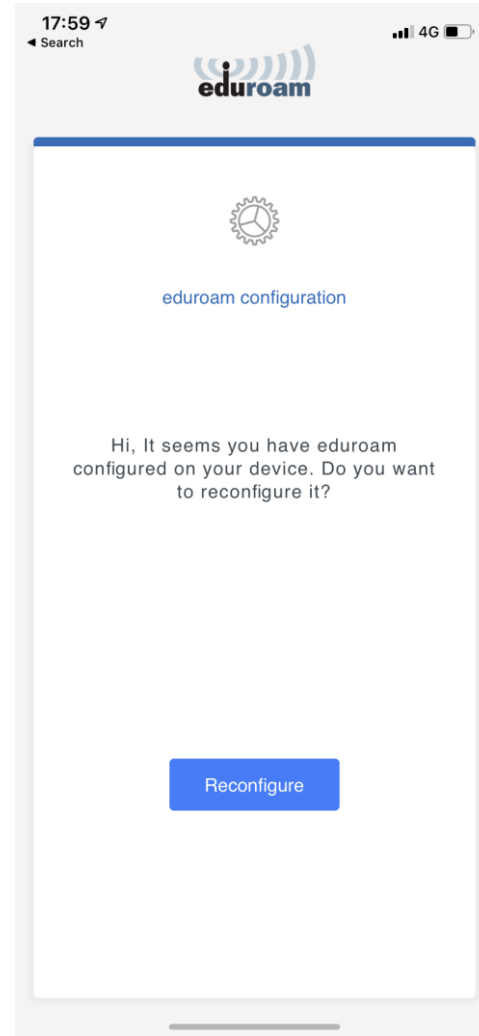
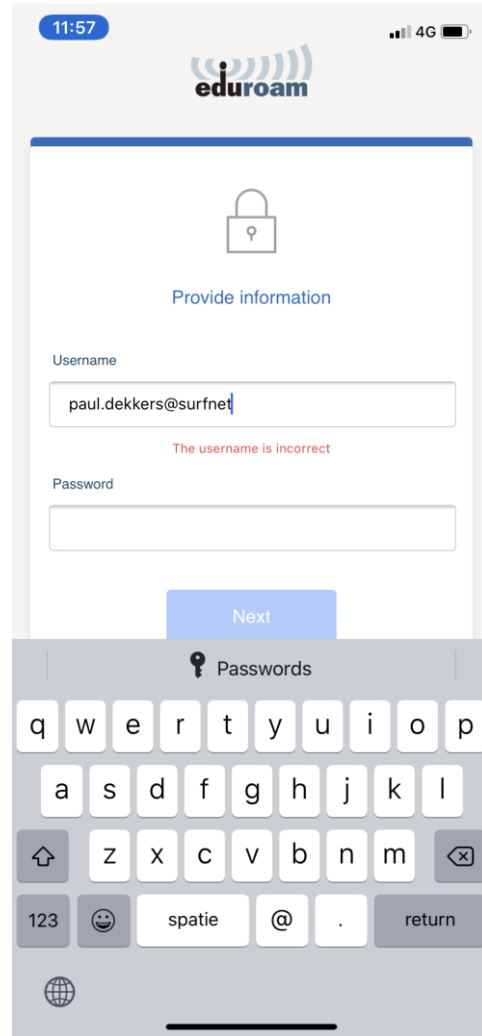
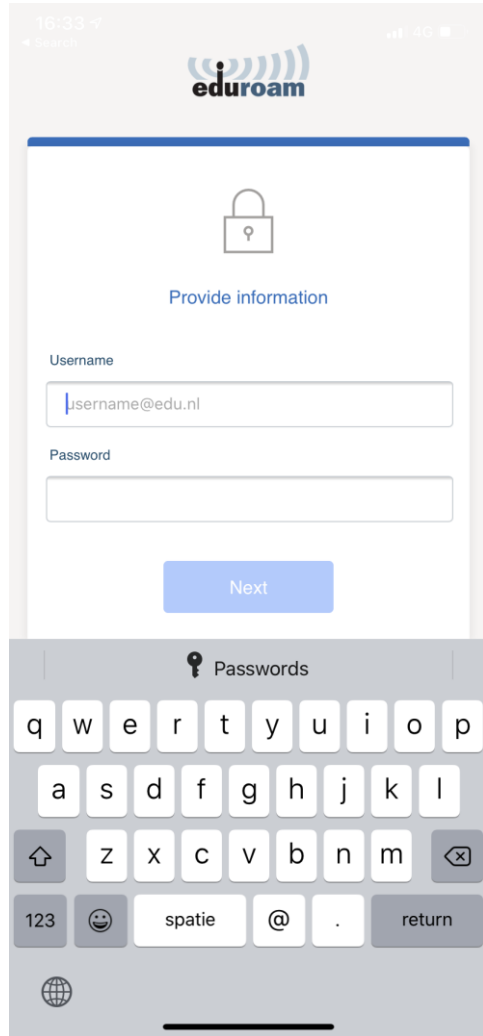
- Chicken-Egg: need connectivity for the app (unless our QR plan works out)



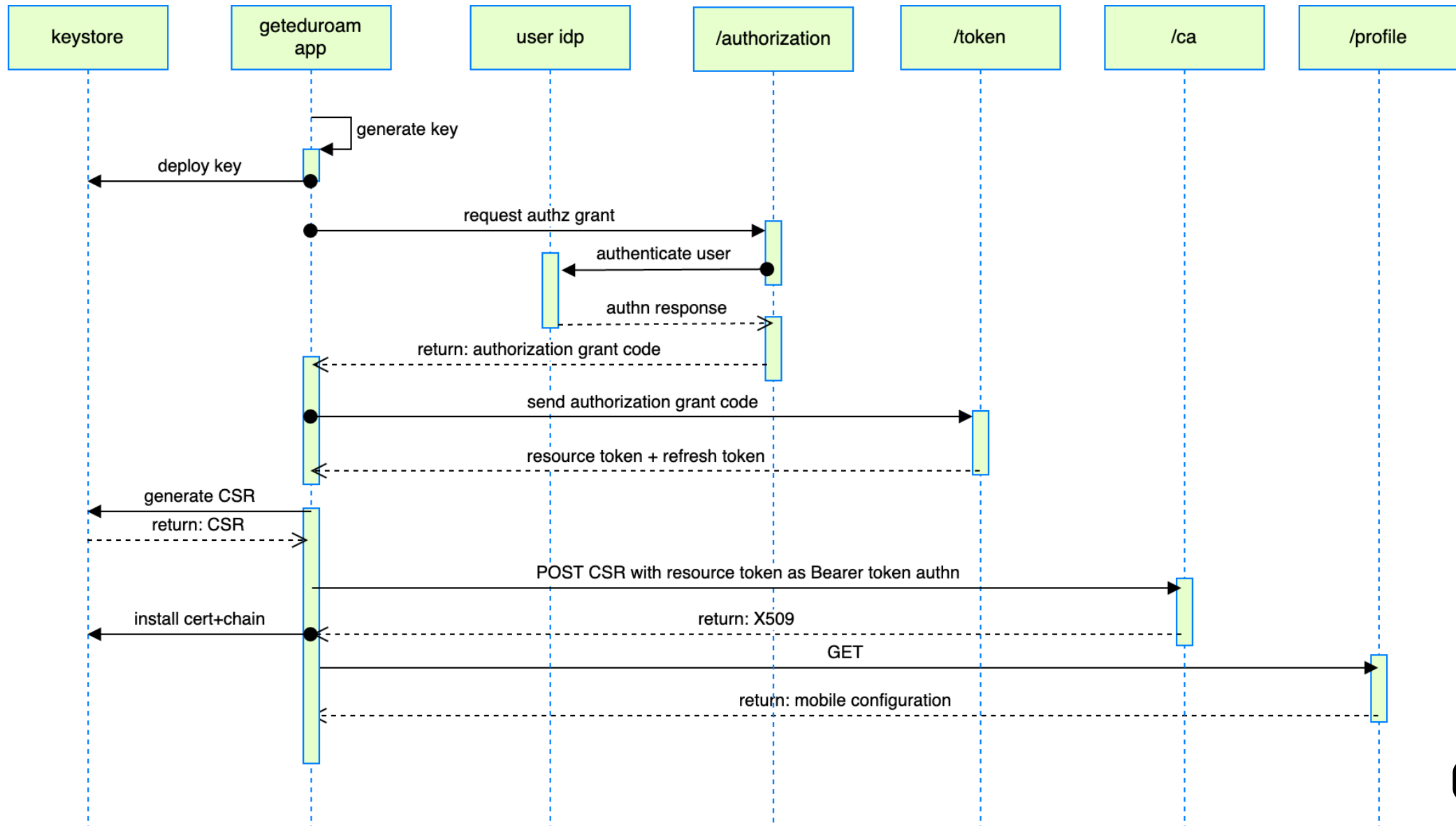
geteduroam client (1)



geteduroam client (2)

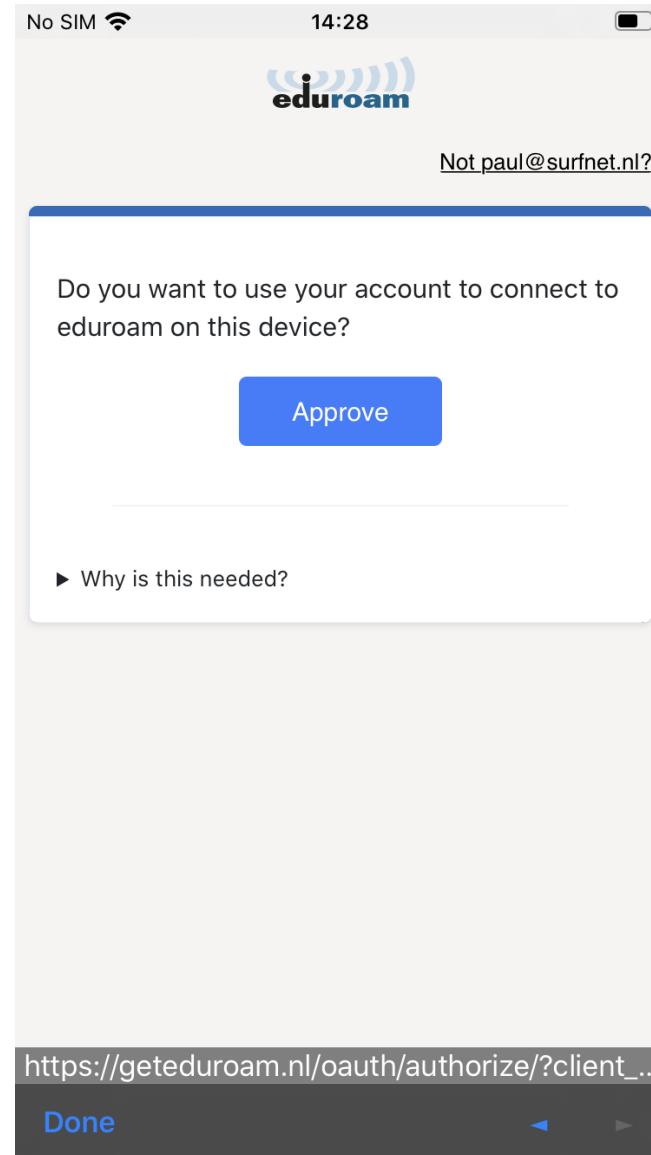


geteduroam certificate workflow (1)



geteduroam certificate workflow (2)

- Select IdP, authenticate at own IdP (via federated auth)
 - This is an option for organizations with SAML IdPs only even cloud-hosted
- Sideloaded any .eap-config data could work, also u/p
 - Can be sourced from internal systems, future: QR code
- Centralized trial service?



geteduroam status

- Phase 1 completed
 - Basic iOS app
 - Basic Android app
 - Windows app
- Phase 2
 - Hotspot 2.0
 - Better WAYF, geolocation
 - Profile-management
 - Credential renewal
 - macOS: app instead of .mobileconfig (possibly Catalyst)
 - ChromeOS (the Android app?)

github.com/getduroam/ionic-app/projects/1

Search or jump to... Pull requests Issues Marketplace Explore

getduroam / ionic-app Watch 3 Star 2 Fork 2

<> Code Issues 30 Pull requests 6 Actions Projects 1 Wiki Security Insights Settings

Phase II Updated 5 hours ago Filter cards + Add cards(2 new) Fullscreen Menu

3 To Do

- Handle redirect in discovery #19 opened by jornane android Phase II
- ChromeOS support #18 opened by jornane android enhancement Phase II
- MacOS support through Catalyst #40 opened by jornane apple enhancement Phase II

4 In Progress

- HS20 using API 28 #43 opened by jornane android Phase II
- REGRESSION: App attempts to configure SSID #Passpoint #46 opened by jornane bug Phase II
- Ability to swipe back (return to previous screen) #38 opened by spaetow enhancement Phase II
- Consistently handle prefilling and checking of the realm #36 opened by jornane Phase II

5 Test

- Support multiple SSIDs #24 opened by jornane Phase II

Sideload

#1 #30 #37 are probably the same issue; flow must be correct and handling of sideloaded files must be done

In short, opening an eap-config via sideloading, downloading it via discovery or receiving it via OAuth must have exactly the same result every time

Added by jornane

3 References

- Crash when sideloading an eap-config file #30 opened by jornane apple bug Sideload
- Sideload profile does not work without internet connection #1 opened by jornane android apple bug Sideload
- Choosing a profile while internet is unstable causes uncaught exception and inconsistent state #37 opened by jornane

Automated as Done Manage

1 Done

- HS20 support #10 opened by jornane android apple enhancement Phase II


Resources

- Mailinglist
 - <https://lists.geant.org/sympa/info/geteduroam>
- Slack channel
 - #geteduroam
- Github resources
 - <https://github.com/geteduroam>
- AppStore, TestFlight
 - <https://testflight.apple.com/join/80AujtVR>
 - <https://apps.apple.com/nl/app/geteduroam/id1504076137>
 - <https://play.google.com/apps/testing/app.eduroam.geteduroam>
 - <http://play.google.com/store/apps/details?id=app.eduroam.geteduroam>



 Paul Dekkers

 paul.dekkers@surf.nl

 @pauldekkers