globalreach

WHITEPAPER

SECURE, SEAMLESS WI-FI FOR CONNECTED PLACES

INTRODUCTION

Cities are getting smarter. And that's important when global urban populations are booming and when a healthy economy - and community - needs to be effective and efficient.

From the bins being emptied on time, to gathering greater insight into the needs and wants of local residents and business, connectivity plays an important role in running a smart city, and understanding and improving future city initiatives.

Wi-Fi in towns and cities can be frustrating and it's known to be a major source of dissatisfaction. Residents and visitors expect to be connected to a high-quality service wherever they are, and personal, business and public sector services suffer when users are disconnected as they walk around a city centre and lose cellular signal. There's also the added pain of having to reconnect on the move.

Making sure that your community is always connected, along with the public services that depend on an internet connection is key to delivering a high standard of life, contributing to well-being enfranchisement and public service efficiency.

Continuing the current practice of asking each device user to enter an email address or phone number each time they want to use a city Wi-Fi service, introduces unnecessary and frustrating barriers.

Upgrading existing municipal Wi-Fi infrastructure and services to the Passpoint standard* provides the opportunity to allow residents, visitors and those who work locally to connect with minimum friction and with added security via an encrypted radio link.

There are now a number of easy ways to give users this automatic and secure connection. Local council tax payers, with a council app can agree to download a profile (an online signup server) to their devices to choose to be automatically connected to the city's Wi-Fi service every time they're in the area. This simple, one-time download securely and seamlessly connects them each and every time they're in reach of an enabled Wi-Fi access point.

The standard is mature. Passpoint-ready Wi-Fi access points have been widely available from leading hardware

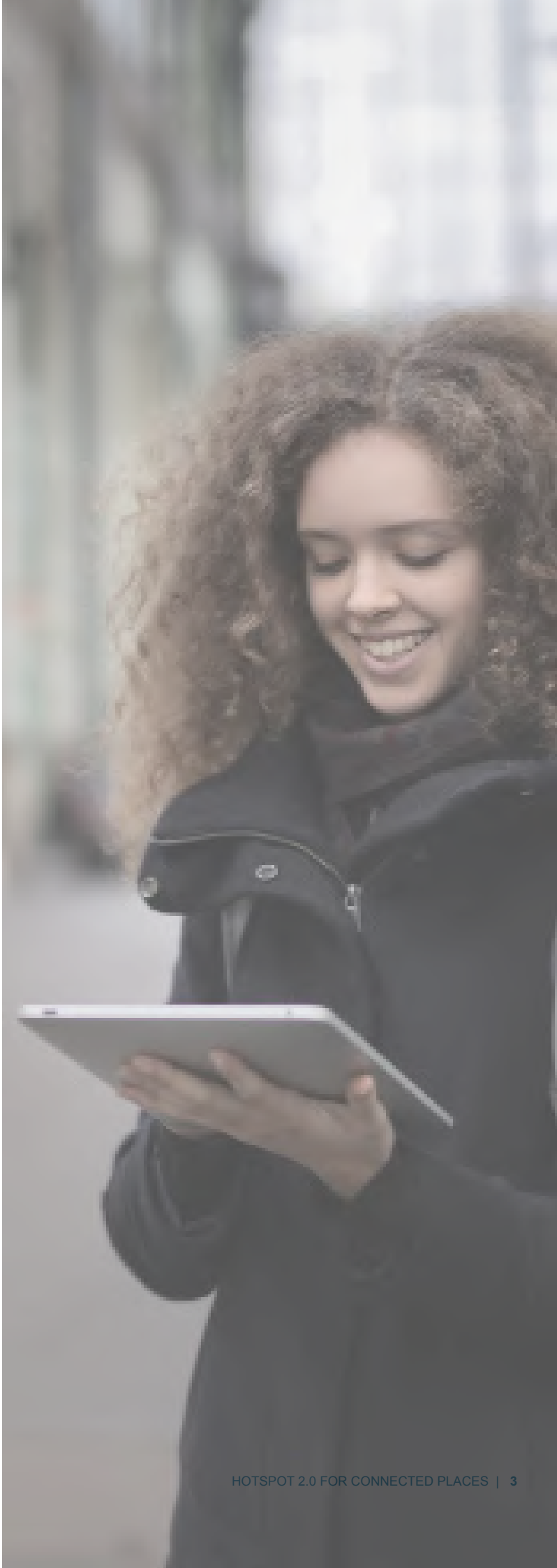
manufacturers for many years. Passpoint also allows consumers to transfer seamlessly between 5G and Wi-Fi, making the user experience ‘cellular-like.’

Not only does it increase resident satisfaction, but it also gives the local authority a direct channel to engage with the community via personalised, relevant communications and service bulletins.

It’s also an opportunity for areas to build Wi-Fi ecosystems of partners that will add value and improve the quality of life, like transport providers, public service offices, local amenities like playing fields and other public spaces, allowing locals to connect seamlessly wherever they are.

Imagine how local shopping, school runs, hospital visits and more can be transformed when residents are automatically connected to the Wi-Fi. This seamless, secure experience should be today’s benchmark for municipal Wi-Fi services.

**Passpoint specification (also known as Passpoint™ by the Wi-Fi Alliance) is based on IEEE standards for Wi-Fi network and user devices.*



HOW Passpoint CAN IMPROVE LOCAL QUALITY OF LIFE

SECURE:

Secure Wi-Fi service protects customers and staff from in-air and man-in-the-middle attacks.

SEAMLESS

- Provision devices onto Passpoint Wi-Fi services in seconds.
- Online signup server supplied through the local authority app, or a web link delivered via publicly available QR codes or NFC chips allows easy online and offline signup.
- One-time provisioning removes the complexity of being connected and enables in-pocket connection across all locations.
- Single sign-on allows residents and workers to automatically and securely connect in the coverage zone, and to roam onto different Wi-Fi networks and ecosystem partners like buses, taxis, trains and local sports centres while retaining individual brand identities (SSIDs).
- Provides a cellular-like experience.
- Supports public sector employees with hidden SSIDs (Wi-Fi network identifier). Enables separate use of the Wi-Fi network by permanent and temporary user groups eg: council workers, road contractors, telecoms engineers, emergency services and contractors.

MONETISE

Towns and cities can also offer their Passpoint networks to third party telco partners, who are looking for high-quality Wi-Fi services to increase their coverage footprints for roaming and for traffic offload. Commercial agreements with these carriers, aggregators and service providers, extends service use and can provide service operators and councils with new revenue opportunities which can, in turn, pay for upgrades to the Wi-Fi service.

DETAILED RECOMMENDATIONS

The availability of high-quality Wi-Fi is one of the top five priorities for consumers and business users - anywhere. It's key to keeping them connected to the people and information that is important to them. And without reliable Wi-Fi, a significant channel for improving the resident's experience through engagement and communication is also lost.

A single sign-on experience across city centres, public buildings, outdoor spaces and associated local partners will greatly improve the community experience. Once the user has the Passpoint profile on their device, the device is 'remembered' by the Wi-Fi service, removing the need to re-enter credentials when the user returns or roams to another part of the city or onto a partner network.

This is made possible by providing local users with a straightforward one-time online signup process with, for example, the local authority's app, with any public sector communications or bills, or by making it available (via QR code) in public places. Imagine how the community experience is transformed when they find that their device is automatically connected as soon as they take it out of their pocket.

Passpoint is an 'over the top' service. This means that it's delivered as an enhancement to existing Wi-Fi hardware. Most hardware, like access points, are Passpoint ready and integration is straightforward via changes to the network configuration. The maturity of the technology is such that residents, workers, public sector employees and contractors can easily benefit from seamless and secure connectivity to mirror today's cellular experience today.

SECURITY

Legal compliance is ensured as the subscriber's connection is authenticated using credentials provisioned by the mobile operator on the user's SIM or via online signup validation - this allows greater traceability of who is on the Wi-Fi and where balancing GDPR and security responsibilities. Hence, municipal Wi-Fi service providers can meet all CSP (Communications Service Provider) and ISP (Internet Service Provider) regulations for providing the service.

Each device receives a one-time provisioning file to automatically configure Wi-Fi settings and encryption without manual intervention. When registered, the user is provisioned with a Passpoint credential which allows them to automatically and securely connect.

For users with devices without a mobile SIM, the onboarding sequence can be shortened further using QR codes or NFC tags which direct them to the online signup server (OSU). This can be embedded in council communications and other public sector collateral to drive greater citizen awareness.

Some Wi-Fi operators have used an authentication method for seamless login using the MAC (Media Access Control) address of a previously connected device. Communications between the device and the access point are unencrypted in this situation. Moreover, the latest mobile handset operating systems updates are randomising MAC authorisation on many devices for other security reasons, meaning that returning users may have to re-authenticate each time. Passpoint overcomes this issue by using encryption between the Wi-Fi access point and the user's device and is, therefore, more secure.

LOCAL AUTHORITY CONTROL & COMMUNITY ENGAGEMENT

The latest Passpoint Release 3 standard also supports location-aware, personalised communications. The GlobalReach solution includes rich presence and location analytics, which give service providers and councils full control of the policies that can trigger location- or event-specific interactions like service updates to bin collection dates or roadworks, and news about local events

These can be triggered by who the user is (resident or business user type), where they are (property or business location), and time (e.g. as when they are most likely to be in the area, or to need a service).

Passpoint R3 makes it possible for councils to determine the experience that they want each user type to have, and to put engagement programmes in place, that use their Wi-Fi services both surprise and delight local residents and businesses, bringing the community closer together.

For example, details of free events can be sent directly to devices as locals enter the town centre. Using Passpoint, Wi-Fi services and related communications are fully-controlled by the council.

ROAMING & DATA OFFLOAD

Passpoint can be used to provide enhanced roaming services. This may enable an integrated roaming service that could deliver frictionless access across all Passpoint Wi-Fi networks at branches and other partners, regardless of the network operator, by providing single sign on (SSO) nationwide. This could transform the overall experience by reducing the frustrations that customers feel by having to login each time.

The opportunity exists to create a seamless roaming experience across all partners. Using commercial agreements customers can roam seamlessly without the need to reconnect or re-enter registration details.

WI-FI ROAMING

Wi-Fi service providers across the network retain their existing SSID, portal and user experience and use a roaming realm or RCOI (roaming consortium ID) which allows all parties to roam across different Wi-Fi networks. This would require a policy to be accepted by participating Wi-Fi operators and may involve a commercial roaming agreement between the Wi-Fi service providers and network operators.

Passpoint can enable network providers to further monetise their Wi-Fi footprints through commercial roaming agreements and, working with roaming partners to seamlessly offload traffic. This, in turn, may help to further fund the infrastructure needed to provide a great municipal user experience.

MOBILE DATA OFFLOAD

The mobile-like, Passpoint connection increases the appeal of these Wi-Fi networks to mobile operator roaming partners. By leveraging carrier-grade Wi-Fi networks the mobile operators can grow their service coverage including ‘hard to reach’ locations, where cellular network performance may be poor.

This may open up a significant new revenue stream for the Wi-Fi network provider and help fund the investment needed to support an improved community experience.

It may be more cost-effective in many cases for a mobile operator to implement Wi-Fi ‘offload’ in this manner and pay fees to the Wi-Fi network provider than to attempt to carry the traffic directly and invest in greater capital spending.

ENABLING IOT

The Internet of Things (IoT) devices/sensors are making it easier to monitor and control municipal functions like parking, traffic, lighting, policing, water and energy flow and rubbish removal. The use of Wi-Fi remains the most prevalent means of connectivity for IoT devices because of the existence of large networks, relatively low cost and ease of deployment.

However, the real power lies within the data collected from these IoT devices which offer a much more granular and in-depth understanding of municipal functions and can help in planning for the future.

IoT can be used to improve the user experience through a number of use cases and by both connecting both resident and public sector services. For example, public safety is an important component of a connected city, with many areas expanding their deployment of video surveillance to both deter crime and collect invaluable information from specific locations or events.

To understand and benchmark IoT network activity demands carrier-grade network authentication and logging as a minimum. It is key to spotting abnormal operations and traffic patterns over these devices.

A cloud-based AAA / RADIUS platform is required that delivers fit-for-purpose IoT authentication, access, policy and audit solution for tens of millions of ‘traditional’ and Internet of things (IoT) devices.

CONCLUSION

Using the latest Passpoint Wi-Fi technology including secure authentication and policy management tools on a consistent basis, will enhance local services, improve efficiency for business and quality of life for local residents.

It can also open new revenue channels for the local authorities and through roaming agreements, may create an equitable way of contributing to the funding of a world-class Wi-Fi network.

To achieve this vision will require a holistic approach between councils and local partners, to create a Wi-Fi experience that keeps residents and workers connected as they move around our towns and cities.

The latest Passpoint technology makes this possible without the local authority and its partners losing their individual identities (and SSIDs).

ABOUT GLOBALREACH TECHNOLOGY

GlobalReach is recognised as a Passpoint Wi-Fi industry leader. Our OSU has delivered secure authentication for some of the largest international Passpoint services since 2014, including the LinkNYC deployment of 1,800 outdoor kiosks in Manhattan, enabling some 20m Wi-Fi sessions per week.

GlobalReach also deployed the first central London Passpoint Wi-Fi network with Ontix in 2019. The outdoor Wi-Fi service runs alongside the existing small cell wireless network and is now available to the public, and for all mobile network operators for seamless roaming connections.

In an alliance between SMARTSEL and Dune Global, GlobalReach also provides users of new public Wi-Fi service in Selangor, with secure login to the public Wi-Fi service using Passpoint universal single sign-on. The network is set to enable smart city services and IoT connectivity to modernise and transform public utilities, transport and communications.

GLOSSARY

ACRONYM	MEANING
AAA	Authentication, Authorisation and Accounting
CoA	Change of Authorisation
CPE	Customer-premises equipment
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
PAS	Portal Aggregation Service
UE	User Equipment
URL	Uniform Resource Locator
VSA	Vendor Specific Attribute
WAG	Wireless Application Gateway
WLC	Wireless LAN Controller

globalreach

sales@globalreachtech.com
+ 44 20 7831 5630