Wi-Fi Roaming Business Case
White Paper

State of the Industry and Market Drivers

Source: WBA Members & PMO
Author: Wireless Broadband Alliance
Version: Final
Date: 02 December 2015
About the Wireless Broadband Alliance

Founded in 2003, the aim of the Wireless Broadband Alliance (WBA) is to secure an outstanding user experience through the global deployment of next generation Wi-Fi. In order to make this a reality, the WBA is currently championing various initiatives in the Wi-Fi ecosystem including Next Generation Hotspot (NGH) trials, Wi-Fi Roaming and its Interoperability Compliance Program (ICP). Today, membership includes major fixed operators such as BT, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Google and Intel. WBA member operators collectively serve more than 1 billion subscribers and operate more than 5 million hotspots globally. The WBA Board includes AT&T, Boingo Wireless, BT, China Telecom, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO, Orange and Ruckus Wireless.

Follow Wireless Broadband Alliance at:
www.twitter.com/wballiance
http://www.facebook.com/WirelessBroadbandAlliance
http://www.linkedin.com/groups?mostPopular=&gid=50482
https://plus.google.com/106744820987466669966/posts

© Copyright 2015 Wireless Broadband Alliance Ltd ("WBA"). All rights reserved. While every effort is made to ensure the information in this report is accurate, the WBA does not accept liability for any errors or mistakes which may arise in relation to the material. All copyright material and trademarks used in this report are the property of their respective owners.
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 organisations 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 organisations 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 organisations 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.
Executive Summary

This white paper examines the commercial and technical aspects of how to make Wi-Fi Roaming – the automatic provisioning of connectivity to end-users across different service providers’ Wi-Fi networks – available to personal devices. A strong focus on the Wi-Fi Roaming business models is provided, leveraging insights from the industry and global operators that already have deployed their Next Gen Wi-Fi ready networks and developed their businesses.

The Wireless Broadband Alliance (WBA) defines roaming set-up best practices for service providers and outlines the reasons for providing roaming services as well as suitable strategies to adopt. Standards are provided for the type of information needed from the Wi-Fi network, together with guidelines on how to exchange relevant information between involved parties.

Aforementioned best practices and technologies are grouped under the umbrella of Next Generation Hotspot (NGH) driven by WBA which is the stepping stone for Wi-Fi Roaming. Nowadays it already led to more than 10 global deployments from top tier operators.

Moreover, WBA maintains a database of operators roaming related data, including the WBA operator ID that is solely provided and maintained by the WBA.

To further engage with the WBA and learn more about Wi-Fi Roaming please contact:

pmo@wballiance.com
Contents

Executive Summary ................................................................................................................... 1
1. Introduction ................................................................................................................... 3
  1.1 What is required to participate? ...................................................................................... 3
2. The Wi-Fi Roaming ecosystem .................................................................................... 4
  2.1 Wi-Fi Roaming architectures .......................................................................................... 5
3. WBA Wi-Fi Roaming framework .................................................................................. 7
  3.1 Setting up roaming service ............................................................................................. 7
  3.2 WRIX Standards ............................................................................................................. 7
  3.3 Wi-Fi Roaming contract templates ................................................................................ 12
  3.4 Interoperability Compliance Program ........................................................................... 12
  3.5 On-going WBA Work to enhance the Wi-Fi Roaming ecosystem ................................. 13
4. Setting the scene – industry trends .......................................................................... 14
5. Business models overview ........................................................................................ 18
6. Use cases/case studies ............................................................................................. 24
  6.1 NTT DOCOMO innovative Wi-Fi Roaming service ....................................................... 24
  6.2 Comcast Secure Wi-Fi Roaming with Liberty Global .................................................... 25
  6.3 AT&T business case template ...................................................................................... 29
  6.4 Boingo Wi-Fi Roaming & Passpoint™ overview ........................................................... 30
7. Conclusion & call for action ...................................................................................... 36
  7.1 Operators with Wi-Fi networks ..................................................................................... 36
  7.2 Operators without Wi-Fi networks ................................................................................. 36
References - Summary ............................................................................................................ 38
Acronyms and Abbreviations ................................................................................................. 39
Participant List ......................................................................................................................... 41

Figures

Figure 2—1 Typical WLAN roaming ecosystem ........................................................................ 4
Figure 2—2 Typical WLAN roaming architecture ................................................................... 5
Figure 2—3 WLAN roaming with direct, bilateral interconnection ........................................... 6
Figure 2—4 WLAN roaming bilateral interconnection using a third party provider .................. 6
Figure 3—1 WRIX framework ................................................................................................... 8
Figure 3—2 WRIX typical flow .................................................................................................. 9
Figure 3—3 WRIX-F timeline .................................................................................................. 11
Figure 6—1 Users and data traffic after the introduction of SIM authentication ...................... 24
Figure 6—2 The number of DCM’s hotspots ........................................................................... 25
Figure 6—3 Boingo Roaming network overview ...................................................................... 30
1. **Introduction**

People are traveling the world more than ever, and are relying on their smartphones and tablets to stay in touch with colleagues, friends and families from abroad. While mobile roaming services have become accessible, it’s estimated that up to 70% of international travellers don’t use traditional mobile services, instead often relying on Wi-Fi networks to stay connected.

For Services Providers (SPs), there’s an opportunity to harness people’s familiarity and acceptance of Wi-Fi to create new services and products, encouraging additional roaming usage and revenues. A managed Wi-Fi Roaming service can greatly improve the overall user experience with regard to:

- Simplifying the connection to a Wi-Fi hotspot
- Seamless roaming between Wi-Fi hotspots
- Better technical performance of a Wi-Fi hotspot
- Secure authentication and connection to a Wi-Fi hotspot
- Privacy for the end-user
- Access to a much larger commercial Wi-Fi network across different geographies and venue types

For Mobile Service Providers (MSPs), specifically, Wi-Fi Roaming creates several benefits to the regular Wi-Fi business:

- Extends the mobile network reach through multiple mobile connectivity methods
- Instantly gain a large footprint of available hotspots rather than growing organically
- Pay for actual usage rather than deploying a network that might not get fully used
- Avoid network capital and operational costs while still providing Wi-Fi services to your customers
- Fast-track smaller operator’s current businesses growth via Wi-Fi Roaming

1.1 **What is required to participate?**

One of the WBA’s objectives is promoting Wi-Fi Roaming for the reasons above. Accordingly, the WBA has instigated a number of organised industry events, member work programmes and cross industry collaboration to facilitate and promote Wi-Fi Roaming. All members across the eco-system can join the technical and commercial work groups and participate in the various programmes. This white paper further outlines the high level technical architecture for different roaming models, the business models themselves and an overview of the various WBA workgroups including Roaming Sustainment, Interoperability Compliance Program (ICP), Wireless Roaming Intermediary eXchange (WRIX) standards, Global Service Provider NGH Registry and RADIUS-Diameter inter-working.
2. The Wi-Fi Roaming ecosystem

There are three primary stakeholders in the Wi-Fi Roaming ecosystem. Due to the communal nature of Wi-Fi, often a single company is involved in providing more than one element of the ecosystem.

Visited Wi-Fi network operators – perhaps the most complex group, a Wi-Fi network is made up of one or more Wi-Fi access points. The owner/operator of a Wi-Fi network may be content to leave access to their network private, not sharing it to global subscribers. But for those who wish to join a Wi-Fi Roaming hub and enable inbound roaming traffic, there is an opportunity to monetize traffic on the network.

Wi-Fi network owners/operators come in all shapes and sizes – for example single site locations like a venue, to multi-site like hotel chains. There are service providers who have built Wi-Fi networks to complement fixed networks such as BT or Comcast, and mobile providers who’ve added Wi-Fi to augment mobile capacity like AT&T. There are millions of one-off locations around the world offering free and open Wi-Fi. And there are aggregators like Boingo or iPass that have built businesses around actively connecting and managing access to pools of Wi-Fi networks. These companies can bring millions of disparate access points into a roaming hub in a single connection.

These are the Visited Network Providers (VNPs), which provide access and Wi-Fi connectivity to subscribers.

---

Figure 2—1 Typical WLAN roaming ecosystem

The Wi-Fi hub – modelled on GSM Roaming, the Wi-Fi hub provides a central connectivity point between the visited Wi-Fi networks and the home subscriber networks. Within the hub, there are two general functions:

Inter-connectivity – maintaining information associated with each Wi-Fi access point in each Wi-Fi network, and managing the authentication/authorization process of an end-customer to that visited network back to their home network database.
Settlement and clearing – accounting of usage between networks and reconciling that usage across the visited Wi-Fi networks to ensure that providers can get paid and users can get billed. To facilitate and standardize this process, which is distinct from cellular roaming, the WBA pioneered the WRIX specification.

There are independent third party vendors offering these services such as Accuris Networks, BSG Wireless, Point Dume and Syniverse. There are MNOs who’ve created groups or departments to support this functionality such as AT&T, Emirates DCH (EDCH), PT Telkom Indonesia, NTT DOCOMO and Vodafone.

Subscribers – these are the end customers who roam and ultimately use Wi-Fi managed by a Visited Network Provider (VNP). To facilitate access, the subscribers may have a downloadable app or have functionality embedded in their device, which helps find appropriate Wi-Fi access points and can manage the connection process. The subscribers will also have an existing billing relationship from their Home Service Provider (HSP), and likely be assigned to service plan that includes Wi-Fi Roaming.

For the purposes of Wi-Fi Roaming, the vast majority of the subscribers are mobile-centric, with a smartphone (because it has Wi-Fi), a SIM. Mobile Network operators who choose to connect with a Wi-Fi Roaming hub provider can enable the appropriate subscribers to access Wi-Fi as defined in their service plan.

2.1 Wi-Fi Roaming architectures

To provide Wi-Fi Roaming services, the VNP and HSP must have interoperability mechanisms in place. Figure 2—2 illustrates the most common Wi-Fi-to-Wi-Fi Roaming architecture based on the WRIX architecture as defined in WBA documentation.

![Typical WLAN roaming architecture](image)

The visited network provides the connectivity to the client devices, but redirects the initial authentication of the roaming client devices to the home network AAA servers, typically via RADIUS (Remote Authentication Dial In User Service) proxy or from the Access Controller. Connection between the networks must be secured using private circuits, MPLS or Virtual Private Network (VPN) tunnels.

The authentication can be done between the home and visitor networks while the accounting and reconciliation of usage for billing purposes may be outsourced to a third party. RADIUS accounting is not lossless, so accounting records between the home and visited network providers might differ from each other. If sufficient resources cannot be allocated to compare the records and manage the discrepancies, the accounting should be outsourced to a third party.

Figure 2—3 does not show a policy controller, which is mandatory in some countries and for operators of a certain size. It is used to set the access policies to roaming customers and can provide feedback from both the visited and home network operators as well as the venue where the users are located.

Operators may have different approaches when developing a roaming strategy. There are two main scenarios available to operators to interconnect their networks, either through a direct connection or by using a third party to
facilitate that interconnection. For the latter there could be several hybrid models from both operators using the same hub or just one operator using a hub provider (see Figure 2—3 and Figure 2—4).

Figure 2—3  WLAN roaming with direct, bilateral interconnection

Figure 2—4  WLAN roaming bilateral interconnection using a third party provider

In a Wi-Fi Roaming environment, there are likely to be a large number of relatively small Visited Wi-Fi Network Providers. A hotel chain, an airport, a convention centre, and perhaps other venues, may all be a part of a subscriber’s Wi-Fi Roaming experience. Thus for the home network service provider to deliver a compelling experience, the broader and denser the visited Wi-Fi network, the more value for the end-user.

As such, the role of a Wi-Fi Roaming hub is quite important in enabling service providers to build and consolidate Wi-Fi footprint quickly, and deliver a compelling experience to their end-users. The Wi-Fi Roaming hub provides the following benefits:

- Consolidate Wi-Fi access across multiple networks/providers into a single ‘Visited Network’
- Manage connectivity, accounting and access with and between a wide variety of Wi-Fi access networks
- Reconcile accounting and usage records between wide variety of networks and providers

To enhance the attractiveness of roaming service, a hub may propose and offer additional services to the HSP (and their end-users), that are absent in the earlier arrangements, after reaching to an agreement with the HSP and VNP. It may be supplemented services unique to the host, unique not only in the literal sense, but, for example, associated with the peculiarities of the local legislation and so forth. In addition, it may be due to the technical features of the VNP network.

3. WBA Wi-Fi Roaming framework

This section provides an overview of WBA work in Wi-Fi Roaming, including: roaming supporting documentation, WRIX standards, ICP, Global NGH Registry and RADIUS-Diameter interworking.

3.1 Setting up roaming service

The WBA roaming process is summarized under the term WRIX or Wireless Roaming Intermediary eXchange. In addition to the WRIX Specification a set of documents are available for the implementation and maintenance of a Wi-Fi Roaming agreement. These are:

- Technical Exchange Document (TED)
- Commercial and Business Exchange Document (CBED)
- User Experience (UE) Recommendations
- Fault Management, Troubleshooting and Customer Care Guidelines
- Location Feed template

Also, the WRIX ID identifies the VNP and HSP. The identifier list of network providers is maintained by the WBA. The ID is a string of variable length containing the operator name and country code. To retrieve this code please contact the WBA PMO.


3.2 WRIX Standards

WRIX (Wireless Roaming Intermediary Exchange) is a set of service specifications published by the Wireless Broadband Alliance to provide a framework for Wi-Fi interconnection, data clearing, financial clearing and the exchange of Wi-Fi location information between operators. The purpose of the service specification is to standardize both technical and business processes between Wi-Fi Roaming Partners.
Figure 3—1  WRIX framework

The WRIX (Wireless Roaming Intermediary Exchange) is comprised of the four specifications listed below. The recommendation is for operators to utilize all four of the specifications. However it is acceptable for operators to utilize the specifications only as guidelines when creating and maintaining Wi-Fi Roaming partnerships.

Specifications:

- WRIX-I: RADIUS Interconnection Specifications
- WRIX-D: Data Clearing Specifications
- WRIX-F: Financial Settlement Specifications
- WRIX-L: Locations Feed Formation and File Exchange Specifications

3.2.1 WRIX-i

The WRIX-I specifies the interconnectivity, authentication and accounting processes between Wi-Fi Roaming Partners. Interconnectivity is established and maintained through either International Private Leased Circuits (IPLCs) or IPSec VPNs. When selecting an interconnectivity method the performance and security considerations must be weighed versus cost. WRIX-I explicitly specifies the use of RADIUS authentication, authorization and accounting (AAA) as the transport of requests between the VNP and the HSP. This enables the support of a vast range of authentication methods including WiSPr, EAP-SIM, EAP-AKA, EAP-TLS, and EAP-TTLS. However the VNP and the HSP must agree bilaterally to which method will be used.
There are three potential parties identified in the WRIX-I Specification:

- **HSP**: Home Service Provider
  - Maintain connectivity linkage
  - On-line proxy routing for RADIUS messages, sent to the correspondent WRIX-i (HSP)
  - Collect raw RADIUS accounting records generated by the proxy routing
  - Mediate raw RADIUS accounting records for wholesale billing
  - Send those records to the WRIX-d (HSP).

- **VNP**: Visited Network Provider
  - Maintain connectivity linkage
  - Proxy routing mediation for RADIUS messages.
  - Receive raw RADIUS accounting records generated by the proxy routing
  - Optionally mediate raw RADIUS accounting records for reconciliation of wholesale billing and send those records to the WRIX-d (HSP).

- **Hub**: An optional intermediary between the HSP and VNP
  - Perform duties on behalf of either the HSP or VNP

Please refer to the WRIX-I Specification document for further information.

### 3.2.2 WRIX-D

The WRIX-D is the data clearing specification of the Wireless Broadband Alliance. Within the specification are clearly defined roles and responsibilities between Wi-Fi Roaming Partners and the timeline of activities. WRIX-D utilizes the records generated from the WRIX-I platform to perform service validation that protects both Wi-Fi Roaming Partners and prevent any potential disputes during financial settlement.

**Figure 3—2 WRIX typical flow**

The process begins by the VNP processing Usage Details Records (UDRs) generated from the WRIX-I RADIUS AAA system to validate, perform exception processing (if necessary) and rate the records. After processing the rates UDRs are transmit to the HSP. The HSP receives and processes the rated UDRs. Upon successful UDR processing the HSP transmits a summary financial data (INPUT SFD) to the VNP as an acknowledgement to record acceptance. The VNP uses the SFD to generate an invoice for the HSP. A hub provider may perform duties on behalf of either the VNP or the HSP.
Please refer to the WRIX-D Specification document for further information.

3.2.3 WRIX-F

WRIX-F is the Financial Settlement Specification of the Wireless Broadband Alliance. By proceeding after the WRIX-D processing, where records are either validated and rated or follow an exception processing method, the WRIX-F ensures that a smooth billing, payment and receivables process occurs every time. The WRIX-F Specification includes detailed reports and a set timeline, which is displayed in this section.

WRIX-F begins by the VPN sending a Summary Financial Document (SFD) to the HSP. The SFD summarizes the traffic usage that occurred on the VPN’s Wi-Fi Network by end-users of the HSP. The SFD is used by the HSP to assist with creating a Net Settlement position between the two Wi-Fi Roaming Partners. Alternatively a hub can be used to either deliver all of the SFDs to each of the HSPs on behalf of the VNP or to receive all of the SFDs from the VNPs on behalf of the HSP.

Once the SFDs are processed the Net Payment Reports (NPRs) are created and shared by both parties. The NPR summarizes the payables and receivables between the Wi-Fi Roaming Partners. Key data elements include settlement type, Net Payment, Net Payee, Net Receiver and currency. A hub provider can act on behalf of an HSP, VNP or both.

Upon acceptance of the NPR between the Wi-Fi Roaming Partners the Wi-Fi operator that is in the Net Payee position will invoice the Net Payer (debtor) based upon the NPR values. In case mismatches are identified in the invoice the Net Payer can raise a dispute. In case of mismatch the disputes rules and limit levels of how to handle the payment are specified in the bilateral agreement. Note: the settlement cannot be carried out in case the invoice not is received. A hub may act of behalf or either or both parties.

Once an invoice is created the debtor pays the Net Amount according to the method as agreed upon in the bilateral agreement. Each party will bear its own bank fees for the payment.
3.2.4 WRIX-L

WRIX-L is the Locations Feed Formation and File Exchange Specifications of the Wireless Broadband Alliance for the sharing of Wi-Fi hotspot Location information. The use of accurate and up-to-date information is crucial to ensure a high quality experience for end-users and maximum the revenue opportunity associated with network usage. Poor quality or out dated location information will result in unsatisfied, frustrated end-customers of the HSP and missed revenue opportunity for the VNP.

The WRIX-L specifies mandatory and operational data. Mandatory data includes critical data elements such as provider information, location information and SSID. This information is provided by the VNP so that the HSP is able to configure the end-user clients to display hotspot Location information and to configure the device to connect to the VNP hotspot once the end-user is within range.

Often a HUB provider will receive WRIX-L data from all VNPs of a HSP and aggregate the data in to one file. This offloads burden from the HSP from receiving data from many sources and provides a single location for all hotspot information.

There are three potential parties identified in the WRIX-L Specification:

HSP: Home Service Provider
- Provides a location file
- Distributes to roaming partners

HSP: Home Service Provider

---

Figure 3—3 WRIX-F timeline

Please refer to the WRIX-F specification document for further information.
• Receives location file
• Uses the location file in connection client software distributed to subscribers

HUB: An optional intermediary between the HSP and VNP
• Act on behalf of either the HSP, VNP or both
• Provides a centralized repository to receive or distribute WRIX-L information

Please refer to the WRIX-L Specification document for further information.

The full suite of the WRIX Specification documents are available on the WBA public website here:

3.3 Wi-Fi Roaming contract templates

We have developed and present here a draft bilateral “remote access” or “roaming” template to assist parties in
developing their relationships to permit their respective subscribers to access each other’s hotspots. We believe
that as Wi-Fi becomes an increasingly important way for individuals to access the Internet that service providers
will desire to provide easy access beyond their own footprint. We have designed this template to assist in that
process. While we anticipate that parties will negotiate individual agreements that suit their circumstances and
needs, this template might provide a sample starting point to assist parties in identifying the multiple business,
operational and legal issues involved. We recognize that systems and legal regimes vary among the membership
and so expect this to be no more than a guide. We have attempted to draft this to provide a reasonable division of
risks while allocating responsibilities as much as possible to the party that should be best able to control or mitigate
a risk factor. To the greatest extent possible, the vocabulary and defined terms used in this template are consistent
with those used elsewhere by WBA. While this template deals with issues that are at times technically, legally and
operationally complex, we have made every effort to draft this template in plain, clear language with a minimum of
“legalese” or technical jargon.

For more information please refer to the templates available at the WBA public website here:

3.4 Interoperability Compliance Program

Traditionally, there have been different methods for implementing Wi-Fi Roaming across the industry. In order to
clarify and standardize these requirements, the WBA created the Interoperability Compliancy Program (ICP). This
program provides operators with a common technical and commercial framework for Wi-Fi Roaming by utilizing the
best practices as defined by the WBA’s WRIX guidelines. The ICP outlines a framework which defines the basic
requirements for roaming and settlement to more advanced models. By doing this the WBA’s Interoperability
Compliance Program facilitates and simplifies the implementation and deployment of Wi-Fi Roaming. The
objectives of the ICP are to:

• Create different tiers of compliance for operators that best describe the capabilities of their networks
• Facilitate the integration of roaming agreements among operators, with the guarantee that operators
follow correctly the WRIX Specifications and roaming guidelines
• Facilitate the interoperability between operators to simplify and accelerate the implementation of Wi-Fi
Roaming
• Support technical integration for roaming agreement, bringing time to market benefits, being
substantially important for new WBA members
• Provide an exchange of Technical and Business Exchange documents to/from a central repository

The WBA provides its operator members a tool called Interoperability Compliancy Checklist. This form is used by
operators to self-evaluate their compliance and roaming capabilities and to share this information with potential
roaming partners. The document allows each company to compare their current capabilities to those of potential
roaming partners and enable them to align their requirements. More than 20 Global operators are now ICP compliant, examples are AT&T, BT, Boingo Wireless, Orange, KT, SKT, among others.

For more information please visit the ICP operator Database on the WBA members extranet: [http://extranet.wballiance.com/apps/org/workgroup/icpopdb](http://extranet.wballiance.com/apps/org/workgroup/icpopdb)

3.5 On-going WBA Work to enhance the Wi-Fi Roaming ecosystem

3.5.1 Next Gen Hotspot Registry

As part of the WBA’s continuing efforts to enable Wi-Fi Roaming across NGH networks, the WBA has begun work on a new global registry which will allow service providers to exchange information more effectively with NGH network operators. The goal is for the WBA to create and maintain a database of Service Provider information needed by network operators and to deliver the information via a mechanized exchange. The definition phase of this project is currently underway.

3.5.2 WBA-GSMA joint taskforces focusing on Wi-Fi Roaming

Background – In the first joint GSMA WBA white paper [1] on Wi-Fi Roaming the need to interwork between the RADIUS and Diameter protocols were identified as an important issue that needed to be addressed by the two industry bodies. This paper is the result of the GSMA and WBA jointly looking at the problem and coming up with a set of recommendations that address the needs of the GSMA and WBA in looking at the problem of RADIUS and Diameter interworking.

Current Scope – The initial scope is limited to RADIUS and Diameter attributes needed to support interworking between 3GPP and WBA Wi-Fi networks. In particular those required to support the specific use cases detailed in this paper, such as Voice over IMS over Wi-Fi and data offload. This includes the relevant billing and authentication message sequences. This is limited to the identified and relevant interfaces based on the principles of the 3GPP architecture. Specifically for this work iteration, the team is addressing only RADIUS to Diameter on the SWa interface.

For more information on how to get involved please contact: pmo@wballiance.com
4. Setting the scene – industry trends

In this section are the results of an industry survey regarding Wi-Fi Roaming. More than 12 global operators have provided their inputs.

**1. Please select your Operator category**

- 20% Mobile Operator
- 20% Cable Operator
- 30% Integrated Operator (Mobile + Fixed)
- 30% Wi-Fi network operator

**2. In which region are you based?**

- 50% Europe
- 30% Asia Pacific
- 20% North America
3. Do you have Wi-Fi Roaming agreements in place?

4. How are currently your roaming capabilities implemented (multiple responses are allowed)?

<table>
<thead>
<tr>
<th>Number</th>
<th>Interconnection via roaming hub</th>
<th>Interconnection direct to partners</th>
<th>Data clearing by roaming hub</th>
<th>Data clearing direct with partners</th>
<th>Financial settlement by roaming hub</th>
<th>Financial settlement direct with partners</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On the Cellular business</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>On the Wi-Fi business</td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
5. What are the main drivers for your Wi-Fi Roaming strategy (multiple responses are allowed)?

- User convenience / retention: 80.0%
- Usage data revenue: 70.0%
- Enhanced coverage: 70.0%
- Enhanced bandwidth: 50.0%
- Indoor coverage abroad: 50.0%
- Aggregation: 30.0%
- Wi-Fi/mobile integration (HetNet): 20.0%
- Community Wi-Fi hotspots: 20.0%

(Note that more than one answer was allowed)

6. Which future Wi-Fi Roaming services you consider most important (multiple responses are allowed)?

- Enterprise services: 20.0%
- Quality of Service management: 30.0%
- Location based services roaming: 50.0%
- Seamless and secure authentication: 60.0%
- Wi-Fi offload wholesale (ROI): 70.0%
- Wi-Fi calling: 80.0%
- Wi-Fi data roaming: 90.0%

(Note that more than one answer was allowed)
7. What barriers do you still see in order to deploy NGH, the prime technology to enable Wi-Fi Roaming (multiple responses are allowed)?

- Shortage of compliant devices: 77.8%
- Insufficient market scale: 33.3%
- Shortage of available infrastructure: 33.3%
- Lack of clear ROI: 33.3%
- Cost of deployment: 33.3%

(Note that more than one answer was allowed)

8. What is the % of your network that currently support Passpoint?

- Less than 10%: 40%
- Between 10%-40%: 50%
- More than 40%: 10%
5. **Business models overview**

1. Which type of retail plan do you offer (or plan to)?

- Paid Cellular + Paid Wi-Fi Bundle: 0%
- Paid Cellular + Free Wi-Fi Bundle: 17%
- Paid Wi-Fi Only: 33%
- Free Wi-Fi Only: 33%
- No offer with Wi-Fi: 17%
2a. For retail, what is your current (or planned) pricing model(s) for Wi-Fi Roaming?

- **Flat rate unlimited**: 100.0%
- **Flat rate capped**: 16.7%
- **Pay-per-use per Mb/Gb**: 33.3%
- **Pay-per-use per Min/Hour**: 33.3%
- **Pay-per-use Week/Day**: 16.7%

(Note that more than one answer was allowed)

2a.1 For retail, do you charge per additional Mb outside any of the plans?

- **Yes**: 29%
- **No**: 71%
2b. For wholesale, what is your current (or planned) pricing model for Wi-Fi Roaming?

(Note that more than one answer was allowed)

2b.1 For wholesale, how does your average Wi-Fi and Cellular (3G, LTE) roaming price range compare?

- Equal (below 20% difference): 20%
- Wi-Fi at least 20% MORE expensive: 80%
- Wi-Fi at least 20% LESS expensive: 0%
2b.2 For wholesale, on the minimum contracted package available to roaming partners, how does Wi-Fi and Cellular (3G, LTE) roaming price range compare?

- Equal (below 20% difference) - 25%
- Wi-Fi at least 20% MORE expensive
- Wi-Fi at least 20% LESS expensive

3. On average how does the Wi-Fi roaming and cellular roaming data usage by your customers compare?

- Wi-Fi less than 5% - 75%
- Wi-Fi between 5%-15%
- Wi-Fi more than 15% - 25%
4. During the last year how did your Wi-Fi Roaming business evolved?

- Up to 10% of growth in terms of revenue: 20%
- Between 10%-25%: 20%
- Between 25%-50%: 20%
- More than 50%: 20%
- (optional) % of growth in terms of total data usage: 20%

5. What are the main users' targets for your Wi-Fi Roaming business?

- Inbound international tourists: 87.5%
- Inbound business users: 87.5%
- Outbound international tourists: 87.5%
- Outbound business users: 62.5%

(Note that more than one answer was allowed)
6. How do you currently inform your roaming customers about Wi-Fi Roaming service availability?

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website information</td>
<td>85.7%</td>
</tr>
<tr>
<td>Local advertisement at partner's hotspot</td>
<td>28.6%</td>
</tr>
<tr>
<td>Phone 3rd party (e.g. aggregator) client</td>
<td>14.3%</td>
</tr>
<tr>
<td>SMS when arriving the country</td>
<td>14.3%</td>
</tr>
<tr>
<td>SMS when signing up for plan</td>
<td>14.3%</td>
</tr>
<tr>
<td>No advertisement</td>
<td>0.0%</td>
</tr>
<tr>
<td>Phone proprietary client</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

(Note that more than one answer was allowed)
6. Use cases/case studies

The following use cases were provided by WBA members and range from different operator types, architecture options, business models and current industry focus.

6.1 NTT DOCOMO innovative Wi-Fi Roaming service

6.1.1 Context

NTT DOCOMO (DCM) launched Wi-Fi Roaming as a bundled service within an unlimited cellular roaming retail plan, with expectation of cost efficiency by data offload and the enhancement of user experience.

In the first few years, DCM was rolling out its Wi-Fi service areas trying to cover the large part of the areas where cellular roaming service was provided. However, the usage at the countries where there were not enough hotspots has been kept lower than expected. Currently DCM is focusing on important countries where a large number of DCM's users visit and sufficient access points are available.

In terms of user experience, DCM introduced SIM authentication for its domestic Wi-Fi service and inbound roaming in 2013 and for outbound in 2014. In domestic usage, the traffic has increased by seven times and the number of users has increased by 10 times in a year (See Figure 6—1).

In outbound usage, more than 75% of registrations are by SIM authentication. Currently DCM is planning to introduce Passpoint™, and the Radius server and the handset released in 2015 summer already support Passpoint™.

![Figure 6—1 Users and data traffic after the introduction of SIM authentication.](image)

6.1.2 Implementation

DCM adopts direct interconnection with operators. Under certain conditions, DCM also chooses the interconnection via a roaming hub for the purpose of better efficiency of both work and cost for making a new connection.
DCM utilizes the WBA bi-lateral agreement template when making a contract with other members, which shorten the time required for closing a contract. TED and CBED are also the standard format for exchanging technical and commercial information, which also make it easy and clear to communicate between operators.

6.1.3 Business model

DCM’s retail plan with unlimited data traffic has the maximum charge. Therefore Wi-Fi is substantially free to heavy users whose charge reaches to maximum and Wi-Fi provides them with great user experience.

On the other hand, for light users Wi-Fi is less attractive since it requires more procedures to use and its coverage area is not as broad as that of cellular. DCM is seeking to provide friendlier, reasonable and attractive retail plan to such light users.

6.1.4 Future plans & development

As the wholesale rate of Wi-Fi is generally lower than that of cellular, DCM stays positive to utilize Wi-Fi Roaming as the means of data offload. DCM is currently reviewing its service areas and seeking operators whose coverage area is nationwide and dominant in specific countries. However such operators still remain in a state of shortage. From an industry perspective, it is desired that such operators increase.

After a large number of hotspots was provided (see Figure 6—2) and SIM authentication was introduced, the usage of DCM’s domestic Wi-Fi network has rapidly increased. DCM also intends to increase the usage of international roaming by upgrading its service offer. DCM believes that the SIM authentication and Passpoint™ will be the strong drivers.

![Figure 6—2 The number of DCM’s hotspots](image)

6.2 Comcast Secure Wi-Fi Roaming with Liberty Global

In September 2014, Comcast and Liberty Global, the two leading cable MSOs (Multi Service operators) in the U.S. and Europe respectively, formed an agreement to offer international Wi-Fi Roaming connectivity to their subscribers.

Comcast has more than 10 million Wi-Fi hotspots across the US while Liberty Global currently has over 6 million Wi-Fi home spots in various European countries like Belgium, the UK, the Netherlands, Ireland, Poland and Switzerland, which will grow to 12 million by mid-2016.
Comcast subscribers will be able to access high-speed wireless broadband using Liberty Global’s Wi-Fi network while in Europe. Similarly, Liberty Global’s subscribers will be able to access the Internet using Comcast’s Wi-Fi hotspots while visiting the US.

The cross-continent Wi-Fi integration will provide an alternative to traditional 3G/4G data services, enabling customers to connect to Wi-Fi securely, protecting the privacy and security of their personal information, and to conserve use on their wireless data plans while traveling abroad.

6.2.1 Implementation

A fundamental challenge faced the implementation at the beginning. Comcast operated a traditional open hotspot network, while Liberty Global utilized secure protocols for authentication. Comcast customers were not equipped with the necessary tools to connect to secure networks and Liberty Global customers were not set up to connect to open partner networks.

Thus, in the original scope of the effort, it was proposed that Liberty Global customers could be enabled to access Comcast’s open Wi-Fi network using a client connection manager and WISPr 1.0. In parallel Comcast would initiate development to add a secure functionality to its network, including a roadmap to use standard WPA2-Enterprise / 802.1x protocols initially, with an evolution to Passpoint™.

Although proven technically feasible by introducing a Liberty Global WISPr App, it was determined that introducing an open SSID solution to the Liberty Global customer base would be too disruptive to the user experience already established. Plans for Liberty Global to utilize Comcast’s open network were halted, and all focus turned to establishing means for both parties to use secure networks. Comcast began deploying secure functionality in certain environments, with plans to extend the functionality across the entire network in 2016.

Comcast also added security features to its XFINITY Wi-Fi App that can be used to manage the distribution and provisioning of secure profiles, as well as connections to various disparate SSIDs used across various third party networks.

Parallel to this, Liberty Global initiated their planned App development in preparation for launching international and transatlantic Wi-Fi Roaming. This connectivity app will provide capabilities to easily ‘on-board’, profile management, SSID prioritization, hotspot finder, analytics and always-best-connected capabilities. Although it is technically possible to setup Liberty Global clients manually via FAQs for access, it was determined that this Wi-Fi connectivity App should be launched in parallel, to mask the complexities to the user pre-support of Hotspot 2.0 Release 2 and an online sign-up (OSU) deployment.

6.2.2 Technical approach

Comcast and Liberty Global agreed on a technical approach that required the Home Service Provider to provision, authenticate, and authorize their own customers when visiting other networks to avoid having the Visited Network Provider get involved with the specifics of the technical architecture and methods being used by the home provider.

Comcast and Liberty Global devised an interconnect specification based upon WBA’s WRIX-i recommendations. This reciprocal solution tunnels all Wi-Fi sessions onto the local VNP Wireless Access Gateway (WAG) where the session is established once 802.1x validation is confirmed against the remote HSP RADIUS platform. All RADIUS authentication and corresponding accounting records are transported across encrypted VPNs where standard attributes and Vendor Specific Attributes (VSAs) are also documented within the interconnect specification.

Although technically possible with the required information available, WRIX-d and WRIX-f were not implemented as no data or financial clearing was deemed necessary at this stage.
This approach also eliminates the need for the Visited Network Provider to view or handle any private personally identifiable data for the user. The approach uses RADIUS-Proxy and standard RADIUS messages to securely authenticate and authorize users when they attempt to connect to the visited network provider’s hotspots.

The entire solution is based on 802.1x and RADIUS standards and is agnostic to which EAP protocol is utilized. Liberty Global and Comcast standardized on EAP-TTLS for non SIM devices for launch, and are able to support any inner authentication method for inbound visitors by proxying the EAP traffic to the home AAA.

**Call setup**

A Liberty Global or Comcast customer device will include a visible outer identity of the agreed realm / NAI to identify itself to the VNP when attempting to connect to a Wi-Fi hotspot. The VNP RADIUS server uses this outer identity to route the EAP–authentication packets back to the HSP network without decrypting the packets. This methodology helps both companies meet certain privacy requirements since the visited AAA never sees any information about the user other than the outer identity, MAC Address, and Chargeable User Identity when a session is established.

The HSP AAA authorizes the user and either sends and ACCEPT or REJECT to the visited AAA. The device and user are treated accordingly. On ACCEPT the device is allowed to establish a session that is anchored on the local VNP’s WAG.

For simplicity and manageability, Liberty Global has implemented their own geo-resilient hub for all external partners to interconnect with which masks Liberty Global’s internal Wi-Fi networks by using its internal Wi-Fi interconnect mesh solution.

The Liberty Global Wi-Fi hub’s sole purpose is to process all external RADIUS Wi-Fi packets to the intended destination as quickly as possible. The hub directs RADIUS authentication requests, challenges and accounting records to the intended internal Liberty Global affiliate destination, controlled by realms or NAIs when supporting HS2.0 capable Wi-Fi networks. The advantages of deploying the Liberty Global hub solution are as follows:

- Central mediation and connect rules
- Data cleansing and manipulation
- Optimised to process many trans/sec quickly
- Future data clearing and settlements when required
- Controlling anonymity of customer data
- Central hub functionality avoiding replication of development on all Liberty Global RADIUS server farms
- Masking the complexity of Liberty Global affiliate Wi-Fi networks to all external partners by providing one point of interconnect therefore avoiding Comcast having to build multiple dedicated interconnects
- Once the internal mesh interconnect is functional then connection to hub is achieved automatically (configuration of new realms directed to hub addresses needed)

This approach allows Comcast to interface with one Liberty Global Wi-Fi interconnect allowing subscribers automatic access to the Wi-Fi footprint of all Liberty Global affiliates throughout Europe consisting of Telenet, Ziggo, UPC, UMKBW and Virgin Media. The reverse is true where all Liberty Global subscribers will gain access to Comcast’s Wi-Fi footprint with all validation and accounting packets being routed via the hub and then automatically onto the internal Liberty Global mesh for validation against the HSP’s RADIUS estate.

**Call flow**

All traffic is handled locally using the visited network’s Access Point and Wireless Access Gateway.
Accounting

A Chargeable User Identity is used to track usage. The visited AAA uses the Chargeable User Identity to track accounting start / stop events and maintain a record of the customer’s data usage. This information is then transferred to the home provider and can be used for reconciliation and settlement.

This capability is also used to anonymize customers’ data where the VNP supports CUI when returned within the access-accept packet from the HSP. The HSP initiates CUI within the access-accept packet for their own subscribers. This ensures that all users’ accounting data owned by the HSP is anonymized by hashing the username used in all records.

6.2.3 Business model

Comcast could include access to the Liberty Global footprint as part of its standard XFINITY Wi-Fi service which is included with XFINITY Internet subscriptions at no additional charge, or potentially as part of a premium Wi-Fi package that would include among other value added features, the ability to access Wi-Fi in a number of premium and international locations. Comcast customers could add this premium Wi-Fi package to their overall services which would be billed as an additional line item on the customers’ monthly invoice.

To fulfil the service, Comcast will enable a separate secure profile that contains the required connection and authentication parameters to enable a customer with the profile to connect to the visited Wi-Fi network. When the user connects to the visited network, the user credentials will be proxied to Comcast for authentication. Comcast will then check the customer entitlements to validate that the user is allowed to access the visited network, and if allowed, Comcast will return an authorization to the visited network provider and access will be granted.

Liberty Global currently plans to announce this transatlantic expansion of Wi-Fi footprint through its partnership with Comcast at no extra cost to their subscribers. Due to the architecture and call flow used, with the WAG acting as the policy enforcement point, future tiers of service could be easily supported where features such as metered services, such as Gold/Silver/Bronze tiers or pay-as-you-go, could easily be implemented.

6.2.4 Future plans & development

Comcast and Liberty Global continue to expand their Wi-Fi footprints to address customer demand for wireless broadband services in the places users most want to connect. This includes partnerships to increase the number of Wi-Fi locations available internationally, for traveling customers that desire an alternative to international 3G/4G roaming. Both MSOs plan to increase awareness of the roaming access through various communications tactics and via their respective Wi-Fi apps for iOS and Android.

The implementation has revealed a number of interesting lessons, and questions that remain to be addressed:

The method to enrol and provision visiting users on-the-fly remains unclear, even with Passpoint™ Release 2, particularly for operators that do not have an open network as part of their construct. This is an important consideration for the industry, particularly as some legacy and new Wi-Fi operators may elect not to support open networks or open SSIDs on their platforms. The current solution is based on the service provider pre-provisioning customer devices before they can access the secure Wi-Fi network.

Generally, provisioning is complicated for end-users and the installation of profiles is not always obvious to the user. The method of distributing profiles to users in a simple manner requires additional work create an optimized experience.

A single interface point and proxy capabilities for network operators that operate multiple distinct and disparate networks needs to be considered to simplify interconnect with other carriers.
The decision of using direct network-to-network integration, versus the use of a hub / clearinghouse intermediary has bearing on accounting, mediation and settlement development, even when using the WRIX standards, and should be considered carefully when designing an interconnect architecture.

6.3 AT&T business case template

AT&T shared a business case template which can be used by operators at large to simulate potential roaming revenues. An example, based on a mid-size MNO with 2M mobile subscribers, is provided below:

### Inputs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Mobile Subscribers</td>
<td>2,000,000</td>
</tr>
<tr>
<td>International Mobility Subscriber Penetration</td>
<td>2%</td>
</tr>
<tr>
<td>International Plan Subscriber Increase From Adding Wi-Fi Hub Service</td>
<td>3%</td>
</tr>
<tr>
<td>International Mobility Plan Price per unit</td>
<td>$30.00 per month per sub</td>
</tr>
<tr>
<td>Percent of International Rate Plan Subscribers Using Wi-Fi Hub Service</td>
<td>5.0%</td>
</tr>
<tr>
<td>Average Wi-Fi Data usage per subscriber per day</td>
<td>18 MB</td>
</tr>
<tr>
<td>Cost per MB</td>
<td>$0.06 MB</td>
</tr>
<tr>
<td>Days of Use per month per sub</td>
<td>8 Days</td>
</tr>
</tbody>
</table>

### One Time Costs

<table>
<thead>
<tr>
<th>Cost Category</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>$10,000</td>
</tr>
<tr>
<td>Client Cost - iOS</td>
<td>$20,000</td>
</tr>
<tr>
<td>Client Cost - Android</td>
<td>$20,000</td>
</tr>
<tr>
<td>Operations Expense (monthly for first 1,000 Subs)</td>
<td>$5,000</td>
</tr>
</tbody>
</table>

### Revenue Summary

<table>
<thead>
<tr>
<th>Revenue Category</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Number of Mobile Subscribers</td>
<td>2,000,000</td>
</tr>
<tr>
<td>Total International Rate Plan Subscribers Before WiFi Offer</td>
<td>40,000</td>
</tr>
<tr>
<td>Incremental International Rate Plan Subs Due to Wi-Fi</td>
<td>1,200</td>
</tr>
<tr>
<td>Total International Rate Plan Subscribers After WiFi Offer</td>
<td>41,200</td>
</tr>
<tr>
<td><strong>Incremental Revenue Due to Wi-Fi Offer (monthly)</strong></td>
<td><strong>$36,000</strong></td>
</tr>
</tbody>
</table>

### Cost Summary

<table>
<thead>
<tr>
<th>Cost Category</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Time Installation Costs</td>
<td>$50,000</td>
</tr>
<tr>
<td>Operations Cost (monthly)</td>
<td>$8,000</td>
</tr>
<tr>
<td>Preferred WiFi Bandwidth Cost (monthly)</td>
<td>$15,821</td>
</tr>
<tr>
<td><strong>Total Expense (monthly)</strong></td>
<td><strong>$23,821</strong></td>
</tr>
</tbody>
</table>
6.4 Boingo Wi-Fi Roaming & Passpoint™ overview

Boingo Wireless has been actively involved in deployment and aggregation of several Wi-Fi networks around the world since 2001. In 2010 Boingo enhanced its footprint by allowing all its users to discover and connect to free public hotspots, it also started building a crowdsourcing database that would crowdsource various Wi-Fi hotspots as and when users connect and then categorize these hotspots based on quality.

Boingo had started envisioning about “Carrier grade Wi-Fi” since then, as a means to allow operators to offload mobile data onto reliable crowdsourced Wi-Fi hotspots. Given all this experience and history with Wi-Fi hotspots, Boingo was in a perfect position to jump onto and lead Passpoint™ technologies, which it started in early 2012 by getting onto Hotspot 2.0. Already being a member as well as on the Board of Directors, Boingo started working closely with WBA participating in several Technical, Marketing and Business workgroups contributing to standards, writing white papers and taking the initiative to collaborate Passpoint™ activities.

Boingo currently has Roaming agreements with more than 140 operators in more than 100 countries, including offloading agreements with 5 of the world’s top 10 mobile operators and 3 out of the 4 of the Tier one U.S. operators, with ticker Wi-Fi. An overview of Boingo’s roaming network is provided below:

### Roaming Network

- **700,000+ Commercial locations**
- **500,000+ Crowdsourced hotspots**
- **140+ Operator partners**
- **100+ Countries**
- **6 Continents**

Airports  Universities  Military  Transit  Restaurants  Malls  Stadiums  Public Spaces

**Figure 6—3 Boingo Roaming network overview**

Boingo Next Generation Hotspot Architecture

This section describes Boingo’s commercial Passpoint™ network Architecture. The network consists of several components including a Wireless LAN access controller with Hotspot 2.0 capable access points, ANQP server, Boingo RADIUS AAA server with access to user database and DHCP server. The venues where Passpoint™
networks are getting broadcasted contain the access points, WLAN controller, DHCP server and ANQP server. The controllers and access points have been upgraded to add 802.11u support, so a Passpoint™ certified device can exchange beacons, probe message and ANQP frames prior to connecting to the network. All Passpoint™ supported Boingo venues broadcast both Boingo Hotspot (open Wi-Fi hotspot) as well as Passpoint™ secure hotspots. The open Wi-Fi hotspot is for backward compatibility and works with all non Passpoint™ devices and the Passpoint™ secure hotspot allows seamless connectivity for Passpoint™ certified devices. Boingo’s AAA servers have been enhanced to provide support for EAP protocols including EAP-SIM, EAP-AKA, EAP-AKA’, EAP-TLS and EAP-TTLS.

Boingo supports username password style of authentication and hence EAP-TTLS is the chosen method. Boingo profiles are configured with the appropriate TTLS attributes. Establishing a secure connection with Boingo networks require two steps:

a. Establishing a secure tunnel between the device and the authentication server which also includes validating the server identity: Boingo AAA server has been configured with a certificate (obtained from a Certificate Authority), this allows the server to authenticate itself so that the mobile device will not end up talking to a Rogue Passpoint™ network. When the device starts a EAP connect request, the server validates itself by sending the certificate details. The device verifies the certificate against its trust root CAs, once confirmed a secure tunnel shall be established.

b. Sending credentials to the server for client side authentication and authorization: The client shall transport username and password in the tunnel for authentication. The AAA server upon receiving the credentials forwards the request to BRM system that shall check the credentials in the database for a successful authentication. The system also further checks for authorization to make sure that only
allowed account types shall gain access. Boingo supports several account types based on region, usage etc. Since Passpoint™ connections are established in the background without user’s intervention, we make sure that only valid accounts get access to the network and other account types shall be denied access (not authorized). Note that all the above steps shall happen in succession without user’s interaction.

The user does not need to use any app or manually select a Wi-Fi network, making the entire connecting experience seamless. As long as the device Wi-Fi radio is turned on, Passpoint™ connections shall be initiated when in venue.

**Figure 6—5  Boingo Passpoint™ connection sequence flow**

**Passpoint™ commercial ecosystem**

It’s been about a year since Boingo started deploying Passpoint™ networks, in this section we shall talk about the commercial deployment data. Commercially Boingo deployed its first Passpoint™ network back in September 2013 at Chicago O’Hare International airport. This location was chosen, as Boingo owns this location and was also one of the first airport that was part of the acquisition of Concourse communications back in 2006. The Network deployment was based on WBA Phase 1 and Phase 2 trials, in an attempt to open up a live commercial location for operators and users to use the location as a test bed. Adding onto that Boingo realized that it was time for Passpoint™ deployments to move out of Labs and into a live commercial location, taking the first initiative to get into unchartered waters.

In Feb 2014, Boingo made a strategic decision to bring Passpoint™ capabilities into 21 of its commercial airports nationwide spread across the nation. This time Boingo took another step of opening up all these locations for its select customers to experience the seamless connectivity. Boingo launched an NGH trial program and to truly experience the seamless experience, the company developed a profile provisioning portal (now live in production https://Passpoint™.boingo.com). This portal allowed the users simply to key in their credentials and Boingo’s systems would then simply provision the device with a Passpoint™ profile. Once the user walks into a Passpoint™ broadcasting venue, the device would then automatically choose and connect to the network without user’s intervention.
As of today the usage and data on Passpoint™ networks is definitely a miniscule compared to the global Wi-Fi usage, but it is an indication that Passpoint™ is starting to grow in every aspect and the seamless connection experience is making users to prefer and connect to Passpoint™ networks, over non secure open Wi-Fi Ecosystem.

Figure 6—6 displays the various industry players involved in the Passpoint™ ecosystem. Venues are where the Passpoint™ networks get broadcasted and users can connect.

One of the main goal of venues is to gain insight about the users and provide a valuable service and potentially improving the service. Then there are the Infrastructure Vendors who provide the network connectivity and communication. The next set of players are Wireless Carriers who are constantly looking for means to offload mobile data onto Wi-Fi, where possible. There are plenty of Wi-Fi hotspots and service providers available, but very few have “carrier grade Wi-Fi” a quality that ensures certain bandwidth and a secure offload mechanism. Last, but not the least are device vendors. Passpoint™ devices play a major role in connecting the users to the Passpoint™ networks, and own the presentation of a seamless experience to users. Rather than trying to be a jack of all trades, Boingo is focusing on being a master of one - venues.

Figure 6—6 Boingo NGH ecosystem

Boingo’s focus is on the Venues and providing them with what they need to be successful. One of the intriguing questions that Passpoint™ poses is how the players within the ecosystem shall co-exist. With devices hopping between cellular networks and various hotspots, new agreements and relationships will inevitably emerge; but exactly what this landscape will look like remains to be seen. Every player in the ecosystem can own users, the venues provide several services including location, advertising, etc. infrastructure vendors facilitate some of these services by being part of and having agreements with the venues. Carriers and operators usually have direct relationship with the users as they are responsible for providing the wireless service. Users buy and own devices and hence device vendors control the presentation of the content to the users.

Finally and most importantly, monetization is a key drive that is making every player in the ecosystem to participate and thrive on. All monetization mechanisms that exist in conventional Wi-Fi also exist in Passpoint™, with an improved user experience. Additionally, Passpoint™ provides new techniques that the ecosystem players can take advantage of for monetization.

The best example is the introduction of On-Line Signup (OLS) server. It allows the Passpoint™ network to enable on the spot registration automatically triggered without user’s intervention. When a user walks into a venue with a Passpoint™ device, the network can detect the user’s presence and automatically and proactively present services to the user, creating monetization opportunities right there.
Deployment and challenges

There have been challenges that Boingo has been facing since the first deployment of Passpoint™ network and has overcome them by providing appropriate solutions. When the first network was deployed in Chicago O’Hare International airport, Boingo subscribers started to connect to the network by creating a profile and this would trigger automatic connections each time the user visits the network. The connections happened irrespective of the subscription plan the user had, and in some cases this caused a connect charge without user knowing about it. Boingo realized this immediately and updated its billing BRM systems to allow only those Passpoint™ connections that would not trigger a charge to the user.

The next issue was a lack of profile provisioning mechanism on supported Passpoint™ devices.

Figure 6—7 Profile provisioning

Passpoint™ network deployments were based off of Wi-Fi Alliance Hotspot 2.0 Release1 Technical Specification and in turn were based off of WBA Phase1 and Phase2 trials. Both these phases did not have a mechanism to securely and seamlessly provision Passpoint™ profiles to devices. To overcome this problem and to provide true seamless connectivity to the user, Boingo developed a provisioning portal https://Passpoint™.boingo.com that would allow its subscribers to download and configure Passpoint™ profiles onto supported devices in a secure manner.
The portal allows user to walk through simple self-explanatory steps to download a profile:

Figure 6—8  Profile provisioning steps
7. Conclusion & call for action

The roaming-related work accomplished by the WBA and the collective strengths of its members have been instrumental in the growth of global Wi-Fi Roaming. The WBA facilitates access to a quality global Wi-Fi footprint, a huge subscriber base, unique expertise and track record, and award-winning technical enablers. The WBA also provides opportunities to engage global partners and influence the industry. It offers a significant value proposition to all wireless broadband operators and ecosystem partners interested in enabling a seamless Wi-Fi experience, delivering global Wi-Fi Roaming and integrating Wi-Fi across mobile technologies for the benefit of end-users.

As mobile operators have learned over the last 25 years of operating mobile networks, roaming is an excellent solution to obtaining coverage, since it is not feasible to construct your own network everywhere that your subscribers may wish to obtain service. Although it may be feasible in some areas for the operator to build their own network with traditional RAN or Wi-Fi, this option is not available in all locations. Roaming, in contrast, multiplies the home operator’s coverage outside of their home market, without requiring capital investment in the build-out.

Operators now want to (a) employ Wi-Fi to reduce their costs and (b) use roaming to increase their coverage. In combination, Wi-Fi has become a roaming network (“Wi-Fi Roaming”) to complement the operator’s own 3G&4G network. operators can use Wi-Fi networks as roaming partners, just as they do other mobile operators’ networks today. In using NGH, operators can use the same technology and processes to roam using Wi-Fi, without requiring the operator to change the way it operates. Just like GSM standardized roaming across cellular operators, we envision NGH providing a Wi-Fi Roaming system that is similarly integrated and available across GSM operators.

7.1 Operators with Wi-Fi networks

Operators who own public Wi-Fi networks (whether as a stand-alone business or as a key complement to their wireless and/or broadband networks) can benefit from many advantages through membership of the WBA. It is an ideal forum to enhance their global coverage and inbound/outbound roaming opportunities for their users. As well as extending technical enablers and providing templates for operators, the WBA has developed common user experience guidelines to make it easier for end-users to locate, identify and connect to hotspots while roaming.

7.2 Operators without Wi-Fi networks

The WBA also assists operators who are focused on mobile and/or broadband technologies and who may not own any hotspots, to leverage the enablers created by the WBA, and the global Wi-Fi footprint of its members, in order to offer Wi-Fi Roaming and mobile data offload to their users. In doing so, the WBA helps mobile operators to address the challenges and opportunities created by an explosive growth in mobile data usage and the increasing availability of dual-mode 3G/Wi-Fi devices such as smartphones, laptops, tablets, game consoles, cameras etc. Similarly, it helps fixed broadband operators to offer seamless Wi-Fi Roaming to their subscribers. The key enabler created by the WBA to facilitate intra-technology roaming and data offload is the Wireless Roaming Intermediary eXchange (WRIX) framework.

All in all, Wi-Fi Roaming services enable network operators to provide authenticated access to their network without owning the user relationship. This section will provide an overview of the strategies that can be employed, as well as key considerations before entering into a Wi-Fi Roaming relationship. The network owner can enter into a roaming agreement with a connection aggregator with potentially very little effort by making an agreement with a Wi-Fi aggregator who takes care of authentication and billing. Taking a bigger part of the infrastructure might make financial and strategic sense for some network operators but not for others. operators should also take into account the fact that successful roaming agreements will increase the amount of traffic on their networks.

NGH is poised to assist the mobile industry in solving a significant problem – delivering much needed capacity while lowering the cost of service. With strong support from all stakeholders, NGH has emerged as an important part of the solution to satisfy subscribers’ demand for mobile data.
For further information on Wi-Fi Roaming, NGH and its applicability, please contact the Wireless Broadband Alliance (pmo@wballiance.com) for on-going status and development updates of these topics.
References - Summary

Wi-Fi Roaming Technical Guidelines are available at the WBA public website:


Roaming Contract Template available at the WBA public website:


Full suite of the WRiX Specification documents are available at the WBA public website:


WBA current work areas (Programs & Projects) targeting Wi-Fi Roaming, Next Generation Hotspot and other relevant areas can be consulted here:

http://www.wballiance.com/key-activites/current-work-areas/

Clarification about WBA public resource centre access – Any individual can create its own username/password to access the public resource centre in a convenient way using this link:

http://www.wballiance.com/resource-center/login/

For more information please contact the WBA PMO at pmo@wballiance.com
**Acronyms and Abbreviations**

<table>
<thead>
<tr>
<th>Term or Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the form of user credentials (typically user@domain and password) service authorization, and session accounting details between devices and networks in a real-time manner.</td>
</tr>
<tr>
<td>802.11i</td>
<td>Protocol for air interface encryption referenced by HOTSPOT 2.0 specifications.</td>
</tr>
<tr>
<td>802.11u</td>
<td>IEEE standard ratified in 2010. Section of the IEEE 802.11u standard deals with automatic network discovery and selection and part of HOTSPOT 2.0 ANQP procedures.</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement, is defined in RFC 4187.</td>
</tr>
<tr>
<td>ANQP</td>
<td>&quot;Access Network Query Protocol.&quot; Part of the 802.11u IEEE standard referenced in the Passpoint™ specification used by the 2011 NGH Trials.</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point.</td>
</tr>
<tr>
<td>APC</td>
<td>Access Point Controller.</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol, is defined in RFC 3748.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>HNP</td>
<td>Home Network Provider.</td>
</tr>
<tr>
<td>Hotspot 2.0</td>
<td>Hotspot 2.0 (HOTSPOT 2.0) - A set of capabilities, including enhanced discovery that enable a 3G cellular or better experience for Wi-Fi users.</td>
</tr>
<tr>
<td>HSP</td>
<td>Home Service Provider.</td>
</tr>
<tr>
<td>IE</td>
<td>Information Element.</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers.</td>
</tr>
<tr>
<td>Inbound Roaming</td>
<td>When a roaming partner’s customer uses home Wi-Fi network.</td>
</tr>
<tr>
<td>IPSec tunnel</td>
<td>IPSec (IP security) is a standard for securing Internet Protocol (IP) communications by encrypting and/or authenticating all IP packets. IPSec provides security at the network layer.</td>
</tr>
<tr>
<td>MO</td>
<td>Management object.</td>
</tr>
<tr>
<td>NAI</td>
<td>Network Access Identifier.</td>
</tr>
<tr>
<td>NGH</td>
<td>Next Generation Hotspot.</td>
</tr>
<tr>
<td>OCSP</td>
<td>Online certificate status protocol.</td>
</tr>
<tr>
<td>OI</td>
<td>Organization Identifier.</td>
</tr>
<tr>
<td>OSU</td>
<td>Online sign up [server].</td>
</tr>
<tr>
<td>Outbound Roaming</td>
<td>When a home customer uses another roaming partner’s Wi-Fi network.</td>
</tr>
<tr>
<td>Passpoint™™</td>
<td>Program in the Wi-Fi Alliance to address Wi-Fi ease-of-use that will deliver HOTSPOT 2.0-certified equipment. See the HOTSPOT 2.0 MRD and HOTSPOT 2.0 specification.</td>
</tr>
<tr>
<td>PLMN</td>
<td>Public land mobile network.</td>
</tr>
<tr>
<td>Term or Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>PMO</td>
<td>WBA Program Management Office</td>
</tr>
<tr>
<td>PPS</td>
<td>PerProviderSubscription [MO]</td>
</tr>
<tr>
<td>Radius</td>
<td>Remote Access Dial-Up User Service. A standard technology used by many major corporations to protect access to wireless networks</td>
</tr>
<tr>
<td>RAN</td>
<td>Radio Access Network</td>
</tr>
<tr>
<td>RSN</td>
<td>Robust Security Network</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module. A specially programmed microchip that inserts into a Global System for Mobile Communications (GSM)-compatible mobile device. The SIM encrypts transmissions and identifies the user to the mobile network. Also called a SIM card.</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security, defined in RFC 5216</td>
</tr>
<tr>
<td>TTLS</td>
<td>Tunneled Transport Layer Security, is an EAP protocol that extends TLS</td>
</tr>
<tr>
<td>UDR</td>
<td>Usage Data Record</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>VNP</td>
<td>Visited Network Provider</td>
</tr>
<tr>
<td>VSP</td>
<td>Visited Service Provider</td>
</tr>
<tr>
<td>WRIX</td>
<td>Wireless Roaming Intermediary eXchange – a modular set of standard service specifications to facilitate commercial roaming between operators. It includes WRIX-i (Interconnect), WRIX-d (Data Clearing), WRIX-f (Financial Settlement) and WRIX-L (Location). Each of these can be deployed by Visited Network Providers (VNP) and Home Service Providers (HSP) either in-house or through an intermediary WRIX service provider.</td>
</tr>
</tbody>
</table>
# Participant List

<table>
<thead>
<tr>
<th>Company</th>
<th>Name – Editorial Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuris Networks</td>
<td>Steve Shaw</td>
</tr>
<tr>
<td>Point Dume / AIRI HK</td>
<td>Nikolay Alexandrov</td>
</tr>
<tr>
<td>Point Dume / AIRI HK</td>
<td>Tom Beirith</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Tim Tweedle</td>
</tr>
<tr>
<td>BT</td>
<td>Steve Dyett</td>
</tr>
<tr>
<td>BSG Wireless</td>
<td>Betty Cockrell</td>
</tr>
<tr>
<td>Boingo Wireless</td>
<td>Kishore Raja</td>
</tr>
<tr>
<td>CableLabs</td>
<td>Michael Smith</td>
</tr>
<tr>
<td>Comcast</td>
<td>Alan Lewine</td>
</tr>
<tr>
<td>Comcast</td>
<td>Cole Reinwand</td>
</tr>
<tr>
<td>Cisco</td>
<td>Gaetan Feige</td>
</tr>
<tr>
<td>iPass</td>
<td>Steve Namaseevayum</td>
</tr>
<tr>
<td>iPaaS</td>
<td>Blaz Vavpetic</td>
</tr>
<tr>
<td>Liberty Global</td>
<td>Stephen Kelly</td>
</tr>
<tr>
<td>Liberty Global</td>
<td>James Luce</td>
</tr>
<tr>
<td>Liberty Global</td>
<td>Nicolas Fortineau</td>
</tr>
<tr>
<td>Syniverse</td>
<td>Dan Klaeren</td>
</tr>
<tr>
<td>NTT DOCOMO Inc.</td>
<td>Masaruni Higuchi</td>
</tr>
<tr>
<td>Orange</td>
<td>Nigel Bird</td>
</tr>
<tr>
<td>WBA</td>
<td>Bruno Tomas</td>
</tr>
<tr>
<td>WBA</td>
<td>Tiago Rodrigues</td>
</tr>
</tbody>
</table>