tnc23

DIGITAL GENERATIONS
TIRANA, ALBANIA | 5-9 JUNE 2023

geteduroam

Paul Dekkers

Tirana

June 6, 2023

GÉANT

Co-funded by
the European Union

geteduroam Goals

- Help users to easily and securely connect to eduroam*

- Simple, single, unified Apps for all end-users and institutions, improving usability and security

- Server software to issue client certificates / pseudo-accounts

* And other networks, like OpenRoaming™ as eduroam user, or govroam

manually configuring eduroam* is not 2023

- Need mutual authentication
- Properly set username, realm, EAP-type, … error prone
- Want to go passwordless
- Can't manually add Passpoint networks
- …
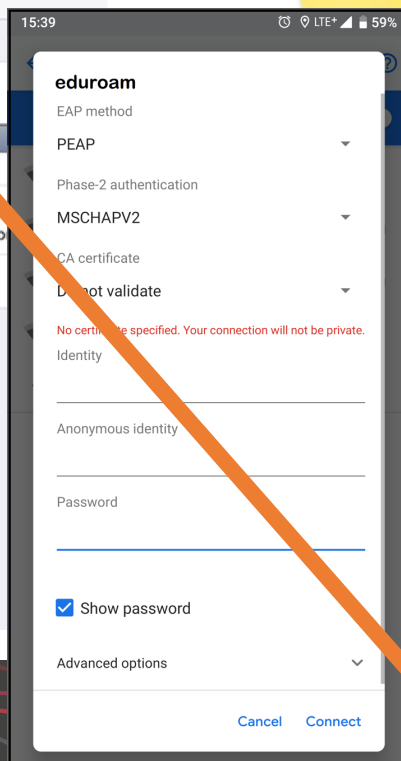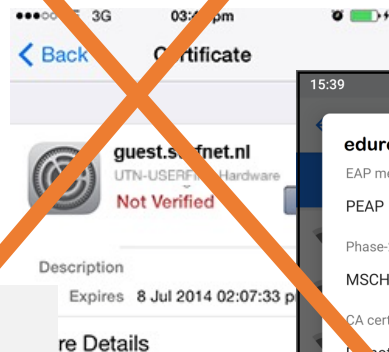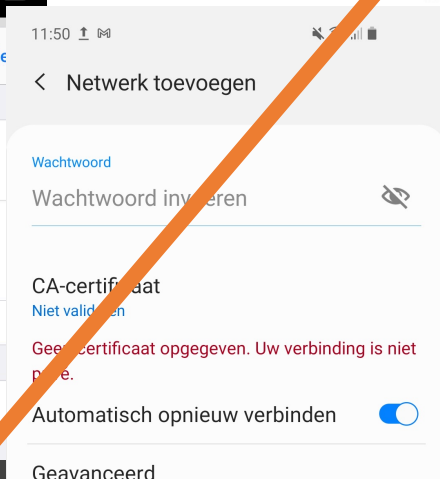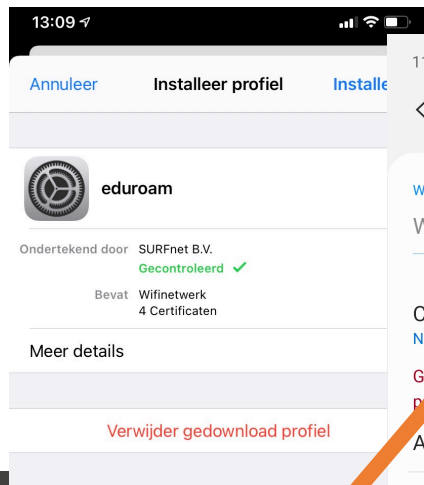
* or any other Enterprise Wi-Fi

The geteduroam project

- Interesting, challenging and relevant
  - Pandemic
  - People working on it, internal and external changes
  - Changing landscape (ie. Android policy changes)

- eduroam is huge, diverse, it's hard to please everyone
  - Diversity in IdP settings (cause of bad App reviews…)
  - Try to consider the need/desires of everyone
    - Regions, NROs, institutions
  - Do very very careful testing
    - To be bug-free
    - Usability testing
  - A lot of communication

Role of geteduroam Commons Conservancy board

- geteduroam established as Commons Conservancy project
  - Open governance model, shared legal infra
  - Similar community projects, such as eduVPN, SimpleSAMLphp, FileSender, IdentityPython
  - Allows anyone to contribute, donate

- Funding so far
  - NORDUnet
  - GÉANT
  - SURF
  - Stichting govroam NL

  - … you? ;-)

- Fund and coordinate development, maintenance and roadmap of Apps, software

THE COMMONS
CONSERVANCY

The geteduroam project, technical aspects

- Relies on eduroam CAT portal for institution profiles, discovery

- Creating Apps is really challenging
  - Android is a very very very diverse ecosystem
  - API deprecations causing a vacuum, example: Android 10
  - Bugs, example: iOS 15
  - Limited APIs, example: ChromeOS, macOS

- Development and maintenance takes a LOT of time
  - New apps under development for 1.5y, still needs a lot of testing
  - Announcement of geteduroam Apps to community came 2y before publication, still some people were surprised

- Creating software is one, supporting it is another
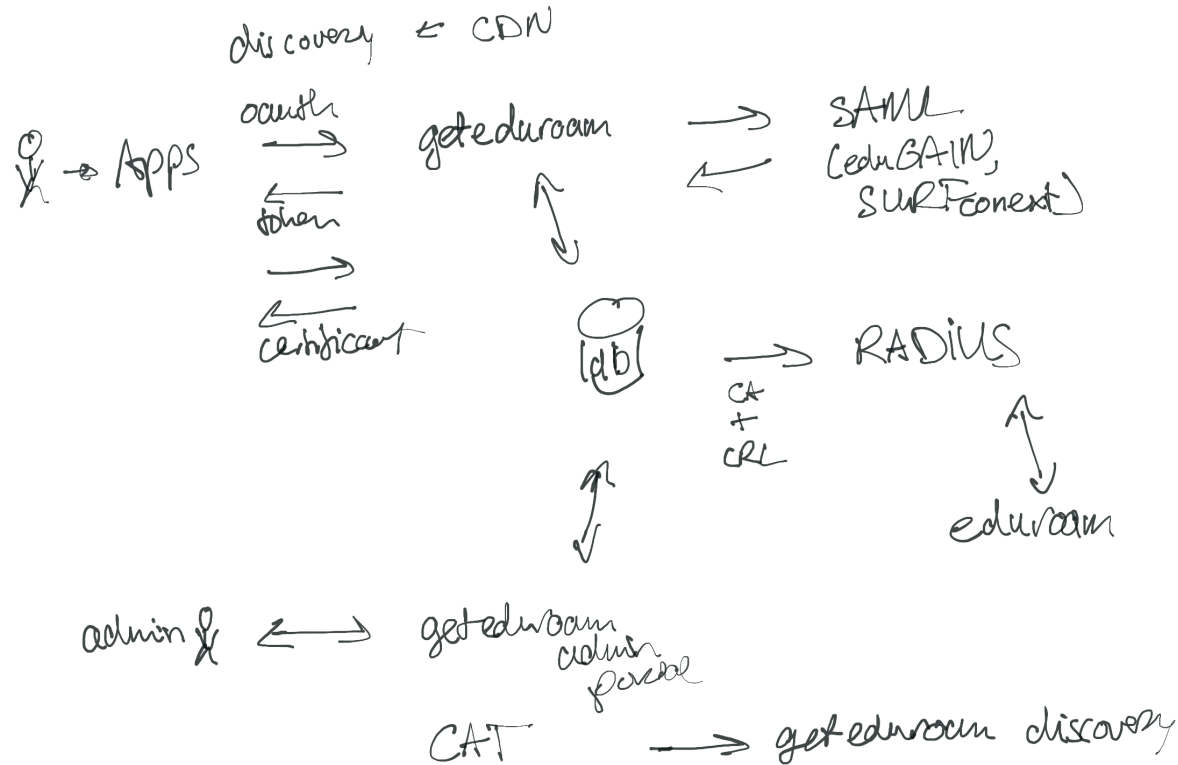
(Hosted) Pseudo accounts

- The geteduroam clients configure mutual authentication,
  so even username/passwords are secure when configured via the Apps

- But client-certificates offer the best security

- Issue client-certificates as 'pseudo accounts' derived from (web, federated) authentication
  - Anything! eduGAIN, Shibboleth, SimpleSAMLphp, ADFS, Azure AD, Google Workspaces, …
  - MFA
  - Auth process familiar to end-users

- Client certificates have a limited lifespan; clients warn users
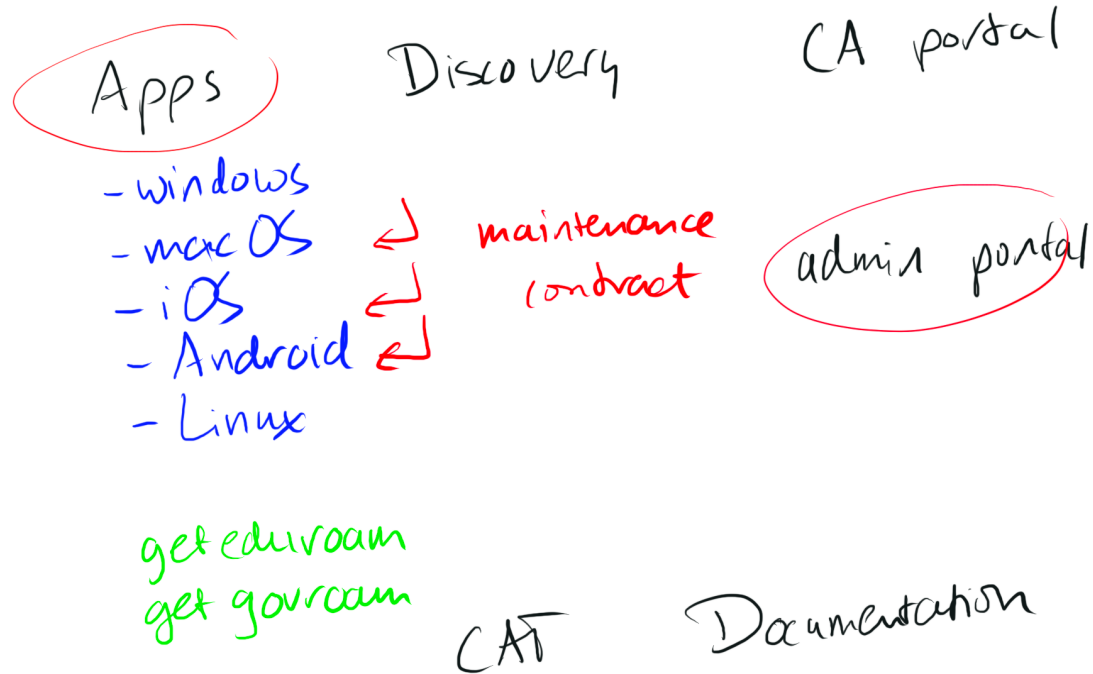- High success-rate in authentications

(Hosted) Pseudo accounts

- Single purpose profiles/certificates: just eduroam

- Passwordless, no password change policies
    - However: need reauthentication/reissue

- Authorization is local, even if NRO or eduroam provides hosted geteduroam IdP

  (APs or local RADIUS can assign VLANs)
    - Even on eg. affiliation:
      i3diflzrhn1xu4o5@student.institution.geteduroam.nl

- Security settings don't allow to be non-traceable

geteduroam components

discovery ← CDN

👤 → Apps

oauth →
← token
→
← certificate

geteduroam

→
←

SAML
(eduGAIN,
SURFconext)

db

CA
+
CRL

→ RADIUS

eduroam

admin 👤 ←→ geteduroam admin portal

CAT → geteduroam discovery

geteduroam components and maintenance contracts

Apps

Discovery

CA portal

- windows
- mac OS
- iOS
- Android
- Linux

maintenance contract

admin portal

get eduroam
get govroam

CAT

Documentation

geteduroam regional IdP authentication servers

- Like a global CDN, authentication close to the user

- Example: EU user visiting South-Africa, fast local authentication

- … then we found out about non-blocking issues with dynamic peer discovery
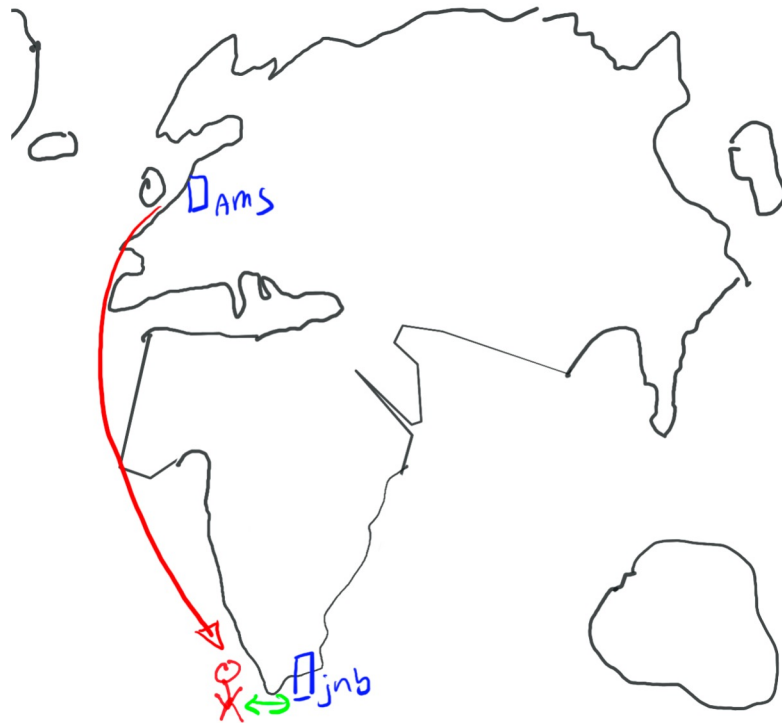
Some numbers

- 255 eduroam + 63 govroam organizations published in discovery

- 72 NL + 22 International via eduroam OT
  - 38510 distinct users (mid may)
  - 113647 pseudo accounts (renewals, multiple devices)
  - ~300k authentications daily

- Several standalone deployments, institutions, NROs, something in ~16% of countries

🇳🇱 🇨🇭 🇫🇮 🇪🇸 🇿🇦 🇩🇪 🇭🇺 🇱🇺 🇬🇷 🇫🇷 🇩🇰 🇸🇪 🇳🇴 🇯🇵 🇲🇾 🇮🇹 🇨🇦

Malaysia has 126 institutions with pseudo-accounts!

App downloads (new users) per month
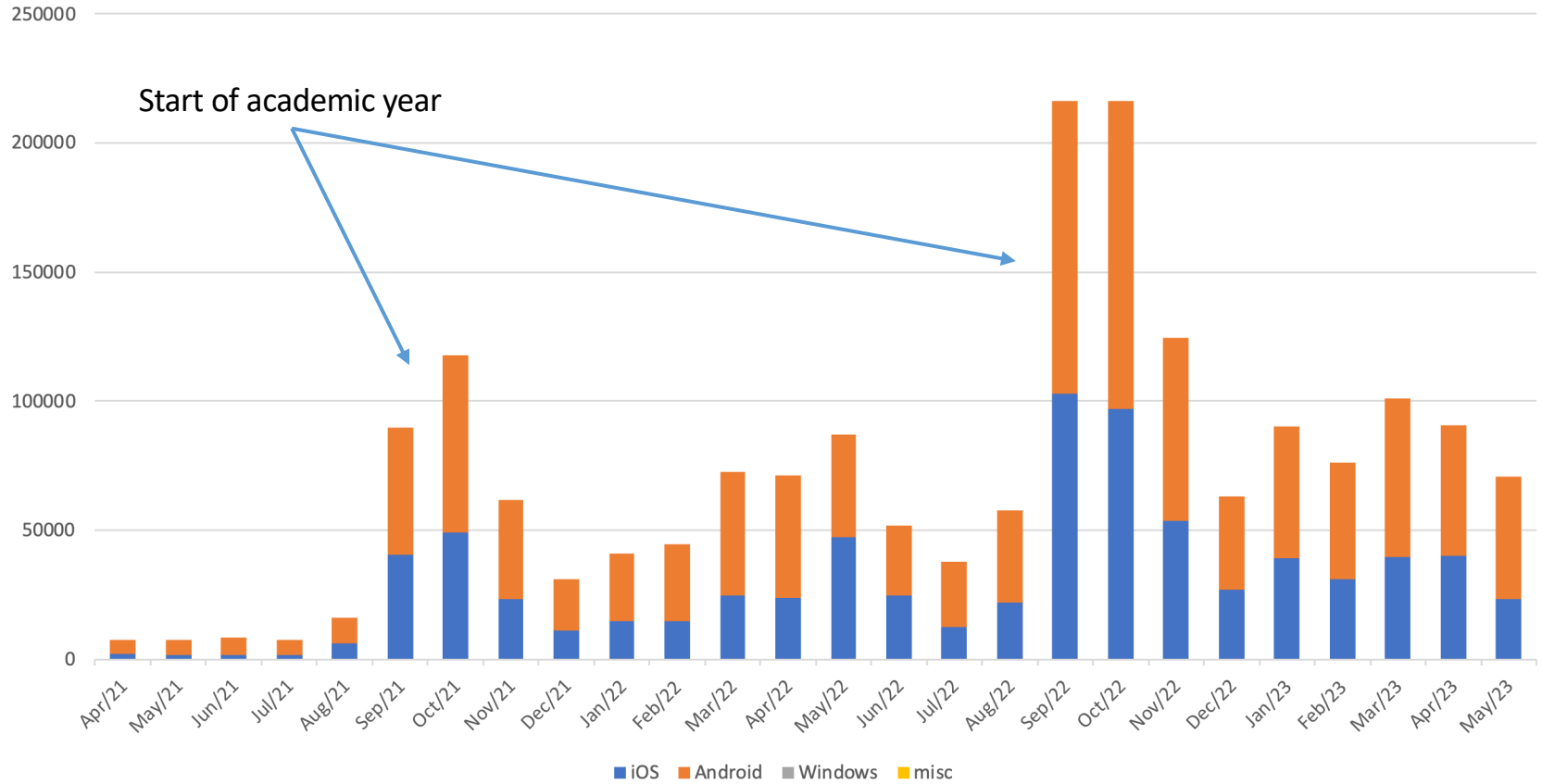
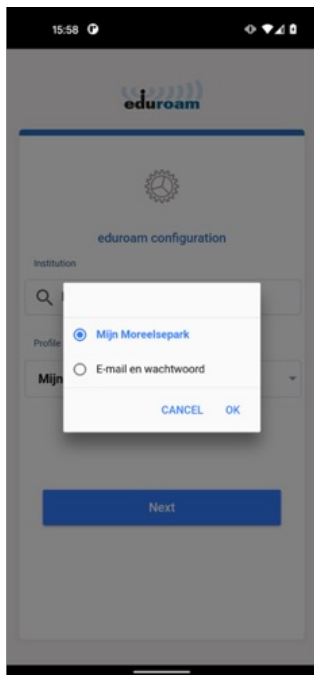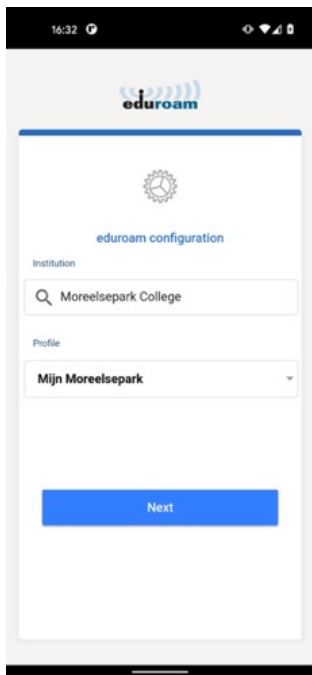discovery access per month

iOS   Android   Windows   misc

14
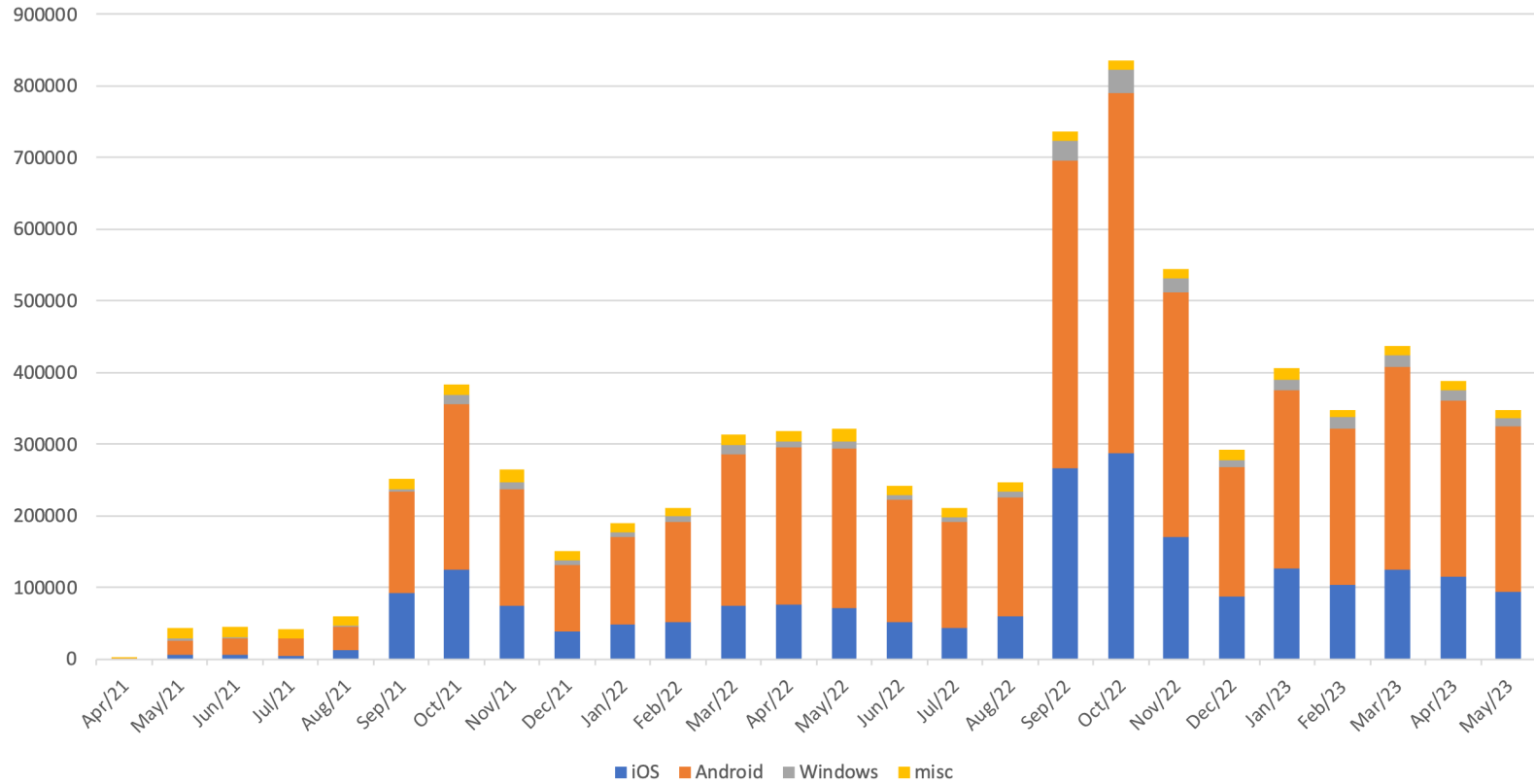
Measurement of success

- Not performing telemetry or anything privacy intrusive

- Institutions claim the burden on the helpdesk is reduced, fewer configuration mistakes

- Pseudo-accounts get a near 100% authentication success-rate

"I believe that geteduroam reduces the number of support calls, both during onboarding and in incidents. One indication of this is the rapid adoption of geteduroam by our helpdesk colleagues, which was not the case with previous installers. I have no evidence to suggest that we are setting the bar too high with geteduroam or that it would result in a shift to mobile data. In summary, I have a very positive impression, and the fact that you have incorporated privacy by design also contributes to this." – C. Houthuijs, Vonk

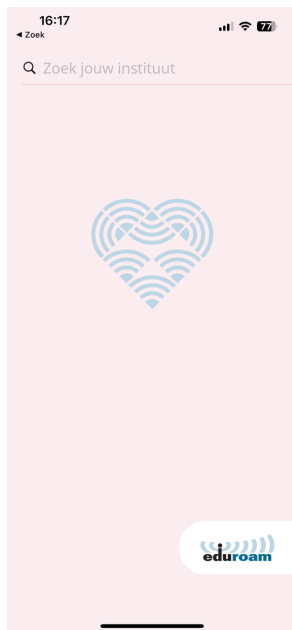# App workflow
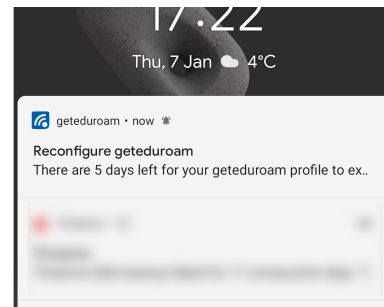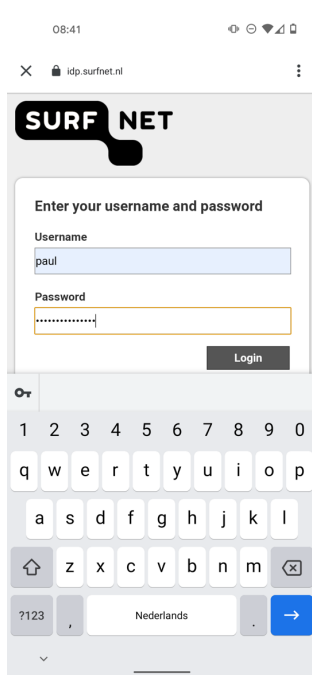
Mobile browser for
web/pseudo-accounts

App workflow, regular accounts

Input validation

new App (Test) versions, iOS & macOS
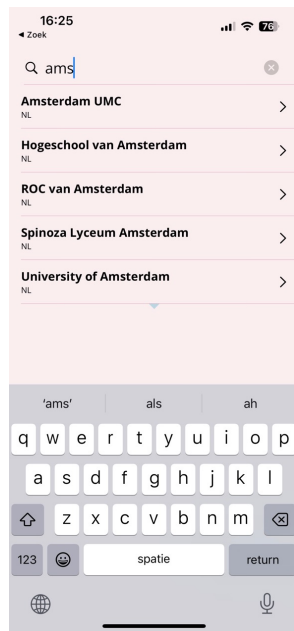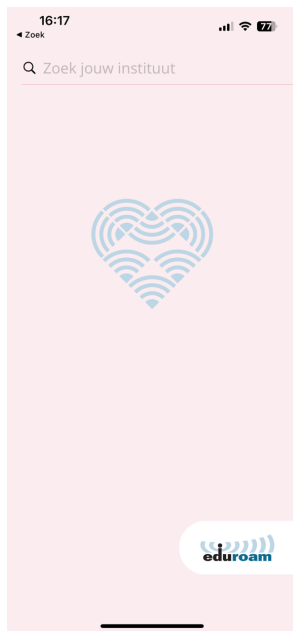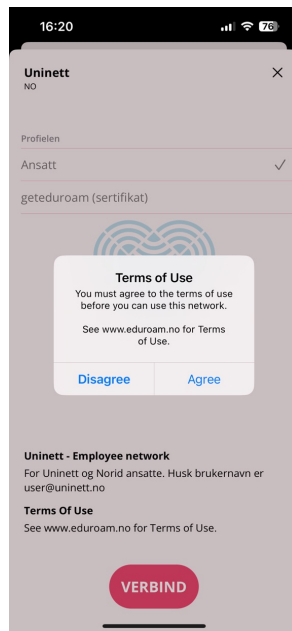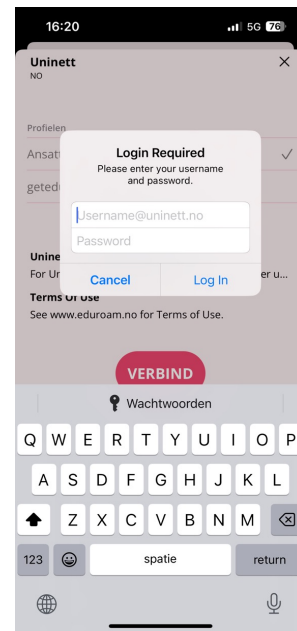

Dark mode
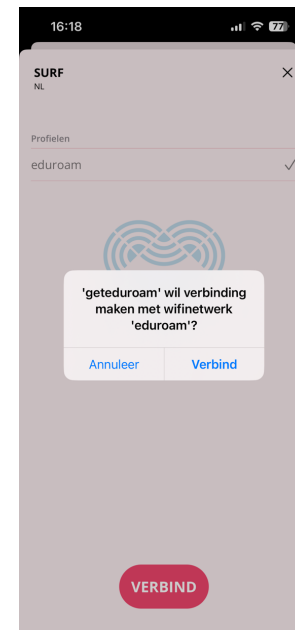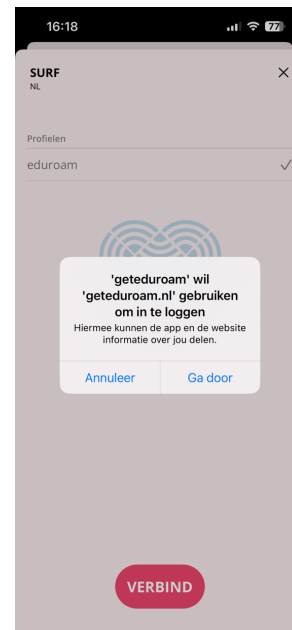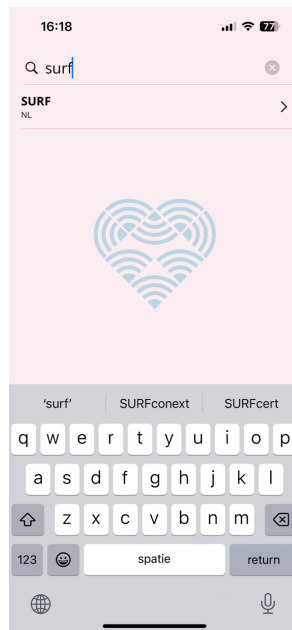
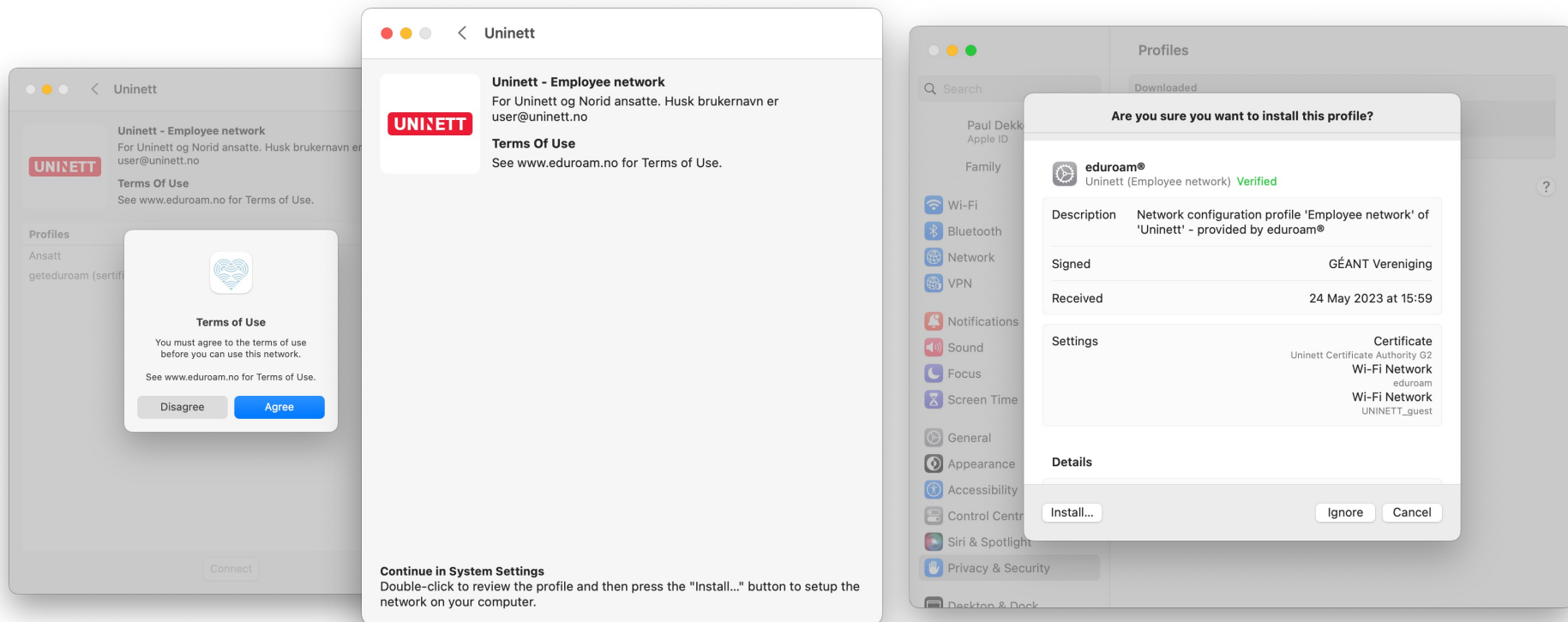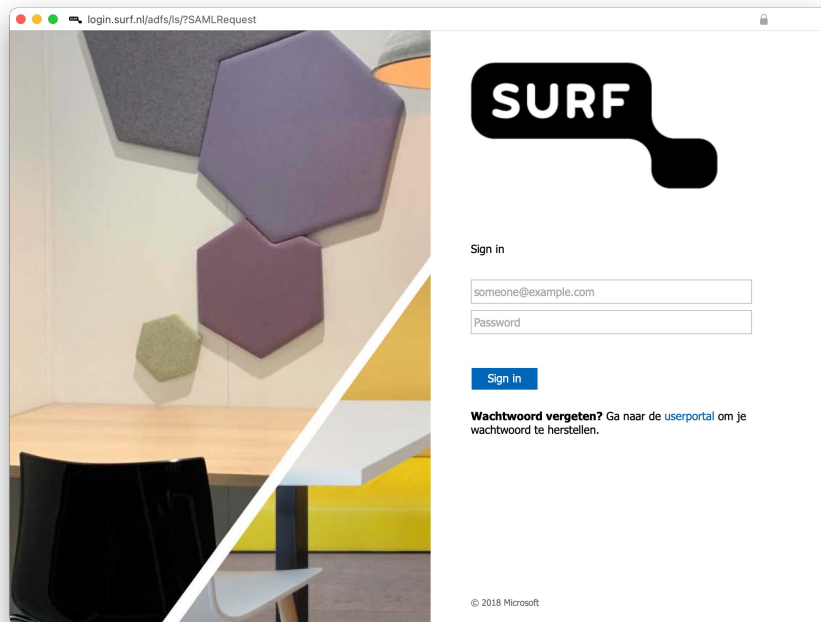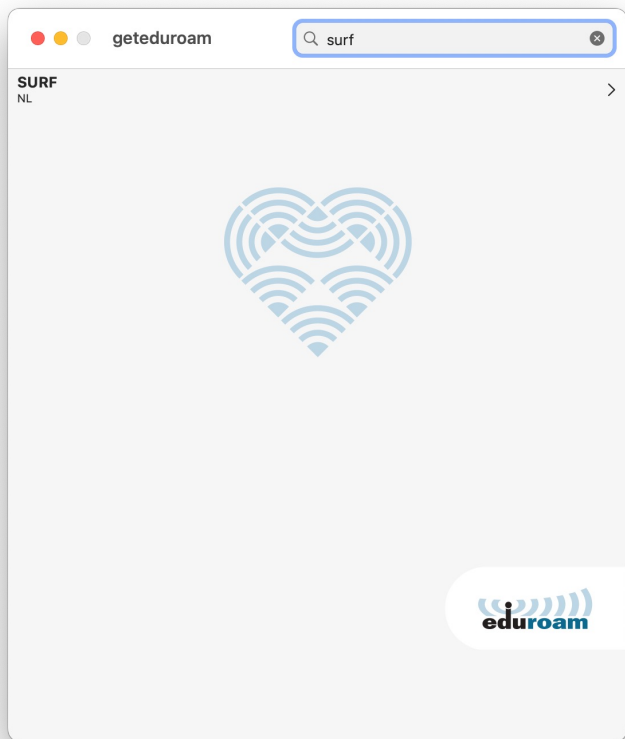# new App (Test) versions, iOS & macOS

discovery

ToS

Passwords
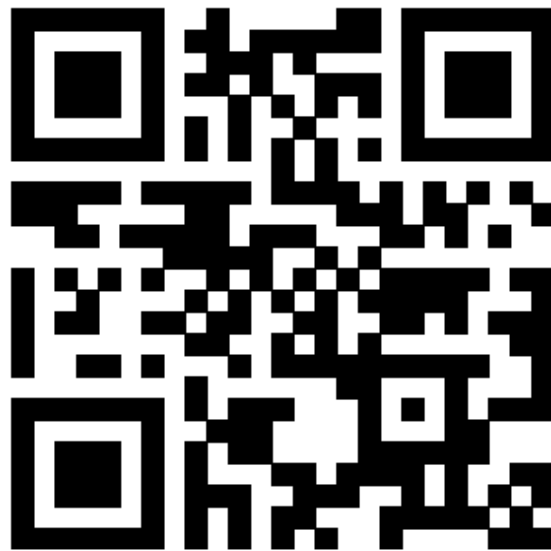
new App (Test) versions, iOS & macOS

new App (Test) versions, iOS & macOS

One More Thing: new App (Test) versions, iOS & macOS

iOS & macOS TestFlight

edu.nl/4m63v

Feedback? testflight@eduroam.org

Linux client, Incubator project

Linux CLI

edu.nl/pdfue

```
~/Repos/geteduroam-linux on ⎇ oauth [!?] via 🐹 v1.20.4 via ❄ impure (nix-shell-env) took 7s
$ make run
go build -o geteduroam-cli cmd/geteduroam/main.go
./geteduroam-cli
Please enter your organization (e.g. SURF): development
Found the following matches:
[1] Graduate Institute of International and Development Studies
[2] Janet Development IDP
[3] Max Planck Institute for Human Development
[4] Southwest Educational Development Center
[5] UK federation (Development)
[6] Development server
Please enter a choice for the organisation: 6
Opening the browser. Please authorize the client...

Your eduroam connection has been added to NetworkManager with the name eduroam (from Geteduroam)
~/Repos/geteduroam-linux on ⎇ oauth [!?] via 🐹 v1.20.4 via ❄ impure (nix-shell-env) took 11s
$ make run
go build -o geteduroam-cli cmd/geteduroam/main.go
./geteduroam-cli
Please enter your organization (e.g. SURF): surf
Found the following matches:
[1] SURF
[2] SURFnet
[3] SURFsara bv
Please enter a choice for the organisation: 1
Opening the browser. Please authorize the client...
```

Feedback? feedback@eduroam.org

Admin portal

geteduroam

- Dashboard
- Configuration >
- **Pseudo accounts**
- User accounts
- Administrator >

Search   👤 dekke002@surf.nl ⚙️

Pseudo accounts   🔽 Filters (2) ✕

☐	Serial ⇅	Requester ⇅	Pseudo account	Realm ⇅	Valid until ⇅	Revoked ⇅	
☐	24759	paul@moreelsepark.geteduroam.nl	4y12lkyu2yc4xj4c	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24760	paul@moreelsepark.geteduroam.nl	l2lmi0v3itn12wyb	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24761	paul@moreelsepark.geteduroam.nl	tbgpxz3o2m5i3sqh	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24762	paul@moreelsepark.geteduroam.nl	zkphkzya50ahutyp	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24763	paul@moreelsepark.geteduroam.nl	on2pmx3r5jbz32jt	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24764	paul@moreelsepark.geteduroam.nl	pkjcndmrinht4p0v	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24765	paul@moreelsepark.geteduroam.nl	eesvxlgw4evza4kb	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24766	paul@moreelsepark.geteduroam.nl	pstw3wtq4gz4k4u3	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24767	paul@moreelsepark.geteduroam.nl	iicjphvgsdk4g2iq	moreelsepark.geteduroam.nl	2023-08-19	NO	⋯
☐	24897	paul@moreelsepark.geteduroam.nl	eevpybpudpuy42p1	moreelsepark.geteduroam.nl	2023-08-22	NO	⋯
☐	25407	paul@moreelsepark.geteduroam.nl	0ep1fx4zjzjdiiji	moreelsepark.geteduroam.nl	2023-08-25	NO	⋯
☐	25576	paul@moreelsepark.geteduroam.nl	fvsph1zxgwfhiwtd	moreelsepark.geteduroam.nl	2023-08-26	NO	⋯
☐	43993	paul@moreelsepark.geteduroam.nl	ulvwqiml3kizjpww	moreelsepark.geteduroam.nl	2023-11-04	NO	⋯
☐	44986	paul@moreelsepark.geteduroam.nl	in2uf1ylbxqrycoy	moreelsepark.geteduroam.nl	2023-11-16	NO	⋯
☐	44987	paul@moreelsepark.geteduroam.nl	kmpym5o33n4oqlok	moreelsepark.geteduroam.nl	2023-11-16	NO	⋯
☐	44988	paul@moreelsepark.geteduroam.nl	p3q5ebjdkl5s004y	moreelsepark.geteduroam.nl	2023-11-16	NO	⋯
☐	54509	paul@moreelsepark.geteduroam.nl	nqs2g1bnpopbei1q	moreelsepark.geteduroam.nl	2024-03-15	NO	⋯

357 results   ‹ Previous 1 … 15 16 17 **18** Next ›

Future

- Continous, sustainable development and maintenance for
  - Apps
    - Android
    - iOS
    - macOS
    - Linux
    - Windows
  - Server-side, features, ease installation
    - CA portal
    - Admin portal
  - Documentation
  - Hosted service, integration
- Investigate support/demand for
  - managed devices, eg. via SCEP
  - new platforms (ChromeOS)
  - …

tnc23

DIGITAL **GENERATIONS**

TIRANA, ALBANIA | 5-9 JUNE 2023

Thank you
Any questions?

www.geteduroam.app

Paul.Dekkers@surf.nl

GÉANT

Co-funded by
the European Union