Eduroam på Android

Vejledning til DeIC-ansatte og personer, der har konto hos DeIC.

Hvis du har Android version 4.3 eller nyere, kan du benytte eduroam CAT:

1. Hent app'en "eduroam CAT" fra Play Butik
2. Fra en browser på telefonen: gå til https://cat.eduroam.org og download xml-profil til brug i app'en

Hvis du har en tidligere version af Android, benytter du følgende vejledning:

Installationen har to faser. Første skridt er at hente DeICs CA-rodcertifikat og gemme det på din enhed. Du skal bruge den indbyggede browser eller Chrome (Firefox kan ikke bruges). Derefter skal du indstille Wi-Fi-forbindelsen til at bruge certifikatet, når du forbinder dig til eduroam.

1. Åbn din browser og gå til www.deic.dk/eduroam/CArootcert
2. Tryk på linket 'Hent CA rodcertifikat'.
3. Hvis telefonen beder dig navngive certifikatet, skal du bruge navnet "DeIC Staff eduroam Root".
4. Angiv, hvad certifikatet skal bruges til: Vælg Wi-Fi.
5. Gem certifikatet.

Installation af netværk

6. Gå ind under "Indstillinger"
7. Vælg fanen "Forbindelse".
8. Gå ind under "Wi-Fi".
9. Tryk "Tilføj Wi-Fi-netværk".
10. Indtast i feltet "Netværks-SSID": *eduroam*
11. I feltet "Sikkerhed": vælg "802.1x EAP"
12. "EAP-metode": vælg "PEAP".
13. "Fase 2-godkendelse": vælg "MSCHAPV2"
14. I feltet "CA-certifikat": vælg *"DeIC Staff eduroam Root"*.
15. I feltet "Identitet": indtast dit eduroam-brugernavn, eksempel: *init@deic.dk*
16. Indtast password under "Adgangskode".
17. Tryk "Gem".

Unødvendig advarsel

Android version 4.4 kommer med en advarsel, når det ny CA rodcertifikat installeres. Advarslen siger: "Netværksovervågning, En trediepart kan overvåge din netværksaktivitet, …" Trods advarslen kan du have fuld tillid til certifikatet – vi har selv udstedt det. Netop derfor advarer android – men det er en misforstået advarsel.

Sådan fungerer sikkerheden i eduroam

Når du forbinder dig til et trådløst netværk på et andet sted end din egen institution, bliver dit brugernavn og password sendt videre til din institution. Hvis den genkender oplysningerne, får det lokale netværk besked om, at du må bruge det.

Kommunikationen er krypteret for at forhindre, at andre kan se dit password. Krypteringen sker ved hjælp af et såkaldt servercertifikat fra serveren på din institution.

Hvis en it-kriminel vil aflytte din kommunikation, kan vedkommende sende et falsk certifikat til din computer/smartphone. Hvis det sker, vil du blive spurgt, om du vil godkende dette certifikat. Det skal du altid svare nej til – også selvom certifikatet har et navn, der ser troværdigt ud.

Under installationen er din enhed sat op til at genkende certifikatet fra din egen institution. Hvis den ikke genkender et certifikat, er det tegn på, at der er noget galt.

Hvis du alligevel svarer ja, risikerer du, at din kommunikation bliver aflyttet. Dermed kan uvedkommende læse dine mails og chat-beskeder, se de billeder du tager og få fat i dine passwords.