# Joining eduroam; eduroam best practices

Identity Management & Federation 2019



## Joining eduroam

In South Africa



## Joining eduroam

You've all done that already, so...



## Joining eduroam

Step 1: Differentiate between identity providers and service providers

No restrictions on who can become service provider

Eligibility for identity providers similar to SAFIRE/SAML

Step 2: Sign a document

Step 3: Make the technology work

• Step 4: ???

Step 5: PROFIT!!!



https://eduroam.ac.za/fag/configuration/

encourage

more service

providers..



## eduroam best practices



### Use eduroam as your primary SSID

- Makes things just work<sup>™</sup> for your users
- Reduces support calls from people who are off-campus
- Means you notice problems sooner

- You don't need to rely on the FLR servers for your users
  - In fact, please don't!!!
- eduroam policy doesn't apply to your own users making use of WiFi on your campus



#### Use eduroam CAT

- eduroam Configuration Assistant Tool
  - Makes things easier for your users
  - Reduces the load on your help desk/service desk
  - Ensures people use the right<sup>™</sup> settings
  - On-boards certificates (can handle rollover)
  - Improves security
- Enrol via https://eduroam.ac.za/manage/
- Send users to https://cat.eduroam.org/

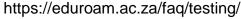




## Maintain a working monitoring account

- Allows the NRO to monitor your realm
- Detects problems that will affect your users when they're away from campus







### Use a valid, self-signed certificate

- The certificates in eduroam protect your user credentials
- Turning off certificate validation is a bad, bad idea™
- Self-signed certificates improve security
- You can on-board certs with eduroam CAT



http://rmg.zum.de/wiki/Datei:Mallory\_lacht.jpg

https://eduroam.ac.za/faq/naptr/



### Send Chargeable-User-Identity

- Chargeable-User-Identity is an unique, opaque, persistent, targeted pseudo-anonymous identifier
- Used by service providers to uniquely identifier a user without compromising privacy
- Helps SP deal with account sharing
- Required by many commercial service providers
- Not supported by Windows Network Policy Server ⊗



## Send Calling-Station-Id

- Generated by wireless controllers or NAS devices
- Typically contains the MAC address of the device connecting
- Helps IdP deal with account sharing

- Okay to hash it to create a targeted, privacy-preserving identifier
  - but think about not hashing OUI



#### Create NAPTR records

- NAPTR records make the full-mesh version of eduroam work
- Can improve efficiency and resiliency for international roaming

example.ac.za. IN NAPTR 100 10 "s" "x-eduroam: radius.tls" "" \_radsec.\_tcp.eduroam.ac.za.

