- OpenRoaming Secure / Seamless / Private
- OpenRoaming: Realized through Innovation and Industry Collaboration
- Mac Randomization
- OpenRoaming – Privacy Built-in
- How To Provision Users
- Provisioning via NFC
- OpenRoaming Provisioning - PC
- IOS Provisioning
- Android Provisioning
OpenRoaming: Seamless, Secure & Private

Zero-touch Wi-Fi onboarding, ensuring a user is always best connected

Secure 802.1x-based authentication, WPA2/3 wireless data encryption

Private by design. Anonymized roaming, personal information is only shared with user consent
OpenRoaming: Realized through Innovation and Industry Collaboration
Changing the wireless onboarding experience

1. Identity Federation architecture & legal framework that can cater to different business models under the same umbrella

2. Federation that dynamically discovers peers & services and allows for secure direct peering

3. Dynamic policy at the edge enables real-time ad-hoc roaming agreements

4. Proxy services connect cloud/web ID to network services

1. Device ecosystem collaboration enable seamless end-user experience

2. Wireless standard to benefit the entire Wi-Fi ecosystem
What about Privacy?

Mac Randomization

NETWORK:
Visibility into visitor onboarding, visitor identity and analytics, across applications that rely on MAC address as a unique identifier will be jeopardized as device manufacturers roll out MAC Randomization.

USER:
The need for privacy. Having a persistent identifier that allows for tracking even if you have not authenticated to the network (no trust relation) violates privacy.
OpenRoaming – Privacy Built-in

1. **Authentication is private**
   Secure and private authentication between user’s device and IDP

2. **User and device are identified in context**
   Identified with persistent Device ID and User ID with IDP context
   IDP shares (anonymized) data in the secured path

3. **IDP shares identities on the user’s behalf**
   IDP manages identity and privacy for the user

4. **Privacy with user consent**
   User controls privacy, identifiers are always persistent
OpenRoaming Demo at the IETF116 reception on Sunday.

Steps:

1. Provision device by installing the users' IDP credentials (e.g., app, profile, etc.).

2. Remove all current SSIDs used so that the device does not have any Wi-Fi access.

3. The device automatically connects to an SSID with OR enabled.

4. When the first SSID is turned off and another OR-enabled SSID is turned on, the device connects to the new one automatically.

The procedure is done securely and seamlessly with Hotspot 2.0 mechanism.

With the app,
- iOS: Download the OpenRoaming Demo App into your phone from Apple App Store. Run it and login with your ID such Apple or Google.
- Android OS: Find the SSID: “OpenRoaming” and click it. Login with your ID such as Google or Samsung. Or, download the App and do same as iOS.

You can visit the OpenRoaming signup page to check the ways more. https://wbaillance.com/openroaming-signup/
Thank You
OpenRoaming Call Flow

OpenRoaming Authentication and Accounting

Device <<device_roams_into_wireless_coverage>> EAP AP/Wireless controller Connector IDP DNS IDP AAA

Device AP/Wireless controller Connector IDP DNS IDP AAA

Access Provider Identity Provider

EAP over RADIUS IDP Discovery (1) TLS tunnel setup (2) EAP Authentication (3)
TLS handshake between Access provider and ID Provider (2)

TLS Tunnel setup between AP and IDP

1. TCP SYN
2. TCP SYN ACK
3. TLS Client Hello
4. TLS Server Hello, Server Certificate, Certificate Request, ServerHelloDone
5. TLS Certificate ClientKeyExchange, CertificateVerify, ChangeCipherSpec, Finished
6. TLS ChangeCipherSpec, Finished
7. IDP AAA verifies Client certificate: certificate chain, validity, revocation, UID vs Operator-ID (optional)
RADSEC EAP Authentication (3): EAP-TTLS

Device

AP/Wireless Controller

Connector

Device scans for wireless coverage

Device selects profile

RADSEC EAP Authentication

Access Provider

EAP Request Identity

EAP-Response Identity (anonymous@cloud.com)

EAP Request TLS exchange

EAP Response TLS exchange

EAP Request TLS inner identity

EAP Response TLS inner identity

EAP Access Accept (unique identifier)

RADSEC access request (User-Name = anonymous@cloud.com)

EAP Request TLS exchange

EAP Response TLS exchange

EAP Request TLS inner identity

EAP Response TLS inner identity

RADSEC Access Accept (unique identifier)

IDP DNS

IDP AAA

Identity Provider

RADSEC Challenge request (request TLS exchange)

RADSEC Challenge response (request TLS exchange)

RADSEC Challenge request (request TLS inner identity)

RADSEC Challenge response (TLS inner identity)

RADSEC Access Accept (unique identifier)

RADSEC Challenge request (request TLS exchange)

RADSEC Challenge response (TLS exchange)

RADSEC Challenge request (request TLS inner identity)

RADSEC Challenge response (TLS inner identity)

RADSEC Access Accept (unique identifier)

RAD SEC access request (User-Name = anonymous@cloud.com)

RAD SEC Challenge request (request TLS exchange)

RAD SEC Challenge response (request TLS exchange)

RAD SEC Challenge request (request TLS inner identity)

RAD SEC Challenge response (TLS inner identity)

RAD SEC Access Accept (unique identifier)
How To Provision Users
Please see here two video demos I have put together.
I started by configuring the NFC tag, once you have done that you can be redirected to whichever site you like. I have used the WBA provisioning portal and the online sign page as examples.
OpenRoaming Provisioning - PC
Download a profile of your choice onto your iPhone that will allow you to seamlessly connect to OpenRoaming.

Access your iPhone settings and you will see ‘Profile Downloaded’.

Install the profile.
Android Provisioning

Android device connecting with a SamsungID

A profile from: wballiance.com/openroaming-signup/
Can also be downloaded to provision your device