OpenRoaming

01.02.2024, Thomas Klein (thomas@thomas-klein.de)

Was stört euch an öffentlichen WLANs?

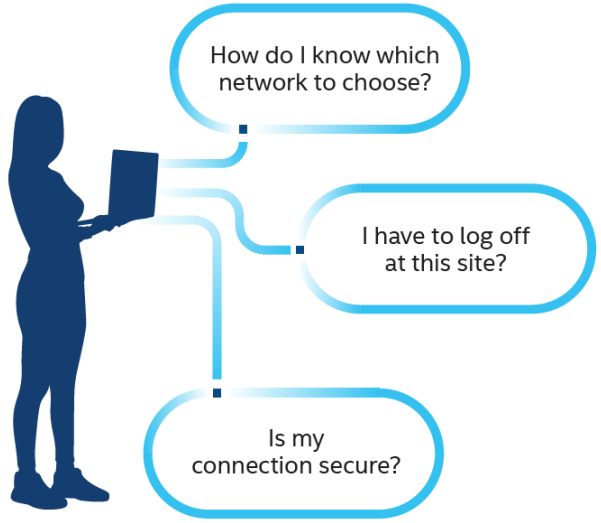
Welche Probleme will OpenRoaming lösen?

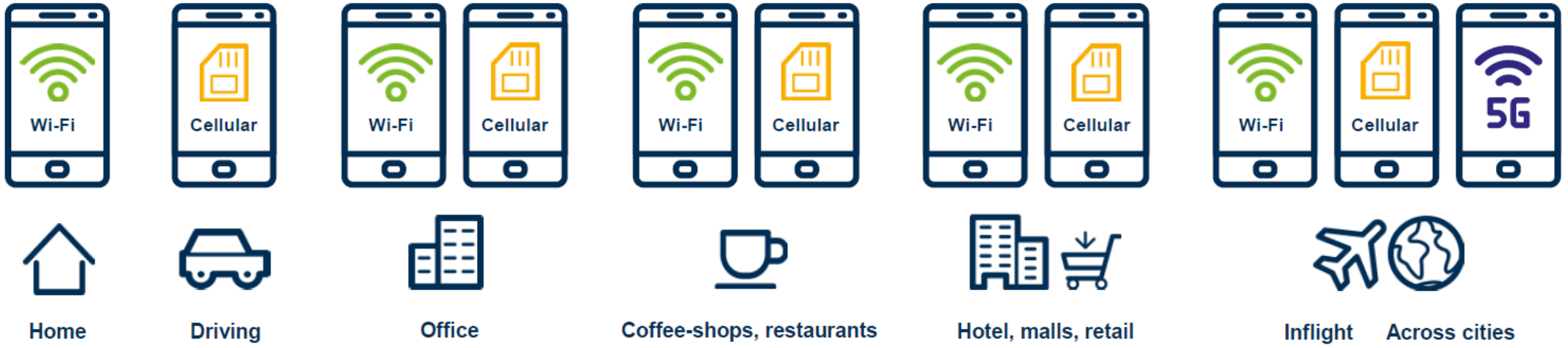
Security & Privacy

How to be sure Wi-Fi is secure and private?

User Experience

How to solve the pain of connecting to Wi-Fi?





Wie löst OpenRoaming diese Probleme?

Einmalige Nutzer Aktion

- Endgerät durch Anmeldung bei einem Identitätsanbieter freischalten
  (Dadurch wird ein Verbindungsprofil auf meinem Endgerät angelegt)

Ab dann

- Endgerät wird nun automatisch und sicher mit allen WLANs die OpenRoaming unterstützen verbunden

Highlights

- Automatische Verbindung mit dem WLAN
- Kein Raten welche WLAN SSID verwendet werden soll
- Sichere, verschlüsselte Verbindung
- Nahtloses roaming zwischen WLAN und 4G/5G

Was ist OpenRoaming?

Die Idee oder Vision von OpenRoaming ist:
Providing Automatic & Secure Wi-Fi Everywhere to Everyone
(Automatisches und sicheres WLAN überall und für alle bereitstellen)

OpenRoaming ist ein offener Industriestandard für einfaches und nahtloses Roaming zwischen Wi-Fi-Netzwerken ohne manuellen Login-Prozess.

Er wird von der Wireless Broadband Alliance vorangetrieben und unterstützt Roaming zwischen Wi-Fi-Netzen und Mobilfunknetzen mit Technologien wie Wi-Fi 6 und 5G.

Der Vorgang des OpenRoamings ist vergleichbar mit dem Roaming in Mobilfunknetzen. Er bietet ein ähnlich hohes Maß an Sicherheit und Benutzerfreundlichkeit.

Quelle: https://www.ip-insider.de/was-ist-openroaming-a-1076933/

Wie funktioniert OpenRoaming?

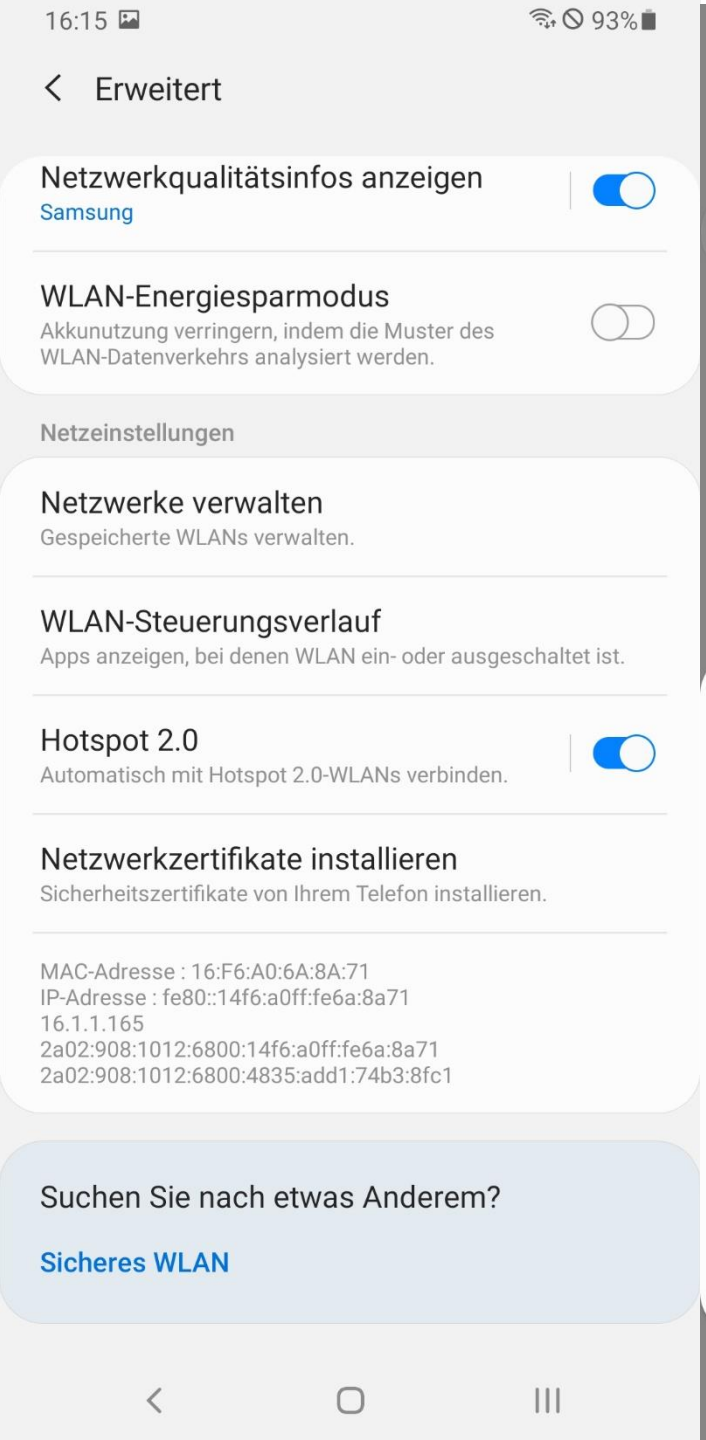
Auf Endgeräten
Auf einem WLAN Access Point mit WLAN Controller
Auf den Radius Servern

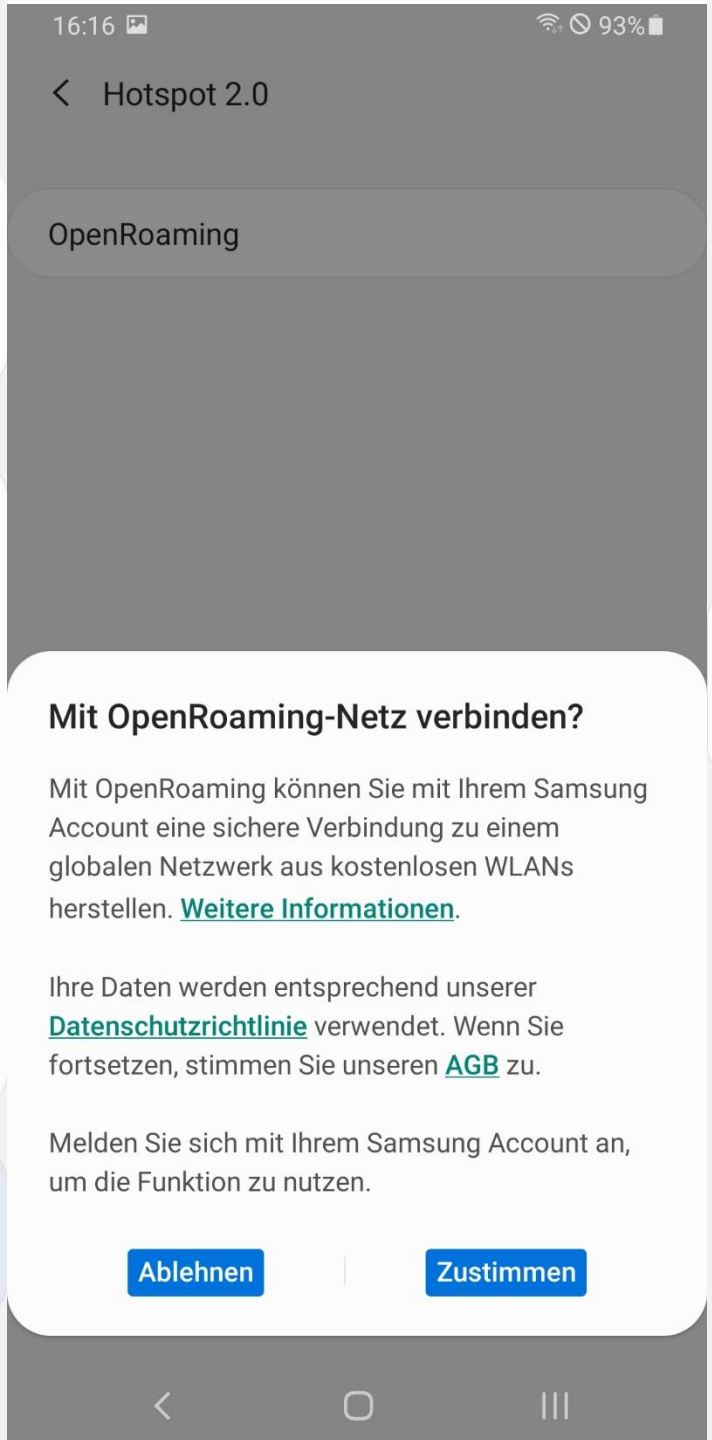
Wie funktioniert OpenRoaming?
Auf einem Handy oder Tablet oder Laptop als Endgerät

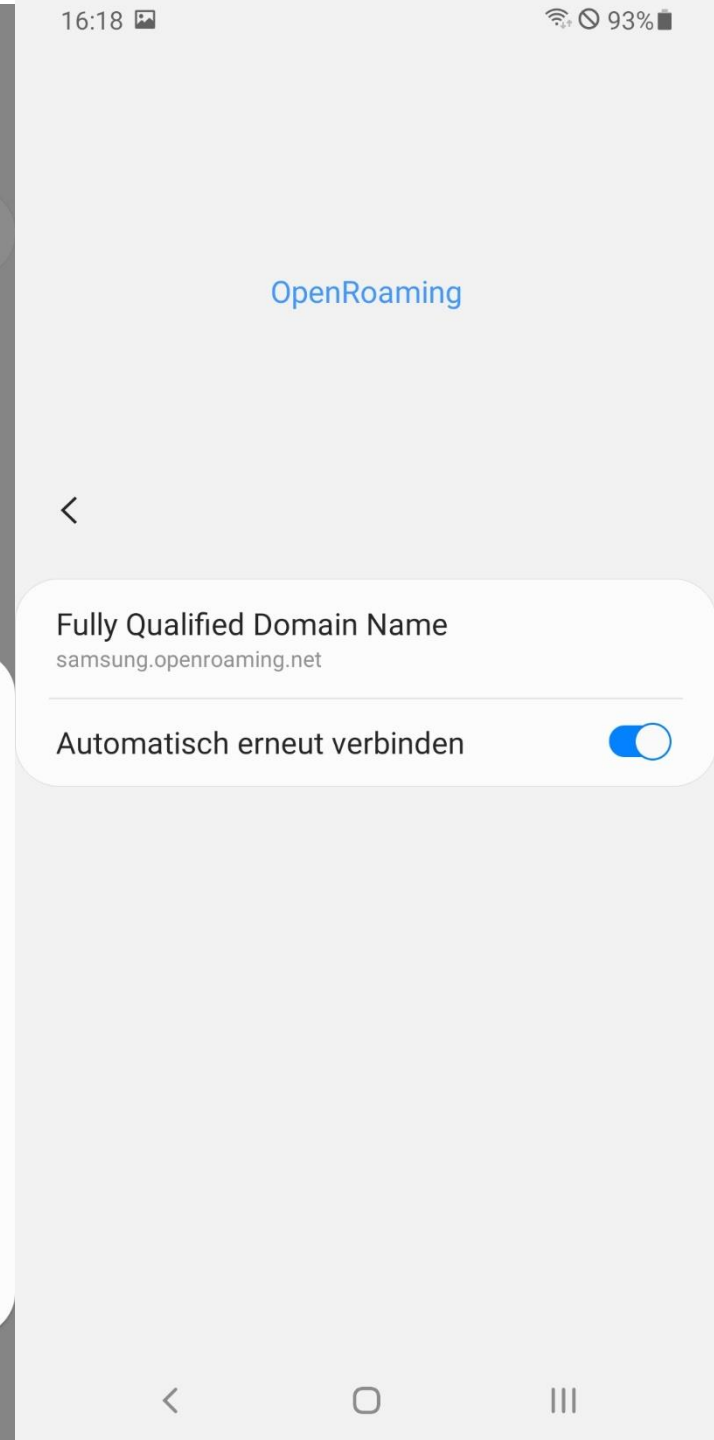
Welche Geräte werden wie unterstützt?

- Mit Native OS Support
  - ✓Samsung Geräte mit Android 10 oder höher (unter Nutzung der Samsung ID)
  - ✓Google Pixel mit Android 11 oder höher (unter Nutzung der Google ID)
- Mit einer OpenRoaming Mobile App
  - ✓Android Geräte mit Android 9 oder höher (unter Nutzung der Google ID)
  - ✓Apple Geräte mit iOS 13.3 oder höher (unter Nutzung der Apple ID)
- Über ein Web Portal
  - ✓Android, iOS
  - ✓Windows 10 & 11, macOS

- Voraussetzungen
  - ✓Das Gerät muss Passpoint/Hotspot 2.0 unterstützen
  - ✓Es muss ein Profil auf dem Endgeräte erzeugt werden (einmalig)


16:15
93%
Erweitert
Netzwerkqualitätsinfos anzeigen
Samsung
WLAN-Energiesparmodus
Akkunutzung verringern, indem die Muster des WLAN-Datenverkehrs analysiert werden.
Netzeinstellungen
Netzwerke verwalten
Gespeicherte WLANs verwalten.
WLAN-Steuerungsverlauf
Apps anzeigen, bei denen WLAN ein- oder ausgeschaltet ist.
Hotspot 2.0
Automatisch mit Hotspot 2.0-WLANs verbinden.
Netzwerkzertifikate installieren
Sicherheitszertifikate von Ihrem Telefon installieren.
MAC-Adresse : 16:F6:A0:6A:8A:71
IP-Adresse : fe80::14f6:a0ff:fe6a:8a71
16.1.1.165
2a02:908:1012:6800:14f6:a0ff:fe6a:8a71
2a02:908:1012:6800:4835:add1:74b3:8fc1
Suchen Sie nach etwas Anderem?
Sicheres WLAN


16:16
93%
Hotspot 2.0
OpenRoaming
Mit OpenRoaming-Netz verbinden?
Mit OpenRoaming können Sie mit Ihrem Samsung Account eine sichere Verbindung zu einem globalen Netzwerk aus kostenlosen WLANs herstellen. Weitere Informationen.
Ihre Daten werden entsprechend unserer Datenschutzrichtlinie verwendet. Wenn Sie fortsetzen, stimmen Sie unseren AGB zu.
Melden Sie sich mit Ihrem Samsung Account an, um die Funktion zu nutzen.
Ablehnen
Zustimmen


16:18
93%
OpenRoaming
Fully Qualified Domain Name
samsung.openroaming.net
Automatisch erneut verbinden

17:23 70%

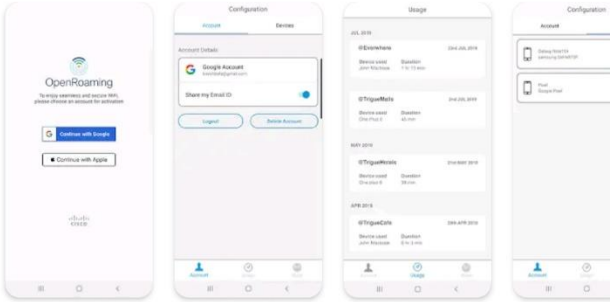
OpenRoaming

Cisco Systems, Inc.

Mehr als 1000
Downloads

0
USK ab 0 Jahren

Installieren



Über diese App

Konfiguriert Ihr Gerät mit kostenlosem, nahtlosem und sicherem WLAN.

Effizienz

Bewertungen & Rezensionen

Noch keine Rezensionen

17:24 70%

OpenRoaming

To enjoy seamless and secure WiFi, please choose an account for activation

Continue with Google

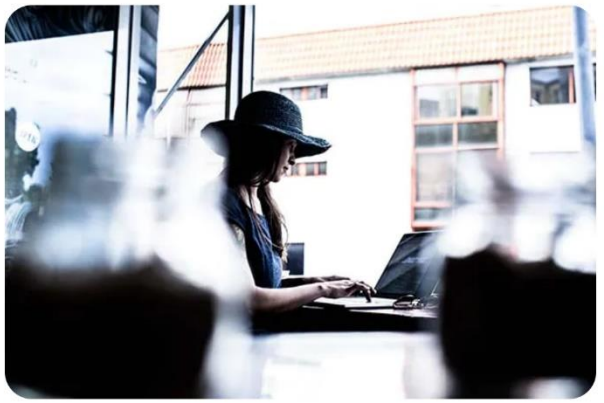
Continue with Apple

17:25 69%

Agreements

Terms and Conditions | Privacy Policy

Cisco Online Privacy Statement



The Trust Center

Cisco is committed to maintaining strong protections for our customers, products and

I Accept OpenRoaming T&C & Privacy Policy

Continue

17:27 69%

OpenRoaming

Über Google anmelden

Anmeldung

Weiter zu openroaming.net

E-Mail oder Telefonnummer

E-Mail-Adresse vergessen?

Wenn Sie fortfahren möchten, müssen Sie zustimmen, dass Google Ihren Namen, Ihre E-Mail-Adresse, Ihre Spracheinstellung und Ihr Profilbild an openroaming.net weiter gibt.

Konto erstellen

Weiter

Deutsch

Hilfe Datenschutz Nutzungsbedingungen

Was ist Passpoint/Hotspot 2.0?

Passpoint/Hotspot 2.0 ist ein Standard der Wi-Fi Alliance, der es mobilen Geräten ermöglicht, sich automatisch mit einem in Reichweite befindlichen Wi-Fi-Hotspot zu verbinden und sich ohne Interaktion des Anwenders zu authentifizieren.

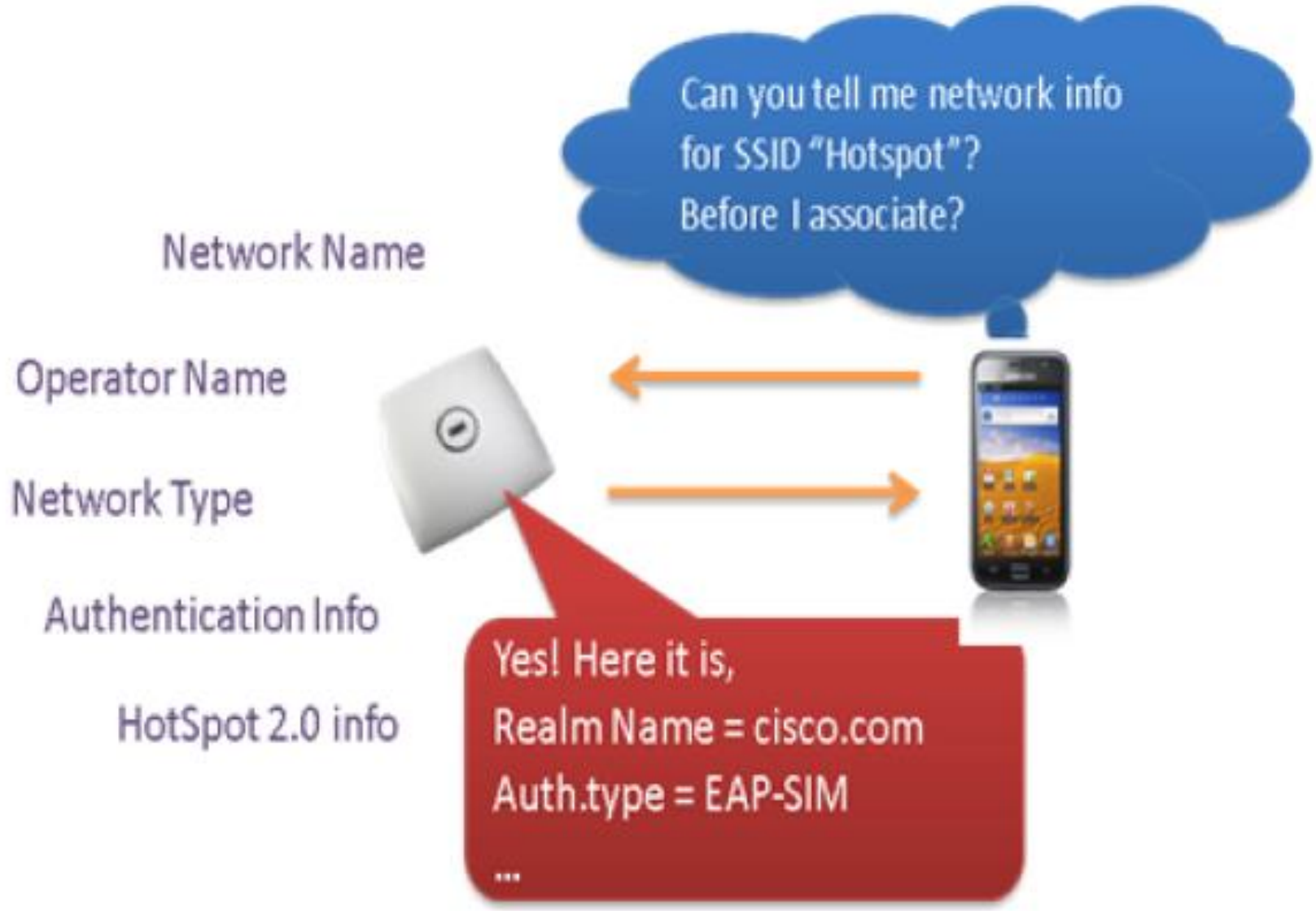
Zugrunde liegt hierbei der IEEE 802.11u Standard von 2011, auf dem Hotspot 2.0 dann basiert.

Passpoint ist die Zertifizierung der Wi-Fi Alliance für Geräte die Hotspot 2.0 unterstützen.

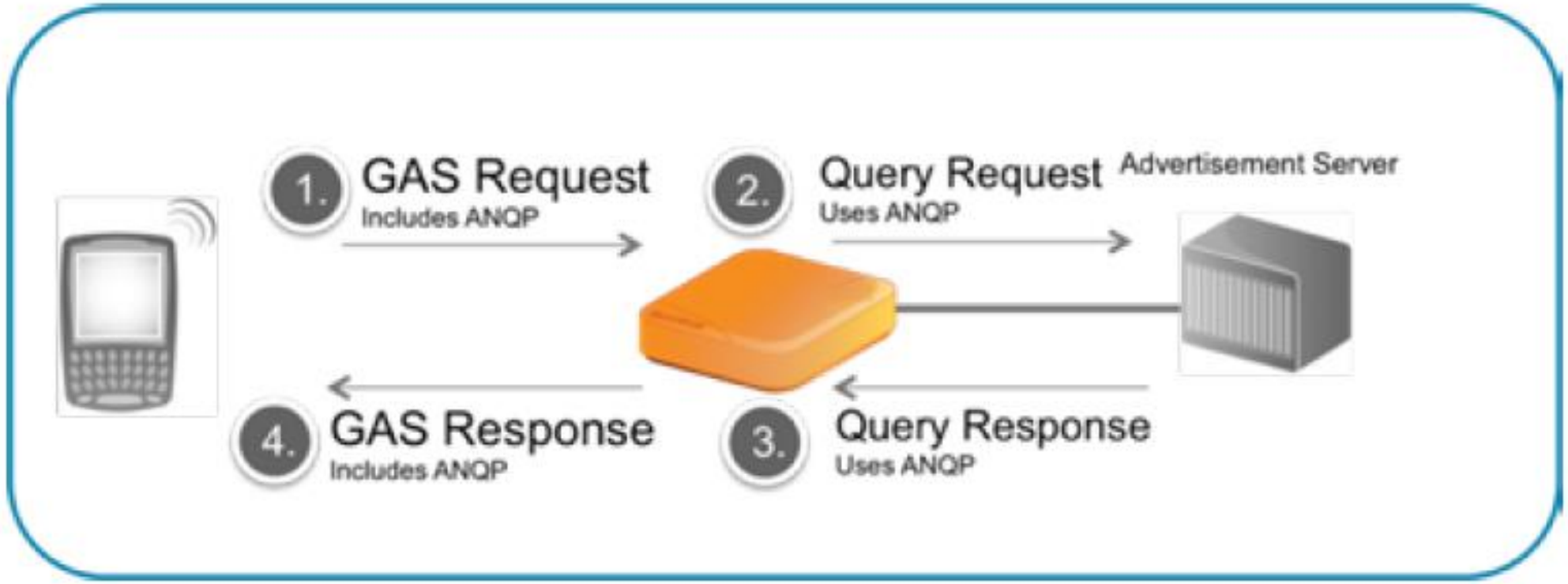
ORGANIZATION	INITIATIVE	DETAILS
IEEE	802.11u	802.11u amendment to 802.11 standard published in February 2011
Wi-Fi Alliance	Hotspot 2.0	Technical program and specification that defines technical requirements for Passpoint™ interoperability certification
Wireless Broadband Alliance	Next Generation Hotspot	End-to-end roaming trials establish common commercial framework for interoperability across networks and devices

Quelle: https://www.ip-insider.de/was-ist-hotspot-20-hs2-passpoint-a-943234/

Wie funktioniert Passpoint/Hotspot 2.0?



Wie funktioniert Passpoint/Hotspot 2.0?

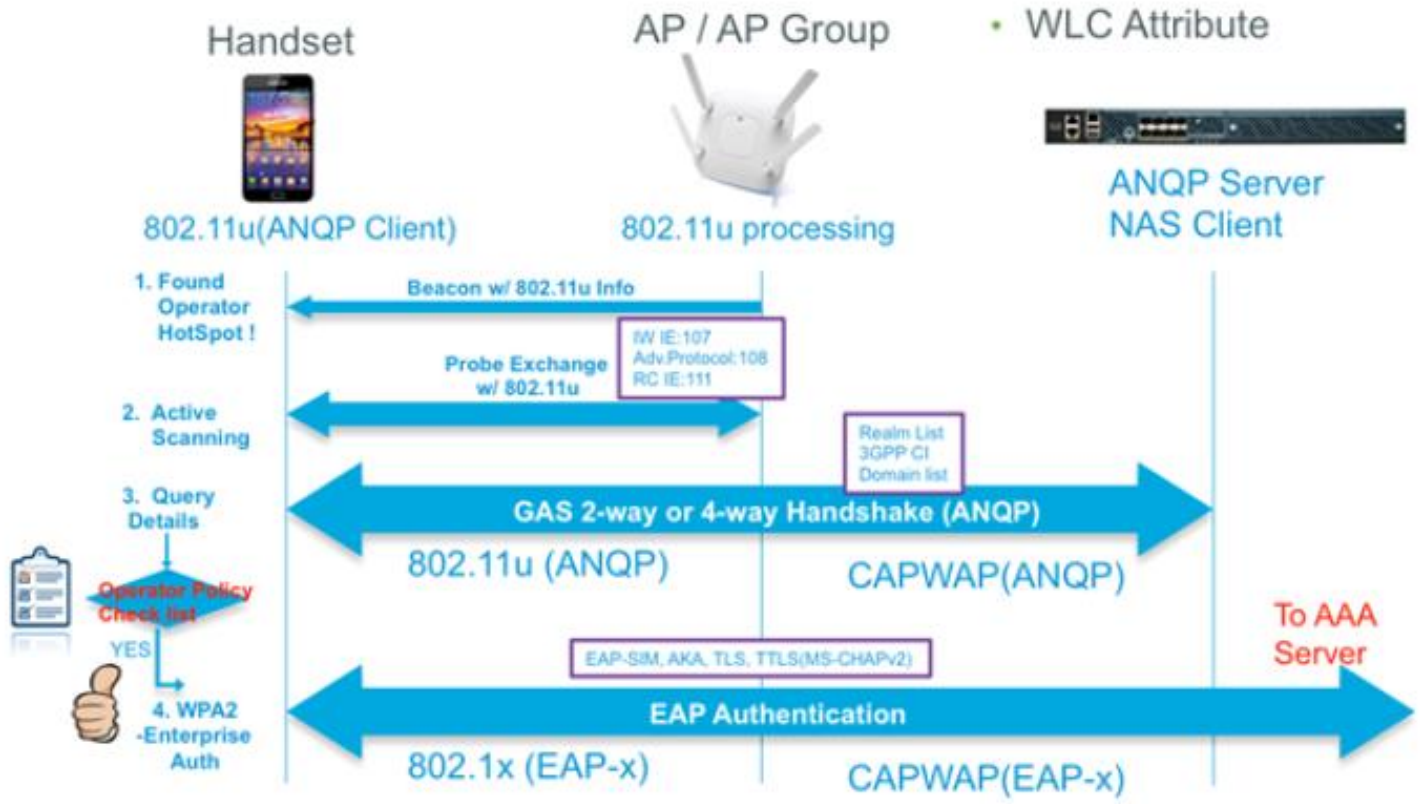


Für einen Technical DeepDeepDive:
https://www.commscope.com/globalassets/digizuite/62767-wp-114159-en-ruckus-how-interworking-works-lr.pdf

Quelle: https://www.commscope.com/globalassets/digizuite/62767-wp-114159-en-ruckus-how-interworking-works-lr.pdf

Wie funktioniert Passpoint/Hotspot 2.0?

Passpoint/Hotspot 2.0 ermöglicht eine Vorab-Kommunikation zwischen dem Endgerät und dem Access Point, bevor sich das Endgerät überhaupt „richtig“ mit dem Access Point verbindet.



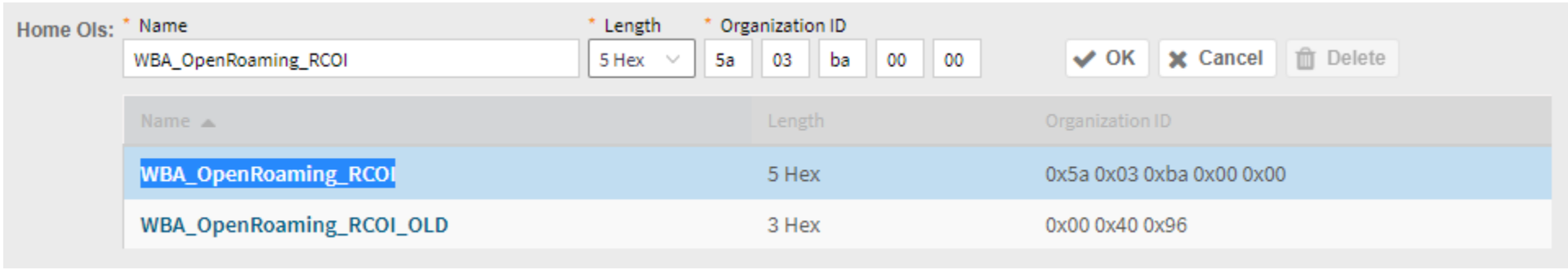
OpenRoaming und Passpoint/Hotspot 2.0

- Passpoint/Hotspot 2.0 funktioniert auch unabhängig von OpenRoaming
- Aber OpenRoaming benötigt Passpoint/Hotspot 2.0 als Grundlage
- OpenRoaming nutzt diese Funktionalitäten um den Endgeräten Zugangsmöglichkeiten anzubieten:
  Mit der SSID OpenRoaming@DB kannst du kostenlos das Internet erreichen
  Du kannst dazu die Google ID und die Apple ID benutzen
  o.
  Mit der SSID OpenRoaming@DB kannst du kostenlos das Internet erreichen
  Du kannst jede beliebige ID der OpenRoaming Federation benutzen
  Du darfst dabei anonym bleiben
  o.
  Mit der SSID OpenRoaming@DB kannst du kostenlos das Internet erreichen
  Du kannst jede beliebige ID der OpenRoaming Federation benutzen
  Du bekommst nur Zugang wenn du dich nicht-anonym anmeldest

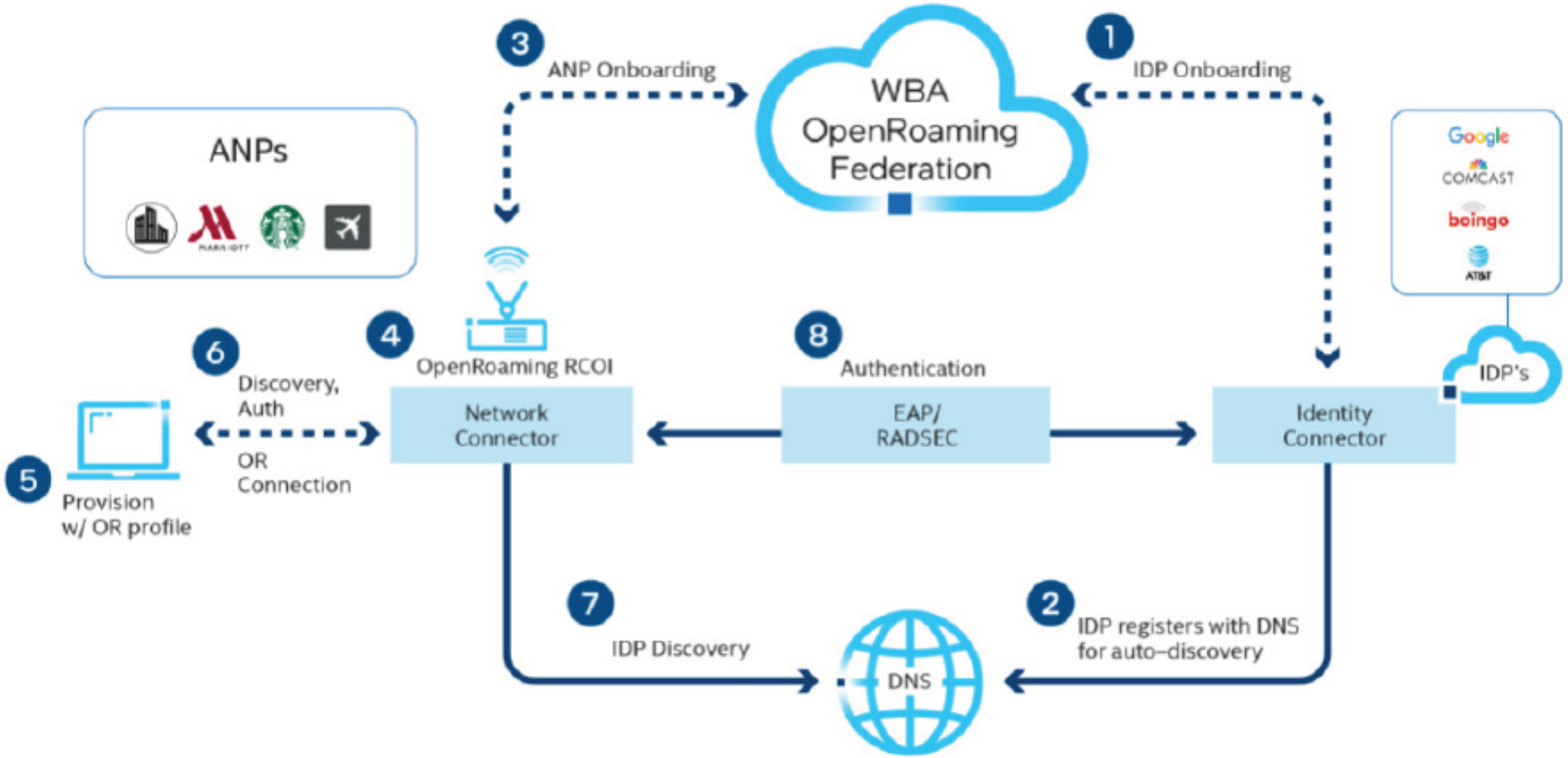
RCOIs - Roaming Consortium Organization Identifiers

OpenRoaming-Settled: BA-A2-D0-xx-xx
OpenRoaming-Settlement-Free: 5A-03-BA-xx-xx

OUI-36 Octet 4								OUI-36 Octet 5			
Bit Position											
B7	B6	B5	B4	B3	B2	B1	B0	B7	B6	B6	B4
LoA	QoS		PID	ID-Type				Reserved – set to 0			



Wie funktioniert OpenRoaming?



Quelle: https://www.intel.com/content/dam/www/central-libraries/us/en/documents/wi-fi-open-roaming-overview-whitepaper.pdf

IDP Discovery via NAPTR

Der anonyme WLAN Benutzer “tnlym9mjoh@samsung.openroaming.net” soll über Radius authentifiziert werden.
Wie findet der lokale Radius den passenden Openroaming IDP Radius Server? Es gibt ja viele IDPs.

host -t naptr samsung.openroaming.net

samsung.openroaming.net has NAPTR record 50 50 "s" "aaa+auth:radius.tls.tcp" "" _radiustls._tcp.samsung.openroaming.net.

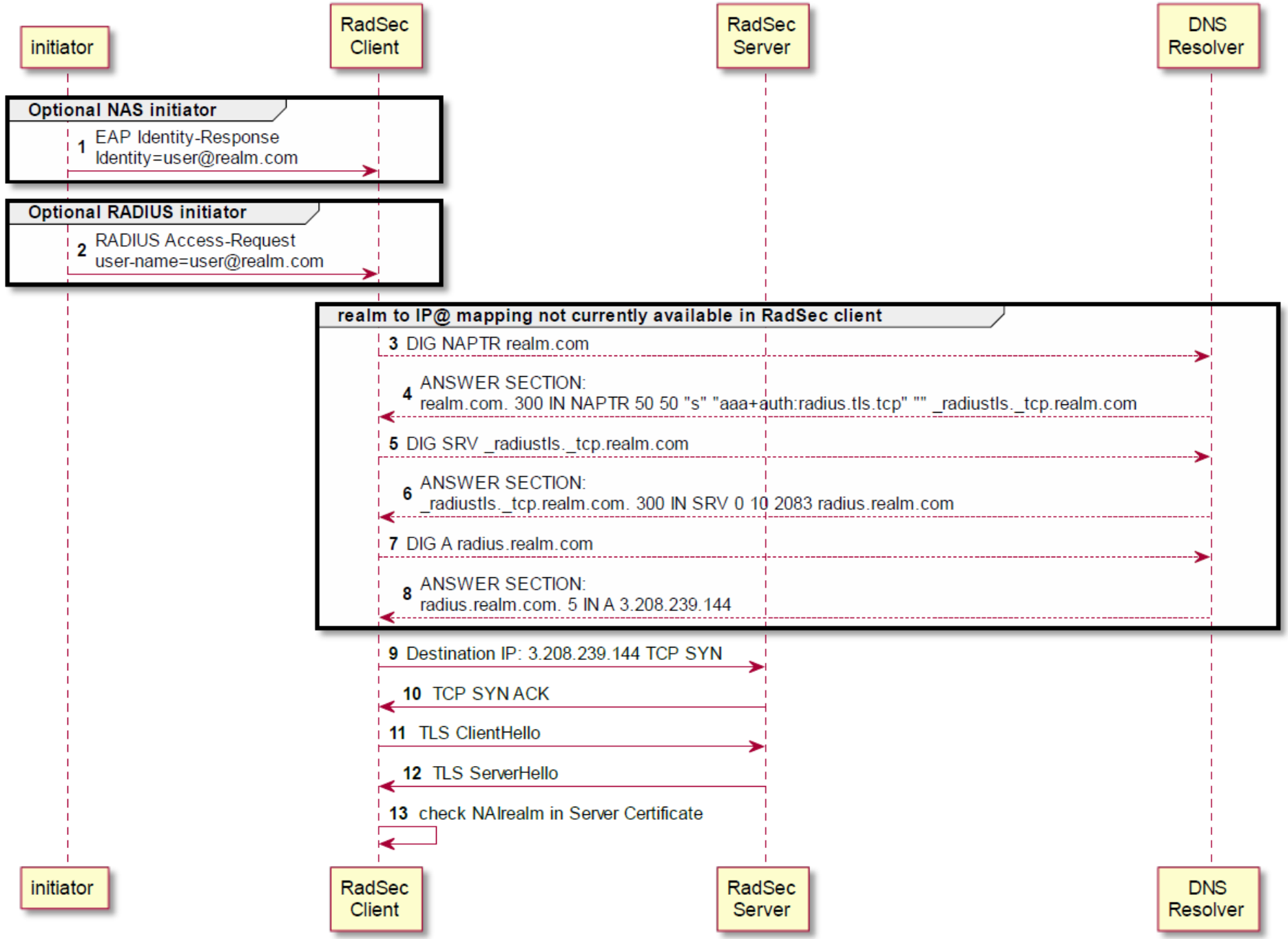
host -t srv _radiustls._tcp.samsung.openroaming.net

_radiustls._tcp.samsung.openroaming.net has SRV record 0 10 2083 idp.openroaming.net.

host idp.openroaming.net.

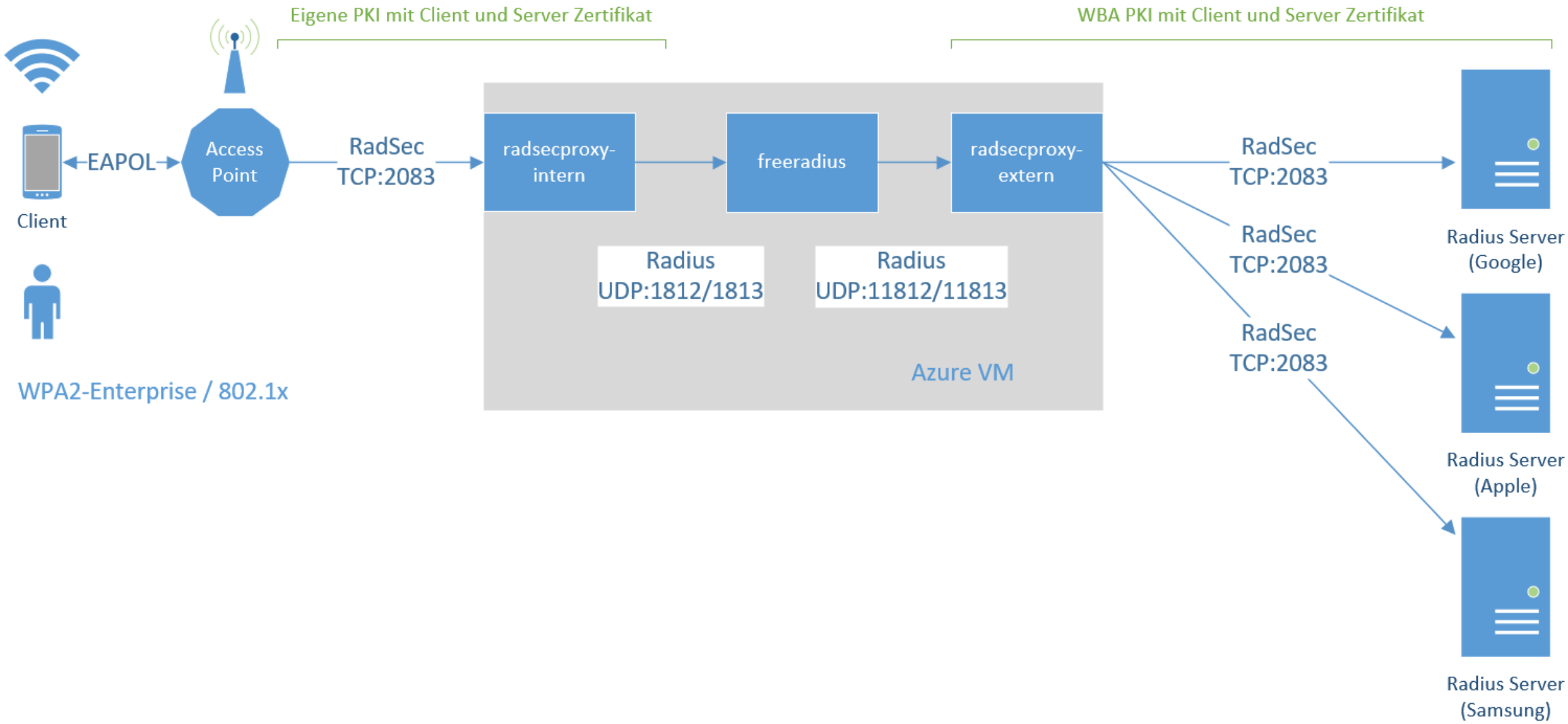
idp.openroaming.net has address 3.208.239.144

Wer mehr wissen will: RFC 7585
Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)

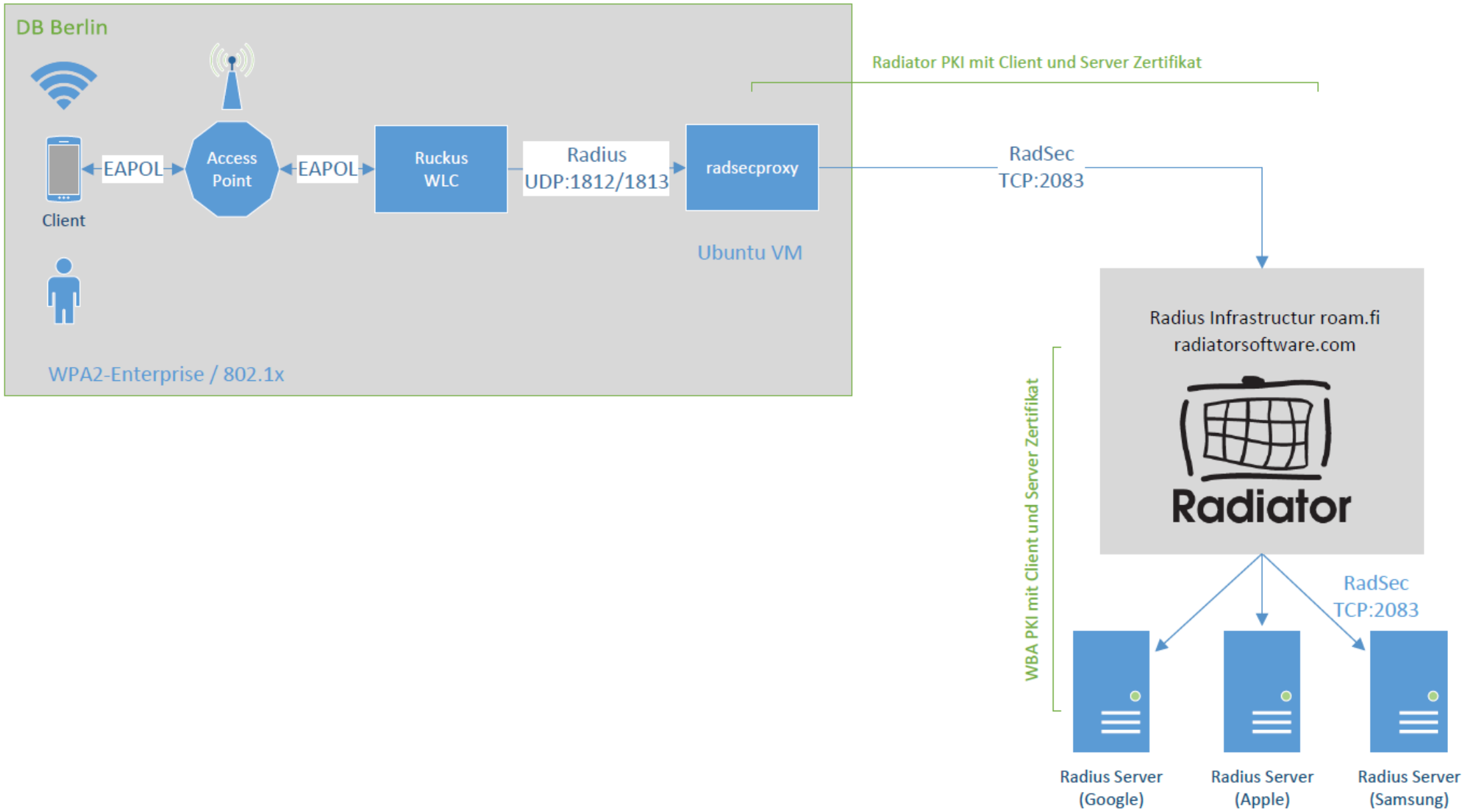

initiator
RadSec Client
RadSec Server
DNS Resolver
Optional NAS initiator
1 EAP Identity-Response
Identity=user@realm.com
Optional RADIUS initiator
2 RADIUS Access-Request
user-name=user@realm.com
realm to IP@ mapping not currently available in RadSec client
3 DIG NAPTR realm.com
4 ANSWER SECTION:
realm.com. 300 IN NAPTR 50 50 "s" "aaa+auth:radius.tls.tcp" "" _radiustls._tcp.realm.com
5 DIG SRV _radiustls._tcp.realm.com
6 ANSWER SECTION:
_radiustls._tcp.realm.com. 300 IN SRV 0 10 2083 radius.realm.com
7 DIG A radius.realm.com
8 ANSWER SECTION:
radius.realm.com. 5 IN A 3.208.239.144
9 Destination IP: 3.208.239.144 TCP SYN
10 TCP SYN ACK
11 TLS ClientHello
12 TLS ServerHello
13 check NAIrealm in Server Certificate
initiator
RadSec Client
RadSec Server
DNS Resolver

OpenRoaming PoC Setup

PoC Plan


Eigene PKI mit Client und Server Zertifikat
WBA PKI mit Client und Server Zertifikat
Client
EAPOL
Access Point
RadSec TCP:2083
radsecproxy-intern
freeradius
radsecproxy-extern
Radius UDP:1812/1813
Radius UDP:11812/11813
Azure VM
WPA2-Enterprise / 802.1x
RadSec TCP:2083
RadSec TCP:2083
RadSec TCP:2083
Radius Server (Google)
Radius Server (Apple)
Radius Server (Samsung)

Letztes Test Setup



Acronyms and abbreviations

Item	Description
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ANP	Access Network Provider
CoA	Change of Authorization
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
HSP	Home Service Provider, a legacy WBA term used to refer to an IDP
I-CA	Intermediate Certificate Authority
IDP	Identity Provider – a term that may be used to refer to an OpenRoaming enabled Home Service Provider, where the provider is not required to deliver any other services except those related to subscriber authentication
LoA	Level of Assurance – a term defined in [13] that describes the degree of confidence in the processes associated with user enrolment and credential management
MCC	Mobile Country Code
MNC	Mobile Network Code
MNO	Mobile Network Operator
NAI	Network Access identifier
NAPTR	Name Authority Pointer
OUI	Organisationally Unique Identifier
QoS	Quality of Service
RadSec	TLS encryption for RADIUS over TCP
RCOI	Roaming Consortium Organisation Identifier
TLS	Transport Layer Security
VNP	Visited Network Provider, a legacy WBA term used to refer to an ANP
WBAID	WBA Identity

Vielen Dank