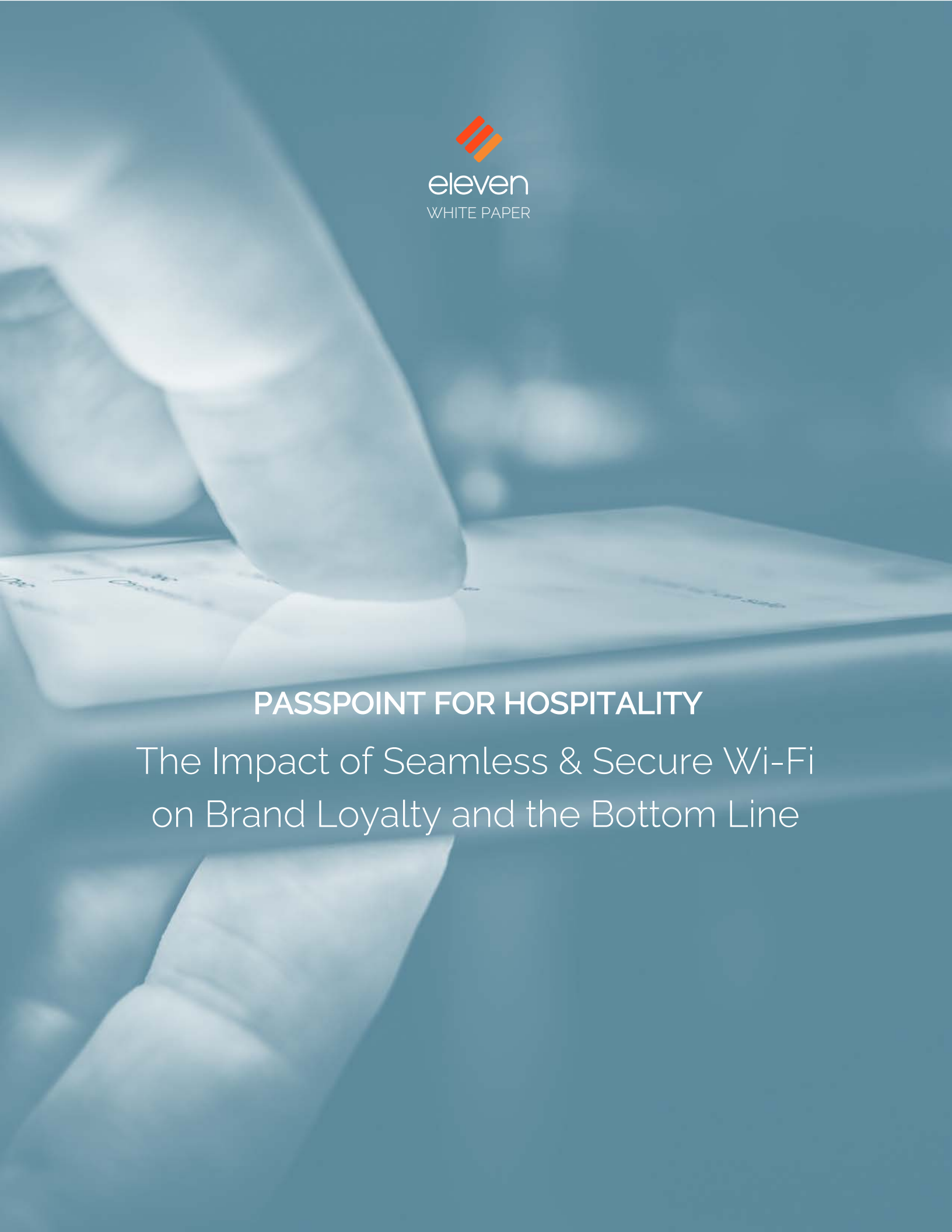


eleven
WHITE PAPER

# PASSPOINT FOR HOSPITALITY

## The Impact of Seamless & Secure Wi-Fi on Brand Loyalty and the Bottom Line

## Executive Summary

*For hotel brands wondering if Passpoint is a viable technology for their Wi-Fi strategy or just another fad—this white paper is for you*

As the Wi-Fi industry continues to evolve and grow at a rapid pace, it is more important than ever for hotel brands to think about Wi-Fi connectivity with a strategic focus on user experience and security. Even though it is critical to building customer loyalty, Wi-Fi is too often considered just an IT function and not given adequate attention from a guest or business perspective. In this white paper, we will explain how Passpoint technology enables simple, seamless, and secure connectivity and the impact it has on brand loyalty and the bottom line, while equipping hotels with the right network infra-structure for the future.

## Problem Statement

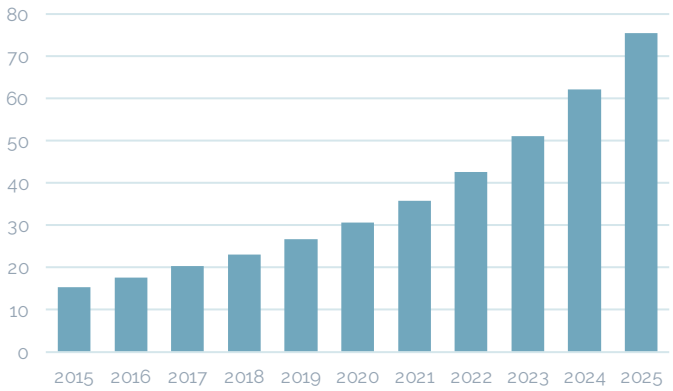
*Complex hotel networks across multiple properties with various providers pose many hurdles to delivering the homelike Wi-Fi experience guests crave*

The guest Wi-Fi experience, while improving, still falls short of consumer expectations. People want Wi-Fi that just works like it does at home; where devices connect automatically and bandwidth is plentiful. This expectation is particularly important to loyalty members who regularly frequent a particular brand or property. However, a property's network infrastructure is inherently nothing like a home network; it is much more complex and when you extend it across an entire brand, the challenge becomes even greater.

Disparate network infrastructures, changes in user devices, rising bandwidth demands and the proliferation of service providers are challenges for any Wi-Fi program. Executing a Wi-Fi strategy that is financially viable and consistent with a brand's vision for excellent guest experience is not an easy task.

## Background

The number of connected devices continues to grow as wireless technology evolves. Both businesses and individuals are searching for secure and reliable Wi-Fi access, yet traditional access methods fall short.




*Connected devices, in billions, worldwide from 2015 to 2025*[1]

Open networks pose numerous security issues and captive portal authentication does not deliver the seamless experience people crave—there is friction with every connection. Authenticating users by memorizing their device's Media Access Control (MAC) address is a step in the right direction, but this approach has its drawbacks as well.

MAC addresses were originally designed to be persistent and globally unique—a way to distinctively identify a device. However, in recent years, MAC address randomization has been gaining traction as a privacy technique that uses random hardware addresses with each connection. This tactic is meant to prevent devices from being tracked or singled out from other nearby devices. While this technique has not been widely adopted yet, there are reports that more and more manufacturers are looking to utilize MAC address randomization to enhance security[2]. Without persistent device addresses, MAC re-authentication could likely become obsolete.

Executing enterprise-grade Wi-Fi authentication of any kind poses many hurdles, especially in hospitality. Most guest networks are managed at the individual property level with local IT managers or service providers selecting hardware and software solutions without a brand strategy in place. Single property networks are created independent from one another without much consistency.

For guests, decentralized Wi-Fi management results in an unpredictable Wi-Fi experience; network names (SSIDs) are not uniform, captive portal branding is inconsistent, login processes vary, and Wi-Fi performance may fluctuate widely. This creates a significant challenge for brands to stitch together various hardware and software platforms and align assorted service providers to deliver a consistent Wi-Fi experience across the brand footprint.

## The Solution

Historically, Wi-Fi has been built with a property-centric view in which each hotel is a separate network with many guests passing through. Instead, we propose that Wi-Fi strategy should be centered on the guest experience across the entire brand's footprint. Passpoint can be deployed as a guest-centric strategy that provides instant and secure Wi-Fi access upon arrival at every property. Passpoint delivers the homelike experience of connecting every time a guest arrives without friction or hassle.

### *Passpoint Defined*

Passpoint, also known as Hotspot 2.0, is a technical specification developed by the Wi-Fi Alliance® (WFA)—a global organization that oversees Wi-Fi interoperability standards. Passpoint leverages several key technologies, primarily IEEE 802.11u and IEEE 802.1x, to allow devices to communicate and associate with Passpoint networks[3].

Passpoint specifies that a hardware device has passed interoperability testing according to the specification. Client devices (smartphones, tablets, laptops, access points, etc.) that pass the certification receive the Wi-Fi Certified Passpoint designation, which means they can successfully connect to Passpoint-certified networks[4].

Passpoint technology standardizes the way that wireless carriers shift traffic onto a Wi-Fi network and provide a seamless one-time authentication process for connecting to a guest network. With Passpoint, hardware and software providers can improve the guest experience and help alleviate challenges experienced by hotel brands that want to deliver modern homelike connectivity.

### *How Passpoint Works*

The most common way to implement Passpoint is to set up a separate wireless network specifically for Passpoint connections. For most properties with modern network infrastructure, introducing Passpoint does not require replacing hardware, service provider, or the central authentication solution.

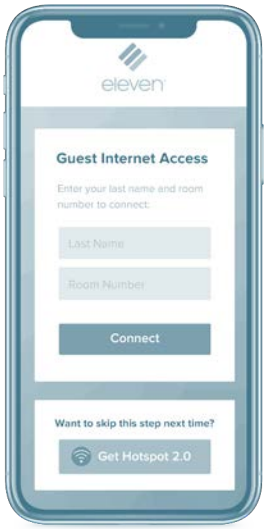
After the Passpoint network is configured, a process must be put in place for guests to install profiles on their devices. For example, a guest may check into a hotel and follow the usual steps to login to the network. A post-connect landing page could offer the guest the option of downloading a Passpoint profile. After this one-time download, they will automatically authenticate with an encrypted connection every time they return to that location or any other participating brand location in the world.

### *Profiles Instead of Passwords*

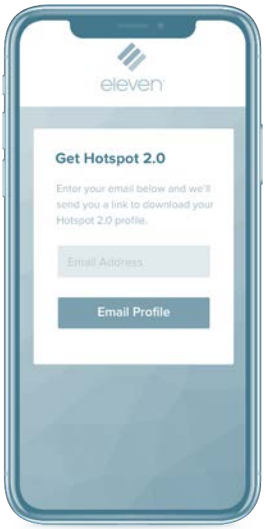
Instead of network passwords or passphrases, Passpoint uses certificates, also called profiles, to authenticate users onto a Wi-Fi network. These secure digital fingerprints are installed via a one-time installation process and are stored on the device. The technology was developed in partnership with hardware manufacturers and network operators to maximize adoption. While almost all new client devices have support for Passpoint, many older devices may not support it. An important feature for any HS2.0 provider is having built-in intelligence to determine if a guest's device is compatible with HS2.0 or not. For non-compatible devices, it is important to notify the user quickly, so unnecessary time isn't spent attempting to install a profile that is not compatible with their device.

Passpoint has evolved since its inception in 2012 and has become more widespread and feature-rich. At first, only enterprise access points had built-in capabilities, but devices have rapidly started to catch up in the last few years. Apple added Passpoint support to iOS 7 in 2013, and Google followed suit in 2015 with an implementation on Android[5]. Expansion from mobile devices to tablets and notebooks have also bolstered functionality, with most mobile device platforms supporting the technology today[6].

**STEP 1**
Guest opts-in to the Passpoint program from the captive portal

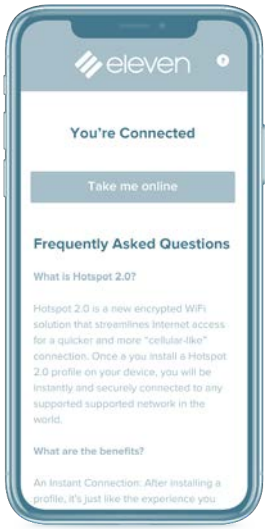



**STEP 2**
Guest enters email to receive link to download a Passpoint profile




**STEP 3**
Guest downloads profiles on their devices from the email link


**STEP 4**
Guest is automatically authenticated at all supported properties



### *Seamless User Experience Boosts Loyalty*

A lot goes on behind the scenes of the Passpoint authentication process, but for many guests this happens without them even realizing it. The primary way a user interacts with Passpoint is during the initial one-time installation of the profile. Guests can receive profiles many different ways. Most commonly, a link to download a profile is sent via email or SMS. Other options include QR code or NFC tags that open up a link to a web page that facilitates the download and installation of the profile.

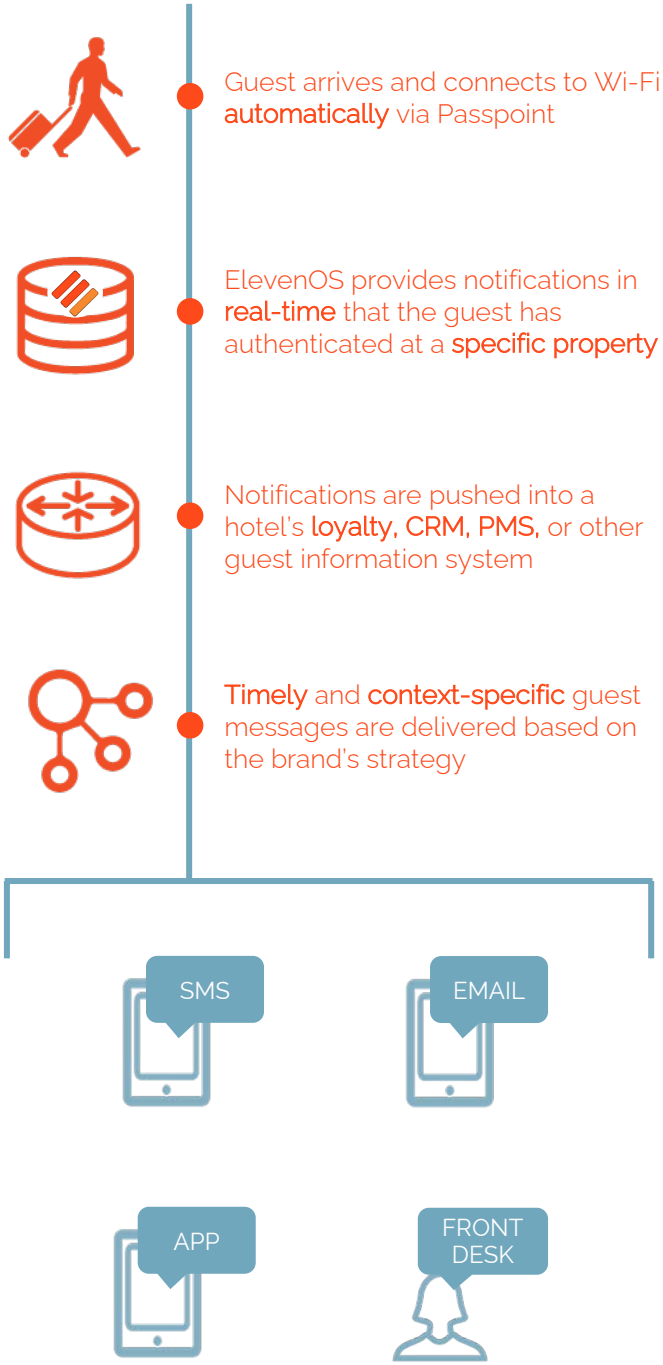
More advanced and customized profile delivery methods include web based single-sign-on (SSO) solutions or even mobile app integrations that allow Passpoint profile management from inside an iOS or Android application. These methods allow Passpoint to be used as an incentive to enroll in a brand's loyalty program by rewarding members with more seamless and secure Wi-Fi access.

Once a Passpoint profile is installed, a guest's device will automatically associate and connect to any supported Passpoint network within Wi-Fi range. The network broadcasts additional information about what devices are allowed to connect to it, which allows guest devices with Passpoint profiles to automatically communicate with the network in order to properly authenticate and connect. Security protocols on the device, network and authentication server ensure that the certificate credentials are correct and that all communication is coming from legitimate sources.

Guests with profiles will be automatically connected to Wi-Fi at all participating properties for any specified period of time (or forever). Attributes can also be added to throttle bandwidth or the total number of devices for associated profiles. For example, a "platinum" member's profile could be associated with higher bandwidth limits when compared to a "silver" member's profile.

### *Guest Engagement with Wi-Fi Data*

With the elimination of the captive portal, many brands are left wondering—what are the customer touchpoints for Passpoint users? If a managed Wi-Fi platform is used to deploy Passpoint across the brand, real-time notifications are made possible. With in-app push notifications, SMS messages or emails, guests can be messaged with timely and contextual communication when using Passpoint networks



### *Enhanced Security with WPA2 Encryption*

Today, many public Wi-Fi networks are open––the connection between guest devices and the network itself is not encrypted and a user's internet activity is vulnerable and can be interfered with. From GDPR to the California Privacy Act to Mark Zuckerberg's 4-hour testimony in front of the US Senate, online privacy and Wi-Fi security has become more important and visible than ever.

With Passpoint, all connections are secured with Wi-Fi Protected Access® 2 (WPA2™). WPA2 is a security protocol and security certification program developed by the WFA to secure wireless networks. It was designed in response to serious weaknesses found in the previous system, Wired Equivalent Privacy (WEP)[7]. WPA2 uses a stronger and more robust encryption method called Advanced Encryption Standard (AES). Passpoint goes beyond just encouraging WPA2 encryption—it requires it for every single connection.

> *"Security is a foundation of Wi-Fi Alliance certification programs, and we are excited to introduce new features to the Wi-Fi CERTIFIED family of security solutions," said Edgar Figueroa, president and CEO of Wi-Fi Alliance. "The Wi-Fi CERTIFIED designation means Wi-Fi devices meet the highest standards for interoperability and security protections."* [8]

As wireless and security technology continues to evolve, the Wi-Fi Alliance is committed to enhancing WPA2 to ensure robust security protections Wi-Fi users, especially via Passpoint.

With guest concerns about digital and network security gaining momentum, a brand's ability to deliver more secure Wi-Fi access is becoming increasingly tied to brand perception and guest loyalty.

### *Evolution of Passpoint Technology*

There have been three releases of Passpoint since it first launched in 2012. The first release (r1) defined the technical core of the Passpoint specification, such as how network discovery occurred and the preliminary security settings, and also kicked off the individual device certifications that have since expanded.

In 2016, the WFA removed the r1 certification, forcing manufacturers to build to the release 2 specification (r2) to become certified. This second release standardized how credentials are provisioned, how they are stored, and how long they are valid. It also includes the ability for online sign-up (OSU), which allows the network to provision Passpoint profiles.

In early 2019, release 3 (r3) was published with a focus on the profile's interaction with networks. One new feature concerned the acceptance of the operator's terms and conditions, which helps providers secure and maintain liability while using Passpoint. Another feature of r3 is the ability to use a single SSID for Online Sign-Up (OSU), which simplifies the user experience when installing the certificate. Three new ANQP elements are enabled, including the Operator Icon Metadata, Venue URL, and Advice of Charge elements[9]. Outside of ANQP, the Roaming Consortium element is also available for application, which identifies roaming partner groups and service providers with security credentials that can be used to connect to a network[3].

Enhancements to the technology include improved data offloading, network detection, and security. Currently the most recent version of all operating systems, including iOS, MacOS, Android, and Windows, support Passpoint r2[10]. A Passpoint network's WPA2 encrypted connection is bolstered by the certification requirement for several additional Extensible Authentication Protocols (EAP) types being supported, including TLS, TTLS/MSCHAPv2, SIM, and AKA. These additional protocols help to authorize and encrypt the connection between the certified device and network.

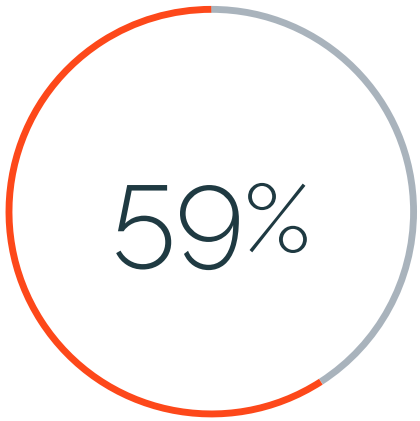
### *Roaming & Wi-Fi Offloading*

Offloading enables cellular providers to intelligently manage capacity and deliver a better customer experience with more efficient network traffic management. Customers are moved dynamically from cellular to Wi-Fi networks as needed, without causing any interruptions in their service.

For brands, cellular offloading represents a new potential revenue stream. Boingo, a leading Passpoint supporters in the United States, reported revenue of $47.5 million from its offloading business in its most recent year (up 50.6% from the prior year)[11].

Over half of mobile traffic (59%) will be offloaded from cellular networks to Wi-Fi by 2022[12]. Wi-Fi and 5G will coexist in our always connected world and people will use them interchangeably. Networks and devices will communicate behind the scenes to choose which wireless technology is best given the circumstances—location, indoor or outdoor, signal strength, etc.

The future of Passpoint networks is centered around brand partnerships and the ability create revenue without disrupting the guest experience. By partnering with carriers and other complimentary services, brands can play a central role in offering a truly frictionless Wi-Fi experience for guests.




*59% of mobile traffic will be offloaded from cellular networks to Wi-Fi by 2022[12]*

## Conclusion

*Seamless and secure Wi-Fi access via Passpoint enables hotel brands of all sizes to build guest loyalty today and future-proof their networks for tomorrow*

The world of Wi-Fi is constantly changing and users continue to demand more bandwidth and less friction. That's why it's time for brands to adopt Passpoint into their Wi-Fi strategy. Guests will benefit from fast, frictionless connectivity while hotel brands will be able to offer better experiences and expand their global footprint. With the recent emphasis around building brand loyalty, Passpoint is an important offering that strengthens the value of loyalty programs.

In addition to brand loyalty, Passpoint has real implications for the bottom line as well. Hoteliers can create potential new revenue streams via Wi-Fi offloading and carrier partnerships. Ultimately, as guest bandwidth demand increases and willingness to compromise on connectivity decreases, the hotel brands who deliver fast frictionless Wi-Fi will win.

Although Passpoint has existed for a while, the technology still has an exciting future ahead. Adoption rates continue to grow among manufacturers and public awareness and demand is picking up as well. Soon, it will not only be thought of as a technology for enterprise businesses and airports, but more widely adopted even in residential applications.

Passpoint technology continues to be refined as AAA servers, OSU servers, roaming partners, and other subscriber management services build out capabilities to more efficiently and effectively manage certificates and credentials. With the ability to deliver simple, seamless, and secure Wi-Fi access, there's no doubt that Passpoint is at the core of the future of guest Wi-Fi.

# Resources


1. "IoT: Number of Connected Devices Worldwide 2012-2025." *Statista*, 2019, www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide.

2. Martin, Jeremy & Mayberry, Travis & Donahue, Collin & Foppe, Lucas & Brown, Lamont & Riggins, Chadwick & C. Rye, Erik & Brown, Dane. (2017). "A Study of MAC Address Randomization in Mobile Devices and When it Fails." 2017, https://www.researchgate.net/publication/314361145_A_Study_of_MAC_Address_Randomization_in_Mobile_Devices_and_When_it_Fails.

3. "How Interworking Works: A Detailed Look at 802.11u and Passpoint Mechanisms." Ruckus Wireless, July 2013. https://webresources.ruckuswireless.com/pdf/wp/wp-how-interworking-works.pdf

4. "Passpoint." *Wi-Fi Alliance*, 2019, www.wi-fi.org/discover-wi-fi/passpoint.

5. Thornycroft, Peter. "Wi-Fi Certified Passpoint Zig-Zags towards Success." *Network World*, Network World, 22 July 2016, www.networkworld.com/article/3098440/wi-fi-certified-passpoint-zig-zags-towards-success.html.

6. Figueroa, Edgar. "WiFi Passpoint: Ready for Prime Time." *Light Reading*, 18 Nov. 2013, www.lightreading.com/mobile/packet-core/wifi-passpoint-ready-for-prime-time/a/d-id/706628.

7. "Wi-Fi Protected Access." *Wikipedia*, Wikimedia Foundation, 17 Apr. 2019, https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access.

8. "Wi-Fi Alliance® Introduces Security Enhancements." Edited by Stephanie Burke, *Wi-Fi Alliance*, 8 Jan. 2018, www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements.

9. "Passpoint Specification Package (Passpoint Release 3)." *Wi-Fi Alliance*, 2019, www.wi-fi.org/downloads-registered-guest/Hotspot_2.0_Specification_Package_v3.0.zip/35974.

10. Thornycroft, Peter. "Using Passpoint for Private Wi-Fi Networks." *Network World*, Network World, 24 Apr. 2017, www.networkworld.com/article/3191494/using-passpoint-for-private-wi-fi-networks.html.

11. "Boingo Wireless Reports Record Fourth Quarter and Full Year 2018 Financial Results." Edited by Melissa Robinson, *Boingo Wireless Reports Record Fourth Quarter and Full Year 2018 Financial Results | Business Wire*, Business Wire, 27 Feb. 2019, www.businesswire.com/news/home/20190227005949/en/Boingo-Wireless-Reports-Record-Fourth-Quarter-Full.

12. "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper." *Cisco*, Cisco, 19 Feb. 2019, www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html.

*ElevenOS is hospitality's #1 cloud-based guest Wi-Fi platform. Contact us for a free Wi-Fi consultation and to learn more about our Passpoint solution for delivering simple, seamless, and secure connectivity to your most loyal guests.*

eleven

www.elevensoftware.com
sales@elevensoftware.com
1 (503) 222-4321