www.pipelinepub.com
Volume 20, Issue 8

OpenRoaming: Wi-Fi as Secure and Seamless as Cellular

By: Jonas Lagerquist

The days when public Wi-Fi connectivity was scattered into separate, potentially insecure islands with cumbersome access through portals may soon be over, at least at locations that have joined the Wireless Broadband Alliance's fast-growing OpenRoaming federation. OpenRoaming has over three million Wi-Fi hotspots globally and counting and has the potential to change how we connect to Wi-Fi networks forever.

As Seamless and Secure as Cellular

The OpenRoaming federation is a collaborative effort among vendors, service providers, identity providers, and venue owners to create a seamless and secure Wi-Fi roaming experience globally for users, irrespective of their location or identity provider.

The vision is to make public Wi-Fi as seamless, globally ubiquitous, and secure as when roaming between cellular networks.

There are two different roles in the OpenRoaming federation. An Access Network Provider (ANP) provides the Wi-Fi network, and an Identity Provider (IDP) authenticates and authorizes users to access the OpenRoaming service offered by the ANP. A member, such as a communications service provider (CSP), can act both as an access network provider, making their Wi-Fi footprint accessible, and as an identity provider for its subscribers.

The word 'provider' in the IDP and ANP terms is not limited to the traditional meaning of 'service provider.' An ANP can be any organization with a Wi-Fi network, such as a hotel or a shopping mall. An IDP can be any organization with a registered user base, such as a mobile handset manufacturer, a loyalty program, or a social network.

The beauty of the OpenRoaming federation is that any IDP and ANP can roam with each other without even being aware that the other party exists. In this article, we will dwell on how this magic is possible and why OpenRoaming does not necessarily have to be as 'Open' as the name suggests.

Traditional Hotspots Versus OpenRoaming

We have all used traditional Hotspots many times and will continue to do so until every hotspot is part of the OpenRoaming federation.

So, what are the main differences between a traditional hotspot with a captive portal and an OpenRoaming hotspot? The short answer is that OpenRoaming provides a seamless and secure experience for the users and the Wi-Fi service providers.

In the case of a traditional hotspot, the user must actively look for a hotspot to connect to, select it, and then manually log in to the service. Typically, the user is onboarded to a so-called open Wi-Fi (SSID), meaning the traffic will have weak or non-existent encryption over the radio link. It is also possible for hackers to appear as legitimate Wi-Fi access points (AP) as there is no verification of the AP.

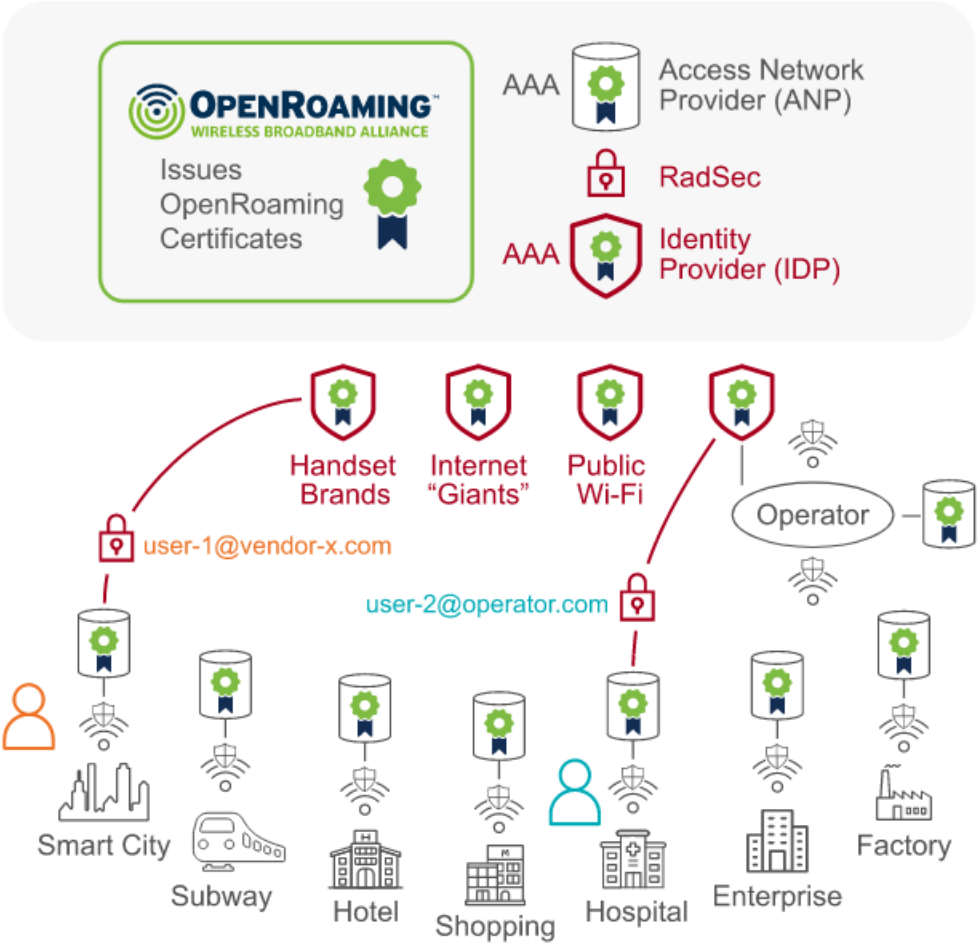

Figure 1.
Source: Enea Whitepaper: All You Need To Know About OpenRoaming Seamless and Secure Wi-Fi Everywhere
https://info.enea.com/openroaming-white-paper

In contrast, OpenRoaming uses the Wi-Fi Alliance Passpoint standard (previously known as Hotspot 2.0) to automatically select the Wi-Fi service and log in to it. The user can only access trusted Wi-Fi access points, and the traffic is encrypted over the radio link, thanks to the secure Extensible Authentication Protocol (EAP) authentication method that is also used to create the encryption keys.

The seamless user experience, with automatic login to the OpenRoaming Wi-Fi network, is achieved through Passpoint's ability to let the device and Wi-Fi access point interact in the background, without any user interaction, to select the Passpoint-enabled Wi-Fi service and agree on what EAP authentication method to use.

It deserves to be said that delivering a seamless and secure public Wi-Fi user experience was also possible before Passpoint and OpenRoaming. Enea has, for instance, helped mobile operators achieve this since 2010 through SIM-based authentication in our Wi-Fi Offloading solution. The difference is that this has been deployed for each operator and their subscribers, while OpenRoaming is a global initiative.

For the first time, an enterprise like a shopping mall, acting as an ANP, can roam with, e.g., several mobile operators acting as IDPs without the requirement for individual technical integrations. This, and the fact that IDPs can choose to roam only with ANPs delivering a certain level of quality of service, makes us believe that OpenRoaming may become the silver bullet for neutral host Wi-Fi Offloading. (See Figure 1 on previous page.)

OpenRoaming is Based on Open Standards

The primary purpose of OpenRoaming is to simplify connecting to Wi-Fi networks while maintaining the highest levels of security and privacy. By establishing a standardized framework for seamless Wi-Fi roaming, OpenRoaming seeks to enhance the user experience, unlock new business opportunities, and drive innovation in wireless connectivity.

As discussed, one of the fundamental principles and the beauty of OpenRoaming is that access network providers, when also acting as identity providers, can roam with each other without being aware that the other party exists. Similarly, identity providers without any Wi-Fi network can authenticate and authorize their users to access Wi-Fi networks in the federation without knowing they exist.

There are five open technology standards enabling the OpenRoaming federation. Below, we will give an overview of these critical standards.

1. Passpoint

OpenRoaming is deployed as a settlement-free service for all (currently the majority) or as a settled service where individual IDPs and ANPs have a financial relation and thus exchange billing and settlement information.

Consequently, OpenRoaming offers two Passpoint Roaming Consortium Organization Identifiers (RCOIs) for accessing the service:

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

The OpenRoaming Passpoint RCOI is a 36-bit value. The first 24 bits are the base RCOI (settled or settlement-free service), and the last 12-bit extension (xx-xx) implements the Closed Access Group (CAG) policies described later. (See Figure 2)

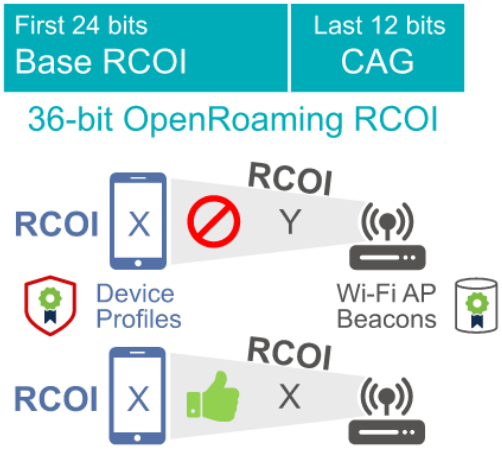

Figure 2.

Source: Enea Whitepaper: All You Need To Know About OpenRoaming Seamless and Secure Wi-Fi Everywhere
https://info.enea.com/openroaming-white-paper

The RCOIs are provisioned in the device's OpenRoaming Passpoint profile(s) and advertised in the Wi-Fi Access Point beacon. Only IDPs and ANPs with fully matching RCOIs will roam, and the user experience will be as secure and seamless as we are used to in cellular roaming.

2. WBA-PKI Certificates

The Wireless Broadband Alliance issues certificates for Access Network Providers (ANP) and Identity Providers (IDP), coupled with their individual WBA Identity (WBAID). The certificate must be installed in the Authentication, Authorization, and Accounting (AAA) servers for both the identity provider and access network provider roles. These WBA-PKI certificates enable trust between members even if they are unaware of each other. The certificates are also a prerequisite for the secure RADIUS (RadSec) communication between the participating AAA servers.

3. RadSec

RADIUS is a networking protocol that authorizes and authenticates users accessing the OpenRoaming federation's Wi-Fi networks. It is also used to send accounting data between the AAA servers of the ANP and IDP. RadSec is a protocol for transportingRADIUS datagrams over TCP and TLS. In OpenRoaming, it is used to maintain integrity and secure communication between the AAA servers.

4. DPD - Dynamic Peer Discovery

Dynamic peer discovery (DPD), specified in RFC 7585, allows ANPs to dynamically discover the AAA servers operated by an IDP through Domain Name System (DNS) lookups. (See Figure 3 on next page)

With OpenRoaming and DPD, the access network no longer needs a particular configuration for each roaming partner. DPD is a game-changer for Wi-Fi roaming and a prerequisite for the OpenRoaming federation.

5. WRIX

The Wireless Roaming Intermediary eXchange (WRIX) Framework has been developed by the WBA Roaming Work Group. Support for WRIX is a prerequisite only for the settled service, and ANPs / IDPs can outsource this function to an ANP/IDP hub provider.

OpenRoaming Needn't be that Open

The word "Open" implies roaming without control. But OpenRoaming does not have to be that open. WBA has incorporated access policies, so-called Closed Access Group policies (CAG), into the OpenRoaming specification. These allow Identity Providers and Access Network Providers to control the characteristics of a roaming partner.

As discussed, the OpenRoaming base RCOI(s) is a 36-bit value. The last 12 bits are encoded to reflect the CAG policies. These policies include whether an Identity Provider will provide the user's identity or whether the user should be anonymous. Another important CAG policy is the level of quality of service (QoS) that an access network provider offers (and an IDP accepts).

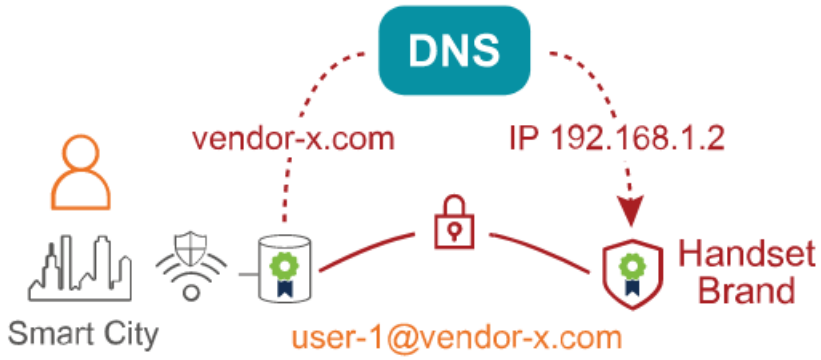

Figure 3.
Source: Enea Whitepaper: All You Need To Know About OpenRoaming Seamless and Secure Wi-Fi Everywhere
https://info.enea.com/openroaming-white-paper

The baseline QoS for an ANP is service availability of over 90 percent and providing each user with 256 Kbit/s sustained speed. This is the minimum requirement for participating in the OpenRoaming federation and, therefore, considered baseline.

All baseline CAG policy bits have zero (0) as the value. If an ANP and IDP do not use the CAG policy extension (last 12 bits), they are perceived to support only the baseline, and all 12 bits are assumed to be zero (00-00).

One of the benefits of encoding policies in the RCOI is that they are applied **before** the authentication. If there is a policy mismatch (RCOI not matching), there is no reason to send an

authentication request, which the ANP authentication server (AAA) will reject immediately. This approach will not overwhelm the AAA with unnecessary authentication attempts.

Another benefit of using the RCOI for policy control is that it is not a new standard dependent on device support. Passpoint has been around since 2012, and nearly all devices active today support this standard if they have installed a Passpoint profile such as the one for OpenRoaming.

The CAG policy RCOI extensions do not have an implicit logic. It is just a matter of matching the exact RCOIs between the IDP and the ANP. As a result, IDPs and ANPs must use multiple RCOIs to cover all cases. ANPs and IDPs must use the RCOI (with its CAG policy extension) to state *what they provide* and RCOIs for *all tiers below*. They must also use RCOIs to state *what they require* and *all tiers above*.

Let's make this more understandable with a few examples.

An ANP offering a settlement-free OpenRoaming service with Silver QoS (Over 95 percent availability, 512 Kbit/s, 5 Mbit/s for video, less than 150 ms latency) must advertise RCOIs that cover both the Silver QoS and the baseline QoS.

An IDP offering to provide the user's identity to the ANP must use RCOIs in the device's OpenRoaming Passpoint profile, covering this case as well as the anonymous user; otherwise, the IDP will only roam with ANPs that insist on getting the user identity.

Given that two additional CAG policies are not covered in this article, and all RCOIs with the CAG policy bit values can be combined in many ways, there is a need to use many, in some cases, tens of RCOIs. But fear not. Provisioning RCOIs is a one-time task for both the IDP and ANP, and it is not that difficult.