WBA OPENROAMING™ INTRODUCTION GUIDE

Source:	Wireless Broadband Alliance
Authors:	APAC Task Group
Issue Date:	September 2024
Version:	1.0.0
Status:	Public

For other publications, visit our website here
To participate in further projects, contact pmo@wballiance.com

About the Wireless Broadband Alliance

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the WBA is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision.

WBA undertakes programs and activities to address business and technical challenges, while exploring opportunities for its member companies. These initiatives encompass standards development, industry guidelines, trials, certification, and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Smart Cities, Testing & Interoperability and Policy & Regulatory Affairs, with Member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

Membership in the WBA includes major operators, service providers, enterprises, hardware and software vendors, and other prominent companies that support the ecosystems from around the world. The WBA Board comprises influential organizations such as Airties, AT&T, Boingo Wireless, Boldyn Networks Broadcom, BT, Charter Communications, Cisco Systems, Comcast, HFCL, Intel, Reliance Jio, Telecom Deutschland and Turk Telekom.

For the complete list of current WBA members, click here.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

www.facebook.com/WirelessBroadbandAlliance

www.linkedin.com/company/2919934/

Undertakings and Limitation of Liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness, and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect, or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third parties.

Table of Contents

1. Introduction 6

2. What is WBA OpenRoaming™ 7

2.1 OpenRoaming Deployments Map – A Crowdsourcing Movement 8

3. Passpoint & OpenRoaming 9

3.1 Onboarding Evolution – A Snapshot 11

4. Addressing Public, Guest and Enterprise Wi-Fi 11

4.1 Common Types of Deployments: 12

4.2 Industries Commonly Utilizing Public Wi-Fi: 13

4.3 How OpenRoaming Addresses Challenges in the Public & Guest Space 13

4.4 How OpenRoaming Addresses Challenges in the Enterprise Space 13

4.5 Enterprise Wi-Fi – Further Deep-Dive 15

5. How to Get Value from OpenRoaming 16

5.1 Roles in the OpenRoaming Federation 16

5.2 Getting Started 17

6. OpenRoaming Technical Diagram Query 20

7. OpenRoaming Components – Onboarding & Credentials 22

7.1 Key OpenRoaming Components Needed 22

7.2 How to Obtain Test Credentials to Start With 22

7.3 Native ID and Example of Onboarding Flow 23

8. Deployment Guide for Wi-Fi OEMs 24

9. APAC OpenRoaming Adoption Challenges 26

9.1 Benefits and Challenges of WISPr 26

9.2 Case Study of Japan - Transforming Public Wi-Fi Access in Tokyo, Japan 28

9.3 Case Study of India – Challenges for OpenRoaming 29

10. Conclusion 29

10.1 WBA OpenRoaming Groups & Resources Available 30

Figures

Figure 1 - OpenRoaming Deployments Map as of July '24 9

Figure 2 - OpenRoaming / Passpoint Parameters 10

Figure 3 - Onboarding Evolution 11

Figure 4 - Onboarding Mechanisms 14

Figure 5 - Roles in the OpenRoaming Federation 17

Figure 6 - OpenRoaming Deployment Diagra 20

Figure 8 - Devices natively supporting OpenRoaming - Examples 23

Figure 9 - Example of Android onboarding 23

Figure 10 – RadSec Client Certificates 25

Figure 11 - Configuration Tags 26

Figure 12 - Components to be Migrated to Passpoint 28

1. Introduction

For over a decade, Passpoint® technology, also known as Hotspot 2.0, has been available to enable automatic and secure association between a device and a Wi-Fi network.

While the process mentioned refers to the industry's best reference when it comes to the quality of experience for the end-user, the fact is that the overall adoption of Passpoint has been slow and often seen as nonexistent. Slow adoption in the past was attributed to cumbersome process of onboarding the Passpoint profile on the user devices, the cost associated with upgrading network to support Passpoint and not so compelling business case.

It is important to understand 'Passpoint' as a combination of two factors: (1) the association mechanism, and (2) the roaming dynamic. End-user device compatibility with Passpoint technology is one of the components for its adoption. Passpoint technology has been developed over the years and most of the end-user devices – smartphones, tablets and laptops – are nowadays compatible with Passpoint. The other component is Wi-Fi network compatibility with Passpoint technology. Greenfield deployments are compatible with Passpoint from the start and legacy deployments are being upgraded to support Passpoint. Passpoint compatibility at both device and network level enables a seamless connection, improving the overall user onboarding experience.

Passpoint technology makes roaming as seamless as what we see in cellular world. It enables capability to have a Wi-Fi enabled end-user device with a Passpoint credential roaming into a third-party network and connecting automatically.

The vision for seamless Wi-Fi roaming experience is to keep the user connected as they move from network to network - whether at home, on cellular networks, in transit, at universities, stadiums, libraries, or on street Wi-Fi—automatically, securely, and seamlessly. While Passpoint appears to be the most promising option for achieving this vision, it also presents the challenge of scaling roaming capabilities.

Scalability has always been the challenge for Passpoint roaming. For example, an access network might be able to establish an agreement with an identity provider, often a mobile operator, as an example, but that same agreement and network configuration need to be replicated to all the different identity providers, leading to a replication and lifecycle management efforts, besides the fact that some Wi-Fi equipment even has limitations on the number of credentials that it allows to be configured.

This is where WBA OpenRoaming™ comes to the rescue - this federated architecture has been developed by WBA members to address the problem of lack of scalability in Passpoint roaming.

Through the creation of a federation that has a common technical and legal framework, OpenRoaming allows a one-to-many relationship, either meaning a network can onboard a multiplicity of identity providers, or vice-versa, an identity provider can allow its users to roam across multiple networks, all through using a single, one-time, configuration.

WBA members believe that OpenRoaming is a much-needed federative service in the industry to ultimately scale up the adoption of automatic Wi-Fi connection, something that is made available now to Wi-Fi, but is also being studied for its expansion within cellular and IoT convergence.

It becomes important that technical concepts are clearly understood and what benefits such federative technological platforms can provide across the industry so that businesses can adopt it faster and address their connectivity needs.

The fact is that basic technical and configuration concepts remain unfamiliar to a wide variety of stakeholders, particularly to equipment OEMs and managed service providers that can benefit immensely with a better understanding of OpenRoaming to support their end-customers.

One common misconception is that Passpoint and OpenRoaming are two different technologies. This is incorrect; OpenRoaming is built over Passpoint and uses the same technology, but the variation lies in the configuration; instead of using specific credentials for each provider, OpenRoaming uses the same credentials for all – hence achieving the mentioned scalability goal.

WBA members therefore believed it would be important to clarify and explain the concepts of OpenRoaming in this whitepaper and develop an introductory guide for the businesses and especially those in the APAC region to this topic. This guide aims to help users learn more on Passpoint and OpenRoaming, understand how the technology works, how OpenRoaming compares with a typical Passpoint roaming scenario and, most importantly, how the different players can benefit from a business perspective.

The members team also attempts to elaborate this introduction guide, with a particular flavor: knowing that the document has been developed by the Asia Pacific (APAC) members of WBA, it would also be important to get a clear picture of what is the context in the region, what are some specific nuances that make this environment unique and how that transform in the overall adoption of OpenRoaming, therefore points that need to be taken into consideration from a product strategy standpoint.

2. What is WBA OpenRoaming™

When done through WBA OpenRoaming™ (hereafter referred to as OpenRoaming or simply OR), Wi-Fi Roaming presents service providers with opportunity to enhance their offerings, improve network performance, generate additional revenue streams, and differentiate themselves in a competitive market. By leveraging OpenRoaming effectively, service providers can strengthen their position in the market and better meet the evolving connectivity needs and quality of experience demands of their customers.

The OpenRoaming federation addresses the following key questions -

1. How can a company such as an Identity Provider (IDP) allow their users to roam across a multiplicity of Wi-Fi networks, automatically, securely, as if they were just roaming in a cellular environment?
2. And, on the opposite side, how can an Access Network Provider (ANP) receive and onboard a multiplicity of different Identity Provider users and have these connected automatically and securely as well?

As previously mentioned, OpenRoaming is built on top of Passpoint technology and creates a standardized federation policy to establish a scalable, one-to-many relationship both from the perspective of those who own the credentials (*Identity Providers*) or those that own the networks (*Access Network Providers*).

When we talk about seamless connectivity, OpenRoaming allows users to automatically 'connect' to Wi-Fi networks without the need for entering passwords and risking being exposed to digital threats in unsecured networks. This means users can move between Wi-Fi hotspots, and all happens automatically and securely.

It is important to understand the 'magic association' (MATCH) process between a device's profile and a network's configuration - the core mechanism that enables automatic and secure Wi-Fi connections through OpenRoaming. This process eliminates the need for users to manually select networks or enter passwords, simplifying the Wi-Fi onboarding experience while maintaining robust security measures.

OpenRoaming is an initiative that builds upon the principles of Passpoint (Hotspot 2.0, a specification based on IEEE 802.11u standard first launched back in February 2011). It simplifies the configuration and authentication process, particularly for users who want to connect to multiple Wi-Fi networks from different providers even in different geographies.

When a user connects to a Wi-Fi network, it requires the user to share its access credentials to the network owner in order to obtain internet access. These access credentials are provided by Identify Providers. Typically, a network owner would need to have a bilateral roaming agreement with an identity provider, such as a carrier, and would later also need to configure this operator codes (PLMN ID) in every hotspot and have someone creating the interconnection means to then onboard the users of that identity provider into its network.

Instead of this traditional one-to-one relationship between an identity provider and a network owner, OpenRoaming simplifies this into a one-to-many relationship because the configuration effort is done one time and for all the federation participations, making it disruptively scalable.

The OpenRoaming federation service consists of 3 layers:

1. Network Automation Component: Enabled by Passpoint technology, this component is necessary to facilitate the automatic and secure match between a given end-user device and a Wi-Fi network. This is done by configuring the Wi-Fi network with roaming consortium codes (RCOI).
2. Cloud Federation Layer: This layer uses Dynamic Peer Discovery (DPD) through DNS to discover a given authentication server (AAA) behind a given credential and to retrieve authorization from this to allow the credential to access the network, besides the compliance with best-in-class practices developed in the WBA Roaming Work Group in terms of legal and network identification. Apart from dynamic discovery, legacy option of defining static routes to discover AAA is also supported.
3. Cybersecurity Layer: This layer benefits from RadSec technology for the interconnection between different servers – the network (client) and the authentication (server) sides, using a Public Key Infrastructure (PKI) policy of Certificates.

2.1 OpenRoaming Deployments Map – A Crowdsourcing Movement

OpenRoaming is being widely deployed across the world. To help users identify where OpenRoaming networks are available, a crowdsourcing tool has been introduced.

Through a partnership between WBA and WiGLE – Wireless Network Mapping, users can download the WiGLE mobile app and detect nearby Wi-Fi networks automatically, registering the SSIDs and RCOIs being broadcasted.

Then, the app allows the user to upload the data to a centralized server, and such networks becomes available online and visible on the map.

It's important to note that the information displayed is non-exhaustive; it serves as an illustration of all the ongoing OpenRoaming deployments taking place.

The rapid expansion of OpenRoaming networks is exciting to witness: - https://wballiance.com/openroamingmaps/ --

Figure 1 - OpenRoaming Deployments Map as of July '24

3. Passpoint & OpenRoaming

OpenRoaming builds upon Passpoint technology and expands it into an open, flexible framework for automatic Wi-Fi connectivity that can be used by various organizations in a one-to-many, scalable relationship. Passpoint, for further clarity, refers to the baseline technology and specification that defines how this automatic and secure association process takes place between a device and a network.

See table-1 below with key differences on what could be considered a 'regular' Passpoint roaming deployment versus what is a state-of-the-art OpenRoaming one.

Parameters	OpenRoaming	Passpoint
Network configuration (operational cost reduction)	Only one code needs to be configured on the Controller (WLC) or Access Point (AP) - the alphanumerical code of the federation – Roaming Consortium Organization Identifier (RCOI). Updates for blacklist of partners is done at AAA or WLC, no need to update the entire infrastructure. Attach & re-attach on the network, faster ANQP "handshake".	Each roaming partner (realms) needs to be configured at the WLC/APs. Each time there a change on the partners realm, it needs to be updated on all infrastructure. Normally carriers have multiple realms, WBA already saw mobile carriers with over 50 realms to be configured.
SSID discovery and authentication	Fast attach & re-attach & authentication on the network, fast ANQP "handshake".	As the number of realms grow the latency to attach & re-attach to the network and authentication increases substantially.
End-to-end roaming	Easily connect to other networks, including airports, hotels, coffee-shops, cities, etc. At the commercial level, joining the federation to partner with all with the possibility of "blacklist" and at technical level interconnection-interoperability is done automatically via RadSec dynamic tunnels.	Each roaming partner needs to have an individual negotiation for roaming agreement contracts and a specific technical implementation of interconnection-interoperability (IPsec VPN tunnels).
Future-proof deployment	If extending deployment to other IDPs, OR enables scalability at a marginal cost, compared with performing another 1 to 1 Passpoint deployment (operational cost saving)	Need to negotiate bilateral roaming agreements with hundreds or thousands of partners.
Policy for QoS & QoE	Policy implementation based on RCOIs, either for QoS or QoE, always having a fast handshake.	Policy can be done at realm level, meaning more realms configuration and latency for handshake will grow.

Figure 2 - OpenRoaming / Passpoint Parameters

3.1 Onboarding Evolution – A Snapshot

To conclude the chapter on how OpenRoaming compares with Passpoint from a roaming and scalability standpoint, it will be helpful to walk through a simple evolutionary diagram on how the onboarding has been evolving over the years, following the technologies made available – first with captive portals, later with Passpoint and more recently with OpenRoaming.

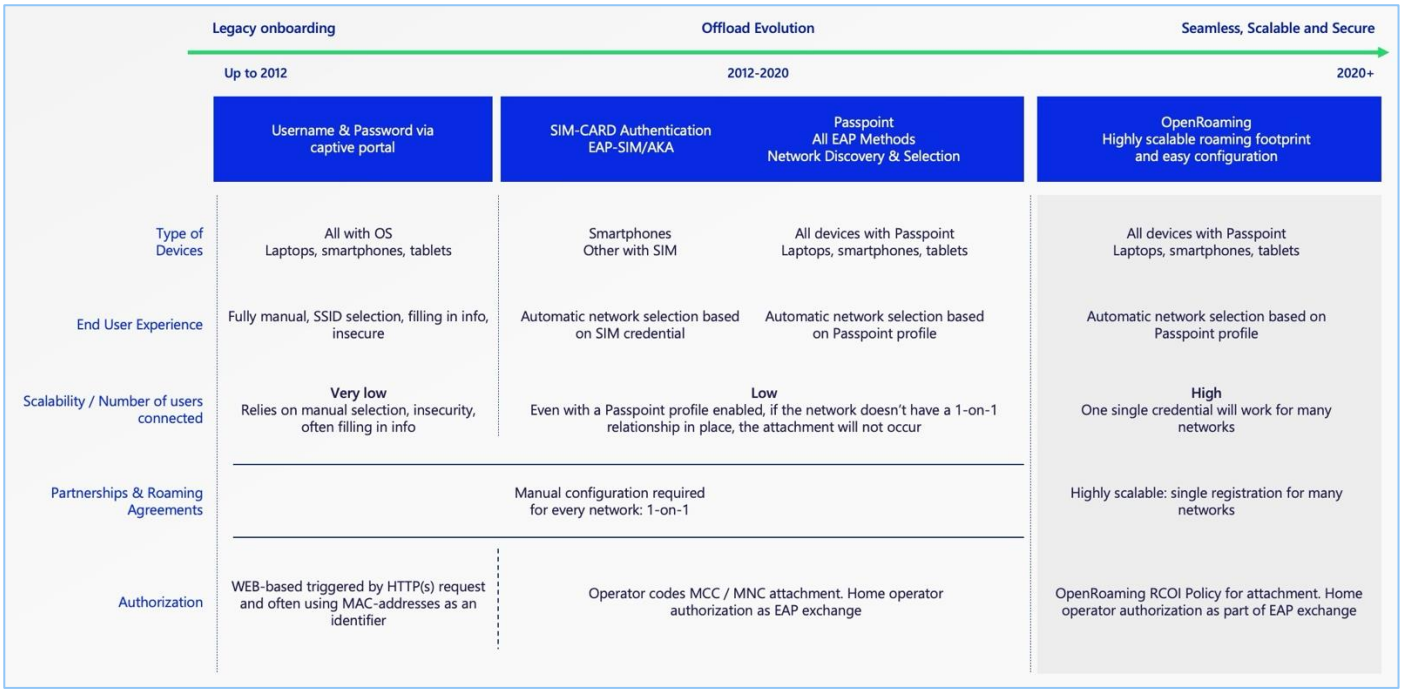


Figure 3 - Onboarding Evolution

4. Addressing Public, Guest and Enterprise Wi-Fi

Public, guest, and enterprise Wi-Fi are globally recognized as three specific verticals that face a series of concerns when it comes to the security of the end-user and ease of onboarding; verticals that can widely benefit from using an automatic attachment that is secure and private for the end-user, while still allowing lawful interception to legal authorities whenever required.

OpenRoaming is designed to streamline and enhance the connectivity experience for public, guest, and enterprise users. The gaps in user experience that OpenRoaming addresses include seamless access, security, privacy, and ease of use. Here's a detailed look at these gaps and how OpenRoaming addresses them:

Seamless access

- OpenRoaming enables users to automatically connect to participating Wi-Fi networks without need to search for SSIDs or any manual login procedures, providing a "connect once, connect everywhere" experience.

- By leveraging identity providers, OpenRoaming allows users to authenticate using their existing credentials (e.g., from their ISP, enterprise, or third party).

Security

- OpenRoaming uses WPA2/3 and other advanced encryption standards to ensure that data transmitted over Wi-Fi is secure.
- It employs robust authentication protocols such as EAP (Extensible Authentication Protocol) to securely verify user identities.
- The use of secure onboarding mechanisms ensures users never need to connect to any untrusted open-security networks and protects against unauthorized access and/or attacks.

Privacy

- OpenRoaming minimizes the amount of personal information required for authentication, enhancing user privacy.
- The use of anonymous credentials where possible reduces the risk of personal data exposure.
- It adheres to global privacy standards and regulations, ensuring that user data is handled responsibly.

Ease of use

- Simplified interfaces and automatic connections reduce the complexity of accessing Wi-Fi.
- OpenRoaming provides a consistent and unified user experience across different networks, enhancing user satisfaction.
- Being compatible with multiple network operators and service providers, OpenRoaming ensures broad usability.

OpenRoaming can effectively address key gaps in the user experience for public, guest, and enterprise Wi-Fi users by providing seamless access, robust security, enhanced privacy, and ease of use. Its federated approach to identity management and commitment to high standards of security and privacy make it a comprehensive solution for modern connectivity challenges.

The following sections explore the specific challenges faced by Wi-Fi in the public, guest and enterprise space, and how OpenRoaming is, as a federated solution, addressing them.

4.1 Common Types of Deployments:

- *Public Wi-Fi* Internet service is a mechanism to facilitate internet connection to end users in any premise/venue where end users can't use cellular service due to coverage or capacity issues or they want to save their cellular data.
- *Guest Wi-Fi*, on the other hand, represents Wi-Fi granted to temporary guests, either in a residential or enterprise space, in a more controlled environment to enable them to get connected to the internet.
- *Enterprise Wi-Fi* is understood as the Wi-Fi connectivity provided to the employees/members of a given company/group, both in terms of internal corporate offices and facilities, but also the capability to roam between each building and even with external third-parties or partners

4.2 Industries Commonly Utilizing Public Wi-Fi:

- Typical Venues: City centres, Airports, Railways Stations, Bus Stations, Public Parks, Amusement Parks, Smart Cities, Malls, Hotels, Resorts, Hospitals, Universities, corner shops etc. are most common venues providing Public & Guest Wi-Fi either as free or a paid service.
- Growing Demand: In recent years, the demand for internet has grown to multiple folds hence this offering has become a crucial service even for Students Accommodations, Military Barracks, and Multifamily Housings. There is also a steep increase in Transportation sector where Public Wi-Fi is provided - e.g., Buses, Trains, Maritime and Aircrafts.

In today's interconnected world, providing internet access to visitors and guests is essential for businesses across various sectors.

Despite the ubiquity of Wi-Fi networks, gaps exist in user experience, security, and interoperability. Cumbersome onboarding procedures, security vulnerabilities, and the lack of interoperability between networks undermine user trust and satisfaction. Users often encounter multiple logins, manual processes, and inconsistent captive portal experiences, hindering seamless connectivity.

Now, imagine experiencing the same seamless Wi-Fi experience you enjoy at home, where you enter your front door and don't think about connecting to your home network - it just works. OpenRoaming offers the same and more, transforming the way users connect to, or roam between Wi-Fi networks, enabling frictionless user experiences and improved security. OpenRoaming addresses key challenges faced by both users and venue operators.

4.3 How OpenRoaming Addresses Challenges in the Public & Guest Space

Looking from a network operator standpoint and the value proposition one gets to offer their end-users:

- OpenRoaming offers fast, secure, and reliable connectivity, enabling users to seamlessly transition between Wi-Fi and 4G/5G networks – Wi-Fi offload.
- Users benefit from an enhanced experience and peace of mind, as personal information remains secure and the risk of joining untrusted networks is mitigated. Additionally, OpenRoaming facilitates personalized experiences through integration with loyalty and payment apps.
- For venues, OpenRoaming streamlines onboarding and security procedures, resulting in improved analytics and a richer data pool for insights extraction. It empowers operators to deliver differentiated experiences, driving customer engagement through personalization and value-added services such as loyalty integration and wayfinding. Furthermore, OpenRoaming complements in-building coverage, enhancing customer experiences, increasing dwell time, and optimizing employee productivity and retailer connectivity.

4.4 How OpenRoaming Addresses Challenges in the Enterprise Space

For enterprises, especially where the users' addition or deletion is very dynamic such as a university, OpenRoaming could be a saviour. Similarly, for medium and large enterprises who may have similar requirements and want to offer a great onboarding experience to only authorized users, without having to bear the costs and hassles of users' management, OpenRoaming could be the potential solution to all the challenges.

- OpenRoaming offers fast, secure, and reliable onboarding, enabling users to seamlessly connect to Wi-Fi as soon as they are in range.
- To ensure only authorized users get connected, an active directory or a user's allow-listing mechanism can be integrated in the AAA at the backend so that only allowed users get connected and any unauthorized users get blocked from connecting to secure enterprise network.
- The enterprise IT team only needs maintain an active directory of authorized users in AAA and all other onboarding hassles, etc. are taken care of by OpenRoaming.

OpenRoaming, therefore, represents a paradigm shift in public, guest, and enterprise Wi-Fi networks, offering seamless connectivity, robust security, and tailored experiences for users while empowering venue operators or enterprise admins with valuable insights and engagement tools. By bridging existing gaps and harnessing innovative technologies, OpenRoaming paves the way for a future where connectivity is truly ubiquitous and effortlessly accessible.

For a more comprehensive understanding, see below the onboarding mechanisms that are often used in the public & guest space, and how they differ:

Method	Description	Advantages	Disadvantages
Pre-Shared Key (PSK)	A password shared with a user to access the Wi-Fi network	Encryption Supported Most used method easily understood	Shared Password, No customer engagement, No session control
Captive Portal	A webpage that the user of the network is required to view and interact with before they can access the network Often requires personal information to bypass	Facilitates a splash page (CNA) promotes brand and provides the user information about the venue. Customer insights can be generated Works with legacy end-user device and Wi-Fi network which are non-Passpoint compliant	May deter some users depending upon information requested or time to connect. Reliability and/or consistent user experience issues impacted by device vendor or default browser. Not Seamless Not Secure
Passpoint & OpenRoaming	A Wi-Fi Profile is provisioned in the end points by respective service provider, which allows seamless connection on the Wi-Fi Network	Secure and Seamless	Though based on 802.1x not all the devices support Passpoint.

Figure 4 - Onboarding Mechanisms

4.5 Enterprise Wi-Fi – Further Deep-Dive

The above section about Enterprise Wi-Fi is a broad level depiction of how OpenRoaming can solve some use cases. However, the Enterprise Wi-Fi requirements could be much more diverse and complex.

We need to understand that there are multiple variables in consideration when an enterprise decides to step ahead in terms of the security and experience provided to their employees, but also to the guests they receive within their facilities.

First, when it comes to the decision of allowing corporate users to automatically connect to the Wi-Fi network, it is important to state that often, for situations as simple as this, the best solution will be a regular deployment of a Passpoint network, i.e., without the need to enhance the deployment to an OpenRoaming one, because the roaming and scalability components are not the demanded ones, we're only looking to allow users from our own company to a specific owned network.

This means that the users' profile with a domain-name that matches our own network will always have precedence over anything else and will be the one selected for the employees to access the network.

So, when does it make sense to talk about OpenRoaming for an enterprise case?

OpenRoaming starts making a lot of sense as soon as we start adding some dimension to the deployment. This means, for instance, receiving external users into our corporate offices, from other Identity Providers, or allowing our users to roam to third-party networks as well. This scalability and roaming capability are something easily guaranteed with OpenRoaming that will have the means to read and install this credential.

Now, when it comes to developing a corporate profile, there are essentially 3 options.

- the company can decide to create their own credentials, and the authentication server, i.e., doing everything themselves, in-house.
- the company can work with a third-party provider – a managed service provider – that will do all the management, will use the corporate's authentication server, and will create credentials for the enterprise to then be distributed across the users. This means that even though there's third-party management, the credentials and the backend systems are still owned by the corporation.
- the company decides to outsource everything, i.e., pay to a third party to create the credentials and manage their own authentication and backend systems, so the company does not need to have and understand any of how it works.

To onboard the employees into a corporate office, they need to have a Passpoint profile installed into their device. This can be done in multiple ways - for instance, if the device is owned by the company, it might come pre-configured with a profile, or we can allow and enforce the need for employees to manually read a QR code and install a Passpoint profile to their phones, laptops, etc. Can also be done through Mobile Device Management (MDM), as a centralized management approach.

But one issue remains that is transversal to all Passpoint deployments: what to do about non-cellular devices such as laptops when they are walking up to the facility and don't yet have a profile? For these cases, an alternative method needs to be secure for connectivity, there's no other way, at least until there's some sort of on-site provisioning solution. To cover for all these cases, planning and using the notion of ahead-of-time provisioning will

be an important one to be transmitted to the employees. Simply installing a corporate application either on phone or laptop can be enough to automatically configure the Passpoint profile with the necessary credentials.

A common question also raised is how to make sure the credentials distributed by the employees are integrated with the Active Directory (AD) or the corporate users' directory, in general. This will depend either on the capability of the network equipment to already have a Passpoint-OpenRoaming product that allows this integration or will need to be developed manually by the managed service provider or an IT team, to make sure that a given profile associated to a user is well integrated and synched with their registry on the corporate database.

Here we're already talking about a 'roaming scenario'. The corporate facilities are supposed to receive external parties automatically and securely. How to do this?

If we configure on the network the OpenRoaming RCOIs, all credentials with matching codes will associate to the network and initiate the authorization and authentication process.

Filtering the inbound traffic, either through allow-listing or deny-listing, those are policies that are then applied specifically on the backend authentication system, following a rationale of 'only A, B and C realms are allowed' or 'no one from realms D, E and F will be allowed'.

Finally, corporations will often want to enable their employees to roam across other owned facilities and even outside, using public or other guest networks that are also 'safe', i.e., they use OpenRoaming for the association and authentication.

For this to happen, including the OpenRoaming RCOIs into the profile configured for the employee will be necessary, because this is the mechanism that will allow the employee to roam to third-party networks.

5. How to Get Value from OpenRoaming

5.1 Roles in the OpenRoaming Federation

OpenRoaming enables devices to establish an automatic and secure connection to Wi-Fi networks. As stated before, it simplifies the onboarding experience on to a Wi-Fi network via established identity provider relations. The goal is clear – to standardize all Wi-Fi onboarding and roaming.

This new ecosystem opens a set of business opportunities related to Wi-Fi offload and roaming. Given the panoply of possibilities, this section addresses the deployment steps to help an organization clarify its role within the ecosystem, and how to get started.

First, let's look at the ecosystem.

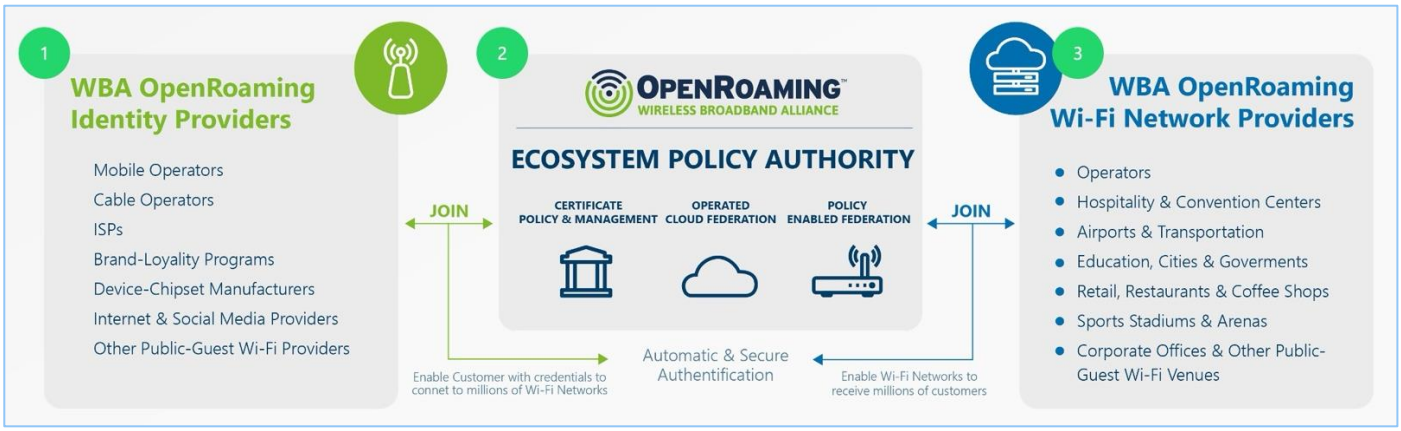


Figure 5 - Roles in the OpenRoaming Federation

There are three possible roles that organizations can play in OpenRoaming:

1. Identity Provider

   Organizations that provide identity profiles (credentials) to their end-users, ranging from operators to software providers or device manufacturers. These are the organizations that will have their clients / subscribers accessing OpenRoaming networks.

2. Ecosystem Broker

   Organizations that focus on clearing and aggregating data, providing interconnection and/or distribute PKI certificates or WBAIDs. Here are all the services an Ecosystem Broker can provide:
   - Interconnection – establishing a dynamic or static routing through a network and an identity provider
   - Data and Financial Clearing / Settlement – making sure traffic exchanges are well accounted and charged, being financially liable for the commercial agreement
   - Distribute PKI Certificates (RA Agent) – Server & Client Certificates - and issue SubIDs (WBAID) 'CLIENT.COMPANYX:US'

3. Access Network Provider

   Organizations that own a network, from an enterprise, sports stadium, or a coffee shop. These are the networks that will receive users with OpenRoaming credentials.

So, the OpenRoaming ecosystem comprises of Identity Providers (IDP), Access Network Providers (ANP) and Ecosystem Brokers. It is important to state that organizations can play multiple roles, even the three of them at the same time.

5.2 Getting Started

STEP 1 – What is the role your organization plays?

Start by expanding on top of your core business. Is your organization an identity provider by default, or does it manage or own Wi-Fi networks, or both? Is your organization in the business of interconnecting and performing data/financial clearing?

These questions vary according to your role:

- If your organization is an ANP: what is the network, location, venue you will select to start deploying OpenRoaming?
- If your organization is an IDP: will you allow all your subscribers to be part of OpenRoaming? Are you segmenting or selecting a first sub-set of users to test the service?

We recommend picking up a starting point, one of the roles to be part of the federation. It does not mean you will not take other roles and expand your reach; it is merely a phased approach.

STEP 2 – What partners do you work with and how will you interconnect?

For simple onboarding onto the federation, we recommend you assess what partners your organization works with, namely in terms of:

- Roaming hubs
- Equipment providers
- IT Integrators

Ecosystem brokers and partners are entities that will be helpful in optimizing your OpenRoaming deployment and business.

OpenRoaming allows for flexible deployment models:

1 - In terms of the interconnection, fundamentally RadSec-based, you might select the following:

- Install and configure RadSec either through:
  - Use a Vendor OEM (Access Point, WLC, Cloud provider) that has an OpenRoaming offering to have this configuration enabled and already done
  - Ecosystem Broker Hub provider (Certificate house, integrator, roaming hub)
  - Software including Open-Source ones – FreeRADIUS, RadSecProxy, Radiator

2 - In terms of partner discovery, typically two options apply:

- DPD – 'Dynamic Peer Discovery' leveraging Domain Name System (DNS)
- Static routing or connection to configure specific IDPs that need to be enabled

STEP3 – Test OpenRoaming end-to-end

See below on section 7 how to obtain test credentials for your end-user devices.
In terms of requiring a PKI Certificate to either issue credentials or configure manually an OpenRoaming network, please contact WBA PMO at pmo@wballiance.com for further assistance and information.
Here's a link you can use to easily request your PKI certificates.
Finally, there are multiple resources available on the WBA collaboration platform – Extranet – that you can use as well to fully comprehend how to setup your identity generation or network.
See key resources below:
OpenRoaming IDP Onboarding Specification
OpenRoaming Technical Framework

6. OpenRoaming Technical Diagram Query

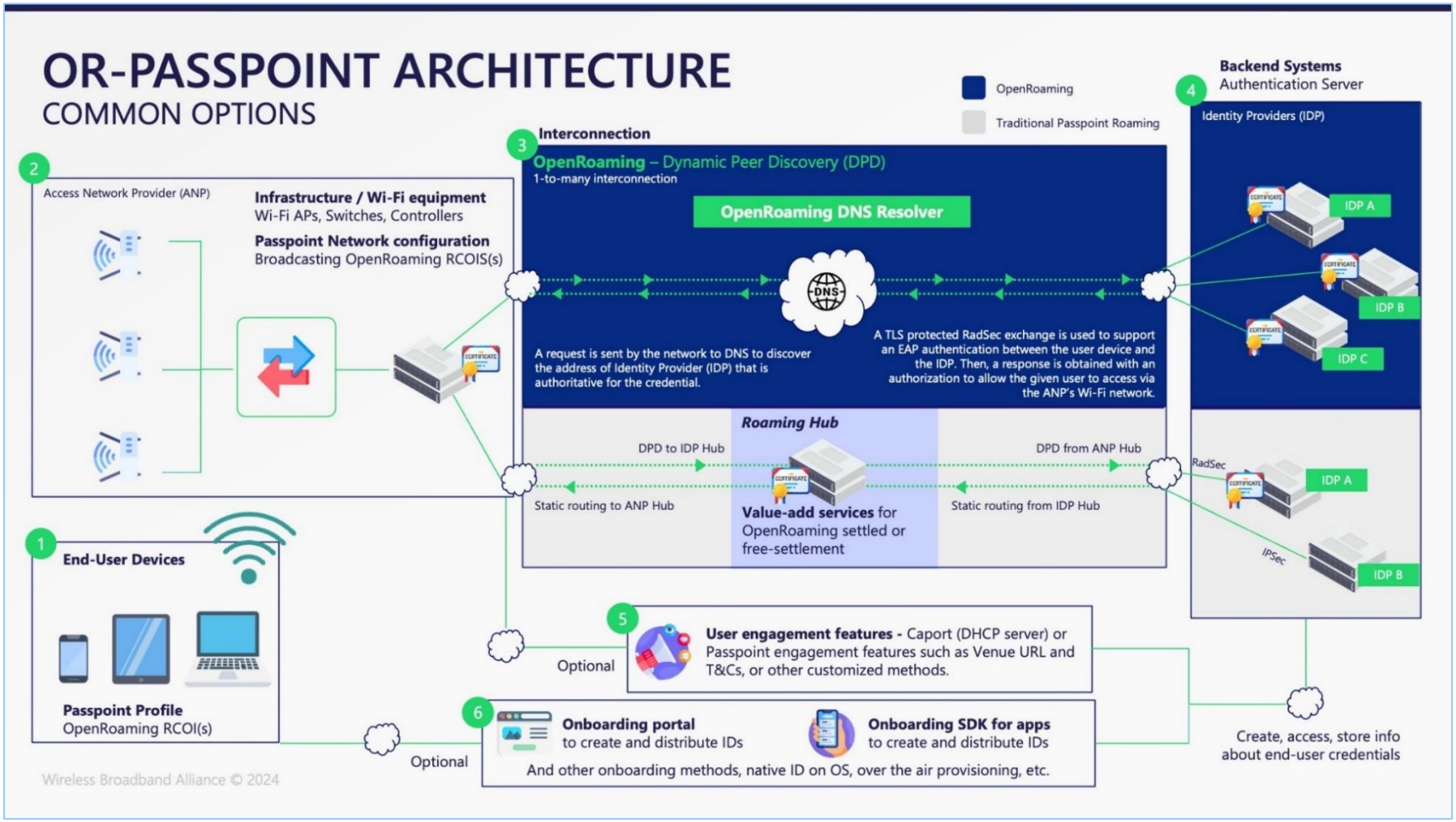


Figure 6 - OpenRoaming Deployment Diagram

PART 1 – End-User Devices

End-user devices, in an OpenRoaming environment, are devices used by the end-user to connect to the OpenRoaming networks seamlessly and securely such as a cell phone, a tablet or a laptop. These devices need to have installed a Passpoint credential with an association 'roaming parameter' – Operator-Name, PLMN ID (MCC/MNC), NAI Realm, Roaming Consortium Organization Identifier (RCOI).

PART 2 – Infrastructure / Wi-Fi Equipment

Wi-Fi equipment corresponds to the infrastructure that a typical Wi-Fi network has in place to broadcast Wi-Fi signal and onboard users to its network.
Going from one-to-many Wi-Fi APs, often including a Wi-Fi controller, the network must configure Passpoint 'roaming parameters' to associate users automatically.

PART 3 - Interconnection

Interconnection corresponds to the protocol method the network provider uses to establish a 'link' to the identity provider backend systems (users' database).

For 1-on-1 relationships, often IPSec tunnels are used or RadSec through TLS PKI certificates.

For OpenRoaming is used Dynamic Peer Discovery (DPD) through RadSec to enable the 1-to-many identity provider automatic cloud resolver.

PART 4 – Backend Systems

Backend systems include all the servers, operating and business support systems that allow an ecosystem broker or operator to facilitate OpenRoaming-Passpoint connectivity back to the end points (AAA servers on each end). These systems, that might also include accounting and billing, are the servers responsible for storing a database with the information of the user and granting him access to a given Passpoint network.

PART 5 – User Engagement Features

User engagement is the ability that a given stakeholder, often the network owner, has to get in touch with the end-user. Particularly important to give visibility to the user on who is providing him this connectivity and good user experience.
User engagement is hereby addressed as (A) Capport API through a DHCP server or through Passpoint features such as (B) Venue URL or (C) T&Cs.

PART 6 – Onboarding / Provisioning Tools

In the context of OpenRoaming-Passpoint there are multiple ways the users can get onboarded - i.e., installing a Passpoint profile / subscription on their device.
From web portals to mobile native Apps to embedded Identity Providers systems from either OS vendors or service providers.

7. OpenRoaming Components – Onboarding & Credentials

7.1 Key OpenRoaming Components Needed

There are key components used to deploy OpenRoaming:

1. RadSec server and client certificates – OpenRoaming uses Public Key Infrastructure (PKI) certificates for RadSec interconnection. How are RadSec certificates used, for simplicity, see the cases below:
   - The server certificates - for IDPs, they need to be installed on the identity management servers If you wish to play the role of IDP, you need to install RadSec certificate on a component attached to your Authentication, Authorization and Accounting (AAA) server or similar
   - The client certificates - for ANPs, need to be installed on a specific local or cloud network component. If you wish to play the role of ANP and you're working with Wi-Fi equipment manufacturers that do not yet have an OpenRoaming product, you'd need to install the PKI certificate on your access network controller and configure RadSec proxy. But there already multiple manufacturers that already have an automated configuration solution for OpenRoaming that will simplify the installation.
2. OpenRoaming Roaming Consortium Organization Identifier (RCOI)

   The OpenRoaming standard defines different RCOIs, that are used for different business models and quality-of-service (QoS) tiers.

   For trial and initial deployment purposes, it is common to start with the following:

   - 5A-03-BA-00-0
     Corresponding baseline QoS tier, no specific identity policy and available to all identity types

Device credentials - End-devices (smartphones, tablets, laptops) needs to be capable of identifying a given network as part of OpenRoaming, therefore the organization needs to ensure the OpenRoaming RCOI – Roaming Consortium Organization Identifier – is included in the Passpoint device credential

7.2 How to Obtain Test Credentials to Start With

Start here - https://wballiance.com/openroaming/profile-signup/

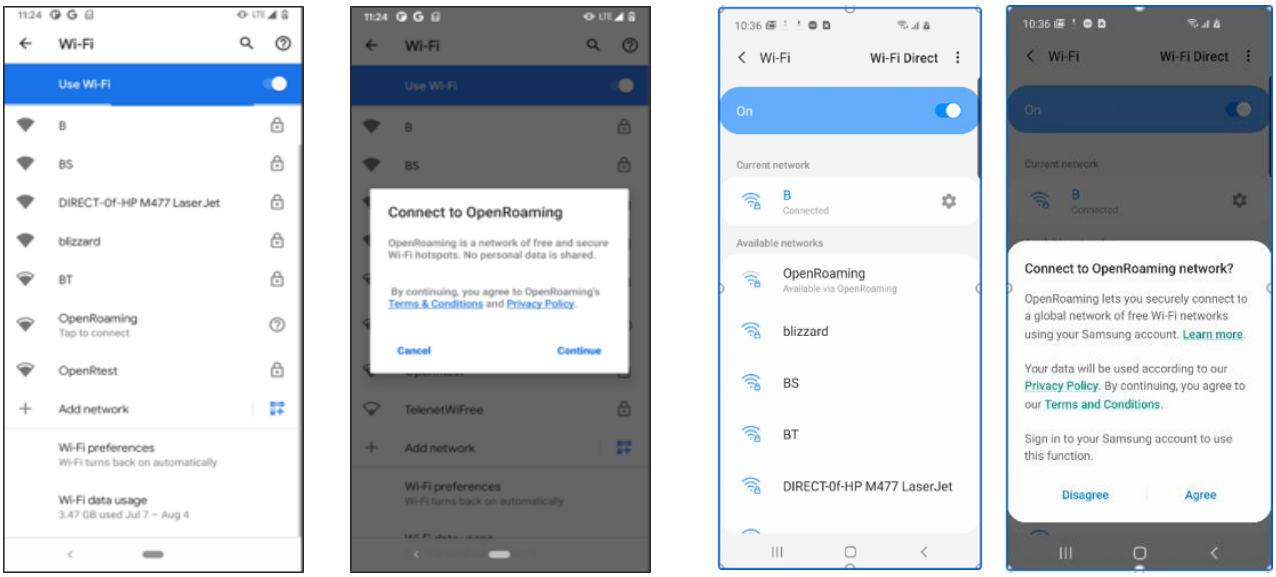
On this page you will find multiple Identity Providers that were kind to provide credentials that you can easily download and use.

Also, if you need further help, get in touch with WBA's Program Management Office (PMO) – pmo@wballiance.com - for setting up the bridge with any ecosystem broker that is willing to help and provide test credentials for an OpenRoaming deployment.

In addition, WBA's PMO also has a set of test credentials and certificates that can be used temporarily and may to provide those to all organizations implementing OpenRoaming.

7.3 Native ID and Example of Onboarding Flow

Devices presently supporting natively OpenRoaming



Native Google Pixel with Google-ID *Native Samsung Galaxy with Samsung-ID*

Figure 7 - Devices natively supporting OpenRoaming - Examples

Out of the box:

- Google Pixel with Android 11
- Samsung Galaxy S9 and above

Example of Android onboarding

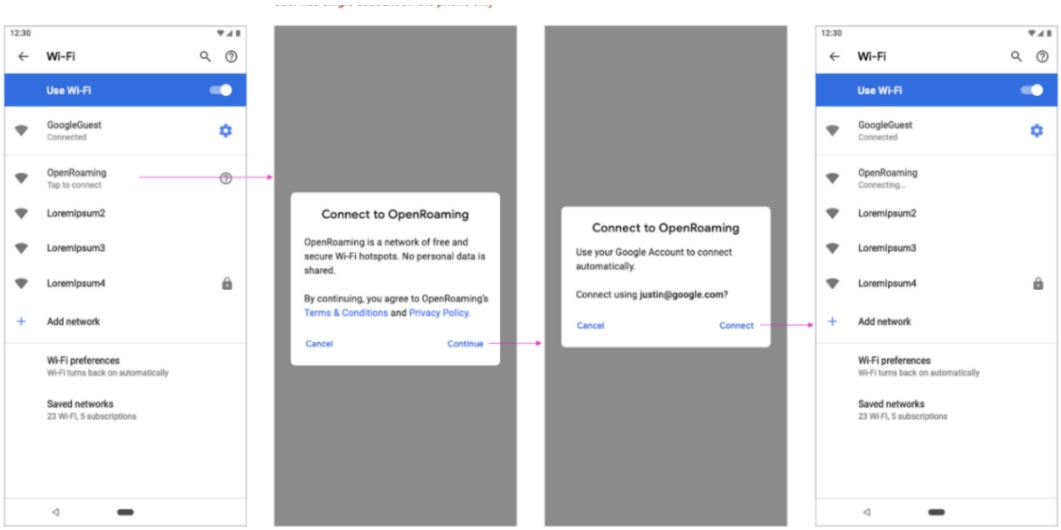


Figure 8 - Example of Android onboarding

8. Deployment Guide for Wi-Fi OEMs

To enable OpenRoaming support on a Wi-Fi access point and allow for simplified installation at the network level, the following general steps are involved:

1. Participation in the OpenRoaming consortium:

   The Wi-Fi access point provider or network operator needs to join the OpenRoaming consortium. This involves collaborating with other organizations and adhering to the OpenRoaming standards.

2. Certificate Authority (CA) Integration:

   OpenRoaming relies on a public key infrastructure (PKI) for secure authentication. The access point must integrate with a Certificate Authority to issue and verify digital certificates for secure authentication.

3. Authentication Server Integration:

   The Wi-Fi access point needs to communicate with an OpenRoaming authentication server. This server is responsible for validating the user's credentials and granting access to the network.

4. RADIUS (Remote Authentication Dial-In User Service) Configuration:

   RADIUS is commonly used for authentication in Wi-Fi networks. The access point may need to be configured to communicate with the RADIUS server, which, in turn, communicates with the OpenRoaming authentication server.

5. User Consent and Privacy Considerations:

   OpenRoaming often involves a one-time registration and consent process for users. The access point should provide a user-friendly interface for users to opt into the OpenRoaming service and agree to terms and conditions.

6. Security Configurations:

   Implementing security measures, WPA 2 as a minimum (preferred WPA3), is crucial for protecting the confidentiality and integrity of data transmitted over the Wi-Fi network.

From an OEM perspective, the Wi-Fi ANPs are the customers. To offer a Wi-Fi solution (Access Points and Controllers) that enables the ANPs deploy an OpenRoaming enabled Wi-Fi network, the following has to be ensured:

1. The Access points MUST support Passpoint
   - Support of HS2.0 (Hotspot 2.0), also known as Passpoint in the offered Wi-Fi solution, is the fundamental requirement to enable OpenRoaming support in the device ecosystem for Wi-Fi ANPs. The idea of Passpoint is that the end-users are identified and authenticated using the credentials that are stored in the network. The clients just need to download a profile that too only once onto the device to sign into the network. The devices then would automatically, seamlessly and securely connect

to an authorized Wi-Fi network anytime they come in vicinity of an OR enabled network with any requirement of client device to discover or manually connect to the Wi-Fi.

2. The controller solution offered by the Wi-Fi OEM MUST provide a functionality for the administrator of the ANP to add Roaming Consortium Organization Identifiers (RCOIs) while creating Passpoint based SSIDs for their network.
   - The Wi-Fi ANP when deploying a network MUST have a way to add the RCOIs as defined by WBA while creating OR SSID on the access points.
   - To ensure a seamless and hassle-free experience for end customers, OpenRoaming has realized a level of policy control using Closed Access Group (CAG) based policies. A Closed Access Group identifies a group of OpenRoaming subscribers who are permitted to access one or more OpenRoaming access networks configured with a particular CAG policy. These Closed Access Group policies are encoded using one or more RCOIs.
   - OpenRoaming defines the use of multiple RCOIs to facilitate the implementation of closed access group policies across the federation. The currently defined RCOIs are:
     i. OpenRoaming-Settled: BA-A2-D0-xx-xx
     ii. OpenRoaming-Settlement-Free: 5A-03-BA -xx-xx

     and where xx-xx refers to the 12-bit extension described by WBA.

   - The OEMs solution to the ANPs (that advertise the OpenRoaming-Settled RCOI) MUST support WRIX-D/F functionality (or an equivalent), either themselves or outsourced to a WRIX hub provider.
3. The controller solution offered by the Wi-Fi OEM MUST provide a functionality to upload the Wi-Fi WBA WRIX end-entity certificates on Radsec Proxy Server.

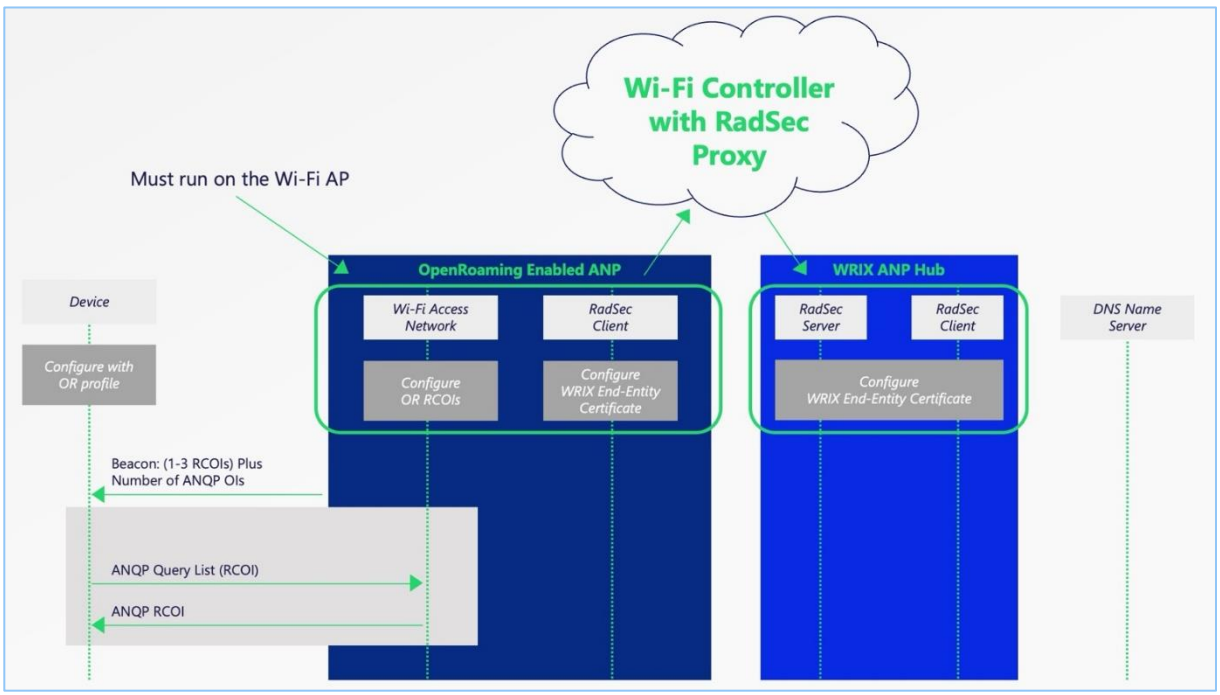


Figure 9 – RadSec Client Certificates

- The APs should radiate the RCOI in the beacons once configured by the controller in the respective SSIDs. Clients read the RCOI in beacons of HS2.0 supported SSID and connect seamlessly and automatically once they have the identity certificates installed.

9. APAC OpenRoaming Adoption Challenges

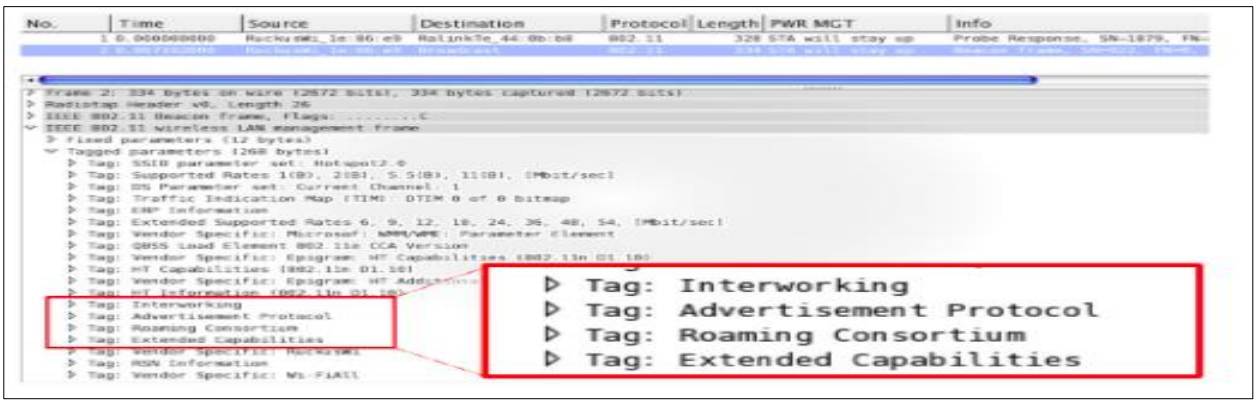


Figure 10 - Configuration Tags

There are various roaming architectures being deployed in Asia for establishing a Wi-Fi roaming bilateral relationship.

Historically, most Wi-Fi Roaming architectures have followed a WISPr-based approach - WISPr (Wireless Internet Service Provider Roaming).

There is an advantage to using WISPr to provide roaming as it is based on RADIUS Proxy and can be deployed on legacy Wi-Fi client devices and Wi-Fi networks that aren't compliant with Passpoint technology. However, most of the Wi-Fi client devices (Android/iOS-based smartphones, tablets, Windows laptops etc.) are Passpoint enabled today, as mentioned previously.

Passpoint adoption, on the end-user device side, is a most prevalent reality in urban areas and steadily growing in the rural ones. People are upgrading their phones, which may be attributed to reduced client devices' prices and improved affordability.

But the same cannot be said about Wi-Fi access network equipment. The upgrade of the existing legacy Wi-Fi network equipment is still very cost intensive, and really requires a strong business case to make such investment.

On a side note, it is positive to see that new deployments, particularly in India, are taking place already recurring to new Wi-Fi 6 standard, and therefore such access points are already, most of them, compatible with Passpoint - which makes it a more reasonable effort, with lower marginal cost, in terms of overall investment.

9.1 Benefits and Challenges of WISPr

Let's start by understanding WISPr and its relevance in the region.

In WISPr, Wi-Fi user authentication is based on RADIUS message (RFC 2865, RFC 2866) exchange with centralized AAA server. The authentication type used are either PAP/CHAP (i.e., Username/Password based) or EAP-TTLS/PEAP with MSCHAPv2 (i.e., certificate for server-side authentication and Username/Password for client-side authentication). Captive Portal based access is possible when PAP/CHAP based authentication is implemented with the help of Network Access System (NAS) situated either at the access point or on a central node such as the controller.

There are pros and cons of such approach as discussed below.

Pros

- Roaming can be enabled on legacy Wi-Fi client devices and legacy Wi-Fi network
- Minimum changes in the existing Wi-Fi network to enable roaming with the help of Radius proxy

Cons -

- All challenges associated with Captive Portal based access –
  a. User has to manually enter the credentials on captive portal
  b. Captive portal detection on the client device is not consistent due to lack of standardised implementation (at client device side and/or network side)
  c. Security issues while exchanging the credentials
  d. Extra implementation of HTTPs proxy in the network to display captive portal of home network to avoid entering User credentials on captive portal of roaming partner.
- Logistics challenges with life cycle management of user credentials and server certificates and its distribution. User has to manually install the certificate on the client device in case of EAP.
- Interoperability challenges with non-Wi-Fi networks such as Cellular, IoT etc.

Apart from standard based WISPr, there are multiple region wide initiatives with differentiated implementation of WISPr as well, for example PMWANI in India.

OpenRoaming (OR) has enabled a federated ecosystem by separating out the functions of Identify Provider (IdP) and of Access Network Providers (ANP) and allowing a Wi-Fi user with identify acquired from any IdP to be able to access the internet on any ANP as long as there is roaming agreement among these IdPs and ANPs. The OR architecture takes care of all the hurdles identified with WISPr type roaming implementation but at the cost of requirement of pass point enabled ANP network.

So, the major hurdle of adoption of OR in APAC region comes from existing legacy Wi-Fi networks in large number which are not Passpoint compliant.

And as we discussed above, the speed of migration from legacy to pass point enabled network is always determined by the ROI (Return of Investment) through new business cases.

Migrating legacy network involves time and cost. Below section discussed about the network node which require migration as well as stakeholder who owns these nodes and require to fund the migration.

Migration and Stakeholders

S.No.	Network Component	How to migrate from Legacy to Passpoint Network	Stakeholders
1	Wi-Fi Clients	Firmware upgrade (possible on limited clients where such updates available) Latest client device	OEM of Client devices
2	Access Point	Firmware upgrade (limited OEM's AP) New access point with Passpoint support Open WI-FI compliant (with default Passpoint support)	ODM/OEM of AP
3	Controller	New controller with Passpoint support Open Wi-Fi controller (with default Passpoint configuration support)	OEM of AP/3rd party controller provider
4	AAA	Upgrade to latest version (FreeRADIUS) with RadSec support	Service Provider
5	User Access Profile from IdP	Install OSU (Online Sign-up Unit) – Deprecated Web Portal/Android or iOS App)	Service Provider
6	Dynamic Discovery of IdP	Enhancement of certificate and update on DNS	Service Provider
7	Captive Portal	Not required Required for user engagement	Service Provider

Figure 11 - Components to be Migrated to Passpoint

Note – The cost aspect is out of the preview of this document and can be derived separately.

9.2 Case Study of Japan - Transforming Public Wi-Fi Access in Tokyo, Japan

The Tokyo Metropolitan Government (TMG) has successfully implemented OpenRoaming to enhance secure and seamless Wi-Fi connectivity across Tokyo. Launched in March 2023, this initiative is part of TMG's broader Tokyo highway data strategy, aimed at connecting residents and visitors through reliable mobile broadband.

In collaboration with KDDI and its subsidiary Wi2 (a member of Cityroam), the project has deployed over 100,000 Wi-Fi hotspots, including key locations like the Nishi-Shinjuku Smart Pole and the Tokyo Marathon 2023 starting point. OpenRoaming is compatible with various platforms, including Android, Mac, Windows, and iPhone/iPad, offering users a streamlined connection experience through the TOKYO FREE Wi-Fi service and Cityroam partners' access points.

The service supports multiple languages and is integrated with major identity providers, making it accessible to a broad audience. With features like real-time location-based information delivery and compatibility with 5G and satellite networks, TMG plans to expand the network to 600 new locations by March 2024.

The successful trial operation of OpenRoaming during the Tokyo Marathon 2023 yielded valuable insights and outcomes, highlighting Wi2 and Cityroam's dedication to expanding OpenRoaming's utilization in large-scale global events. Currently, negotiations are underway with several cities to extend the coverage of OpenRoaming, reinforcing its potential impact on a wider scale.

This initiative has been promoted through extensive online and offline marketing efforts, with TMG continuing to encourage other municipalities and private companies to adopt OpenRoaming, positioning Tokyo as a leader in secure, public Wi-Fi.

9.3 Case Study of India – Challenges for OpenRoaming

Government of India has approved a nation-wide Public Wi-Fi Program called Prime Minister's Wi-Fi Access Network Interface (PM-WANI) which has introduced new players in the public Wi-Fi ecosystem namely Public Data Office (PDO), Public Data Office Aggregator (PDOA) and Application Providers.

PMWANI is federated network by design and has separated out the Wi-Fi user authentication and authorization functions in the network. This is synonymous to IdP and ANP of OpenRoaming respectively. It has also further disaggregated/separated Access Network into PDO and PDOA. PDOs are last mile Wi-Fi coverage provided by installing Wi-Fi access points and connecting them to internet backhaul. PDOAs performs aggregation function for multiple PDOs and provide Wi-Fi core services.

The major Wi-Fi network in India is deployed by MNOs at public places and neutral ISPs on railway stations and other public places. Majority of these networks are deployed as legacy Wi-Fi network and so far, Passpoint support is not enabled by any of MNO or ISP.

PMWANI architecture is based on legacy Wi-Fi network which allows all the existing Wi-Fi players to migrate their network to PMWANI with ease. This become a hurdle when migration is required to OR.

So, it is important to work towards evolving the roaming architecture where legacy networks and regional architectures can co-exist and integrate with global initiatives such as OpenRoaming.

10. Conclusion

This paper aims to provide a comprehensive guide on OpenRoaming focusing on the business needs of enterprises who are looking to implement roaming functionality in their networks. It covers the technical aspect of roaming, how roaming is supported by Passpoint technology, what are the challenges of creating a large-scale roaming network, how OpenRoaming layers are built over Passpoint technology addressing the scalability issues through a federated architecture approach. Additionally, it explores opportunities OpenRoaming offers, how stakeholders can configure their networks, deploy and use OR to improve their business needs and serve their clients efficiently.

This instruction guide also discusses the hurdles in deploying OpenRoaming where legacy Wi-Fi networks without Passpoint support are prevalent and regional public Wi-Fi initiatives in APAC region especially in India.

Future work will explore possible mitigation to integrate the legacy Wi-Fi networks with OpenRoaming and recommend technical architecture along with other aspects of OpenRoaming to accelerate the adoption in the APAC region.

10.1 WBA OpenRoaming Groups & Resources Available

Throughout this document, the team has described all the business opportunities associated with the adoption of OpenRoaming for Public, Guest and Enterprise Wi-Fi, alongside with a comprehensive technical analysis on what makes OpenRoaming unique – how to get started, what role your organization can play and even a guide on how to develop your OR product if you're an equipment vendor.

The group would like to emphasize the importance of the underlying technologies such as Passpoint, RadSec and Public Key Infrastructure (PKI) and the concept of Dynamic Peer Discovery (DPD) that truly enables the scalable dimension of the federation.

On the following page, you will find a full list of standing documents that have been developed by the OpenRoaming and WBA Roaming Work Groups in the WBA over past years. WBA Members are able to access all those materials through the referenced links; but importantly, you will find substantial information going from the technical standard and legal framework to contract templates, onboarding guides for IDPs and ANPs, documentation on WBA's PKI certificates policy, amongst others.

Finally, below is a list of the various Work Groups within the WBA related to OpenRoaming and the ongoing work they are conducting as of the time of this report. Access to details is exclusive to WBA members:

Activities	Status & Next Steps
WBA OpenRoaming Technical Standards	OpenRoaming has seen its Release 3 to be launched in 2022, including an updated legal framework already with settled services agreements and a whole set of new APIs available for the members. The work group is now dwelling into custom-QoS parameters and integration with Private 5G networks, in a work that should summarize the Release 4. There's upcoming work regarding integration with IoT to be started once release 4 is out.
WBA OpenRoaming Implementers	These are monthly meetings where WBA members share openly the progress, they are doing in terms of their OpenRoaming deployments, sessions that are scheduled for informal information exchange, in which an update in terms of the technical standards group is also provided to the team.
Roaming Work Group	The Roaming WG (RWG) has developed the roaming standard called Wireless Roaming Intermediary eXchange (WRIX) in which OpenRoaming is also based. The RWG develops and maintains the WRIX framework updated with the industry state-of-the-art, and is a go to group for all things related with roaming, accounting, billing, location & security.

WBA OpenRoaming for IoT & FIDO Device Onboard (FDO)	The industry sees a rise in automatic onboarding, notably in IoT and headless devices, with FIDO Device Onboard (FDO) by the FIDO Alliance leading the way. FDO allows seamless self-installation and connection without human intervention. Define system architecture, interfaces, flows, and other key elements to guide the solution through implementation, testing, and industry deployments. Execute testing and deployment opportunities to validate and roll out the integrated solution effectively.
Mission Critical & Emergency Services	Highlight Wi-Fi's potential for mission-critical and emergency services, assess regional and nationwide Wi-Fi initiatives for critical services, detail the latest 802.11be functionalities. Define new requirements for mission-critical and emergency services support over Wi-Fi, create a strategic plan for WBA's technical and legal frameworks.
Federated Onboarding Service (FOS) for OpenRoaming	The FOS project is looking to solve a major problem in the industry related with Passpoint subscription provisioning into users' devices. The team has finished work on a Market Requirements Document and is now looking to develop an open-source technical solution to allow provisioning within the OpenRoaming federated ecosystem. The work will carry on within 2023 focused on a proof of concept for the given technology.
Testing & Interoperability Work Group	The T&I WG is a flagship group in terms of Passpoint technology advancement, testing and trialling new user features. The group typically raises new requirements for broad Passpoint & OpenRoaming adoption and actively liaises those requirements and case studies with peer organizations for fostering standardization.
Access Network Metrics	After Phase 1 completion around the Key Indicators Framework to detect performance and healthiness of an access network, the team is now establishing the way to stream the data to different stakeholders, working on a WRIX API and encoding mechanisms.

IF YOU'RE INTERESTED IN PARTICIPATING OR WANT TO LEARN MORE ABOUT ANY OF THESE TECHNICAL ACTIVITIES, REACH OUT TO THE WBA PMO OFFICE AND GET INVOLVED.

[CLICK HERE TO ENGAGE!]

Repository of WBA Resources

Document Name	Requires WBA Membership
OpenRoaming Federation Technical Standard	LINK - InfoCentre
OpenRoaming IDP Onboarding Specification	LINK - InfoCentre
OpenRoaming SubID API	LINK
OpenRoaming Agent API	LINK
OpenRoaming Config API	LINK
OpenRoaming I-CA API	LINK
OpenRoaming Legal Framework	LINK - InfoCentre
OR End-User Privacy Policy Template	
OR End-User Terms & Conditions Template	
OR WBA to Broker Agreement Template OR Broker to Broker Agreement Template OR Broker to ANP Agreement Template OR Broker to IDP Agreement Template	
OR ANP Agreement Template	LINK
OR IDP Agreement Template	LINK
WRIX PKI Certificate Policy	LINK
WBA Certificate Validation and TLS profiles	LINK - InfoCentre
PKI RadSec Operator Deployment Guidelines	LINK - InfoCentre
PKI RadSec End-Entity Deployment Guidelines	LINK - InfoCentre
PKI Registration Authority (RA) Agreement	LINK
Issuing Intermediate Certificate Authority (Issuing I-CA) Provider Agreement	LINK
Root CA Provision Agreement	LINK
Policy Intermediate CA Provider Agreement	LINK
OR TED	LINK
OR CBED	LINK
OR-config-FreeRADIUS	LINK - InfoCentre
OR-config-radsecproxy	LINK - InfoCentre

Acronyms and Abbreviations

Item By order of appearance	Description
HS2.0	Hotspot 2.0 – also known as 'Passpoint'
WBA	Wireless Broadband Alliance
OR	WBA OpenRoaming™
IDP	Identity Provider
ANP	Access Network Provider
RCOI	Roaming Consortium Organization Identifier
AAA	Authentication, Authorization and Accounting
DPD	Dynamic Peer Discovery
PKI	Public Key Infrastructure
DNS	Domain Name Server
PLMN ID	Public Land Mobile Network
QoS	Quality of Service
QoE	Quality of Experience
WLC	Wireless Lan Controller
AP	Access Point
ANQP	Access Network Query Protocol
VPN	Virtual Private Network
FQDN	Fully Qualified Domain Name
WPA	Wireless Protected Access
EAP	Extensible Authentication Protocol
ISP	Internet Service Provider
CAN	Captive Network Assistant

PSK	Pre-Shared Key
MDM	Mobile Device Management
WBAID	WBA Unique Organization Identifier
OEM	Original Equipment Manufacturer
NAI Realm	Network Access Identifier Realm
TLS	Transport Layer Security
URL	Uniform Resource Locator
CA	Certificate Authority
RADIUS	Remote Authentication Dial-In User Service
CAG	Closed Access Group
WRIX	Wireless Roaming Intermediary eXchange
FIDO	Fast Identity Onboarding
FDO	FIDO Device Onboarding

Links

By order of appearance:

- OpenRoaming Crowdsourced Map as of July 2024: https://wballiance.com/openroamingmaps/
- OpenRoaming certified partners as of July 2024: https://wballiance.com/openroaming/certified-partners/
- PKI Certificates request & submission link: https://wballiance.com/openroaming/pki-submission/
- OpenRoaming IDP Onboarding Spec: https://extranet.wballiance.com/higherlogic/ws/groups/5d84bfbc-bbd6-437f-89ff-7034b52b226c/documents
- OpenRoaming Technical Framework: https://extranet.wballiance.com/higherlogic/ws/groups/5d84bfbc-bbd6-437f-89ff-7034b52b226c/download/20686/latest
- WBA Tested Set of Credential Providers: https://wballiance.com/openroaming/profile-signup/
- OpenRoaming Case Study of Japan: Driving Connectivity in Smart Cities

Participants

Name	Company	Role
Bhuvnesh Sachdeva	HFCL	Project Leader
Cade Herringe	Telstra	Project Co-Leader
Hideaki Goto	Cityroam	Project Co-Leader
Sandeep Agrawal	C-DOT India	Chief Editor
Mark Grayson	Cisco	Editorial Team
Prakash Bharti	Boingo Wireless	Editorial Team
Bruno Tomás	WBA	Editorial Team
Jonah Ross	WBA	Editorial Team
Pedro Mouta	WBA	Editorial Team
Varun Kanchan	Alethea	Project Participant
Ang Kwang Tat	AntLabs	Project Participant
Anand Sarasambi	Atria	Project Participant
Bradd Yu	Browan	Project Participant
Jun Yamaguchi	Eduroam	Project Participant
Raymond Lim	Extreme Networks	Project Participant
Christy Chan	HKT	Project Participant
Rishikesh Ghare	Indio Networks	Project Participant
Atul Amdekar	JIO	Project Participant
Hanjin Joh	KT Corporation	Project Participant
Sai Dhiraj Amuru	Plume	Project Participant
Vipin Mishra	Shyam Spectra	Project Participant

Vineet Nayyar	Shyam Spectra	Project Participant
Anthony Agustin	Smart Communications	Project Participant
Jerome Almirante	Smart Communications	Project Participant
Mitsuhito Sasaki	Softbank Corp	Project Participant
Toma Gotani	Softbank Corp	Project Participant
Nayan Banka	TATA Communications	Project Participant
Vaibhav Koli	TATA Communications	Project Participant
Lawrence Maddison	TATA Communications	Project Participant
Jamsheed Sukhadwala	TATA Communications	Project Participant
Alex Uliana	Telstra	Project Participant
Chris White	Telstra	Project Participant
Naoto Komatsu	Wire & Wireless	Project Participant
Subramani Rajendiran	Zebra Technologies	Project Participant