

eduroam WLAN

Sergi Doménech Guzy, Mareike Janßen, Anna-Lena
Kramer, Tobias Seydel



Inhalt

Einführung

Funktionsweise

Sicherheit

Betriebswirtschaftliche Einordnung

Zukunftsvision

Was ist eduroam?

EDUCATION ROAMING



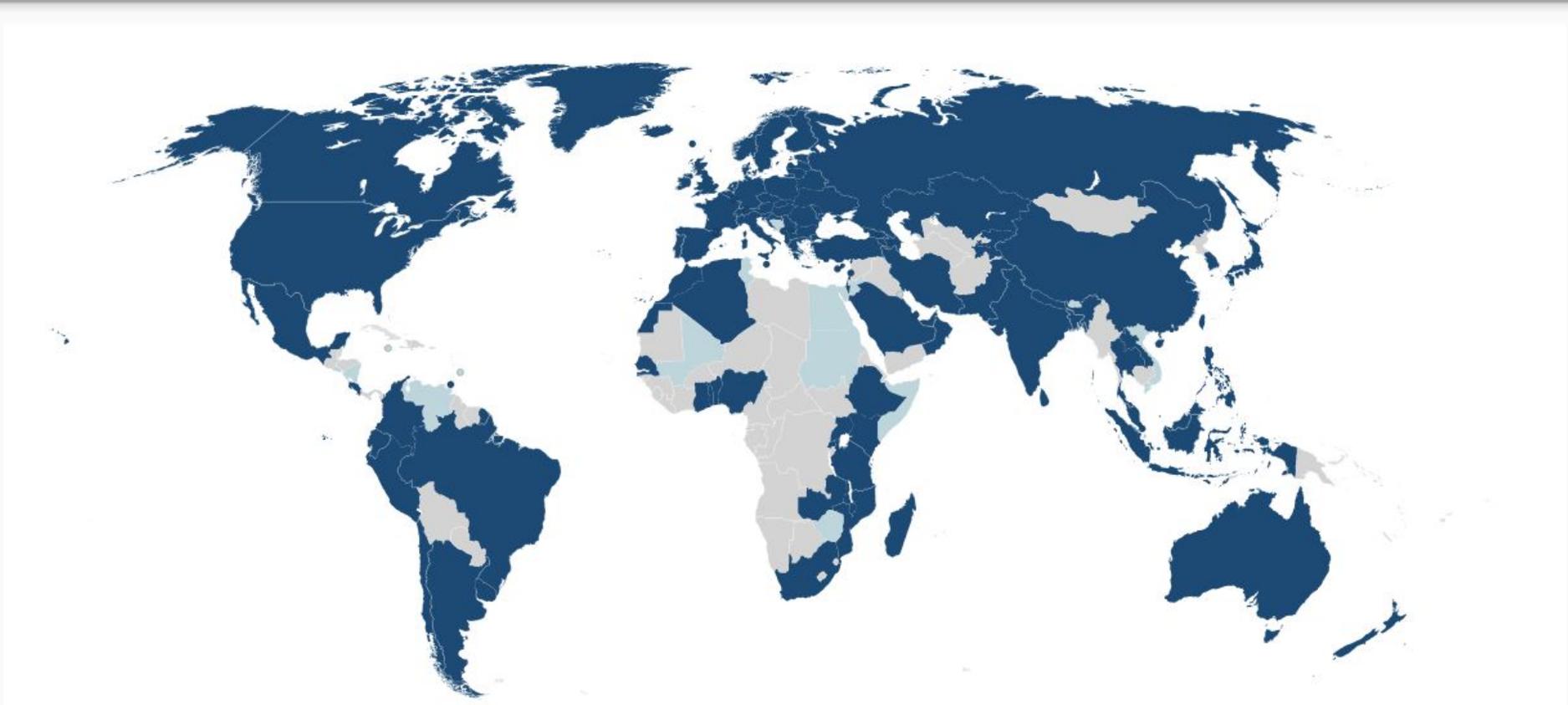
Sign-in once and access wherever you are.

Open your laptop and be online.

Wie hat sich eduroam verbreitet?

- **2002** Gründung durch „GÉANT“ (Forschungs- und Bildungsnetzwerk Community in Europa)
- **2003** Start in 6 Ländern (Niederlande, Deutschland, Finnland, Portugal, Kroatien, UK)
- **2004** erstes nicht-europäisches Land (Australien)

- **Heute** 106 Länder, über 10.000 Standorte
16 Länder mit Pilot Projekten



Von wem wird eduroam verwaltet?



unterstützt + koordiniert

- Verbesserung Technologie und Sicherheit
- weltweite Verbreitung/Verteilung
- technologische + organisatorische Standards

GeGC (Global eduroam Governance Committee)

...



Technischer Aufbau

Confederation top-level
RADIUS Server (TLR)

Federation-Level RADIUS
Server (FLR)

Identity Provider (IdP) +
Service Provider (SP)

TLR

- Zuständig für große geografische Bereiche
- Leitet Anfragen an FLRs oder andere TLRs weiter

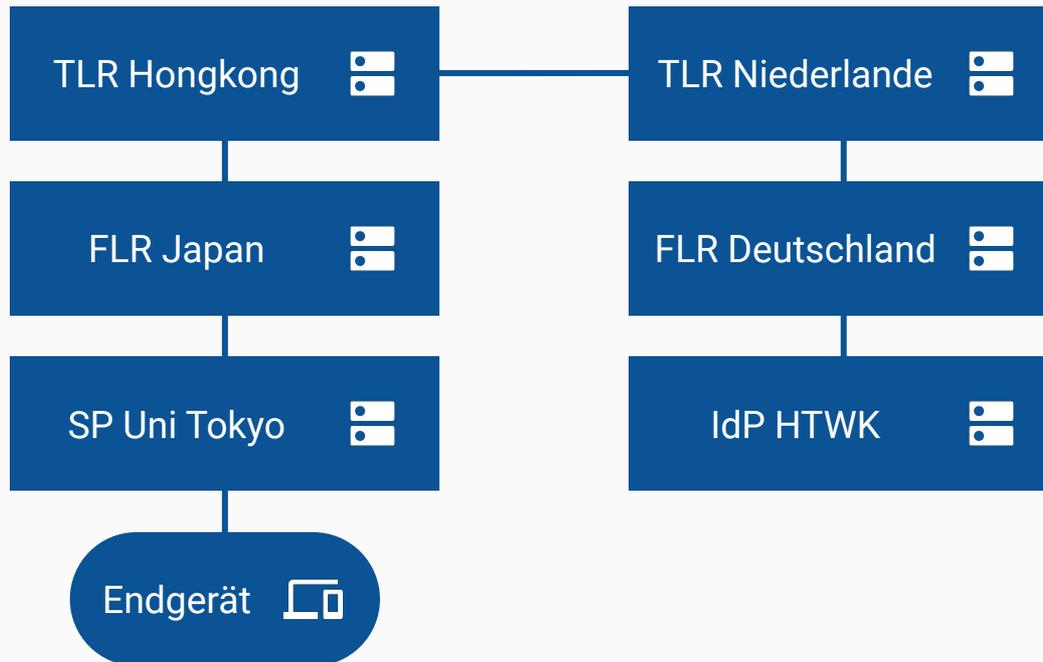
FLR

- Länderspezifische Server
- z.B. FLR für Deutschland: zuständig für alle *.de Server
- Leitet Anfragen zwischen TLR und untergeordneten IdPs/SPs weiter

IdP + SP

- RADIUS Server der Institutionen
- IdPs: Authentifikation der User
- SPs: Netzwerkverbindung zum Nutzer

Beispiel Nutzeranfrage



Software

- keine spezifische Software vorausgesetzt
- muss lediglich die Spezifikationen erfüllen
- z.B. Radiator (TLR, FLR), FreeRADIUS (SP)

Sicherheit

Genutzte EAP Methoden:

PEAP

TLS

TTLS

FAST

- sichere Übertragung der User Authentifizierungsinformationen vom Service Provider (SP) zum Identity Provider (IdP)
- Voraussetzungen für genutzte EAP Methoden:
 - gegenseitige Authentifizierung (Login überall möglich)
 - Verschlüsselung der Anmeldedaten (nur für den IdP sichtbar)

Sicherheit

- Unsichtbarkeit des “echten” Nutzernamen im RADIUS
- Nutzung von äußerer & innerer Identität
 - äußere Identität: sichtbarer “Nutzername” im RADIUS und für die teilnehmenden Parteien
 - innere Identität: eigentliche Nutzer-Informationen, nur sichtbar für den Nutzer selbst und den IdP

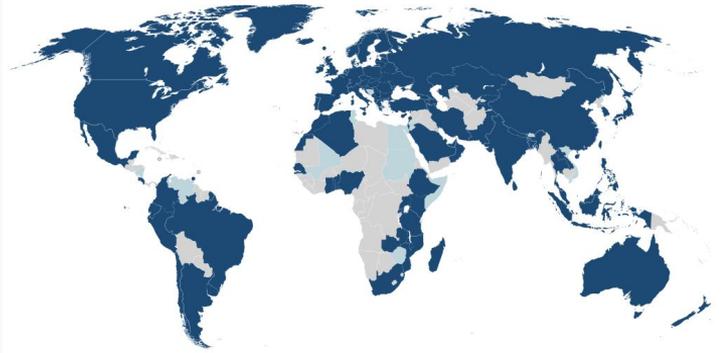
Sicherheit

- Ordnungsgemäße Einrichtung auf den Geräten der Nutzer
 - WPA2/AES wireless encryption, IEEE 802.1X authentication und von Institution verwendete EAP (Authentifizierungsprotokoll) Methode muss unterstützt werden
- Einrichtung des Gerätes für jede Institution spezifisch
- Institutionen stellen "eduroam Configuration Assistant Tool (CAT)" Installer für verschiedene Geräte bereit
 - Automatisierte Einrichtung

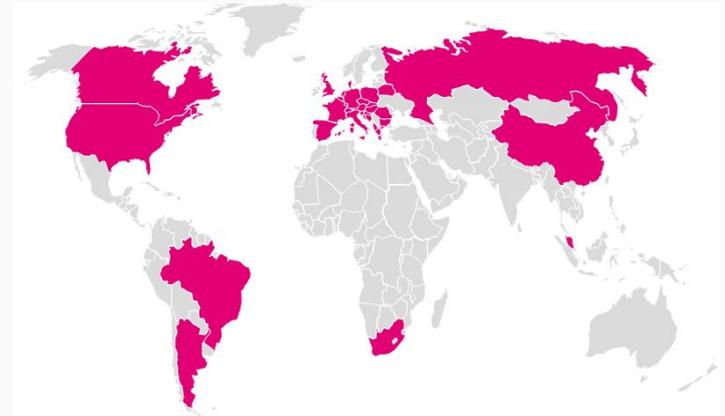
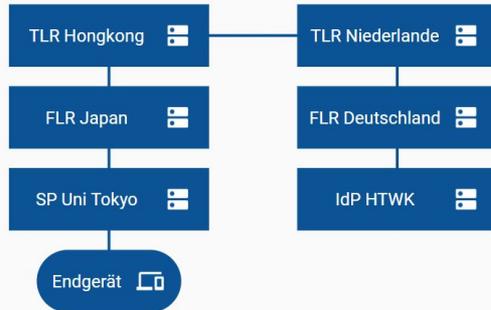
Kostenbetrachtung*

- Eduroam WLAN verfolgt keine Gewinnerzielungsabsichten
- alle nutzungsbasierten *Kosten* obliegen den teilnehmenden Institutionen:
 - *Fixkosten*
 - Infrastruktur für u.a. WLAN, Server usw.
 - Personalkosten für Betrieb und Wartung
 - *Variable Kosten*
 - Nutzungsgebühren Eduroam
 - Lizenzkosten in Abhängigkeit der Nutzerzahlen (Produktabhängig)

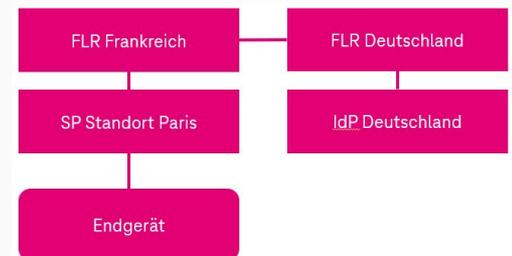
WLAN Roaming in der betrieblichen Praxis am Beispiel der Deutschen Telekom



106 Länder
über 10.000 Standorte



53 Länder
Ø 659 Standorte pro Land
229 170 Mitarbeiter



Ziele & Zukunftsvisionen



- Gründungsmitglied OpenRoaming - Initiative
- **Ziel: Millionen Netzwerke weltweit verbinden**
- keine Einschränkung auf Bildungseinrichtungen
- nahtloser Übergang von WLAN zu WLAN
- keine Anmeldebarrieren
- höhere Sicherheit als öffentliche Netzwerke

Fragen?

Quellen

<https://www.eduroam.org/>

https://www.geant.org/Services/Trust_identity_and_security/Pages/eduroam.aspx

<https://www.dfn.de/dienstleistungen/eduroam/>

<https://wiki.geant.org/collector/pages.action?key=H2eduroam>

Telekom AG: DT Halbjahresbericht 2020 ; Abgerufen am 20.11.2020 unter
<https://www.telekom.com/de/investor-relations/finanzpublikationen>

Bunsen, G. (2016). Eingrenzung von Risiken durch Diebstahl von EduroamCredentials. In P. Müller, B. Neumair, H. Reiser, & G. Dreo, 9. DFN-Forum Kommunikationstechnologien (pp. 107–113). Bonn: Gesellschaft für Informatik e.V. (GI).

Sebastian Brenza, Andre Pawlowski, and Christina Pöpper. (2015). A practical investigation of identity theft vulnerabilities in Eduroam. In Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '15). Association for Computing Machinery, New York, NY, USA, Article 14, 1–11. DOI:<https://doi.org/10.1145/2766498.2766512>

Nutzeranzahl



Kostenorientiert

Leistungsorientierung