BWCAMPUSNETZ

Zukunftsfähige Konzepte für die Campusnetze
an Universitäten und Hochschulen

Nahtlose Vernetzung an Universitäten und Hochschulen durch OpenRoaming

Federführung bei der Erstellung dieses Dokuments: Universität Stuttgart
Kontakt: team@bwcampusnetz.de

OpenRoaming

OpenRoaming ist wie eduroam ein Netzzugang über 802.1X im WLAN und nutzt entsprechend mindestens die WPA2-Enterprise (bzw. WPA3-Enterprise auf 6GHz/WiFi6E) Unterstützung der WLAN-Clients für den Aufbau einer sicheren WLAN- Verbindung. Analog zur bekannten eduroam Föderation existieren auch wieder Identity Provider und Service Provider (bei OpenRoaming benannt als „Access Network Provider"/ANP). Wie schon bei eduroam kann eine Einrichtung eine oder beide Rollen einnehmen.

OpenRoaming kann damit als eine Weiterentwicklung des föderierten WLAN-Netzzugangs gesehen werden, den die Hochschulen bereits von eduroam kennen. Wegen seiner Herkunft und Vorgaben der eduroam Policy ist der eduroam Verbund auf Einrichtungen der Forschung und Lehre (Higher Education) als Identity Provider beschränkt.

Grundsätzlich ist es möglich, dass beliebige WLAN-Infrastrukturanbieter rein als Service-Provider an eduroam teilnehmen, jedoch ist die Verbreitung an z.B. Hotels, Flughäfen, Bahnhöfen etc. bisher nicht nennenswert (in Deutschland) zu finden. Die Forderung nach der statischen SSID „eduroam" machen den Dienst für die Allgemeinheit wenig attraktiv und praktikabel (eine Alternative mit Passpoint existiert zwar theoretisch, aber ist bei den Nutzern nicht ausreichend verbreitet). Das hat bisher die Verbreitung von eduroam außerhalb der Einrichtungen der höheren Lehre stark limitiert. Netzwerke im öffentlichen Raum bzw. im Bereich „Hospitality" haben typischerweise schon eine 802.1X SSID für eigene Benutzung, z.B. für Personal, Geräte- Zugang (Zahlungsverkehr), Premium Kundennetz oder als „sichere SSID" des entsprechenden Serviceproviders. Da die Menge an SSIDs pro Accesspoint in der Luft begrenzt ist, wird bei OpenRoaming auf den 802.11u Standard gesetzt, um keine statische SSID zu erzwingen. Durch diesen Standard kann (als „HotSpot 2.0" Konfiguration) das Endgerät eine Menge Profile installiert haben, die Roaming Consortia über so genannte Roaming Consortium Identifyer (RCOI) zugeordnet sind. Eine technische Übersicht über die Möglichkeiten und Abhängigkeiten der Konfigurationen von Infrastruktur und WLAN-Endgeräten findet sich in dem Whitepaper „All You Need To Know About OpenRoaming" der Enea AB.[1] Durch die Nutzung einer zentralen SSID für alle 802.1X Zugänge lässt sich über RADIUS ein entsprechendes Profil pro Gerät bzw. Geräteklasse hinterlegen, so dass die Ausnutzung der Kapazität auf der Luftschnittstelle (AirTime) optimiert wird. Lediglich

Geräte, die kein 802.1X beherrschen (z.B. IoT Sensoren oder Appliances) oder die noch kein Profil installiert haben, müssen auf ein entsprechendes alternatives WLAN ausweichen. Hierfür strahlt die Uni Stuttgart ein offenes WLAN mit Captive Portal sowie ein PSK-WLAN für IoT aus.

Da im OpenRoaming der Identity Provider bereits bestätigt, dass Clients den Nutzungsbedingungen von OpenRoaming zugestimmt haben, als ihnen das entsprechende Geräteprofil ausgehändigt wurde, bedarf es aus rein technischen Gründen keiner erneuten Prüfung am SP/ANP und dadurch auch keines Captive Portals für entsprechende AGB oder Acceptable Use Policy im WLAN-Zugangsnetz (da diese Regeln eben bereits festgelegt sind und diesen zugestimmt wurde). Für das Abuse- Handling ist im OpenRoaming Standard die Bereitstellung von Chargeable-User- Identities (CUI) vorgeschrieben, so dass eine eindeutige Zuordnung jederzeit sichergestellt ist. Darüber, wie der entsprechende Identity Provider zu erreichen ist, gibt es jedoch noch keine technisch einheitliche Lösung und Vorgabe.

Aktuell sind große Identity Provider im Kontext OpenRoaming neben einzelnen Mobilfunkanbietern (z.B. AT&T US) auch die Mobilfunkgerätehersteller (z.B. SAMSUNG, Google, teilweise auch Apple), die entweder im Betriebssystem direkt oder über entsprechende Apps entsprechende Profile bereitstellen, so dass ein sicherer WLAN- Zugang ohne weitere Konfiguration sofort ausgewählt werden kann.

Die Erfahrung hat gezeigt, dass ein relevanter Anteil der Nutzer über diese Arten von Profilen verfügt und dass darüber der WLAN-Zugang sofort auf breiter Basis genutzt wird, sobald die SSID ausgestrahlt wird. Eine konkrete Aufforderung der Nutzer oder Führung durch Konfigurationsassistenten ist nicht nötig. Für Nutzer, die lediglich Dienste aus dem Internet benötigen, ist diese Art der Bereitstellung eines sicheren WLANs also in etwa mit eduroam vergleichbar, bis eben auf den Punkt, dass die notwendigen Profileinstellungen bereits auf dem Telefon verfügbar und hinterlegt sind. Durch diese Niederschwelligkeit entfällt jegliche Notwendigkeit der Nutzer auf entsprechende Mobiltelefon-Hotspot Funktionalität zurückzugreifen, um beispielsweise Tablets ohne Mobilfunk-Option mit Netzwerk zu versorgen.

Wer als eduroam Einrichtung an OpenRoaming teilnehmen will, kann dies über eingehende NAPTR Einträge im DNS jederzeit umsetzen, da SURF einen entsprechenden Proxy betreibt. Erläuterungen der notwendigen Details wurden auf der 79. DFN Betriebstagung im Forum Mobile IT vorgestellt.[2]

Im Rahmen der Beteiligung am Forschungscampus ARENA2036 hat die Uni Stuttgart ebenfalls einen eigenen IdP – unabhängig von eduroam aufgebaut.

Auf der 79. DFN-Betriebstagung hat der DFN in Aussicht gestellt, dass möglicherweise auch bald durch den DFN ein entsprechender Proxy bereitgestellt werden könnte. Belastbare Daten für einen Umsetzungszeitraum liegen jedoch Anfang März 2024 noch nicht vor.

Durch die oben ausgeführten Einschränkungen ist zwar technisch möglich, OpenRoaming auf den RCOI für „higher education“ (5A:03:BA:08:00) einzuschränken, jedoch würde das inhaltlich auf dieselbe (eduroam) Nutzergruppe hinauslaufen. Diese ist über eduroam schon ausreichend gut abgedeckt und hätte dadurch keinen Vorteil. Ebenso wäre diese nicht auf eine reine Passpoint-Konfiguration zu migrieren, da nicht alle Endgeräte ausschließlich mit Passpoint-Profilen abgedeckt sind und ohnehin Profile für die SSID „eduroam“ an anderen Standorten auch weiterhin benötigen. Eine Weiterführung der SSID „eduroam” ist daher auf absehbare Zeit unabdingbar.

Falls jedoch der offene OpenRoaming RCOI (5A:03:BA:00:00) akzeptiert würde, könnte der WLAN-Controller bzw. der RADIUS-Server nicht zwischen (akademischen) Gästen der Universität Stuttgart sowie den lediglich „zufällig“ auf dem Campus der Universität Stuttgart befindlichen Dritten unterscheiden. In enger Abstimmung mit dem Rektorat und der Rechtsabteilung der Universität Stuttgart – unter Berücksichtigung haushaltsrechtlicher Anforderungen, den Aufgaben einer Universität gemäß LHG sowie der Hausordnung – betreibt das Rechenzentrum einen „offenen“ (d.h. ohne WPA2/3) WLAN-Zugang für Gäste, die kein eduroam-Konto besitzen. Um Zugang zum Internet zu bekommen, muss ein Gast an einem „Captive Portal“ sowohl die Nutzungsordnung akzeptieren, als auch bestätigen, ein eingeladener Gast der Universität zu sein - z.B. Teilnehmer einer wissenschaftlichen Konferenz oder des Studium Generale oder Stadtnutzer der Universitätsbibliothek. Diese formale Zustimmung bzw. Erklärung wäre daher bei Nutzung von OpenRoaming mit den allgemeinen und uneingeschränkten RCOI nur durch zusätzliche Schaltung eines vergleichbaren Captive Portals möglich. Der offensichtliche technische Vorteil gegenüber der Lösung mit dem offenen WLAN wäre dann nicht mehr gegeben, so dass wir bis eine andere politische bzw. rechtliche Lösung für dieses Problem gefunden werden kann, das OpenRoaming auf dem Campus nach einer kurzen praktischen Erprobungsphase wieder abgeschaltet haben.

1 Versionsverlauf

Version	Datum	Änderungen
1.0	22.03.2025	Initiale Veröffentlichung

Literaturverzeichnis

[1] *All You Need To Know About OpenRoaming*. Adresse: `https://info.enea.com/openroaming-white-paper` (besucht am 31. 12. 2025).

[2] S. Kiesel und K. Krause, *eduroam vs. OpenRoaming vs. offenes WLAN*, 79. Betriebstagung des Vereins zur Förderung eines Deutschen Forschungsnetzes (DFN), Berlin, Germany, Okt. 2023. Adresse: `https://www.dfn.de/wp-content/uploads/2023/03/BT79_MobileIT_eduroam-openroaming.pdf`.