Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

eduroam vs. OpenRoaming vs. offenes WLAN

Sicherer WLAN-Zugang, föderiertes Identity Management und wie das zukünftig zusammenpassen könnte

Dr. Sebastian Kiesel, Kilian Krause
sebastian.kiesel@tik.uni-stuttgart.de
kilian.krause@tik.uni-stuttgart.de
79. DFN Betriebstagung, 2023-10-18

tik

Universität Stuttgart

Zahlen und Fakten

- 1829 gegründet, hat sich die frühere Technische Hochschule zu einer forschungsintensiven Universität mit überwiegend ingenieur- und naturwissenschaftlicher Orientierung entwickelt, zu deren besonderem Profil die Vernetzung dieser Fachrichtungen mit den Geistes- und Sozialwissenschaften gehört.
- 22.000 Studierende an 10 Fakultäten
- 270 Professoren und Professorinnen, 3.500 wissenschaftlich Beschäftigte, 1.800 nichtwiss. Beschäftigte
- 2 Campus-Standorte, 140 Gebäude 350.000 m^2 Hauptnutzfläche
- HLRS: Tier-1 HPC
- Starke Kooperation mit außer–universitären Forschungs–einrichtungen
- Im Herzen einer der stärksten High-Tech-Regionen Europas

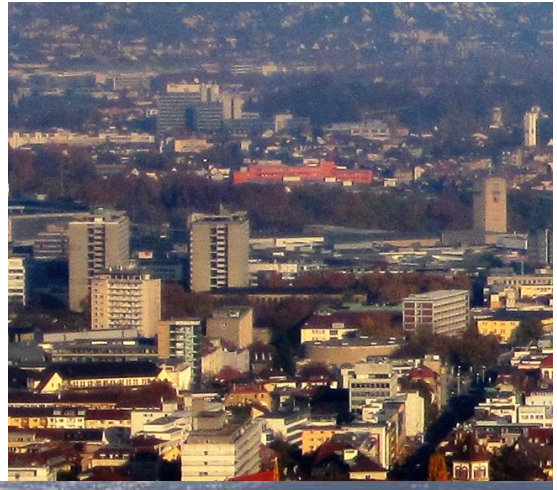
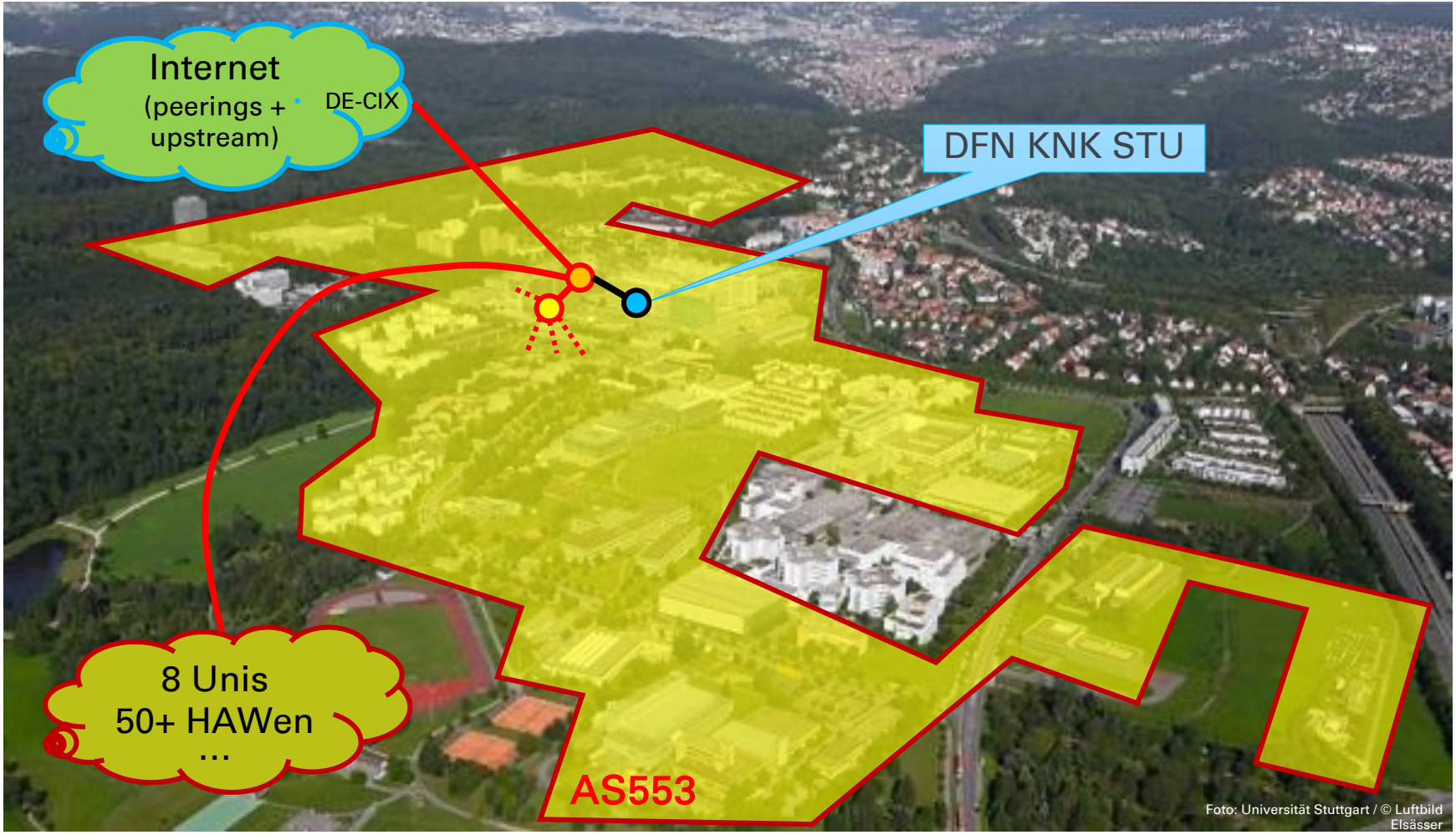


Foto: Universität Stuttgart / © Luftbild Elsässer


Internet
(peerings + upstream)
DE-CIX
DFN KNK STU
8 Unis
50+ HAWen
...
AS553
Foto: Universität Stuttgart / © Luftbild Elsässer

Identitäts-Föderation

- **Service Provider (SP)**
  - Bietet einen Dienst an (z.B. Internet-Zugang über WLAN)
  - Erlaubt Dienst-Nutzung erst “nach Rücksprache” mit dem IdP → “relying party”
  - Nutzt Profile vom IdP, stellt selbst keine eigenen aus (bei z.B. WLAN)

- **Identity Provider (IdP)**
  - Registriert Nutzer (gemäß Policy)
  - Stellt Nutzungsprofile entsprechend an die Nutzer aus (bei z.B. WLAN)
  - Authentisiert und autorisiert Nutzer (“auf Anfrage” des SP)
  - Liefert Identität an den SP (immer oder nur in bestimmten Fällen)
  - Optional: liefert weitere Attribute des Nutzers (z.B. Gruppenzügehörigkeiten)
  - Optional: Erhebt Entgelte vom Nutzer und verrechnet sie mit dem SP

Einrichtungen können sowohl IdP als auch SP sein!

eduroam vs. OpenRoaming

- **eduroam**
  - Weltweite Identitäts-Föderation für WLAN-Nutzung in akademischem Umfeld
  - Universitäten / Hochschulen haben i.d.R. beide Rollen (IdP + SP)
  - Generelle Offenheit, SP-Rolle auch an Dritte zu geben (z.B. Konferenzen)
  - Technisch: EAP + RADIUS
- **govroam**
  - Weltweite Identitäts-Föderation für WLAN-Nutzung im Behörden-Umfeld
  - Ministerien und Verwaltungen analog zu eduroam in beiden Rollen (IdP, SP)
- **OpenRoaming**
  - Eine weitere Föderation ohne Beschränkung
    → mit Beteiligung kommerzieller Unternehmen
  - Technisch: ähnlich, aber moderner – siehe später

Universität / Hochschule als IdP für WLAN

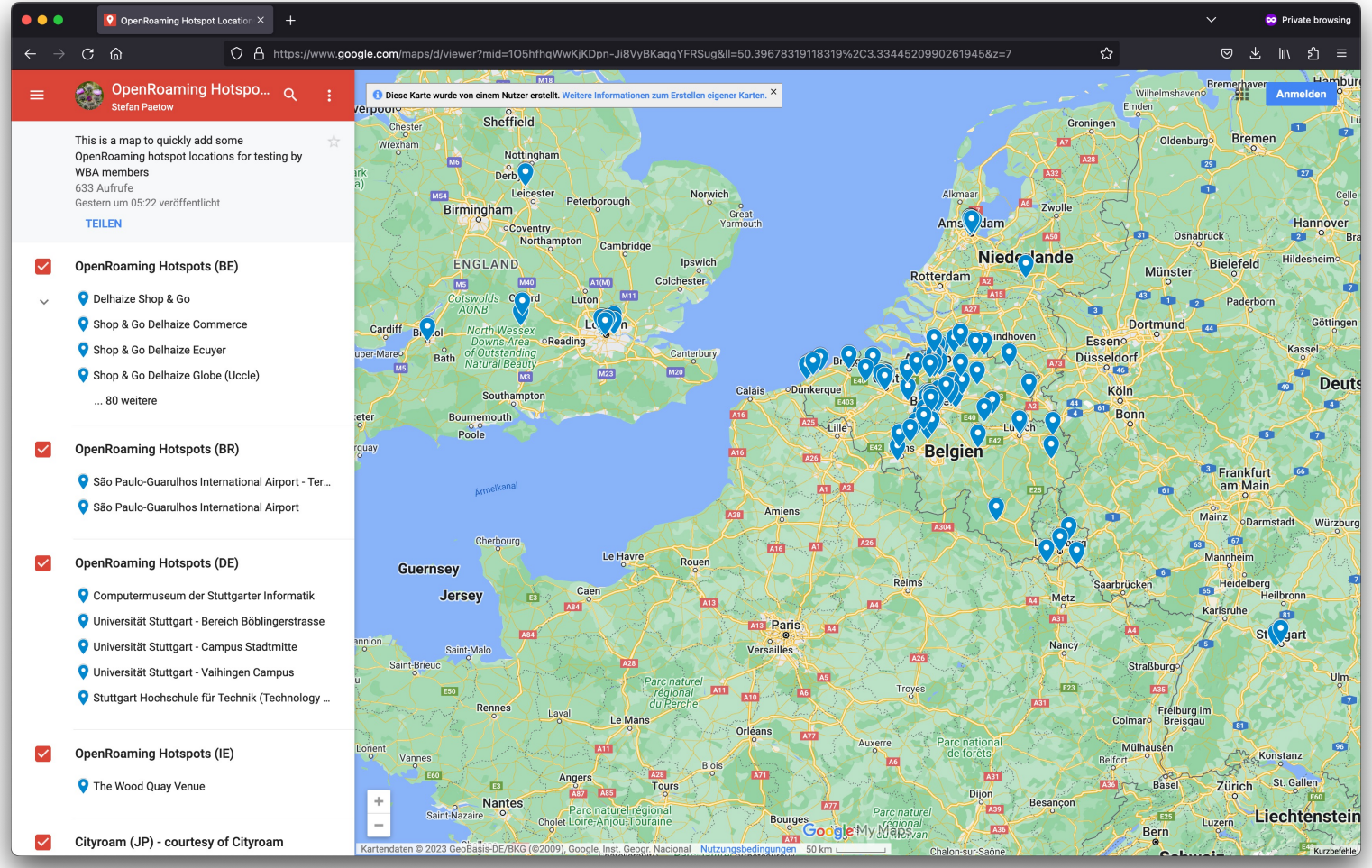
- **Warum?**
  - Wenn Mitglieder / Angehörige auf Reisen gehen, können sie WLANs (typisch: eduroam) in der jeweiligen Föderation nutzen

  → effizienteres Arbeiten auf Dienstreisen

- **Was ist zu beachten?**
  - Datenschutz / Privacy → normalerweise nur pseudonyme ID übermitteln, Aufdeckung der wahren Identität nur in begründeten (Missbrauchs-)Fällen
  - Pseudonyme Identität kann seitens des IdP dynamisch sein (Chargeable-User-ID)
  - Sonstige rechtliche Verpflichtungen

- **OpenRoaming**
  - Lohnt es sich, ein IdP zu werden (zusätzlich zu / anstelle von eduroam)?
  - Was ist zu tun / zu beachten?

Where is OpenRoaming?



Standards hinter OpenRoaming

HotSpot 2.0

Passpoint

OpenRoaming

802.11u

RCOI / OUI

Howto OpenRoaming IdP

- **eduroam**

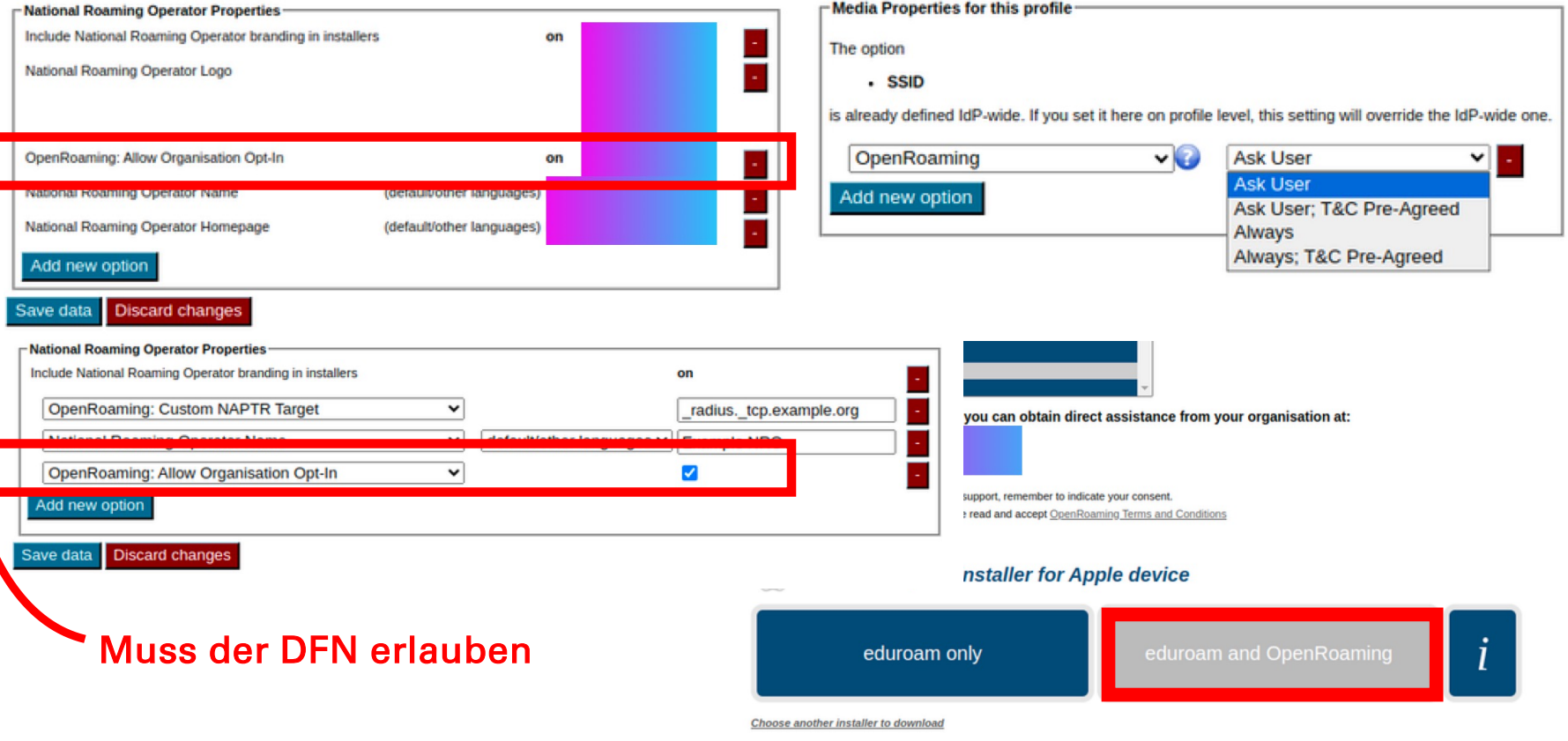
```
$  dig +short uni-stuttgart.de NAPTR
100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.eduroam.de.
$  dig +short _radsec._tcp.eduroam.de. SRV
0 0 2083 tld1.eduroam.de.
0 10 2083 tld2.eduroam.de.
0 20 2083 tld3.eduroam.de.
$
```

- **OpenRoaming**

```
$  dig +short uni-stuttgart.de NAPTR
100 10 "s" "aaa+auth:radius.tls.tcp" "" _radsec._tcp.openroaming.eduroam.org.
$  dig +short _radsec._tcp.openroaming.eduroam.org. SRV
0 0 2083 openroaming1.eduroam.org.
$
```

→ IdP über eduroam Föderation (**braucht nur Profil auf den Clients!**)

OpenRoaming und cat.eduroam.org



Universität / Hochschule als SP für WLAN (in Identitätsföderation)

- **Warum?**
  - WLAN-Zugang für die eigenen Mitglieder/Angehörigen
  - WLAN-Zugang für “Gäste” (z.B. Kooperationspartner sowie neue eigene Geräte)
- **Was ist *möglicherweise* zu beachten?**
  - Identifikation des Teilnehmers (bei Bedarf / immer)
    - Bei Funktionsstörungen / Sicherheitsvorfällen (z.B. Verdacht auf Virenbefall)
    - Bei Missbrauch (z.B. Urheberrechtsverletzungen), ggf. Vorratsdatenspeicherung
  - Beschränkung auf bestimmte Gruppen von Gästen

    → z.B. “akademisches Umfeld”
    - Haushaltsrechtliche Fragestellungen
    - Anforderungen des Upstream-ISP bzw. NREN
    - Rolle als Anbieter von Telekommunikationsdiensten
- **eduroam kann das! Was bietet OpenRoaming?**

Warum reicht eduroam nicht?

- SSID == eduroam (passt nicht überall)
- Überlappende WLAN-Ausleuchtungen problematisch
- SP Kreis in der Praxis limitiert (keine Verbreitung an z.B. öffentlichen Plätzen)
- Onboarding/Bootstrapping braucht zusätzlichen Weg ins Netz
  (IdP-Kreis limitiert)

5G to the rescue?

WLAN vs. 5G

- **Neubauten und energetische Optimierungen**
  - Beschränkung der Mobilfunk-Erreichbarkeit im Gebäude
  - HF-dichte Fassade nur aufwändig zu überwinden

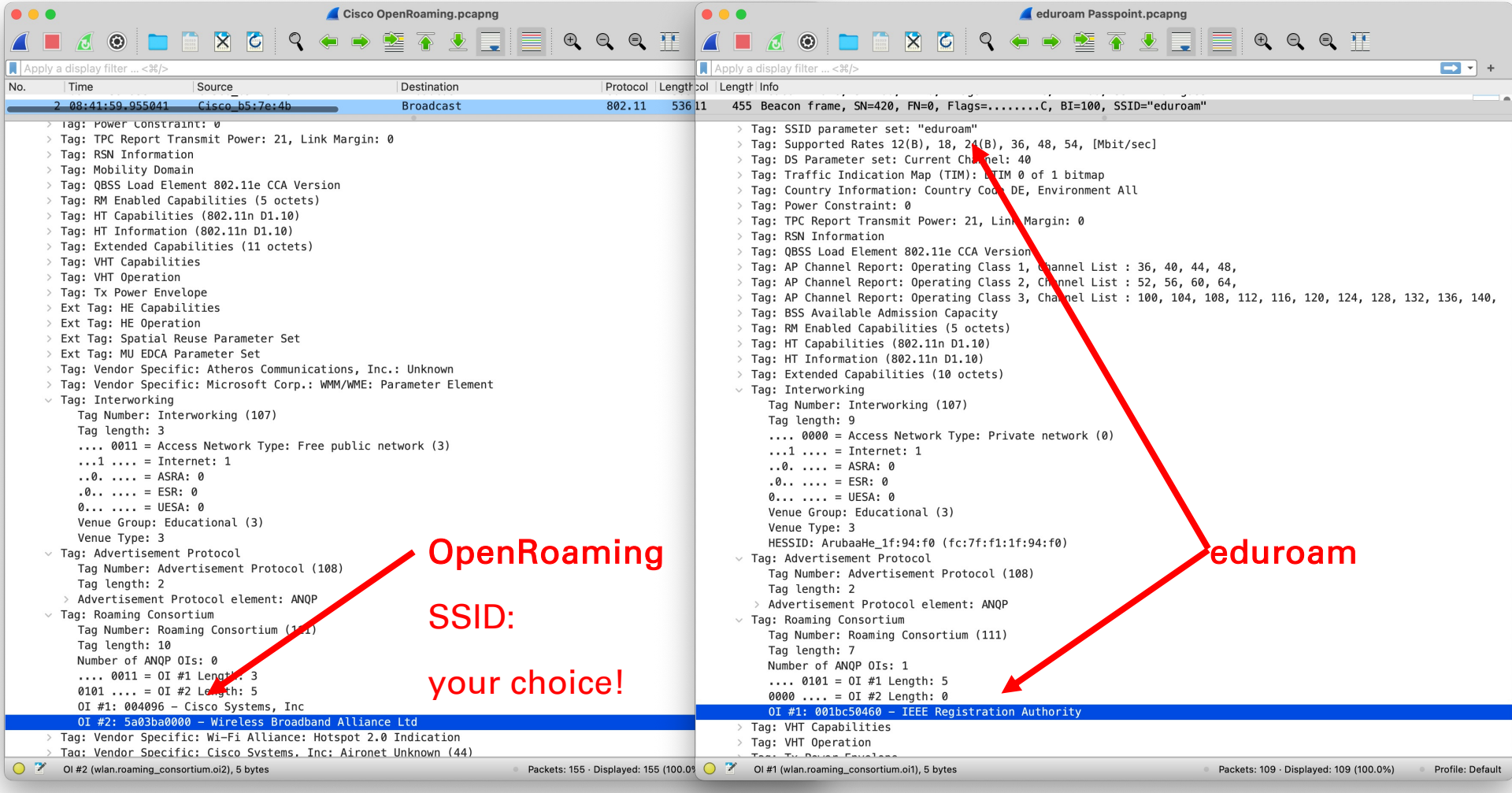
- **Mobilfunk indoor?**
  - Passive Antennensysteme (DAS) sind TEUER ($$$)
  - 5G Remote Radio Heads (RRH) ebenfalls

- **Gäste? BYOD!**
  - Tethering - ”weil es einfacher ist”
    → WLAN-Design wird komplett torpediert (FÜR ALLE!)

Howto OpenRoaming SP

- RADIUS mit shared secret: openroaming-ap.eduroam.org
  (statisch via Paul Dekkers, OR selbst rein auf RadSec ohne statische Routen)
- Für RadSec: OpenRoaming CA kommerziell verfügbar
- Géant als Teil der WBA arbeitet an eigener intermediate CA
  → perspektivisch werden Zertifikate in eduPKI auch für OpenRoaming angeboten
- Operator-Name "`4EDUROAM`" (ggf. "`4EDUROAM.<domain>`" t.b.d.)
- Typische RCOI in OpenRoaming (https://wiki.geant.org/pages/viewpage.action?pageId=133763844)
  - OpenRoaming Baseline participation **5A-03-BA-00-00**
  - Education only **5A-03-BA-08-00**
  - Cisco OpenRoaming Legacy 00-40-96 (z.B. OpenRoaming app)
- eduroam® Géant Passpoint (non-OpenRoaming) **00-1B-C5-04-60**
  - Wird schon jetzt über geteduroam automatisch installiert

RCOI im Beacon



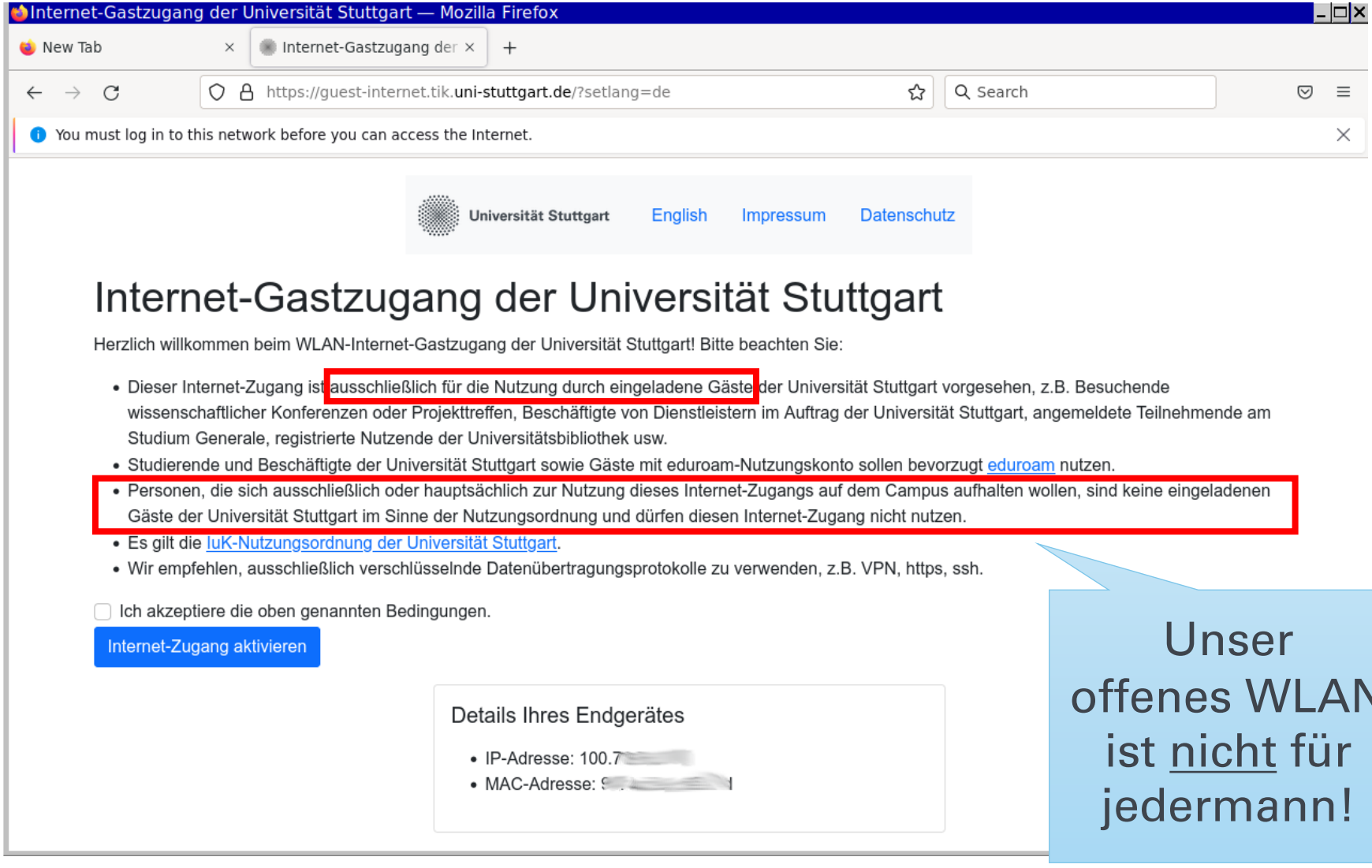
eduroam vs. OpenRoaming

- Unabhängigkeit von SSID == eduroam öffnet Möglichkeiten
  - z.B. in Shopping Malls, Flughäfen, Bahnhöfen, Hotels, …
- Onboarding wird erleichtert (BYOI, “eh da Identität” – z.B. Google/SAMSUNG)
- Überlappende Ausleuchtungen konkurrieren nicht mehr
  (eduroam zweier Einrichtungen)
- WLAN-Ausleuchtung wird nicht durch Tethering belastet
  (WiFi schon verbunden)
- RadSec direkt ab eigenem RADIUS vermeidet SPOF
  - RadSec mit X.509 TLS hat andere Fehler/Probleme/Herausforderungen

Exkurs: Das “offene WLAN” der Universität Stuttgart

- **Ausgangssituation**
  - Viele “Gäste” ohne eduroam-Konto benötigen bzw. wollen WLAN
    - Projektpartner aus der Industrie
    - Dienstleister / Handwerker im Auftrag der Universität
    - Studium Generale / Stadtnutzer der UB
  - 3. TMGÄndG = “offenes-WLAN-Gesetz” (2016) → Wegfall Störerhaftung
  - Aber: darf das Uni-RZ kostenloses WLAN für wirklich jedermann anbieten?

- **Lösungsansatz**
  - Offenes WLAN mit Captive Portal
    → Zustimmung zur Nutzungsordnung
    → Selbst-Erklärung durch Nutzer, ein “eingeladener Gast” der Universität zu sein
  - Routing des Verkehrs via VRF “extern” zu kommerziellem Internet-Upstream


Internet-Gastzugang der Universität Stuttgart — Mozilla Firefox
New Tab
Internet-Gastzugang der
https://guest-internet.tik.uni-stuttgart.de/?setlang=de
Search
You must log in to this network before you can access the Internet.
Universität Stuttgart
English
Impressum
Datenschutz
Internet-Gastzugang der Universität Stuttgart
Herzlich willkommen beim WLAN-Internet-Gastzugang der Universität Stuttgart! Bitte beachten Sie:
Dieser Internet-Zugang ist ausschließlich für die Nutzung durch eingeladene Gäste der Universität Stuttgart vorgesehen, z.B. Besuchende wissenschaftlicher Konferenzen oder Projekttreffen, Beschäftigte von Dienstleistern im Auftrag der Universität Stuttgart, angemeldete Teilnehmende am Studium Generale, registrierte Nutzende der Universitätsbibliothek usw.
Studierende und Beschäftigte der Universität Stuttgart sowie Gäste mit eduroam-Nutzungskonto sollen bevorzugt eduroam nutzen.
Personen, die sich ausschließlich oder hauptsächlich zur Nutzung dieses Internet-Zugangs auf dem Campus aufhalten wollen, sind keine eingeladenen Gäste der Universität Stuttgart im Sinne der Nutzungsordnung und dürfen diesen Internet-Zugang nicht nutzen.
Es gilt die IuK-Nutzungsordnung der Universität Stuttgart.
Wir empfehlen, ausschließlich verschlüsselnde Datenübertragungsprotokolle zu verwenden, z.B. VPN, https, ssh.
Ich akzeptiere die oben genannten Bedingungen.
Internet-Zugang aktivieren
Details Ihres Endgerätes
IP-Adresse: 100.7
MAC-Adresse:
Unser offenes WLAN ist nicht für jedermann!

VRF Campus vs. VRF External

eduroam (staff-account@uni-stuttgart.de)

```
$ sudo traceroute -T www.tu-berlin.de
traceroute to www.tu-berlin.de (130.14
 1  ras-r2-eduroam-staff.in.uni-stuttg
 2  c1-ras-r2.in.uni-stuttgart.net (14
 3  b2-c1.in.uni-stuttgart.net (141.58
 4  stu-eti-a99-bu1.belwue.net (193.19
 5  cr-fra2-be15.x-win.dfn.de (188.1.2
 6  cr-erl2-be5.x-win.dfn.de (188.1.14
 7  cr-tub2-be10.x-win.dfn.de (188.1.1
 8  kr-tub248.x-win.dfn.de (188.1.235.
 9  enc-fp.gate.tu-berlin.de (130.149.
10  en-dist2-en-core.gate.tu-berlin.de
11  e-ns-e-n.gate.tu-berlin.de (130.14
12  www.tu-berlin.de (130.149.7.201)
$
```

Gast-WLAN

```
$ sudo traceroute -T www.tu-berlin.de
traceroute to www.tu-berlin.de (130.14
 1  guestwlan-capport-nat-r1.in.uni-st
 2  ras-r2-guestwlan-x.in.uni-stuttgar
 3  c1-ras-r2-x.ext.uni-stuttgart.net
 4  b2-c1-x.ext.uni-stuttgart.net 141.
 5  stu-eti-a99-bu1-100.belwue.net (12
 6  fra-decix-a99-hu0-1-0-3.belwue.net
 7  * fra-decix-a99-hu0-1-0-0.belwue.n
 8  80.157.200.197 (80.157.200.197)  7
 9  d-ed6-i.D.DE.NET.DTAG.DE (217.5.71
10  cr-tub2-be9.x-win.dfn.de (188.1.14
11  kr-tub248.x-win.dfn.de (188.1.235.
12  kr-tub248.x-win.dfn.de (188.1.235.
13  en-dist2-en-core.gate.tu-berlin.de
14  e-ns-e-n.gate.tu-berlin.de (130.14
15  * www.tu-berlin.de (130.149.7.201)
$
```

Zusammenfassung / Ausblick

- **OpenRoaming ist eine Identitätsföderation für WLAN**
  - Technisch vergleichbar mit eduroam
  - Mit kommerziellen Teilnehmern → neue rechtliche Fragestellungen
- **Teilnahme als IdP**
  - (Noch) nicht dringend erforderlich, da es (noch) wenige SPs gibt → jetzt probieren
- **Teilnahme als SP**
  - Könnte das Problem der Identifizierung (z.B. bei Urheberrechtsverstößen) lösen → brauchen wir (derzeit) aber nicht: keine Störerhaftung → offenes WLAN
  - Keine Einschränkung auf bestimmte Nutzergruppen (z.B. nur Hochschul-Angehörige)? → haushaltsrechtliche Fragestellungen + Regeln des NREN!
  - Ausnutzung von BYOI für Onboarding/Gäste/…
  - Beobachten, rechtliche Rahmenbedingungen klären!

Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

Vielen Dank!

Dr. Sebastian Kiesel

E-Mail sebastian.kiesel@tik.uni-stuttgart.de
Telefon +49 (0) 711 685-62503
www.tik.uni-stuttgart.de

Universität Stuttgart
Technische Informations- und Kommunikationsdienste (TIK)
Allmandring 30A
70550 Stuttgart

Universität Stuttgart
Technische Informations- und
Kommunikationsdienste (TIK)

Vielen Dank!

Kilian Krause

E-Mail kilian.krause@tik.uni-stuttgart.de
Telefon +49 (0) 711 685-64512
www.tik.uni-stuttgart.de

Universität Stuttgart
Technische Informations- und Kommunikationsdienste (TIK)
Allmandring 30A
70550 Stuttgart