

# deutsches forschungsnetz

# DEN



## Aktuelles zu eduroam/easyroam

DFN Betriebstagung | 18./19.10.2022

Ralf Paffrath



# Agenda

- ▶ eduroam CA
- ▶ easyroam im Regelbetrieb
- ▶ AK Mobile IT

# eduroam CA

- ▶ Seit Anfang März 2022 im Regelbetrieb
- ▶ Primärer Einsatz für die RadSec Infrastruktur, RADIUS Infrastruktur ???
- ▶ 3 Jahre Laufzeit, flache PKI Hierarchie
- ▶ Vergabe von Zertifikats – Attributen: eduroam SP und eduroam IdP
- ▶ Gründe:
  - DFN-PKI (Global) wird eingestellt,
  - Vorgaben u.a. durch CA/Browser Forum, z.B. kürzere Laufzeiten, etc.,
  - Anzahl der PKI's gering halten,
  - etc.
- ▶ Neue RadSec Zertifikate nur mit eduroam CA

# easyroam im Regelbetrieb(1)

- ▶ Was ist easyroam?
  - ▷ ...ein Weg zur Integration von eduroam in die DFN-AAI
  - ▷ ...ein optionales AddOn zur eduroam Infrastruktur
  - ▷ ...mehr als nur ein managed eduroam IdP
  - ▷ ...mehr Sicherheit in eduroam
  - ▷ ...ist ausschließlich EAP-TLS (zertifikatsbasierte Anmeldung in eduroam)
- ▶ Angebot richtet sich sowohl an kleine Einrichtungen mit wenig Ressourcen als auch an große Einrichtungen im DFN

## easyroam im Regelbetrieb(2)

- ▶ Pilotphase 1 Jahr
- ▶ Startschuss war der 01.09.2022
- ▶ Aktuell ca. 30 Einrichtungen mit insgesamt über 100.000 Personen
- ▶ Täglich melden sich bis zu 10.000 Endgeräte via easyroam in eduroam an
- ▶ Anleitungen für Nutzende und Admins (s. <https://doku.tid.dfn.de/de:eduroam:start>)
- ▶ Unterstützung aktueller Geräte (iOS, ANDROID) durch easyroam app's
- ▶ Unterstützung älterer Geräte s. Anleitungen

# DIE TEILNAHME AN EASYROAM IST FREIWILLIG

- ▶ >99% aller Einrichtungen weltweit in eduroam nutzen Kennung/Passwort (EAP-TTLS, PEAP)
- ▶ Seit Jahren Sicherheitsbedenken:
  - ▷ Nutzende können Zertifikatsüberprüfung abschalten,
  - ▷ Wörterbuchangriff,
  - ▷ Erkennung kompromittierter Passwörter schwer möglich,
  - ▷ Missbrauch durch Weitergabe,
  - ▷ Unbekannte Anzahl kompromittierter Passwörter in eduroam.
- ▶ easyroam nutzt keine Kennungen/Passwörter in eduroam, ausschließlich Zertifikate (EAP-TLS)

# Teilnahme an easyroam

- ▶ Erfolgt über die “weiche Migration zu easyroam”:
  - ▷ Abgelöst: herkömmliche Anmeldung (passwortgestützt) → easyroam (zertifikatsbasiert)
  - ▷ Zeitlich begrenzter Parallelbetrieb (maximal 6 Monate) passwortgestützt → zertifikatsbasiert
  - ▷ Genauer Ablauf s. <https://doku.tid.dfn.de/de:eduroam:easyroam-regelbetrieb>
- ▶ Keine Verpflichtung an easyroam teilzunehmen

## Weitere Infos zu easyroam

- ▶ S. <https://doku.tid.dfn.de/de:eduroam:start>
- ▶ Kontakt: [easyroam@dfn.de](mailto:easyroam@dfn.de)

- ▶ Aktuelles zu easyroam im Regelbetrieb im DFN mit Demo  
Ralf Paffrath (DFN-GS)
- ▶ eduVPN: Architecture Changes in Version 3.X, etc. with Demo  
François Koman (eduVPN)
- ▶ Skizze und Planungen für ein Netzkonzept: Neue Wege mit den DFN-Diensten  
eduVPN und easyroam  
Tobias Irlinger (Hochschule München)