Neues aus eduroam

85. DFN-Betriebstagung – Forum Mobile IT | 07.10.2026

Jan-Frederik “Janfred” Rieckers

Agenda

- Perspektive eduroam-Metadatenportal
- Aufräumen der radsecproxy-Konfigurationen
- Neuerungen beim eduroam CAT

eduroam Metadaten-Portal

Perspektive eduroam-Metadatenportal

- Aktuell: primär “Konfigurationsoberfläche” für radsecproxy
- Nähere Zukunft: “echtes” Metadaten-Portal mit Verwaltung von mehr Daten
  - Verwaltung von Kontakten (technisch/vertraglich/User-Support)
  - Verwaltung von Standorten, Neuauflage der eduroam Map
- Große Perspektive:
  - (Teilweise) Abbildung von eduraom auch im Teilnehmerportal
  - Erstellung von “Test-Accounts”, insb. für Service-Provider
  - Monitoring des Verbindungsstatus der RadSec-Clients/Server

Perspektive eduroam-Metadatenportal

- Aufruf in die Runde:

Welche Features würdet ihr gerne im eduroam Metadatenportal gerne sehen?

Vorschläge gerne an mich (persönlich, Mail an eduroam@dfn.de, Telefonat)*

* Nicht alle Vorschläge werden wir auch umsetzen (können)

radsecproxy Konfiguration

Aufräumen der radsecproxy-Konfigurationen

- Viele radsecproxy-Konfigurationen sind zum Teil historisch gewachsen
- Config teilweise veraltet, teilweise über die Zeit “verschlimmbessert”
- Z.T. dadurch Performance-Einbußen bzw. Einschränkung der Redundanz
  - Teilweise auch keine “Vorwärts-Kompatibilität” mit geplanten Änderungen in der radsecproxy-Konfiguration der Föderationsserver
- Durch neue radsecproxy-Versionen haben sich Empfehlungen des DFN geändert

- Mein Aufruf: Jetzt einmal radsecproxy-Konfiguration aufräumen!

Config aufräumen – tld3.eduroam.de

- Dritter Föderationsproxy, für bessere Redundanz
- Von vielen Einrichtungen immer noch nicht eingetragen!
- IP-Adresswechsel bei der Migration zum DFN-CERT, IP-Adresse ggf. in Firewall nicht geändert

- Problem: Wenn tld3 nicht eingetragen/freigegeben ist, aber eine andere Einrichtung über tld3 Anfragen verschickt, kommen die Anfragen nicht an
- Für volle Redundanz: tld3 auch im Default-Realm-Block eintragen.

Config aufräumen – Zertifikatsprüfung

- Alte Empfehlung:
  ```
  CertificateNameCheck Off
  MatchCertificateAttribute SubjectAltName:DNS:/^tld1\.eduroam\.de$/
  ```
- Noch ältere Empfehlung: `CN` statt `SubjectAltName:DNS`
- Notwendig, wenn Server mit `Host <ipaddr>` konfiguriert wurde, bei Konfiguration über DNS-Namen ist die Konfiguration nicht notwendig.
- CN soll nicht mehr verwendet werden, MatchCertificateAttribute eigentlich nicht für (alleinige) Namensüberprüfung gedacht.
- Seit radsecproxy 1.10: Neue Konfigurationsoption `ServerName`
- Verwendung: Ersetzen der beiden oberen Zeilen durch folgendes:
  `ServerName tld1.eduroam.de`
  (`tld1` bei den anderen Servern natürlich durch `tld2` oder `tld3` ersetzen)

Config aufräumen – Servernamen der tlds

- Aktuell haben alle drei tld-Server das selbe Zertifikat
- Im Zuge der Umstellung wurde ggf. ein `CN:/^tld3\.eduroam\.de$/` bzw `tld2` auf tld1.eduroam.de (CN des aktuellen Zertifikats) gesetzt
- Wichtig: Zertifikate werden ggf. in Zukunft wieder pro Server aufgetrennt, dann funktioniert das nicht mehr.
  - Zertifikate werden immer den korrekten SubjectAltName:DNS haben, deshalb immer darauf prüfen. `ServerName` tut das automatisch.

Config aufräumen – Übersichtsseite

- https://doku.tid.dfn.de/de:eduroam:anleitungen:radsecproxy:deprecated
- (Gerade im Aufbau, noch nicht öffentlich verlinkt)

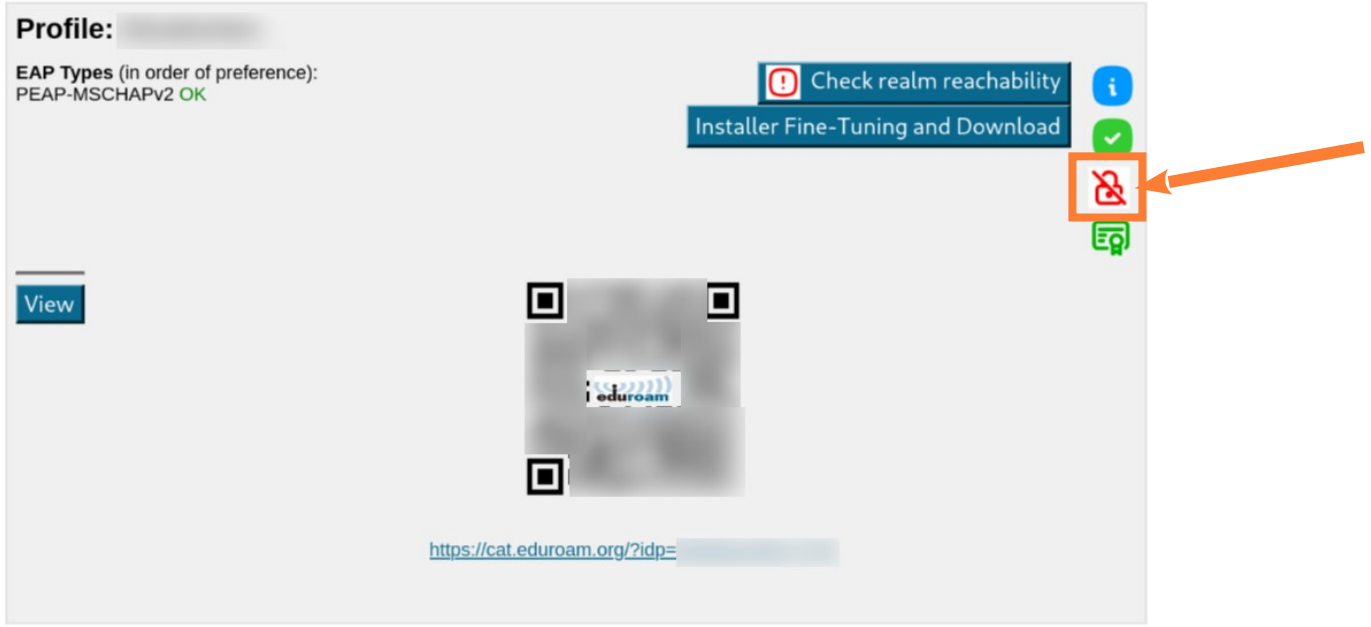
eduroam CAT Updates

eduroam CAT Updates

- CAT zeigt nun den Admins mehr Hinweise
  - Nutzung von anonymer Identität in Profilen
  - Zertifikatswarnungen
  - Statische Verbindungs-Tests
  - Admin-Verwaltung

eduroam CAT – Anonyme Identität

- Bei allen Profilen für EAP-TTLS/PEAP sollte eine anonyme Identität hinterlegt werden
  - Schützt die Privatsphäre der Nutzenden
- CAT warnt, wenn Profile keine anonyme Identität konfiguriert haben.



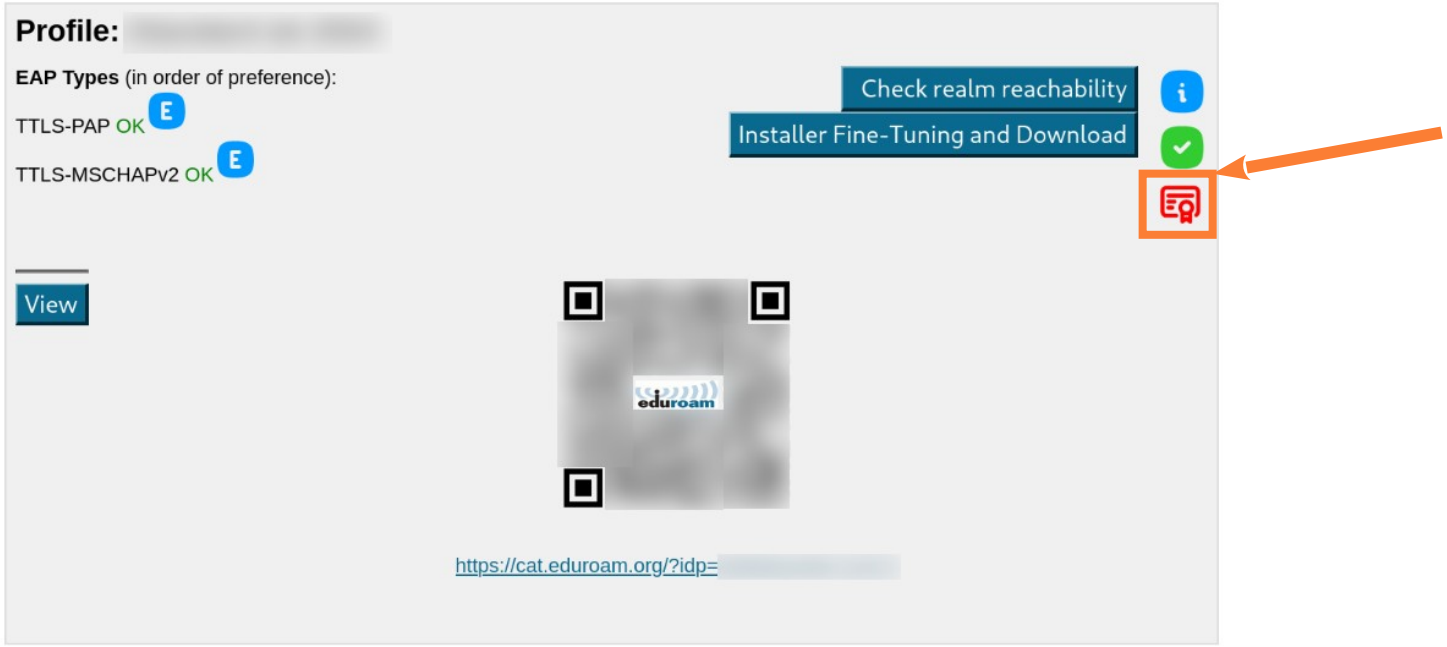
eduroam CAT – Statische Tests

- CAT testet die Erreichbarkeit und Übereinstimmung mit Konfiguration
- Bei Fehlern wird das angezeigt. (Rot = Kritisch, Gelb = Warnung, Blau = Information)



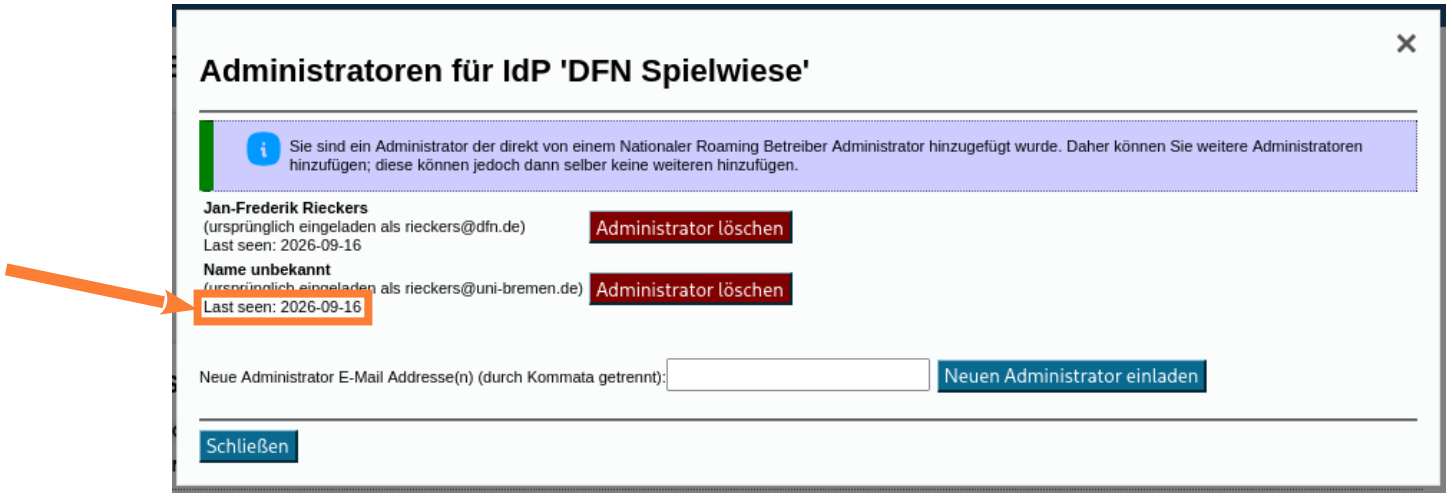
eduroam CAT – Statische Tests

- CAT prüft, ob die im Profil hinterlegten Zertifikate gültig sind
- Zeigt an, wenn Root- oder Intermediate-Zertifikate ausgelaufen (oder < 30 Tage gültig) sind
- Profile sollten dringend angepasst werden
- Neue Profil-Downloads brauchen das alte Zertifikat eh nicht mehr.



eduroam CAT – Admin-Übersicht

- Anzeige des letzten Login-Zeitpunkts für Admins
- Warnung für DFN-Admins, wenn Admins seit > 1 Jahr nicht eingeloggt waren
- Hinweis für Admins in der Einrichtung, dass anderer Admin ggf. nicht mehr aktiv ist
- Bitte an alle: mind. 1x pro Jahr einloggen



Kontaktdaten und Mailinglisten

- dfnroaming@listserv.dfn.de – Mailingliste für alle Ankündigungen, die eduroam betreffen (d.h. auch für easyroam-Einrichtungen)
- easyroam@listserv.dfn.de - Mailingliste für alle Ankündigungen, die easyroam betreffen (insb. easyroam-Portal, easyroam-RADIUS-Server etc.)
- eduroam-d@listserv.dfn.de - Community-Mailingliste für eduroam (Moderiert von der Uni Bremen)
- eduroam@dfn.de - Support-Kontakt für eduroam (z.B. auch Anbindung an die Föderationsinfrastruktur, eduroam SP für easyroam-Einrichtungen)
- easyroam@dfn.de - Support-Kontakt für easyroam (easyroam-Portal, Probleme mit dem easyroam-RADIUS-Server, API, ...)
- Für Kontakt zum Thema Mobile-IT-Forum: markus.krieger@uni-wuerzburg.de

Haben Sie noch Fragen?

- Kontakt
  - Jan-Frederik Rieckers

    E-Mail: rieckers@dfn.de
    Telefon: 0049 30 884299-339
    Fax: 0049 30 884299-370

    Anschrift:
    DFN-Verein, Geschäftsstelle
    Alexanderplatz1
    10178 Berlin
  - eduroam Support

    E-Mail: eduroam@dfn.de
    Telefon: 0049 30 884299-9120
    Fax: 0049 30 884299-370

