

# Geteduroam for the people

En kort odysseé och berättelse om var vi står och är på väg...  
....av Herr Nilsson med flera

# Problembild (vad försöker vi lösa?)

- Alla är mer eller mindre överens om att den säkraste inloggningmetoden för eduroam är EAP-TLS (klient certifikat istället för lösenord)
- Problemet är dock att korrekt och enkelt till klientenheten provisionera alla delar i klientcertifikatet, EAP-TLS profil samt Passpointinställningar (för att möjliggöra OpenRoaming mm).
- Vissa saker går att göra manuellt men blir fort komplicerat och lätt att göra fel medans andra bara går att konfigurera via en profil eller ett program.
- Det populära och välanvända verktyget CAT (Client Assistant Tool) är bra men saknar bra stöd för att enkelt sätta upp EAP-TLS (klientcertifikat måste hämtas separate och tillhandahållas under installation).
- Kommersiella verktyg finns som t.ex. SecureW2, Xpressconnect med flera men kan upplevas som kostsamt om inte pengar och prio finns.
- Tänk om det fanns en App som de mest problematiska enheterna (mobiler/paddor) löste detta?

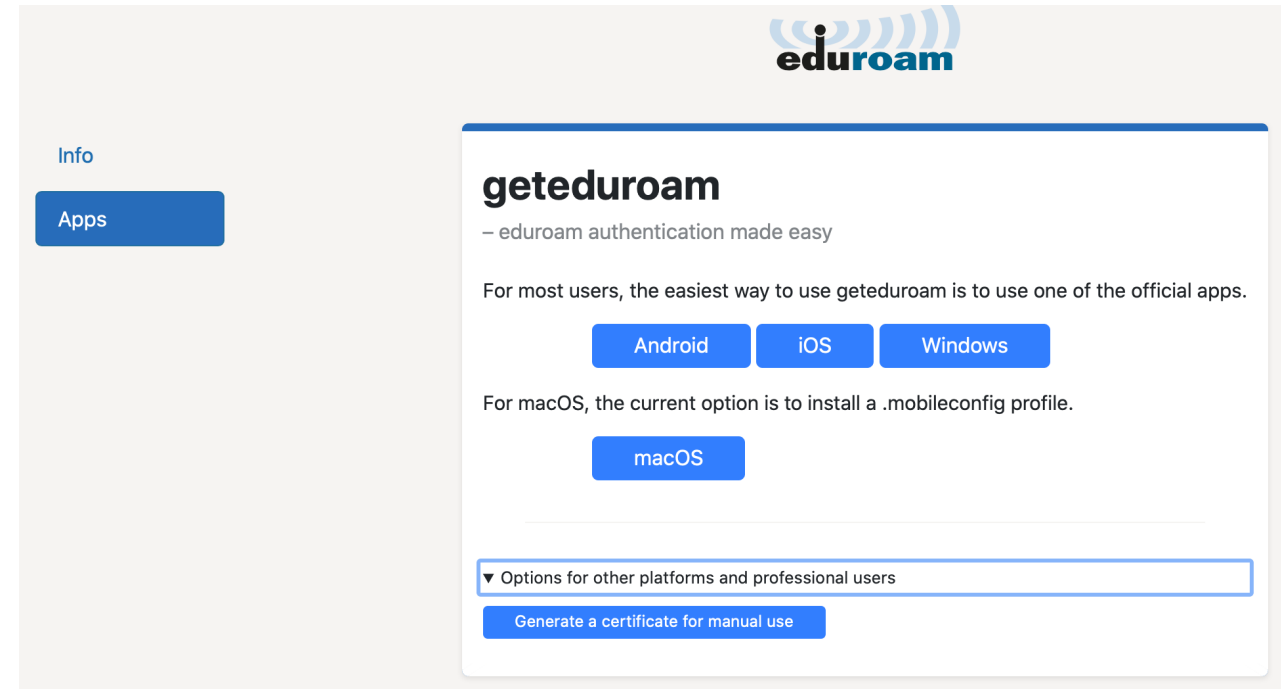
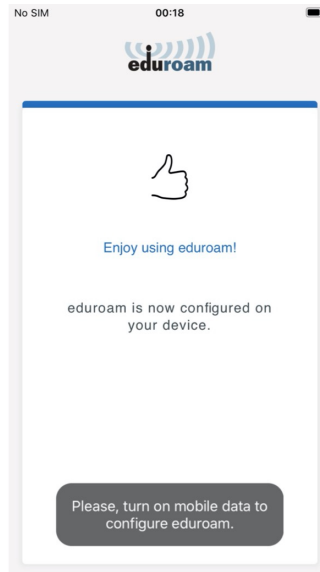
# Geteduroam to the rescue!!



- 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 Technical Roadmap

- Psuedo account portal development For the python version:
  - Short perspective (2-3 months):  
Whitelist function with ability to set who will get pseudoid and not.  
(also look into IdPs outside of edugain like Azure??)  
Real SQL platform (Separate certificate root and so on from other data)  
Admin tools for local institution admins to go and check PsuedoID-RealID, to revoke client cert and other admin duties Pilot use with customer in order to get feedback  
Logghandling for FreeRadius (current tools sufficient? EduDB? )
  - Long perspective (1-3 years and forward):  
Migration of code needed for future development with things like API and so on. Analyze how to handle root or server-certificate in a Database?  
Improving security, i.e. by introducing HSMs
  - For the php version:  
Client-server communication (discovery):
  - Easy installation of the portal (for institution and organization admins) New version (v2) of the Let's Wi-Fi API  
OIDC next so SAML?

Ideas not yet on the roadmap:

- Introducing helpdesk accounts in addition to admin accounts to provide user support SCEP and Intune

## Clients

- Native Android version
- Native macOS version
- New iOS version
- Linux version
- ChromeOS support (via onc)
- Windows client
  - multi language
  - network removal feasibility?
  - features required for CAT use?
- Whitelabeling

# Projektstatus

En servermiljö (baserad på PHP) finns framtagen.

Appar för Android, iOS samt Windows finns framtagna och fler finns i Roadmap

Och ja, det fungerar men innan vi kör igång på Sunet fanns en del saker att lösa:

- Ursprungliga utvecklare har antingen slutat (men jobbar delvis vidare) eller har på grund av hög arbetsbelastning inte haft möjlighet att dokumentera och överlämna projektet till andra inklusive oss för vidare utveckling samt enklare driftsättning.
- Vissa administrativa funktioner för institutioner egna admins saknas (men arbete pågår).
- Vissa oklarheter kring hur EAP-profiler paketeras samt anpassningar för de som vill nyttja geteduroam för onboarding och köra egen Radius.
- Dessutom (inte akut) är ett arbete påbörjat med att migrera servermiljön till Python för framtidssäkra vidare utveckling framöver.

# Så vad var planen för denna session?

- Att ha ett storstilat öppnande av Sunets geteduroam-tjänst för folk att börja testa innan de som vill gå vidare och börja nyttja geteduroam.
- Tyvärr visade det sig lite svårt då vissa saker inte fanns dokumenterade (ännu) och vår nuvarande instans uppvisade ett antal problem. Det visade sig att de enda som sitter inne med informationen för få det att fungera är de nuvarande/tidigare utvecklarna och de har tyvärr av olika anledningar inte varit tillräckligt tillgängliga de senaste månaderna.
- Detta är dock detaljer som behöver fixas så projektet är på inget sätt i fara. 😊

# Så vad händer nu?

- Arbetet med dokumentation och informationsöverföring fortsätter med möten var annan eller tredje vecka.
- Så fort vi känner att vi fått fram den info vi saknat görs en ny driftsättning.

# Bonusfråga/diskussion

- När vi nu kommer igång med geteduroam som succesivt kommer att förbättras, skulle en vidareutvecklad version/variant av geteduroam vara en lösning för gästaccess?



# Avslutningsvis

- Ja, men när kan vi komma igång då????
- Alla problem borde vara lösta innan "Sommaren" 😊
- Frågor på det?





SUNET