Konsten att få eduroam säkert

Anders Nilsson
Hans Berggren

The story so far…..

Alla vill köra eduroam och trycket från användarna att få access är hård på alla IT avdelningar

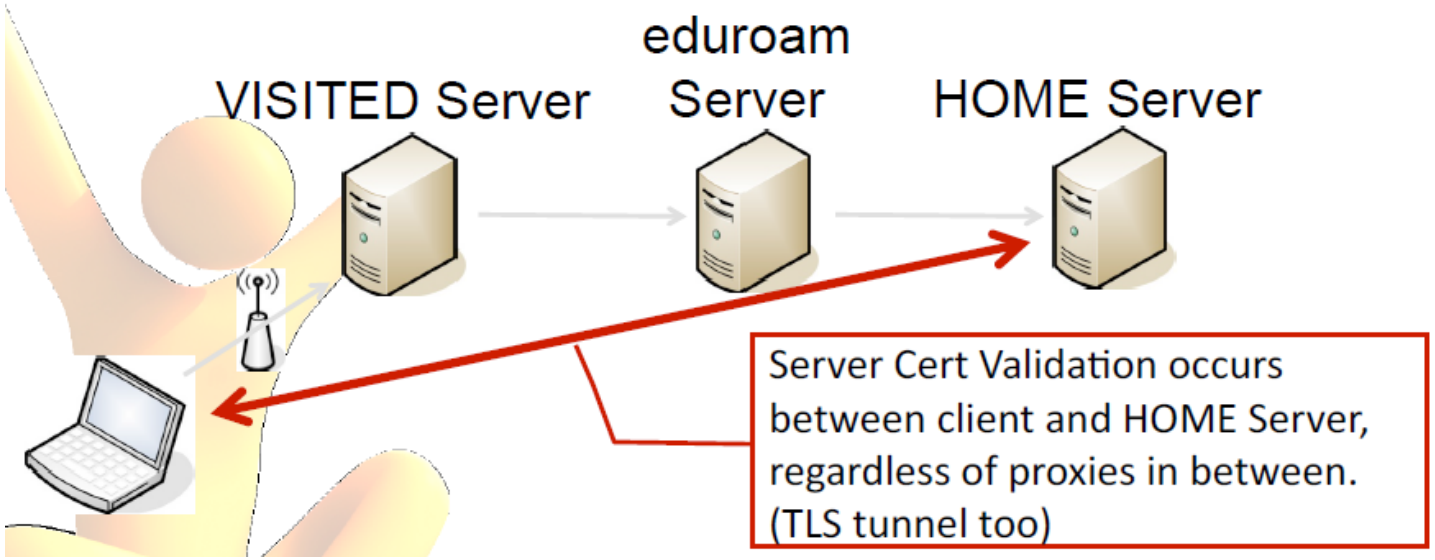
- Brist på instruktioner leder till tillfälliga instruktioner

Skydda ditt user/lösenord

- Säkerheten i eduroam är starkt beroende av Radius servercertifikat verifiering.
- Inte alla kunder har möjlighet att fullt ut verifiera certifikatet och IT-support människor kämpar för att ge bra säkra instruktioner.
- Trycket och viljan bland användare att få alla sina enheter att ansluta till eduroam är stor och ibland glömmer man att tänka på och testa säkerheten.
- Trend mot Single Sign On (SSO) med samma autentiseringsuppgifter för allt.

eduroam & Server Cert Validation

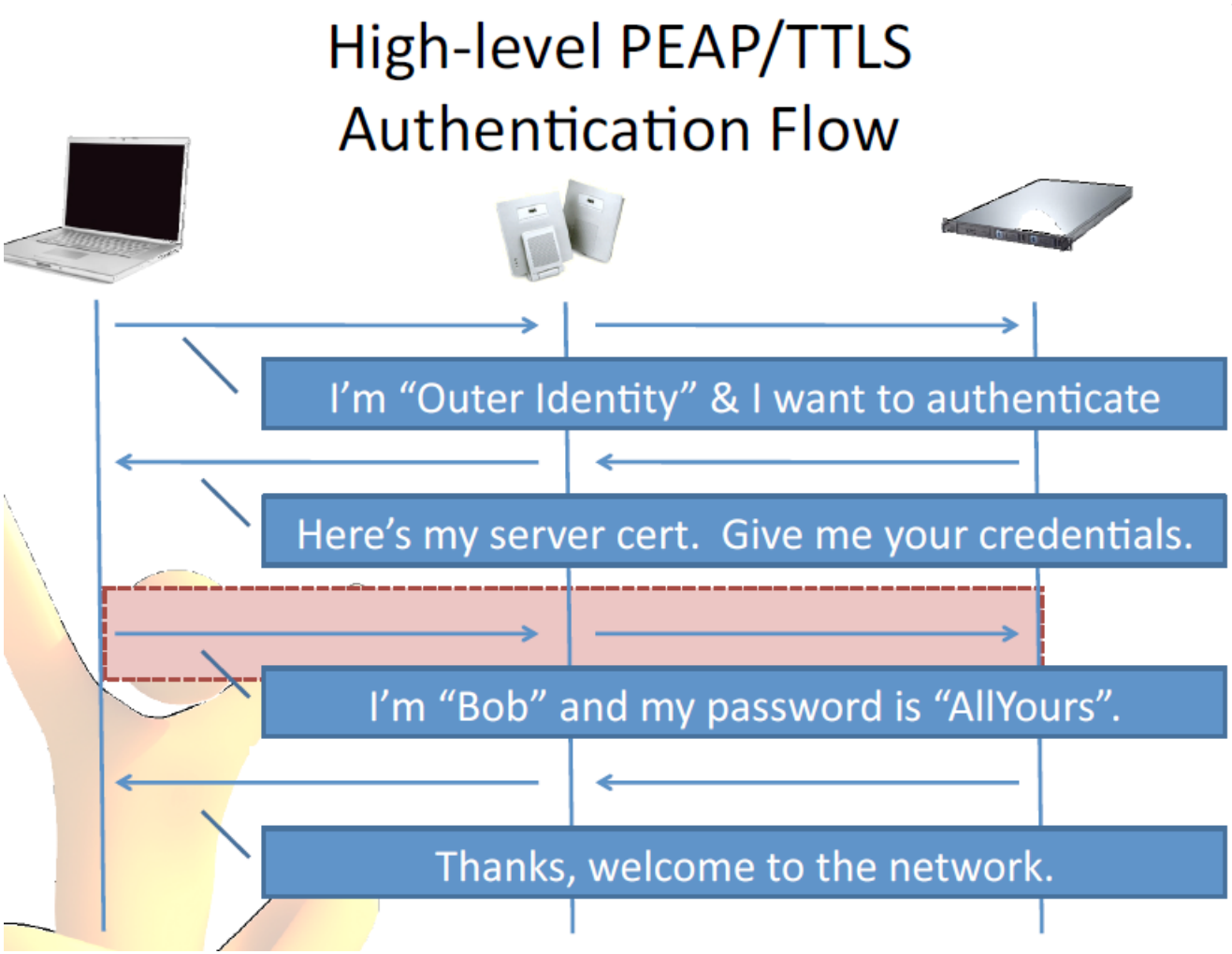
- eduroam uses RADIUS proxy protocols.
- Server certificate exchange occurs between client and HOME RADIUS server.
- Fully-specified server certificate validation is critical within eduroam.



Vilka EAP metoder gäller

- **RFC4017 - EAP Requirements**
- **• Specifies requirements for EAP methods**
- **• All standard EAP methods must provide:**
- **– Mutual authentication**
- **– Resistance to dictionary attacks**
- **– Protection against MitM attacks**
- **– Protected ciphersuite negotiation**
- **• EAP methods that fail these requirements**
- **– EAP-MD5, EAP-OTP, EAP-GTC, LEAP**
- **• EAP methods that pass these requirements**
- **– PEAP, TTLS, EAP/TLS, EAP-FAST**

Hur funkar eduroam för de flesta?



Ska jag då lita på RADIUS-servern?

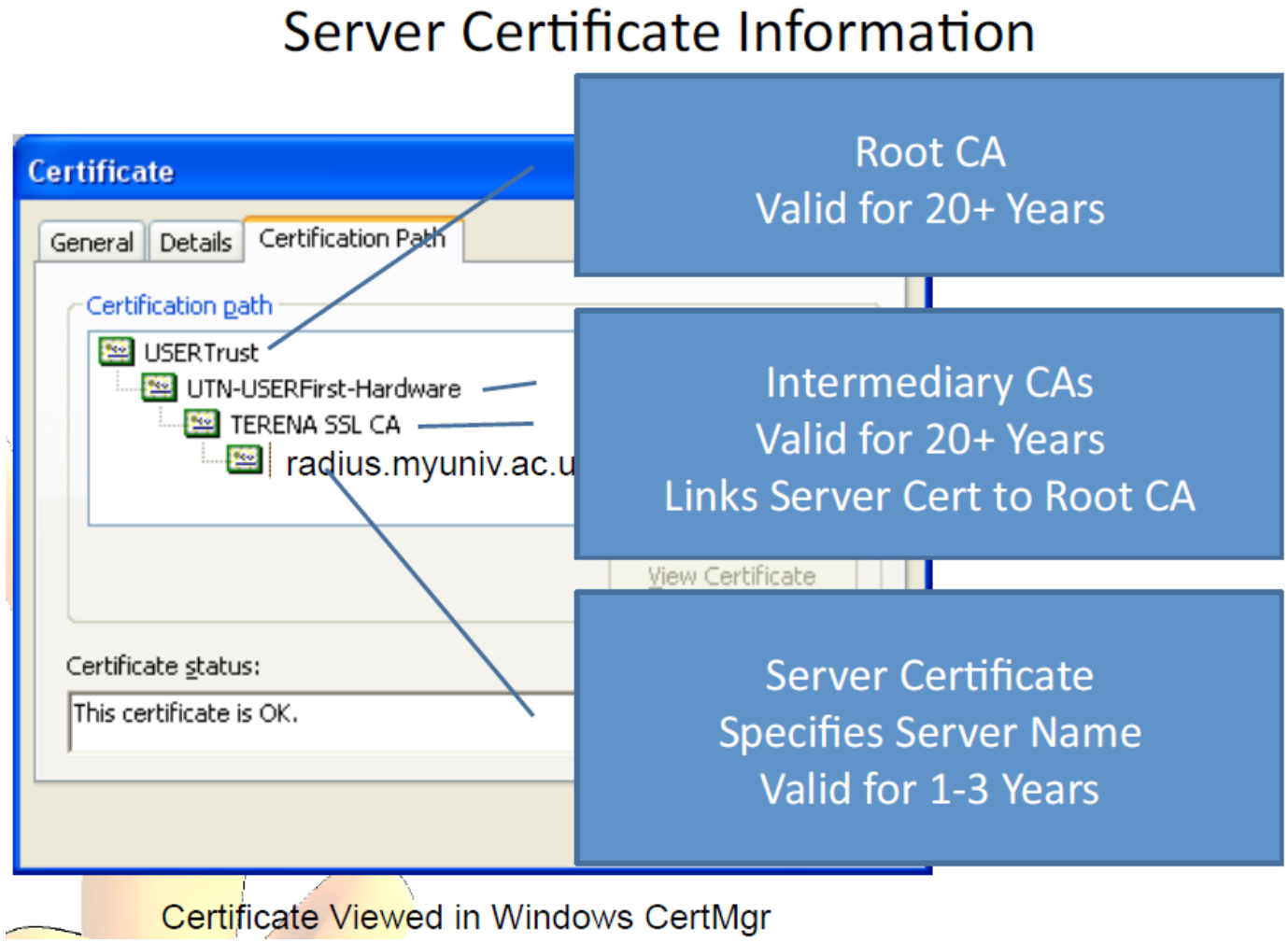
Tänk på att:

- Ingen validering av AP / Switch på fysiska lagret
- AP kan eller inte kan vara legitimt
- AP / Switch väljer RADIUS-server, inte klienten
- Det kan vara illegalt nät
- Det Kan vara ett felaktigt konfigurerade nätverk

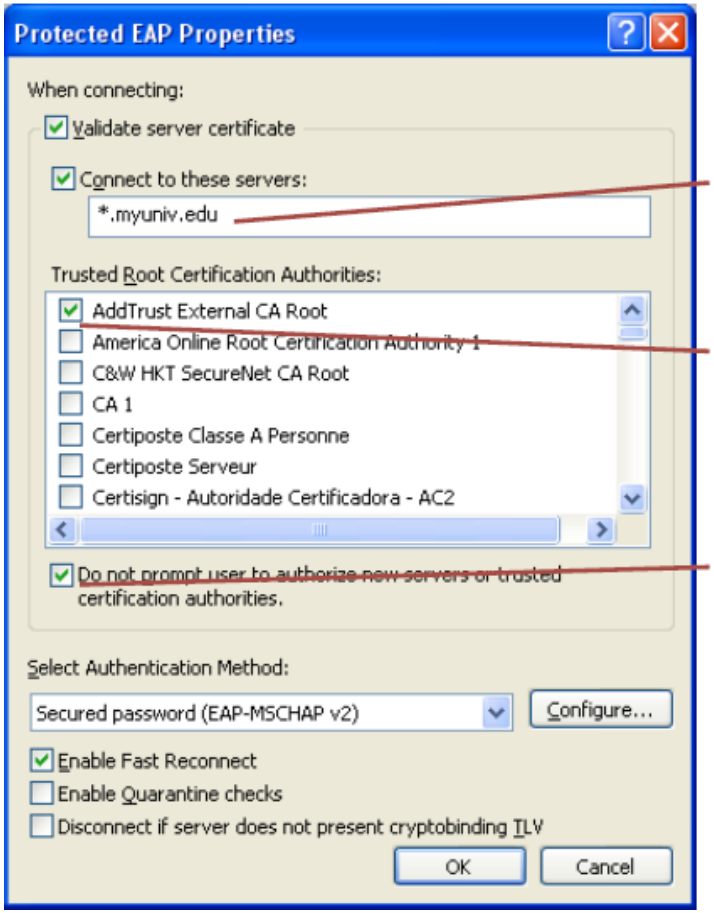
RADIUS-servern kan vara illegal:
Att lämna credentials till fel RADIUS-server är dåligt för alla parter.

- Nätverk: Utsatt för orättmätigt får tillgång
- Användare: Utsatt för nätverk sniffa & manipulation

Anatomi av ett ”vanligt” servercert



En korrekt Radius server verifiering.



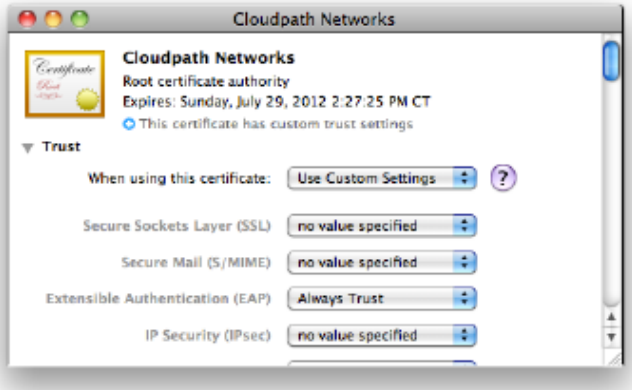
Verify that the server certificate is:

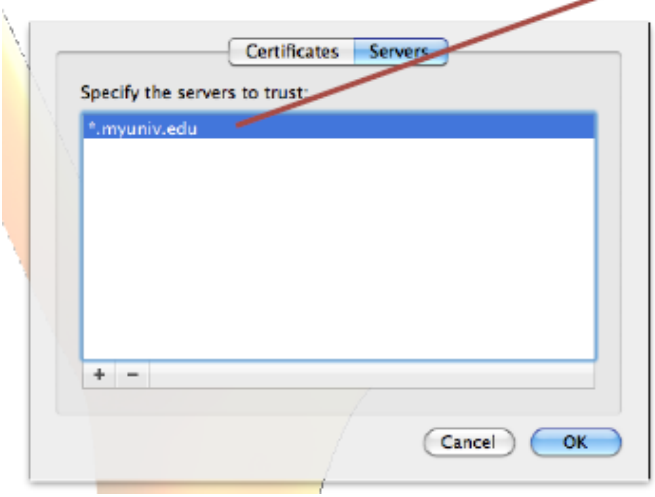
1. For any server in myuniv.edu domain (may be single name, list of names, or wildcard)
2. Signed by AddTrust External CA Root (if multiple by name, look at thumbprint by dbl-click).
3. If certificate is invalid, authentication will be refused if certificate is untrusted (don't ask user to interpret cert).

Wireless - Configured per SSID

Wired – Configured per NIC

Mac OS X Configuration





Root CAs are marked “trusted” for EAP (802.1X) in Keychain.

Trusted Root CAs are generic, not tied to single SSID.

Snow Leopard & iPhone allow SSID to specify trusted server names.

If untrusted server cert, will always prompt unless:

- AllowTrustException = false on iPhone
- Server name specified on Snow Leopard

Demo tajm!

Så vad är då problemen?

- Vissa klienter stöder att verifiera både CA och servernamn på Radiuscertifikat.
- Vissa klienter saknar över huvudtaget möjligheten att verifiera certifikat
- Bristfälliga instruktioner (klicka vidare här).
- IT avdelningen rekommenderar enheter som aldrig går att få säkra.

Vad säger SWAMID

För identiteter är SAML och eduroam likställda:

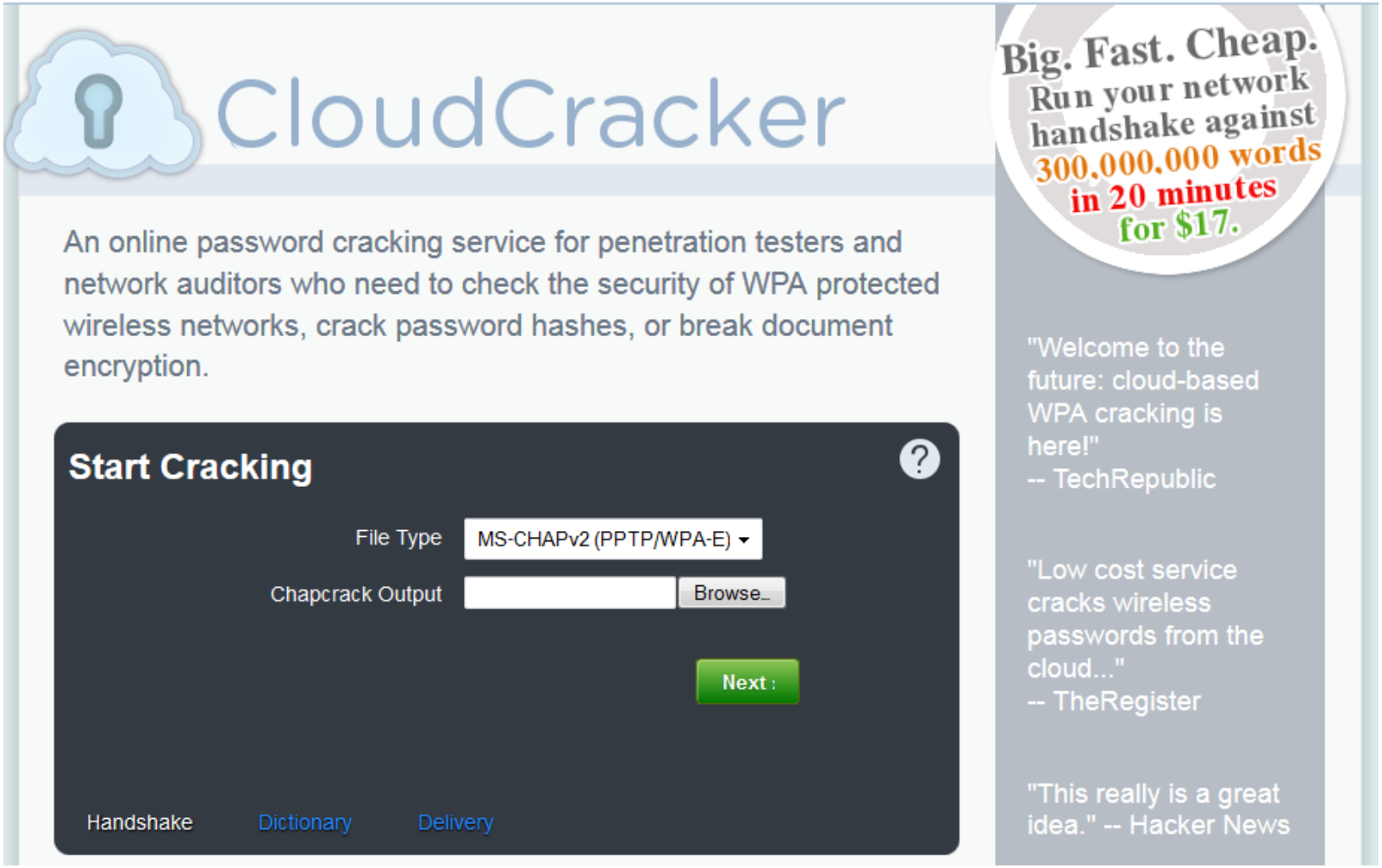
http://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance+Level+1+Profile+-+Draft

- 5.1.3 All network communication between systems related to Identity or Credential management MUST be secured and encrypted.
- ***Guidance:*** *Always use TLS/SSL or similar for establishing encrypted communications between endpoints. Clients and servers needs to be mutually authenticated. An example of clients can be the webpage for changing passwords and the server can be the Identity management back-end (e.g. Active Directory).*
- 5.1.4 Subjects MUST be actively discouraged from sharing credentials with other subjects either by using technical controls or by requiring users to confirm policy forbidding sharing of credentials or acting in a way that makes stealing credentials easy.
- 5.1.5 The organisation SHOULD take into account applicable system threats and apply appropriate controls to all relevant systems.

Vad kan konsekvenserna bli då?

- Karantän från SAML access.
- Nedgradering från LOA2 till LOA1
- I värsta fall avstängning.

MSCHAP-v2 då??
No problems, vi har ju ”Cloud services”……



Är eduroam konceptet kört då????

NEJ! Vi kan fortfarande använda eduroam säkert om:

- Skriv ordentliga instruktioner (inte mer bara klickar på OK utan att verifiera certifikatet)
- Använd MDM programvara för att konfigurera enheter (CAT eller andra BOYD verktyg)
- Undvik om möjligt att återanvända dina inloggningsuppgifter för andra verifieringar (SSO syndrom) om du vill stödja enheter som inte gör ordentlig kontroll.
- Undvik att använda apparater som inte stöder validering RADIUS-server (Bara säga nej till Windows Phone 7, osäkert om WP8 funkar)
- Vissa enheter stöder bara CA-root verifiering (använd en egen CA-root och förlita dig inte på kommersiella)
- Använd inte ”credentials” utan snarare klientcertifikat (EAP-TLS) för högsta säkerhet.
- Vid nyttjande av PEAP eller EAP-TTLS använd inte samma ”credentials” för SAML och eduroam.
- Lita inte på din enhet. Testa och verifiera att enhetens supplikant korrekt verifierar Radius certifikat.

Så med säkra klienter är det bara att köra på!