IoT Interoperability

Dynamic Roaming

Source: WBA IoT Workgroup
Author(s): WBA Members
Issue date: 22 May 2018
Document status: Final

WIRELESS BROADBAND ALLIANCE
DRIVING NEXT WIRELESS EXPERIENCE

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to resolve business issues and enable collaborative opportunities for service providers, enterprises and cities, enabling them to enhance the customer experience on Wi-Fi and significant adjacent technologies. Building on our heritage of NGH and carrier Wi-Fi, the WBA will continue to drive and support the adoption of Next Generation Wi-Fi services across the entire public Wi-Fi ecosystem, having a focus on four major programmes: Carrier Wi-Fi Services, Next Generation Wireless & 5G, IoT, and Connected Cities. Today, membership includes major fixed operators such as BT, Comcast and Charter Communication; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel. WBA member operators collectively serve more than 2 billion subscribers and operate more than 30 million hotspots globally.

The WBA Board includes AT&T, Boingo Wireless, BT, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO and Orange. For a complete list of current WBA members, please **click here**.

Follow Wireless Broadband Alliance at:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/groups/50482

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.

CONTENTS

1 Introduction 2
2 The Categorization of IoT Devices and Roaming 3
3 Benchmark on scaling existing roaming solutions 7
3.1 Wi-Fi Roaming 7
3.1.1 How it works 8
3.1.2 Interoperability 9
3.2 Conventional Cellular Roaming 10
3.2.1 How it works 11
3.2.2 Service Interoperability 13
3.3 LoRa Alliance Roaming 14
3.4 MulteFire Alliance Roaming for Neutral Host Networks 16
3.4.1 MFA Courtesy Access 18
3.5 Eduroam 19
4 IoT Roaming 21
4.1 Types of Roaming Scenarios 21
4.2 Expansiveness of IoT Roaming Use Cases 23
4.2.1 Asset Tracking and Monitoring 24
4.2.1.1 Wi-Fi based Asset Tracking 24
4.2.1.2 Bluetooth Beacon Based Asset Tracking 25
4.2.1.3 LoRa based Asset Tracking 25
4.2.1.4 Sigfox based Asset Tracking 26
4.3 Identity, Roaming and Enterprise Use Cases 26
4.3.1 Enterprise 5G Roaming Use Case 28
4.4 Providing courtesy access using Neutral Host Networks 29
4.4.1 Monetizing courtesy access 29
4.4.2 Use of Enterprise Acceptable Use Policies and Liability Disclaimers 30
5 Baseline WBA Technical Framework to Address Roaming 32
5.1 Intro to generic roaming Functions 32
5.2 The WRIX Framework 32
5.3 Overview of WRIX Interfaces 34
5.4 Functional Activities by WRIX Module 38
5.5 WRIX Security 40
6 Enhanced functionality that may be used to support additional IoT roaming requirements 40
6.1 Flexible Framework for IoT Authentication 40

6.2 IPv6 41
6.3 Re-Use of WRIX d/f by non-RADIUS based IoT systems 41
6.3.1 Generalized UDR for IoT Data Clearing 41
6.3.2 Generalized Summary of Financial Data for IoT Financial Clearing 42
6.4 Billing and Charging impacts on IoT roaming 43
6.4.1 Split Billing 44
6.4.2 Batch Billing 44
6.4.3 Aggregated Usage Reporting 44
6.4.4 Bulk Data Reporting 44
6.4.5 Possible Enhancements to WRIX 45
6.5 Automating WRIX Security 46
6.5.1 Automated Peer Discovery 46
6.5.2 Automated security 47
6.5.3 Automated Revocation 48
6.5.4 Different Scenarios for Deploying Automated WRIX Security 48
6.6 IoT Application Security 50
6.7 Automated Settlement 52
7 Summary of gaps identified and recommendations 52
7.1 Framed-IPv6-Attribute and Framed-IPv6-Prefix support 52
7.2 Generalized UDR for IoT Data Clearing 53
7.3 WRIX Record Encoding 53
7.4 Monitoring Split Billing Adoption 53
7.5 Adoption of RADSEC between WRIX Hub providers 53
7.6 Adoption of DNSROAM for automating HUB-to-HSP Connectivity 53
7.7 Adoption of DNSROAM for automating VNP-to-HUB Connectivity 54
7.8 IoT Application Security 54
7.9 IoT Ease of Use 54
7.10 WRIX enhancements for MulteFire Alliance Support 54
7.11 5G Non-3GPP Subscription Identifiers 54
7.12 Impact of automated clearing and settlement 55
8 Next steps for the WBA 55
8.1 Dissemination and implementation of the framework 55
8.2 Industry Joint work 55

FIGURES

Figure 2-1: North America M2M/IoT Connections (Millions) 4
Table 2-2: Mapping between IoT market segments, applications and access technologies 6
Figure 3-1: Different entities involved in providing a Wi-Fi roaming service 8
Figure 3-2: Overview of international roaming technology and operations [14] 11
Figure 3-3 Required Commercial links for international roaming [14] 12
Figure 3-4: LoRa End-to-End System Components 15
Figure 3-5: LoRaWAN Roaming Back End Interfaces 15
Figure 3-6: MulteFire EAP-Based Neutral Host Network 16
Figure 3-7: MulteFire Neutral Host Network Roaming Architecture 17
Figure 3-8: Eduroam Architecture 20
Figure 3-9: Different Alternatives for Delivering Eduroam Authentication 20
Figure 4-1: Smart Skiing Asset Tracking Use Case [27] 25
Figure 4-2: Authentication of Traditional Enterprise Endpoints 26
Figure 4-3: Evolution of the enterprise environment 27
Figure 4-4: Authentication of IoT Endpoints with Remote Identity Provider 27
Figure 4-5: NAI-based 5G roaming for non-3GPP subscription identifiers 28
Figure 4-6: Value of Wireless Coverage, by Enterprise Type (Source Mobile Experts) 30
Figure 4-7: Contrasting user experience in different mobile data environments. 31
Figure 5-1: WRIX Functionality with interconnect via a Transit/Hub and settlement via Data and Financial Clearing House 35
Figure 5-2: WRIX Functionality with Direct Interconnect and Direct Settlement 36
Figure 5-3: WRIX Functionality with Direct Interconnect and Settlement via Data and/or Financial Clearing House 37
Figure 5-4: Summary of WRIX module functionality 38
Figure 5-5: Statically defined WRIX Security/RADIUS Hierarchy 40
Figure 6-1: Batch Billing [Source GSMA CLP08 [37]] 43
Figure 6-2: Introduction of RADSEC to secure interfaces between WRIX-I HUB providers. 48
Figure 6-3:Using a combination of RADSEC and DNSROAM to automate the security between WRIX-I HUB providers. 49
Figure 6-4: Automating the security between WRIX-I hub and HNP 49
Figure 6-5: Automating the security between VNP and WRIX-I hub 50
Figure 6-6: Federated identity translates the user's local identity into a SAMLassertion [47] 51
Figure 6-7: IETF's Application Bridging for Federated Access Beyond web architecture 52

TABLES

Table 2-1: Growth in IoT devices Source: Gartner (January 2017 [3]) 3
Table 2-2: Mapping between IoT market segments, applications and access technologies **6**
Table 3-1: LoRa Alliance defined Roaming Scenarios 14
Table 4-1: Example SIgFox usage plans 22
Table 4-2 IOTONE Industries, Functional Areas and Enabled Capabilities 23
Table 6-1: WRIX SFD Content [38] 45

Executive Summary

When the team started on this paper the goal was to continue the momentum created by the Internet of Things: New Vertical Value Chains & Interoperability whitepaper with a focal objective to outline how the Wireless Broadband Alliance could assist the entire IoT market, regardless of technology, in the evolution of IoT Device roaming, leveraging today's Wi-Fi Roaming capabilities. The team is pleased to report that we have not only accomplished that task but have also identified several opportunities for WRIX (Wireless Roaming Intermediary eXchange), which is the WBA's specification to facilitate Wi-Fi Roaming, to increase its capabilities, longevity and industry value by evolving to support IoT roaming use cases.

One common theme of this paper is something we all know, the Internet of Things (IoT) is not simply a trend or a fad. IoT is a revolution that is growing at a massive rate for both the consumer and business markets. Today there are already more deployed IoT devices that humans. By 2020 there is forecasted to be over 20 billion devices. Similar to the evolution of computers, increased mobility will become an an even more vital necessity as IoT continues to evolve and the need for cross network roaming of devices will grow in importance.

When assessing the IoT market, the immediate challenge is the diversity of the IoT devices, technologies and use cases. An IoT device can range from a Bluetooth speaker used by a consumer to a "smart" trash can used by a municipality on a MulteFire network. To address this challenge, the team outlined and categorized the various technologies and industry segments. The team then focused solely on those technologies that are most likely to require cross network roaming.

Next the team outlined how roaming is being accomplished today on different types of networks such as cellular, Wi-Fi, LoRa and MulteFire. The purpose of this is to demonstrate commonality of design, terms and functions of roaming regardless of technology. Examples of commonality include concepts such as a "home services provider" that owns the device or user and the "visited network provider" that provides network access to that roaming device or user. Other examples include functions and services such as interoperability, signaling, data clearing and financial settlement. This section is concluded with the outline of IoT Roaming use cases .

With the IoT explosive growth trend presented, the importance of roaming outlined and the fundamentals of roaming explained, the paper moves to provide a more detailed description of the WRIX (Wireless Roaming Intermediary eXchange) modules. These modules include Network, Interconnection, Data Clearing, Financial Clearing and Location. While these WRIX specifications may not, in most cases, be able to be directly applied to a given IoT Technology, the purpose of the standard is clearly presented and, minimally, the concept could be applied when creating or evolving roaming designs and specifications for a particular platform.

One of the greatest values of this paper was the discovery of many opportunities to enhance the functionality for existing technologies, including WRIX, in areas such as authentication, security and automation. Examples include the use or enhancement of WRIX to support RADSEC. Others include addressing IPv6 and various wholesale billing scenarios. These findings were the foundation for creating the Summary of Gaps and Recommendations. Finally, the document is concluded with suggested Next Steps.

We hope that you enjoy the paper and encourage you to reach out to the Wireless Broadband Alliance for further information or to inquire about participating in future projects.

1 Introduction

The WBA's 2020 vision describes a future of evolution and diversification that reflects the new market opportunities that are emerging for Wi-Fi and other license-exempt wireless access networks to support Internet of Things (IoT), smart city services, massive big data and so on [1]. These evolutions represent several significant areas that are expanding the monetization potential for un-licensed access.

To summarize the IoT Market, the WBA has published the Internet of Things: New Vertical Value Chains & Interoperability whitepaper that outlines the vertical markets, technology and value chains [2]. Contained in that whitepaper is the outline describing the requirement for roaming of IoT devices, where an IoT devices connects to a network other than the "home" network of the device to increase connectivity and reach. IoT Roaming creates several major challenges including:

- How to build a scalable solution to support a potentially massive number of devices roaming on non-home networks?
- How to overcome interoperability challenges that can occur between technologies?
- How to put in place a secure and scalable authentication, authorization and accounting framework?
- Is there a way to perform rating, clearing and settlement between the "home" network and the "visited" network?

The purpose of this paper is to utilize both the Internet of Things: New Vertical Value Chains & Interoperability whitepaper and the WRIX methodologies to:

- Summarize the current IoT Roaming Landscape
- Outline existing IoT Roaming Solutions
- Offer Industry Use Cases that require IoT Roaming
- Specify the requirements needed to facilitate IoT Roaming now and in the future
- Deliver an overview of how WRIX Standards facilitates Wi-Fi Roaming today
    - Interoperability
    - Clearing
    - Settlement
- Provide a recommendation of how the WRIX Standard could be applied to the IoT industry to facilitate roaming including security recommendations
- Identify gaps
- Offer next steps

2 The Categorization of IoT Devices and Roaming

The Internet of Things is experiencing significant growth in both consumer and business environments and, as such, it should be expected that there will be a consequential impact on the roaming infrastructure used to support such IoT services.

In a series of studies, Gartner Inc. has reported that 8.4 billion connected things, or "IoT" devices, will be in use in 2017, an increase in 31 percent over 2016 [3]. To put this in to context, the present world population is approximately 7.5 billion, which means there are now more connected IoT devices than humans. Connected devices growth is further forecasted to reach around 20 billion devices by 2020.

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.1	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Grand Total	**6,381.8**	**8,380.6**	**11,196.6**	**20,415.4**

Table 2-1: Growth in IoT devices Source: Gartner (January 2017 [3])

This growth will require significant scaling of the end-to-end systems, including the network connectivity used to support vast numbers of IoT services and devices. Roaming is one of those essential systems and moving forward, it will be imperative to address IoT scalability requirements in those systems.

Indeed, recent research published by Starhome-Mach, a global provider of roaming services, indicates that the number of cellular roaming registrations attributable to IoT devices had doubled over 12 months and in 2015 already represented 7% of all roaming connections [4]. Furthermore, research published by Machina, estimated that in 2015, 25% of all M2M SIMs deployed in Europe were exclusively supporting roaming use cases [5]. Finally, the Starhome-Mach report concluded with the possibility that by 2020 "as many machines as people will be roaming".

Already there are large scale investments in researching, designing and deploying a wide range of technologies in hopes to address the estimated 2020 IoT market size of $3.7B [6]. Participants include industry groups, chipset manufacturers, hardware OEMs, operators, enterprises and services providers all working together to address a fast-moving market. Examples of these technologies and deployments include:

- COMCAST deploying LoRa networks in Atlanta, Baltimore, Boston, Denver, Detroit, Indianapolis, Miami, Minneapolis/St. Paul, Oakland, Pittsburgh, Seattle and Washington, D.C. [7]

- SigFox networks already deployed in 18 countries and registering over 7 million devices in its networks
- The MulteFire Alliance membership continues to grow with multiple trials taking place [8]
- The use of the CBRS was demonstrated at a Motor Speedway to show how the spectrum can be used to host an LTE network and deliver 360-degree 4K video streaming from inside the race cars traveling around the track [9]

However, compared to these alternative wireless access technologies, the use of Wi-Fi remains the most prevalent means of connectivity for IoT devices because of the existences of large networks, relatively low cost and ease of deployment [10]. Importantly, from the WBA's perspective, research [11] indicates that from a North America perspective, while cellular based network connectivity is being driven by connected vehicle use cases (car, fleet, truck), non-cellular connectivity will dominate in terms of absolute numbers, as illustrated in Figure 2-1.

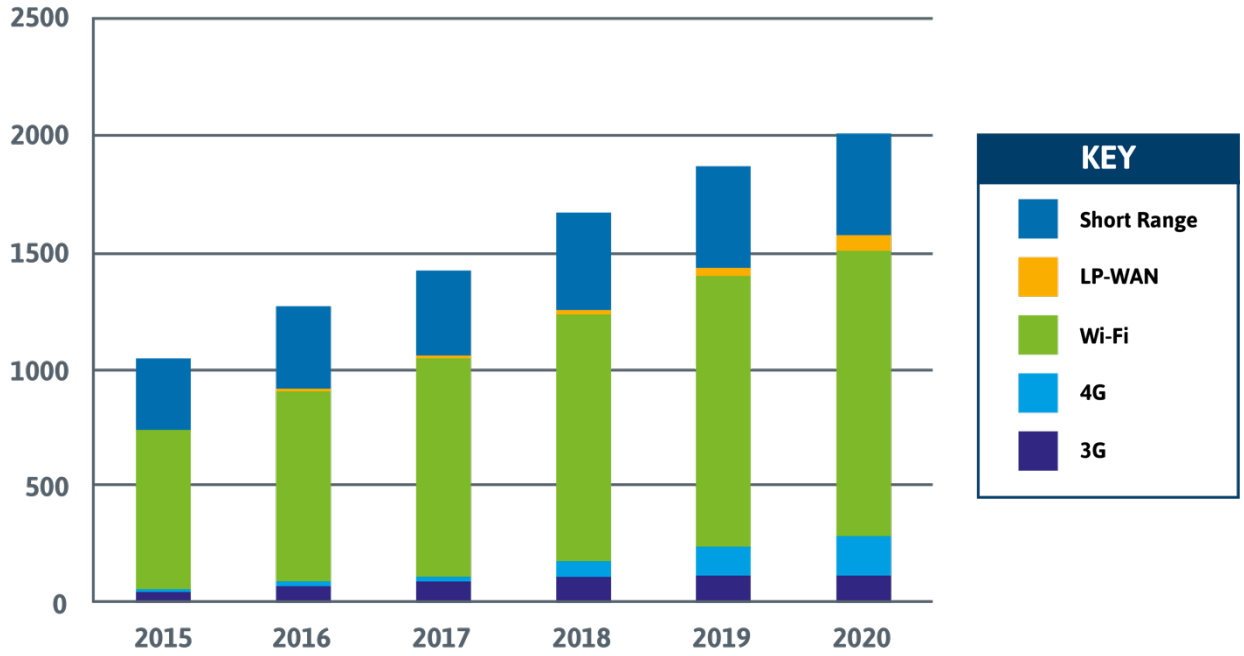


Figure 2-1: North America M2M/IoT Connections (Millions)

Due to its prevalence and maturity, the specifications and methodologies developed by the WBA, such as the WRIX specifcation for Wi-Fi Roaming, can be leveraged across the IoT Market for lessons learned, best practices and standards when developing each technology's roaming specifications. The WRIX specification will be covered later in this paper. For now, let's continue to further define the existing IoT market.

When assessing the current IoT market, two of the major challenges quickly become apparent: 1) the wide range of technologies involved and 2) an extortionate number potential of use cases. To assist

with the rationalize the IoT Market, the WBA's Internet of Things: New Vertical Value Chains & Interoperability whitepaper [2] outlined five major IoT segments:

- Healthcare
- Industrial
- Buildings
- Home
- Energy

Within each segment there are vast amounts of different devices types, technologies and use cases. For example, device types can range from low-end door monitoring devices, to asset tracking, to sophisticated monitoring equipment. To better describe the IoT devices, these are further categorized within the WBA's Internet of Things: New Vertical Value Chains & Interoperability whitepaper based upon the device's Unlicensed Access Technology. The categories include:

- Short Range
  - IEEE 802.15.4
  - Bluetooth
  - Zwave
  - IEEE 802.11ad (Wi-Gig)
- Medium Range
  - Wi-Fi
  - IEEE 802.11ah (Wi-Fi HaLo)
  - IEEE 802.11p
- Long Range
  - LoRa
  - MulteFire
  - SigFox
  - Wi-Sun
  - Ingenu
  - DASH-7
  - Weightless

Examples of mapping applications and access technologies within the Internet of Things: New Vertical Value Chains & Interoperability whitepaper include:

Market Segment	Applications	Access Technologies
Healthcare	Patient monitoring Home healthcare Medical imaging	Proprietary technologies, Bluetooth and 802.15.4 primarily in use. Wi-Fi targeting this market segment.
Industrial	Sensor/actuator networks for process control Automation Monitoring Maintenance Asset tracking	Wired and proprietary technologies currently primarily in use. Wi-Fi, LP-WAN, WiGig (and cellular) targeting this market segment
Buildings	Heating ventilation air conditioning Lighting Surveillance	802.15.4, ZWave, and Wi-Fi.
Home	Smart lighting Thermostat control Security systems Smart appliances Smart entertainment	ZWave, Wi-Fi, Bluetooth, and 802.15.4.
Energy	Smart metering Outdoor lighting	802.15.4 and LP-WAN (and cellular) currently primarily in use. Wi-Fi, Wi-Fi HaLow, and LP-WAN targeting this market segment.

Table 2-2: Mapping between IoT market segments, applications and access technologies

While connectivity is a fundamental requirement for an IoT device, not all IoT devices will be “roaming enabled”, which is the ability to utilize an access network of a 3rd party. For example, a stationary “connected smart metering” device belonging to a power company that only utilizes a specific wide area network deployed by a municipality may never be considered to be roaming. Primary examples of IoT scenarios that may require roaming typically focus on asset tracking, itself covering a broad set of use cases that include:

- User or asset needing autonomous mobility (both between national service provider networks or outbound roaming partners / networks)
- Cross border tracking requirements (on outbound roaming partners / networks)

This paper will focus on the common requirements necessary for an IoT device to be able to connect to a non-home access network, successfully authenticate, enable accounting and facilitate subsequent billing while taking into consideration potential security and scalability concerns. In other words, to be able to “roam”. As such, this whitepaper will primarily focus upon specific technologies that are either

already performing network roaming, are presently being enhanced to support network roaming, and/or could evolve to support network roaming in the near future. Examples of these technologies include:

- Wi-Fi
- LoRa
- MulteFire

Technologies that are presently not in position to support devices that "roam", such as Bluetooth, or are designed to support only closed networks, such as SigFox, will not be covered in detail in this whitepaper. If you would like to learn more about these segment, technologies and use cases we suggest you read the Internet of Things: New Vertical Value Chains & Interoperability whitepaper.

3 Benchmark on scaling existing roaming solutions

As outlined above, the Internet of Things is experiencing an explosion of growth in both the consumer and business environments. As such, it should be expected that there will be a consequential impact on the operations, development and evolution of the networks used to support all those IoT devices and services. Roaming is one of those essential network sub-systems and moving forward it will be imperative to address the IoT interoperability, scalability and security requirements in those systems. In this section we will provide an overview of how some technologies currently facilitate device based roaming today. Common to all these of technologies and methodologies are:

- Definitions of Home Service Providers and Visited Network Providers
- Authentication of Devices and/or users
- Network Interoperability
- Usage Recording

The usage of these common components ensures that each device, and associated user where applicable, will be able to utilize a roaming network, use defined signaling exchanges to support the authentication and authorization of the device by the Home Service Providers, and ensure that the Visited Network Providers is in position to be compensated for its services and allowing the two network providers to receive the details of the usage.

3.1 Wi-Fi Roaming

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.

1. **Home Service Provider (HSP) Subscribers** –To facilitate access, 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 HSP, had to accept the HSP's

policies, including those describing acceptable use, and likely be assigned to a service plan that includes Wi-Fi Roaming.

2. **Visited Wi-Fi Provider (VNP)** - The owner/operator of a Wi-Fi network may be content to leave access to their Wi-Fi network private, not sharing it to global subscribers. But for those who wish to support such use cases, they can enable inbound roaming traffic; for example, by joining a Wi-Fi Roaming hub and enable inbound roaming traffic - there of course is an opportunity to monetize the additional traffic on their network.
3. **HUB & Clearing House** - 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.

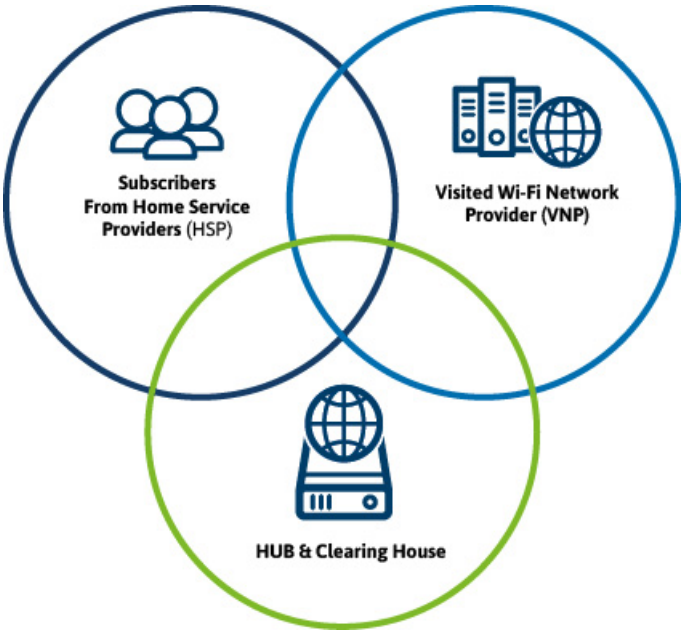


Figure 3-1: Different entities involved in providing a Wi-Fi roaming service

3.1.1 How it works

The Wireless Broadband Alliance developed the Next Generation Hotspot (NGH) specifications to make the Wi-Fi user experience as easy, seamless and secure as a cellular experience. NGH takes the established hotspot model and builds new levels of ease of discovery, security of connection and efficiency of service, leveraging the Wi-Fi Alliance's Hotspot 2.0 specification [12].

When a Hotspot 2.0-capable Wi-Fi device comes within the range of a Hotspot 2.0-capable access point, it will automatically start a signaling exchange with that access point to determine its capabilities. Some of the data that is exchanged may include:

- The name of the Wi-Fi network operator / service provider
- List of roaming partners that are supported
- Other things related to the service, such as backhaul bandwidth, current load etc.

The device is able to use this information to automatically decide whether to connect to a particular Wi-Fi network, e.g., in preference to possibly other overlapping networks.

After having selected a network, the Wi-Fi device initiates an EAP authentication. Unlike cellular systems which have been built on a foundation of identities based on International Mobile Subscriber Identities (IMSIs) and SIM based authentication, Wi-Fi roaming is based on the concept of Network Access Identifiers (NAIs) which are of the form “user@realm” and a flexible authentication framework.

- An EAP-Response/Identity message is used by the device to signal its NAI to the Visited Network Provider. Unlike in cellular, the Wi-Fi device may choose to hide its true identity from the access network and may signal “anonymous@realm” to the visited network.
- The visited Wi-Fi access network uses the “realm” portion of the identify to identify the home service provider.
- The visited Wi-Fi access network embeds the NAI and EAP message in a RADIUS Access Request message and routes the message towards the home service provider, possibly via a direct signaling link, but more commonly via one or more roaming hubs.
- The roaming hubs use the realm portion of the NAI to further route the message towards the home service provider.
- The home service provider embeds an EAP message in the returned RADIUS message and this is signaled all the way back to the visited network operator which recovers the EAP message and forwards it to the Wi-Fi device. In this way, the EAP exchange is directly between the Wi-Fi device and the Home Service provider.
- An EAP dialog follows which is used to support the chosen EAP methods, which for Passpoint certified devices include either EAP-SIM, EAP-AKA, EAP-TLS or EAP-TTLS. As part of the EAP method, the Home Service provider can recover the permanent identity of the device in a secure fashion.
- After the home service provider has authenticated the device, it replies with an EAP-Success message and includes keying material, generated as part of the EAP exchange, in the RADIUS Access Accept message, as well as an optional Chargeable User Identity that should be used in accounting records generated by the visited network provider.
- The visited network provider forwards the EAP-Success message to the device which will have independently generated its own keying material as part of the EAP exchange. The keying material is then used to protect the Wi-Fi air interface.
- The visited network provider generates RADIUS accounting messages for the Wi-Fi usage, including the Chargeable User Identity and signals these to the home service provider.

3.1.2 Interoperability

WBA WRIX (Wireless Roaming Intermediary eXchange) is a modularized set of service specifications to facilitate commercial roaming between operators. It includes WRIX-i (Interconnect), WRIX-l (Location) WRIX-d (Data Clearing) and WRIX-f (Financial Settlement). Each of these can be deployed by Visited

Network Providers (VNPs) and Home Service Providers (HSPs) either in-house or through an intermediary hub provider.

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) [13]. 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. Also, the ICP outlines a framework which defines the requirements for roaming and settlement from basic connectivity to more advanced models. By doing this the ICP facilitates and simplifies the implementation and deployment of Wi-Fi Roaming.

The assessed categories range from:

- Interconnect Requirements
- Authentication Methods
- Connection Bandwidth Requirements
- Network Discovery and Selection Features
- NGH Network Security
- NGH Network Management
- Network Access Security Types
- User Experience
- WRIX-i WRIX Attributes Supported
- WRIX-d Charging Models and Data Clearing
- WRIX-f Settlement Methods
- WRIX-L Directory File Management - Location Type Classification
- Customer Care/Support
- Information Exchange

There are currently more than 20 global operators, across 5 different continents who have currently achieved an ICP tier level to support the development of their businesses.

3.2 Conventional Cellular Roaming

Cellular Roaming enables a cellular customer to maintain connectivity and receive uninterrupted service even when geographically outside the network coverage range of their mobile service provider, also known as the "Home Service Provider" ("HSP"), so long as the HSP has a roaming agreement with another mobile service provider in range of the handset. The mobile service provider that will provide service to the cellular subscriber on behalf of the HSP is called a "Visited Network Provider" ("VNP").

Figure 3-2: Overview of international roaming technology and operations [14]

3.2.1 How it works

Cellular Roaming is both commercial and technical. For example, ideally both operators will utilize the same cellular technologies required for handset access and communication. If the technologies differ then an interoperability solution must be used. Additionally, the two operators also must have a signed "roaming agreement" that contains the legal terms between the operators. The most important elements for Cellular Roaming are:

- The existence of a "roaming agreement defined terms" that defines the legal terms between the operators
- Utilization of the same technologies handset access and communication, such as bandwidth frequency and access methods, or an interoperability solution is leveraged
- Mobility Management, which is a core function of cellular networks, that tracks the location of a cellular subscriber's location and enables calling, messaging and other mobile phone services to be accessed by a subscriber
- Common authentication, authorization and accounting ("AAA") charging procedures
- Interconnection of operators for signaling and AAA messages
- Clearing and Settlement procedures

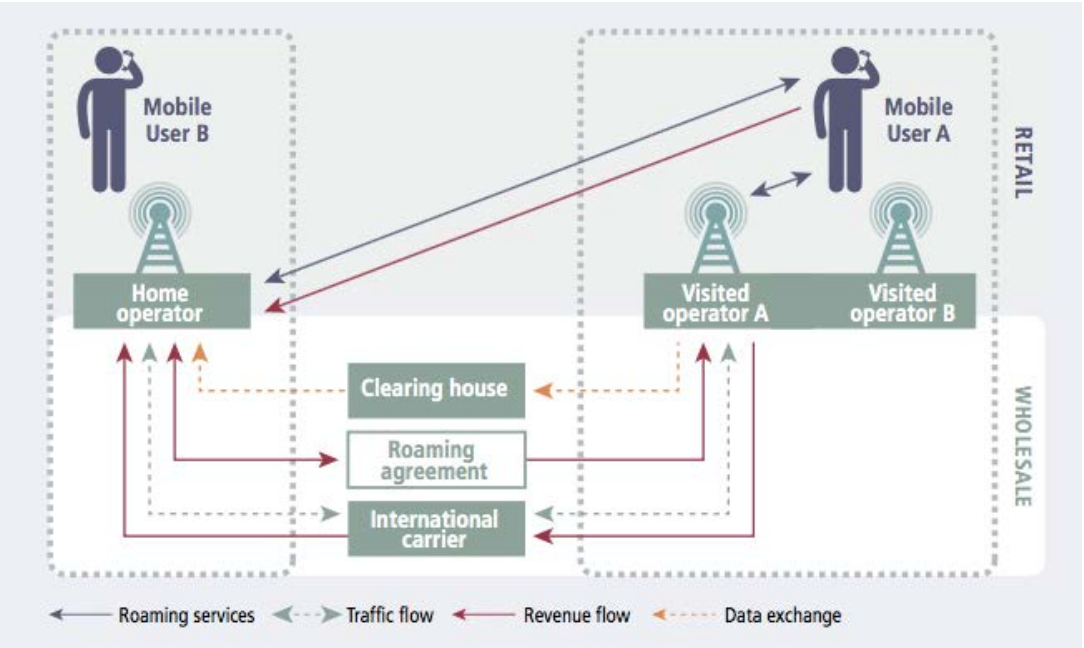


Figure 3-3 Required Commercial links for international roaming [14]

The process flow for a call between a Cellular Subscriber A on their home network to a Cellular Subscriber B that is roaming internationally includes:

- Cellular Subscriber B's HSP has a roaming agreement with the VNP where Cellular Subscriber B is presently located
- Cellular Subscriber B's handset attempts to attach to the VNP
- As part of the attach procedure, the VNP recovers the identity (IMSI) of the Cellular Subscriber B and uses the IMSI to identify the Cellular Subscriber B as not being a subscriber of the VNP
- The VNP recovers the Mobile Country Code and Mobile Network Code from the IMSI of the Cellular Subscriber B and uses this information to route a location update request message to Subscriber B's HSP.
- The HSP and VNP exchange messages to allow the VNP to authenticate Cellular Subscriber B using their SIM card credentials.
- After Cellular Subscriber B has been authenticated and authorized to receive roaming service from the VNP, Cellular Subscriber B's subscriber data, including details of the specific services that the subscriber is authorized to access, is downloaded to the VNP
- Cellular Subscriber A attempts to call Cellular Subscriber B
- The call is routed to Cellular Subscriber B's HSP and the HSP locates the user on the VNP

- The call is routed to the VNP and Cellular Subscriber B receives the call
- The usage is tracked by the VNP and recorded into a Transferred Accounts Procedure (TAP) file.
- The VNP will utilize the TAP files to bill the HSP for the services it provided to Cellular Subscriber B while on their network
- Commonly a clearing house will receive and process the TAP files on behalf of either or both operators to provide a settlement position among the operators
- The HSP will also use the TAP file(s) to bill the subscriber for the international usage

Similar processes are used to provide data, messaging and other mobile services to a subscriber.

3.2.2 Service Interoperability

Interoperability among operators is vital to deliver services and expand coverage for cellular subscribers. While it is the desire for many for LTE to further move the cellular industry under a common set of phone standards there currently remains a vast array. For example, just considering interoperable voice services, these can have different access networks involved, including:

- 2G/3G - the most widely adopted standard for voice roaming and commonly referred to as GSM/UMTS as it has evolved
- CDMA – Code Division Multiple Access that was developed by Qualcomm and mostly prevalent in the United States
- LTE – Long Term Evolution is based upon GSM standards, but as it does not include a circuit switched component, needs to use IP based IMS for supporting Voice of LTE (VoLTE) to deliver voice service.
- VoWi-Fi – Voice over Wi-Fi is not necessarily an exclusive technology to mobile operators but, when deployed by MNOs, can leverage the same IMS framework used to support VoLTE

In today's cellular roaming world, it is common for operators and/or intermediates to utilize some form of an interoperability solution. One example is performing message translations of Diameter to SS7. Translating SS7 to Diameter enables a non-LTE network or legacy network component to connect and utilize the LTE networks or services that may require Diameter.

3.3 LoRa Alliance Roaming

The LoRa Alliance is driving the adoption of the LoRaWAN protocol that has been optimized for low cost, low power battery powered IoT devices that leverage a Chirp Spread Spectrum based physical layer. From an identity perspective, LoRaWAN re-uses the IEEE-defined 64-bit Extended Unique Identifier (EUI-64). From a roaming perspective, LoRa defines the use of an application identity, AppEUI, which is used to uniquely identify the application provider (i.e., owner) of the end device.

The LoRa Alliance is defining various different Roaming Scenarios as described below [15], defining backend interfaces between Network Server to Join Server and Network Server to Network Server to support such scenarios shown in Table 3-1.

Scenario	Description
1	Service provided over multiple public partner networks, with non-nomadic devices within a regulatory zone
2	Service provided over multiple public partner networks, with nomadic devices that have been previously activated in operator's own network within a regulatory zone
3	Service provided over multiple public partner networks, with nomadic devices within a regulatory zone
4	Device migrating from a private to a public network within a regulatory zone
5	Nomadic nodes migrating across networks where the radio regulatory requirements change

Table 3-1: LoRa Alliance defined Roaming Scenarios

Figure 3-4 below shows a representation of the back-end LoRa components, including the LoRa Gateway that terminates the LoRa Radio interface, the LoRa Network Server (NS) that terminates the LoRaWAN MAC protocol, the LoRa App Server (AS) that terminates the application security and the LoRa Join Server (JS) that is responsible for authenticating the LoRa devices onto the network.

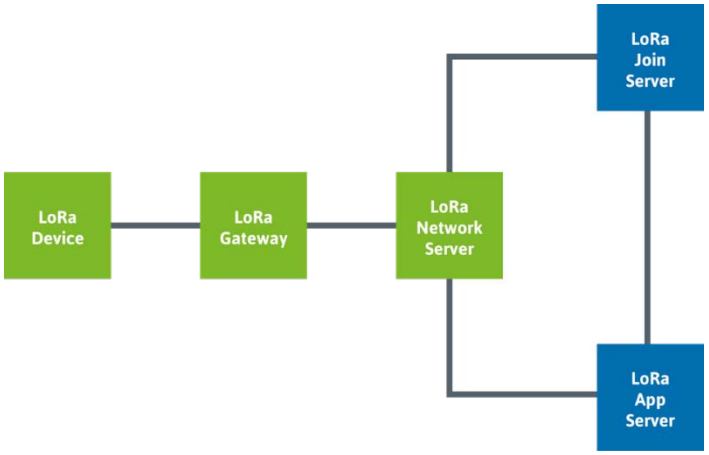


Figure 3-4: LoRa End-to-End System Components

In addition to the visited LoRa Network Server to LoRa Join Server roaming interface, the LoRa Alliance defined roaming model has an additional roaming interface defined between the Visited Network Server and the Home Network Server, as illustrated in Figure 3-5. The Visited Network Server is responsible for terminating the LoRa MAC protocol between the Network Server and the End-Device and the Home Network Server is where the various profiles of the end-device are stored. The Visited Network Server is signaled information to identify the Home Network Server by the LoRa Join Server during the join procedure.

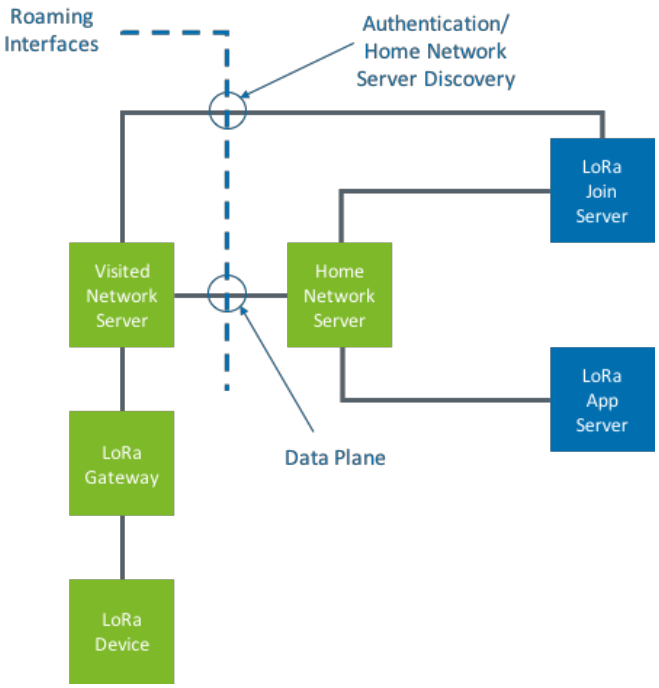


Figure 3-5: LoRaWAN Roaming Back End Interfaces

In contrast to other roaming solutions, the LoRa backend interfaces make extensive use of HTTP1.1 with JSON encoded payloads for the roaming interfaces between Visited Network Server and Join Server and between the Visited Network Server and the Home Network Server.

The process flow for how the roaming LoRa device receives service includes:

- The LoRa Device attempts to join the visited LoRa network by signaling a Join Request including a JoinEUI
- The LoRa Network Server in the visited network uses DNS to look up the IP address of the Join Server corresponding to the JoinEUI
- The LoRa Network Server signals the Join Request within a HTTPS message to the Join Server
- The Join Server processes the Join Request and responds to the LoRa NS in the visited network with a Join Answer, including the address of the Home Network Server
- The LoRa NS in the visited network forwards the Join Accept message to the LoRa device
- When the LoRa NS in the visited network receives an up-link frame from the LoRa device, it forwards it to the Home LoRa Network Server

3.4 MulteFire Alliance Roaming for Neutral Host Networks

The MulteFire Alliance has augmented the baseline LTE cellular architecture to enable deployments of MulteFire RAN by a neutral host operator including being able to support deployment scenarios where a Standalone Deployment is integrated with “external interworking” [16].

More specifically, a significant enhancement defined by the MulteFire Alliance for supporting the Neutral Host Network is the ability to support EAP based authentication [17], as illustrated in Figure 3-6.

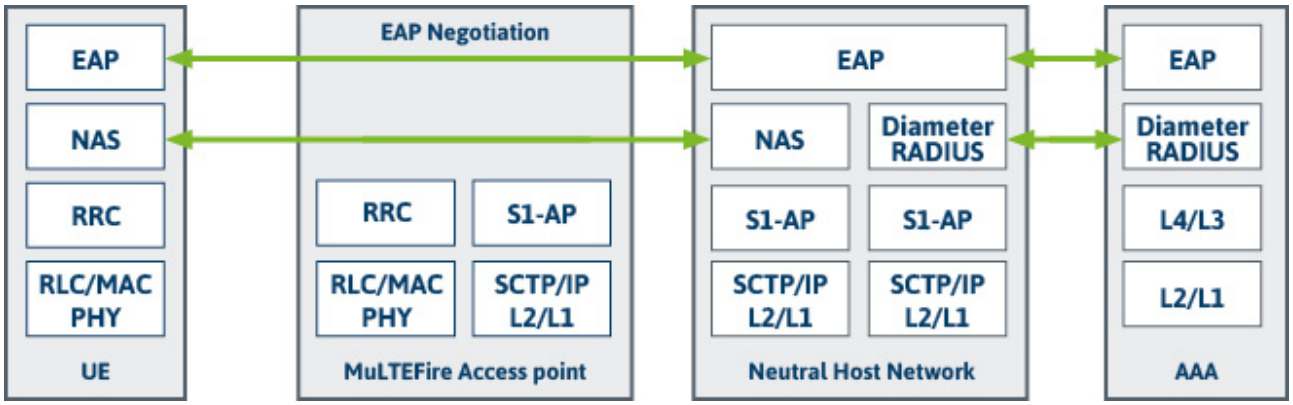


Figure 3-6: MulteFire EAP-Based Neutral Host Network

Leveraging this EAP support, Figure 3-7 illustrates two different options for Neutral Host Network. The first is equivalent to the un-trusted WLAN model where the SWa-N interface is used to authenticate the UE equipment using EAP-AKA' within the MulteFire environment. Just as with untrusted WLAN access, successful authentication and authorization will enable the UE to get connectivity with an external IP Network directly from the Neutral Host Gateway. As expected, the SWa-N interface is similar to the SWa interfaces, as defined in 3GPP TS 23.402 [18] between Untrusted Non 3GPP Access and 3GPP AAA Server.

The second option is equivalent to the trusted WLAN model, where now the STa-N interface is used to authenticate the UE equipment using EAP-AKA' within the MulteFire environment, and successful authentication triggers the establishment of an S2a tunnel between the Neutral Host GW and the home operators PDN-GW. As expected, the STa-N interface is similar to the STa interfaces, as defined in 3GPP TS 23.402 between Trusted Non 3GPP Access and 3GPP AAA Server.

Details of the specific changes from the standardized 3GPP interfaces, including Access Network Identity and Access Type are defined in [16].

.

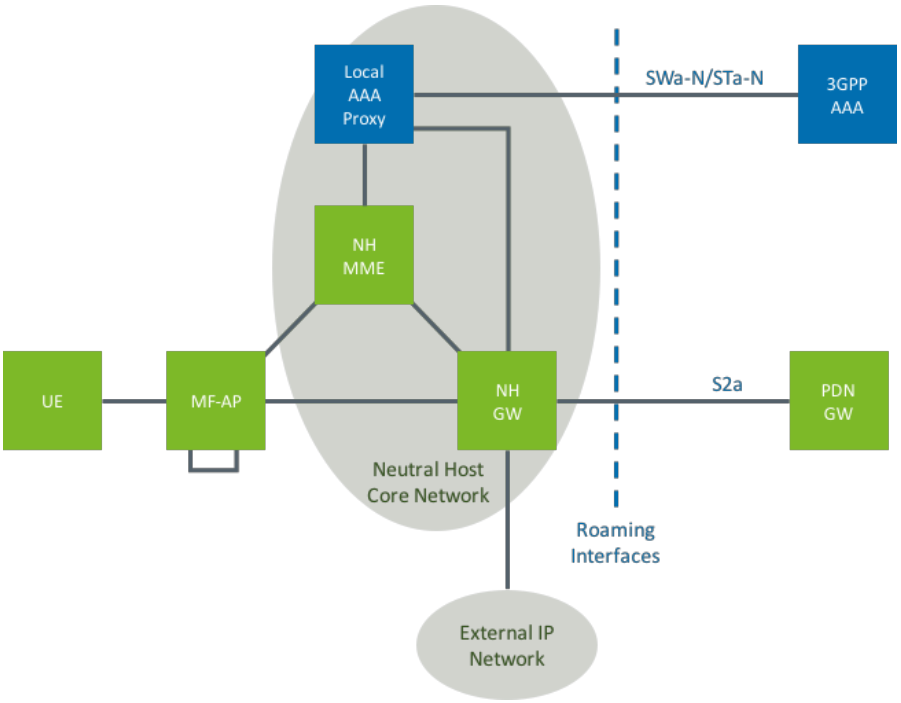


Figure 3-7: MulteFire Neutral Host Network Roaming Architecture

The process flow for how the a MulteFire device receives service in a visited Neutral Host Network includes:

- MF cells supporting NHN access mode broadcast a Neutral Host Access Mode Indicator as a PLMN-ID
- MF cell can also advertise an indicator that it supports S2a based trusted mode access
- When the Attach Request message is received from the UE, the NH MME initiates the EAP authentication process
- UE provides its identity in a form of NAI
- The local AAA Proxy uses the realm portion of the NAI to route AAA transactions for the UE. The Access Network ID AVP is used to signal that the request originates from a MulteFire network
- The 3GPP AAA Server authenticates the MulteFire device using EAP-AKA'
- The NHN may support accounting, but because neither SWa nor STa interfaces defined between the Local AAA proxy and the 3GPP AAA support accounting, Diameter Accounting based on IETF RFC 7155 is used
- The Local AAA proxy shall map the accounting information identity used within the NHN to the Diameter User Name (User-Name) attribute, provided by the AAA in the Diameter EAP authentication response.

3.4.1 MFA Courtesy Access

MulteFire introduces the concept of a special service called "courtesy access". This allows access to the Neutral Host Network (NHN) without establishing subscription credentials with the courtesy access provider. The NHN announces support for this type of access in the broadcast information.

To use courtesy access, the device shall be provisioned with a certificate. The device connecting to the NHN for courtesy access indicates its intention to use the courtesy access by using a special "Courtesy Network Address Identifier" (NAI) in the initial EAP exchange. When requesting the courtesy access, the device excludes the Access Point Name (APN) in the attach request. The courtesy NAI shall have value "@courtesy.mf.invalid.". The username part is omitted.

The local AAA Proxy at NHN detects the use of special courtesy NAI and engages the preconfigured AAA server responsible for courtesy access authentication and authorization using the EAP-TLS procedure. The NH-Mobility Management Entity (MME) and the Local AAA shall not query DNS for name resolution when detecting the special courtesy NAI. During the TLS handshake, the AAA server shall present the server certificate to the UE for validation of the authorization domain. The AAA server shall request the Device certificate from the UE and the UE shall provide it to the AAA server. The Device certificate may be provisioned using special mechanisms mentioned in the MFA specification

When the UE accesses the network for courtesy access:

- The Device Certificate presented by the UE may be validated by the AAA responsible for the courtesy access;
- The UE identity presented in the Device Certificate may be checked against the database of forbidden UEs;
- Upon completion of TLS handshake and EAP-TLS protocol, security keys are put into place for protecting the NHN transport;
- A PDN connection for courtesy access is established with security context. NHN policy decides the authorized QoS parameters (e.g. QoS parameters for the default bearer and whether the UE can establish dedicated bearers). No additional PDN contexts are created for courtesy access.

For courtesy access the solution specified for Initial Attach for NHN Untrusted access mode can be used with the following adaptations:

1. UE discovers a MulteFire NHN advertising courtesy access.
2. The UE initiates ATTACH procedure using “courtesy” NAI and no APN.
3. NHN invokes EAP procedure with the UE. The AAA providing courtesy access authentication and authorization conducts EAP-TLS with the UE. The AAA shall request device certificate during the TLS handshake.

Both normal service and courtesy access may be provided simultaneously by the NHN.

Whether any additional actions are required by the user prior to initiating data communications are part of the application (e.g. accepting terms and conditions) are out of scope for this procedure. Courtesy access remains available until either user, the responsible AAA, or the NHN decide to terminate it.

3.5 Eduroam

Eduroam (education roaming) is a secure, worldwide roaming service developed for the international research and education community (https://www.eduroam.org) and is supported by GÉANT, the pan European research and education network and individual institutions. Eduroam is based on the same IEEE 802.1X standard and hierarchy of RADIUS proxy servers used for Carrier Wi-Fi roaming, and eduroam allows any user from an eduroam participating site to get network access at any institution connected to eduroam.

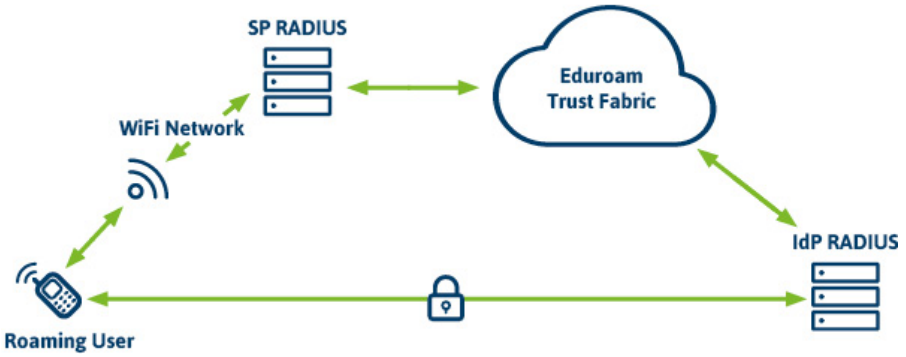


Figure 3-8: Eduroam Architecture

Compared with carrier Wi-Fi, eduroam is always free for its users, there is no charge for eduroam use world-wide. The providers of eduroam hotspots make the service available to benefit all members of the research and education community. In 2017, eduroam provided over 3.6 billion national authentications (where users from another institution in the same country authenticate their Wi-Fi access via eduroam), a 21% year-on-year increase. In addition, in 2017 eduroam provided international roaming across 85 countries, supporting more than 834 million international authentications, a 18% year-on-year increase [19].

There are three options for realizing the Eduroam federation, as illustrated in Figure 3-9:

- A RADIUS based hierarchy using an Eduroam Top-Level RADIUS (ETLR) server
- A RADIUS based hierarchy which is protected using RADSEC using a Top-Level RADIUS server
- A dynamically discovered RADIUS solution using RADSEC

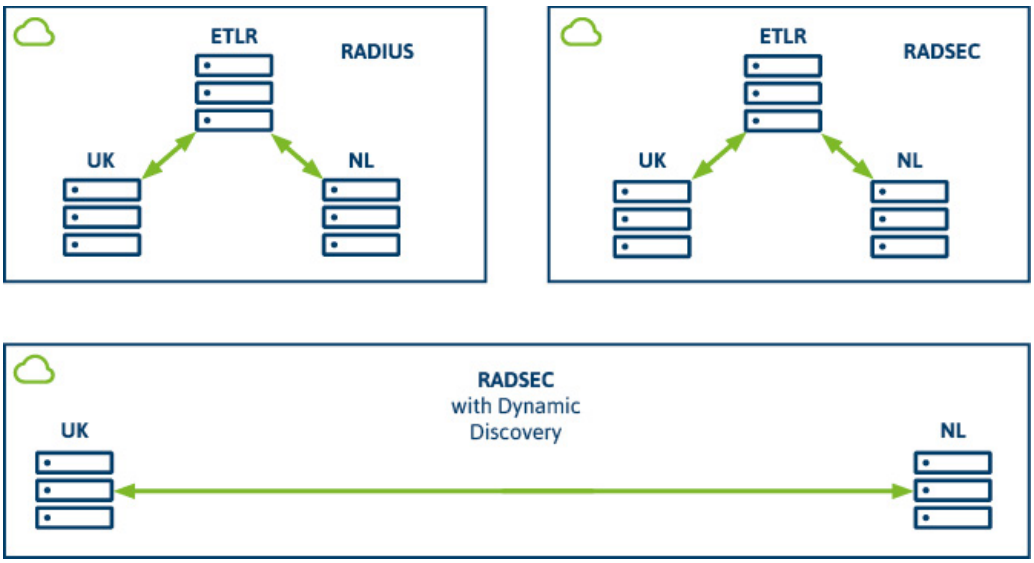


Figure 3-9: Different Alternatives for Delivering Eduroam Authentication

The process flow for the dynamically discovered RADIUS server used to support an eduroam user A on a visited eduroam network includes:

- The visited academic/research institution belongs to a National Research Organization that has signed the Eduroam compliance statement
- The eduroam organizations publish eduroam service information, including acceptable use policy and links to eduroam policies
- The home academic/research institution (Home IdP) enables dynamic discovery by configuring their DNS resource record
- An eduroam user A moves into coverage of the Wi-Fi network provided by the visited academic/research institution, the Visited Network provider, (VNP)
- The eduroam user A's device identifies a Wi-Fi network broadcasting the eduroam SSID
- The eduroam user A attempts to authenticate to the network using EAP/WPA2. The exact EAP type is determined by the home academic institution, and may be EAP-TLS, EAP-TTLS, PEAP, EAP-FAST or EAP-PWD [20]
- The VNP recovers the identity of the home academic institution from the realm of the NAI/EAP-Identity and identifies the user as being from a non-local realm
- The VNP uses DNS to match the NAI realm to a Naming Authority Pointer (NAPTR) record
- The VNP uses the discovered RADIUS server address to establish a TLS connection. The TLS uses X.509 certificates provided by the GÉANT eduPKI service. The Home IdP uses its certificate to enable the VNP to verify that the RADIUS peer is authoritative for the NAI realm
- The VNP and Home IdP exchange EAP/RADSEC messages that are used to authenticate the eduroam user A's device. The VNP SHOULD identify itself using Operator-Name RADIUS attribute
- The eduroam user receives Wi-Fi connectivity from the VNP which should include support for IPv6
- The usage is tracked and other logs are retained by the VNP. Importantly usage information will typically NOT be provided to the Home IdP in RADIUS Accounting messages

4 IoT Roaming

4.1 Types of Roaming Scenarios

Compared to conventional roaming which can be based on some transient period of time where a subscriber is travelling outside the coverage of their home network, IoT can see the emergence of new business models. According to the business models being developed, roaming can function on a permanent or a transitory basis, e.g., the three scenarios described below [21]

- Scenario 1: The connected device is travelling periodically (e.g. a car used for a leisure trip or a tracked asset within a medical facility being transferred between locations).
- Scenario 2: The connected device is used most of the time on the basis of permanent roaming, but the object is moving either within one country or across borders (e.g. a car which is sold abroad).
- Scenario 3: The connected device (e.g. smart meter, sensors) is used on the basis of “permanent roaming” but is not travelling at all, often with a long period of usage. Furthermore, it is questionable whether in this case the connected device can be called a mobile device at all, since it is not used in a mobile fashion. However, it certainly is roaming, as it is connected to a visited network which is not responsible for provisioning the service.

Moreover, the roaming scenarios will also be impacted by the network connectivity requirements necessary to support a particular IoT use case. Earlier analysis of IoT Vertical Value Chains by WBA has highlighted the significant divergences in network connectivity requirements [2]. Using data averaged over a deployment of 100K networked devices within an industrial IoT environment], some IoT devices used up to 1 GByte/device/month, i.e., an order of magnitude that is broadly equivalent to smartphone consumption, whereas other devices used as little as 25 kbytes over an entire month. The IoT use cases that result in these very small and/or infrequent connectivity requirements have been a focus of new LPWAN systems. For example, the plans offered by SIGFOX on their IoT network look to support varying numbers of messages, with ranges from 49 kBytes per device per month down to 700 Bytes per device per month [22]. These ultra-low consumption figures can be contrasted to some other examples of roaming tariffing that allow small amounts of usage, typically associated with initial DNS traffic, that is not reconciled against connected usage.

Plan	Number of messages per device per day	Monthly total assuming 12 byte message
Platinum	140	~49kByte/device/month
Gold	100	~35 kByte/device/month
Silver	50	~18 kByte/device/month
One	2	~700Bytes/device/month

Table 4-1: Example SIgFox usage plans

4.2 Expansiveness of IoT Roaming Use Cases

A distinguishing factor of the IoT environment is the diversity of industries, functional areas and propositions. IOTOne (www.iotone.com) lists over 800 IoT case studies, across 24 industries, 12 functional areas and delivering 14 core propositions, as illustrated in Table 4-2.

Industries	Functional Area	Proposition
Aerospace	Operations & Maintenance	Data Acquisition and Management
Automotive	Production and Manufacturing	Remote Access & control
Machinery		Asset Tracking and Monitoring
Oli & Gas		
Rail & Metro	Facilitates Maintenance	Inventory Management
Computer & Personal Electronics	Logistics	Energy Management
Medical Equipment		
Biotechnology	Quality Assurance	Facility Climate Control
Heavy Vehicle		Environmental Health & Safety
Mining	Procurement & Sourcing	
Shipping		
Agriculture	Environmental Health & Safety	Predictive maintenance
Renewable Energy		Data Virtualization
Construction		Environmental Monitoring
Healthcare	Product Development	Overall Equipment Effectiveness
Telecommunications		
Smart Grid	Research & Development	
Chemicals		Mass Customization
Fast Moving Consumer Goods	Information Technology	Infrastructure Access & Security
Paper & Pulp		
Pharmaceuticals	Sales & Marketing	
Plastics & Rubber		Quality Assurance & Control
Furniture & Home	Human Resources	
Food & Beverage		

Table 4-2 IOTONE Industries, Functional Areas and Enabled Capabilities

The case studies documented above are vast in subject, however specific roaming propositions across the spectrum are nascent, especially with emerging technologies like LPWAN. The following sections focus on IoT roaming proposition of asset tracking, where there has been a great deal of activity and innovation. A cross-section of "standard" wireless access technologies such as RF, BLE and Wi-Fi as well as LPWAN are compared.

4.2.1 Asset Tracking and Monitoring

Traditionally, asset tracking technologies have used GPS, BLE or RFID technologies that broadcast position and are used for physical asset tracking as well as tracking of "human assets" wearing badges. The use cases can be characterized by whether there needs to be a real-time feed or alternative use cases that don't require consistent real-time updates or detailed monitoring. The traditional connectivity option for wide-area real-time tracking has been to use cellular. However, this is not without its limitations, e.g., in terms of power draw and rural coverage.

Conventionally, non-real time asset tracking has used RFID where low-cost passive tags are tracked when interrogated by a reader, requiring fixed reader infrastructure to be deployed, or alternatively employing individuals to carry a mobile reader past the tags.

Alternative options are now emerging that leverage low-power, wide-area network (LPWAN) standards such as LoRa and Sigfox. As an example, Semtech has recently developed a LoRa-based "Nano-tag" reference design, a disposable, ultrathin and low-cost tag that can be integrated into disposable systems or attached to assets to communicate a specific trigger of an event [23]. The LoRa-based nano-tag will be available in both flexible tape and paper substrates, and can be deployed across numerous Internet of Things (IoT) verticals that utilize the event data to enable smarter decision making. In these cases, monitoring is event-based and real-time monitoring is not required. Additionally, alternative short range technologies like RF and BLE can be used.

Similarly, in March 2017, SIGFOX announced its "Spot'It" tag that includes geolocation capability [24]. The user can opt for a low-cost geo-location service that locates a tag with an accuracy of approximately 5km, or alternatively pay for a more precise location accuracy, or 1km or 500m.

Examples of IoT Asset Tracking and Monitoring use cases Include:

4.2.1.1 Wi-Fi based Asset Tracking

The cost of Wi-Fi tags is decreasing and enable asset tracking solutions. Internet of things (IoT) smart logistics and asset monitoring company, Armada (http://www.armada.net/), develops a supply chain visibility platform and places its "internet of things" tiles, or 9-volt battery sized tracking devices, into shipments. This enables distributors to look into the location of their assets. More interestingly, Armada has announced a partnership with iPass. Now whenever one of its "tiles" comes into range of a hotspot, it will be able to roam onto the Wi-Fi network and send its information to Armada's supply chain platform [25].

4.2.1.2 Bluetooth Beacon Based Asset Tracking

US retailer Target is adding an improved indoor mapping component to its mobile app, designed to help shoppers find their way through stores and locate the products they need. They are referring to the feature as a “GPS for your shopping cart.” Instead of simply showing a static map, or noting the aisle number where a product can be found, the new Target application will actually show your own location on the map, as indicated by a blinking dot.

Target has been updating all its stores with new, energy-efficient LED lighting. It chose to purchase fixtures that have Bluetooth beacons built-in. These beacons are what allow Target’s app to locate shoppers in the stores, and then guide them to products, as needed. Target will also be using the beacon technology to highlight which of its “Cartwheel” deals are near your current location [26].

4.2.1.3 LoRa based Asset Tracking

Because of their very low power requirements and low cost, Low Power Wide Area technology is being proposed for supporting a wide range of asset tracking services. One such proposal is the Smart Skiing service developed by CEA (http://www.cea.fr/). In one scenario, a European skier uses a skiing travel bag with an integrated LoRa sensor [27]. When visiting the Winter Olympics in 2018, the European skier travels with their skis in order to experience the Olympic slopes. The ski travel bag includes sensors to measure external conditions, whereas the skis have an integrated location sensor. This information is displayed using an application on his smartphone. The roaming service between Europe and Korea enables to switch from a telecommunication operator to another, seamlessly for the skier.

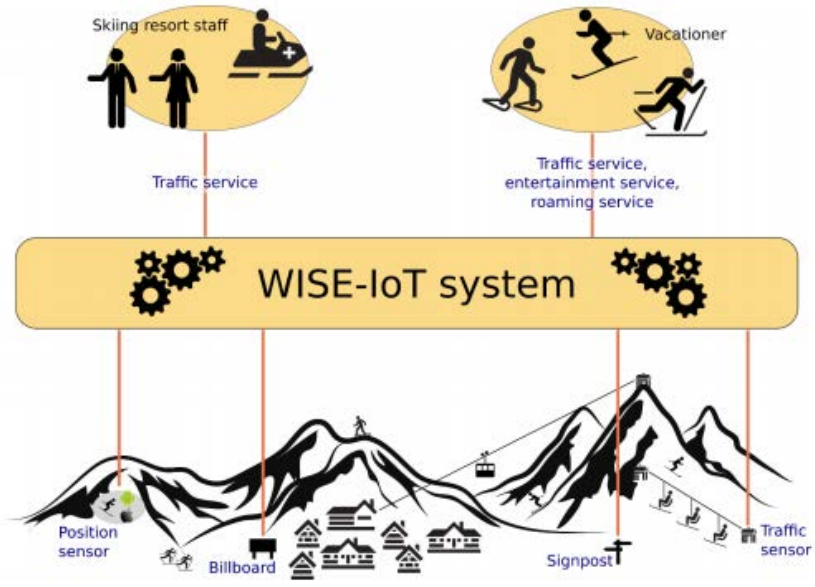


Figure 4-1: Smart Skiing Asset Tracking Use Case [27]

4.2.1.4 Sigfox based Asset Tracking

Airbus faced a global logistics challenge, wanting to increase visibility of various assets, improve transport cycle times and reduce lost items. Operating across multiple countries in Europe as well as having USA and China operations, Airbus needed a low cost solution for locating things both indoors and outdoors. The tracking devices needed to have a 3 year battery life when sending 20 messages/day and outdoor location accuracy requirements of 20m. Airbus turned to Sigfox to provide the connectivity for its asset tracking system, allowing Airbus to follow up on thousands of recyclable packages in real time as they transit through various warehouses and international departments [28].

Note, in contrast to Wi-Fi's global bands, LoRa and SIGFOX are deployed in different bands across different geographies. However, roaming requirements have traditionally required the unlicensed band to be harmonized over multiple countries. At its recent Sigfox IoT World Expo, the company announced a new service called Sigfox Monarch that allows modules to communicate more easily with local networks as they move around the world [29].

4.3 Identity, Roaming and Enterprise Use Cases

EAP/WPA2 has been widely deployed within the enterprise environment for supporting traditional use cases of providing wireless connectivity to computers, tablets and smartphones. The RADIUS authentication server will typically integrate with an external local identity store. For example, the RADIUS server may leverage Microsoft Active Directory to authenticate an enterprise user, or it could leverage an LDAP bind operation to locate an enterprise user in the database and recover credentials to enable the user to be authenticated.

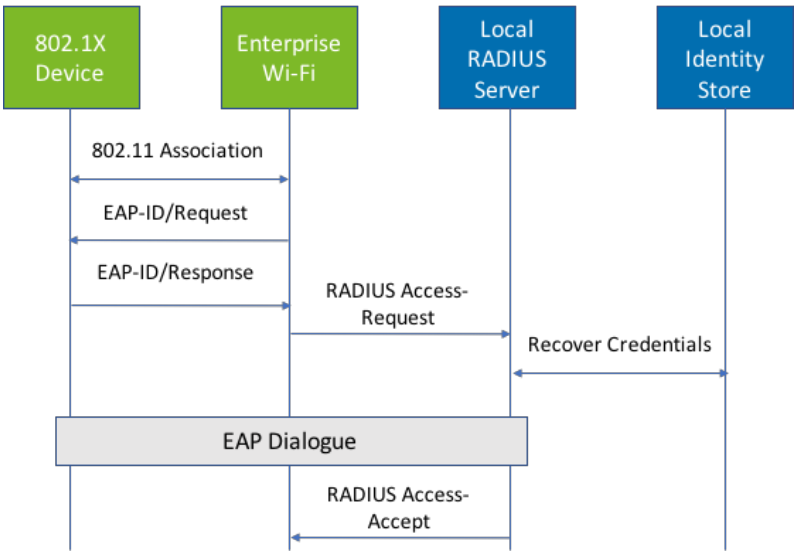


Figure 4-2: Authentication of Traditional Enterprise Endpoints

Compared to this traditional environment, where enterprise IT needs to scale to 100s of users and low single number of devices per employee and where the identity/credentials are all managed within the local IT environment, the emergence of IoT will likely see the enterprise environment characterized by 100,000 of devices that may use many different credential types and be supported by a wide range of identity providers.

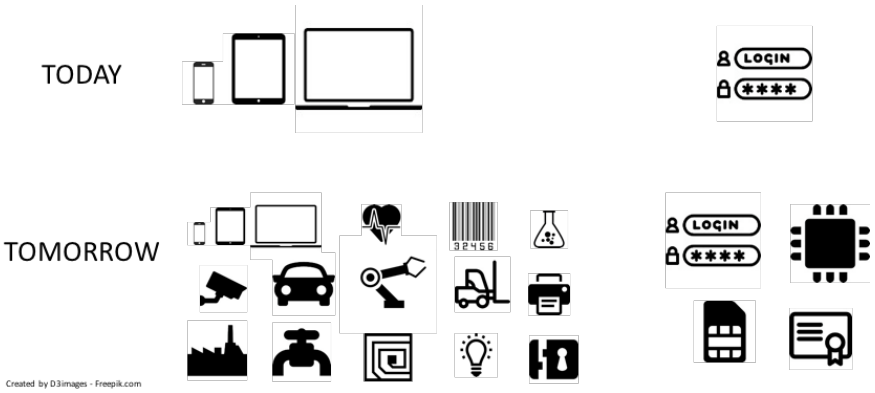


Figure 4-3: Evolution of the enterprise environment

In one sense, this means that the new devices can be considered as “roaming” into the Enterprise environment, with the need to support EAP authentication using a Home Identity Provider that is outside the enterprise’s domain. Hence, these new enterprise IoT use cases may trigger the adoption of Next Generation Hotspot techniques used today to support conventional roaming within a Passpoint-based Service Provider environment, and re-apply/adapt those to address emerging requirements within the Enterprise IoT environment.

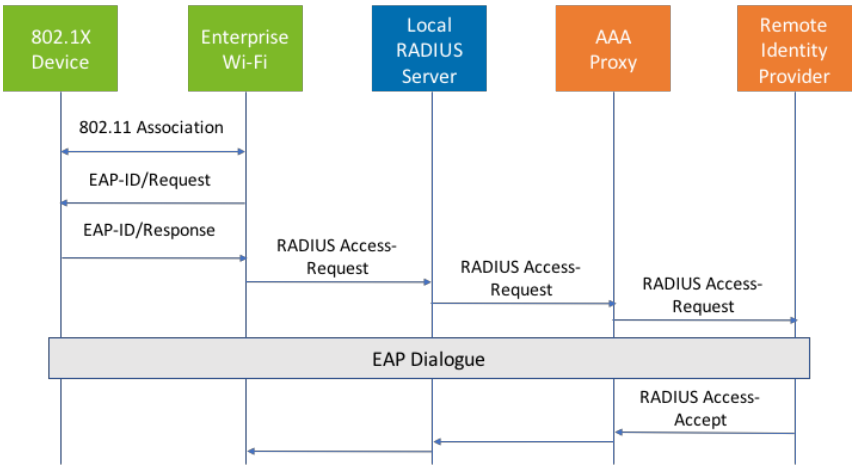


Figure 4-4: Authentication of IoT Endpoints with Remote Identity Provider

4.3.1 Enterprise 5G Roaming Use Case

New industrial use cases for IoT within a 5G environment are discussed in [30]. These include scenarios whereby the credentials used are managed by a non-MNO entity, in the industrial automation case, corresponding to the factory owner. These are called “Non-3GPP subscription identifiers” in [31].

However, the 3GPP study into next generation security aspects is clear that 3GPP roaming is only based on 3GPP subscription identifiers. Even though an identifier of the type "sensor12345@factory.example.com" can be used within a 5G industrial automation environment, because 3GPP roaming is not based on NAI, the non-3GPP subscription identifier cannot be used in roaming scenarios.

However, there may be scenarios where such a capability is desirable. One example use case is the localization of assets within an enterprise environment that, whilst primarily may be used to provide support for on-site logistics, may also cover scenarios where assets, such as forklifts, auto guided vehicles and vessels, move outside of the enterprise site environment. Such a scenario then motivates the support for a “roaming” use supporting 5G access by the non-3GPP subscription identifier outside of the factory environment.

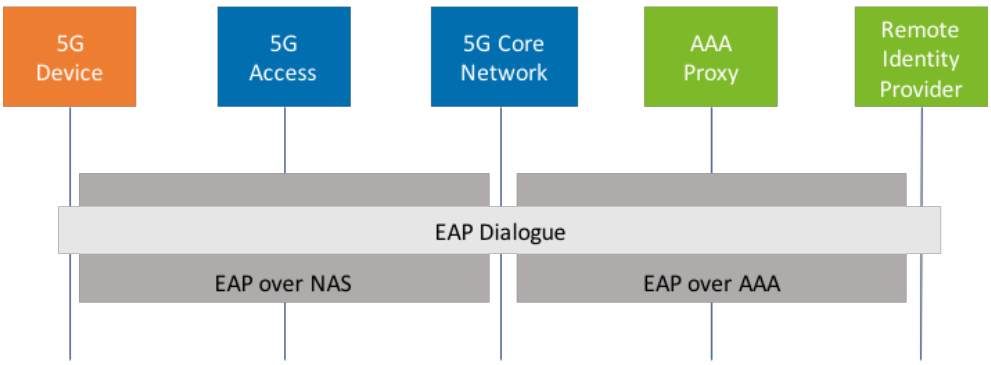


Figure 4-5: NAI-based 5G roaming for non-3GPP subscription identifiers

4.4 Providing courtesy access using Neutral Host Networks

The current enterprise environment enables enterprise employees to automatically authenticate to enterprise Wi-Fi networks using EAP. However, the above description highlights the enterprise environment of tomorrow will be far more heterogeneous. Not only enterprise employees, but partners, contractors, visitors and public may be offered connectivity to the enterprise network acting as a neutral host network. The massive numbers of IoT devices within the enterprise environment will be provisioned with a wide range of credentials, managed by a wide number of identity providers. This neutral host enterprise network may offer connectivity to these different devices using different technology. Some IoT devices may be connected using Ethernet based networks, others type of devices may connect using Wi-Fi based technology, still other may use 3GPP derived technology, e.g., MulteFire Alliance defined architectures configured in Neutral Host Network configuration.

4.4.1 Monetizing courtesy access

The enterprise use cases can be characterized as providing connectivity in order to support some alternative value proposition. Because the Enterprise business is monetizing the IoT deployment by alternative means, e.g., enhancing worker productivity, delivering connectivity in smart buildings to increase energy efficiencies, making their venue more amenable to visitors, the overall requirements to support roaming based monetization of access may be diminished. In particular, Mobile Experts have compared the economic value of indoor coverage/connectivity for the Mobile Network Operator and contrasted that with the value provided to the enterprise [32]. Figure 4-6 illustrates the imbalance of derived value, indicating the significant disparity with the enterprise often deriving significant economic benefit that relies on wireless coverage, a situation that is surely set to be exacerbated by the pervasive adoption of wireless IoT devices within the enterprise.

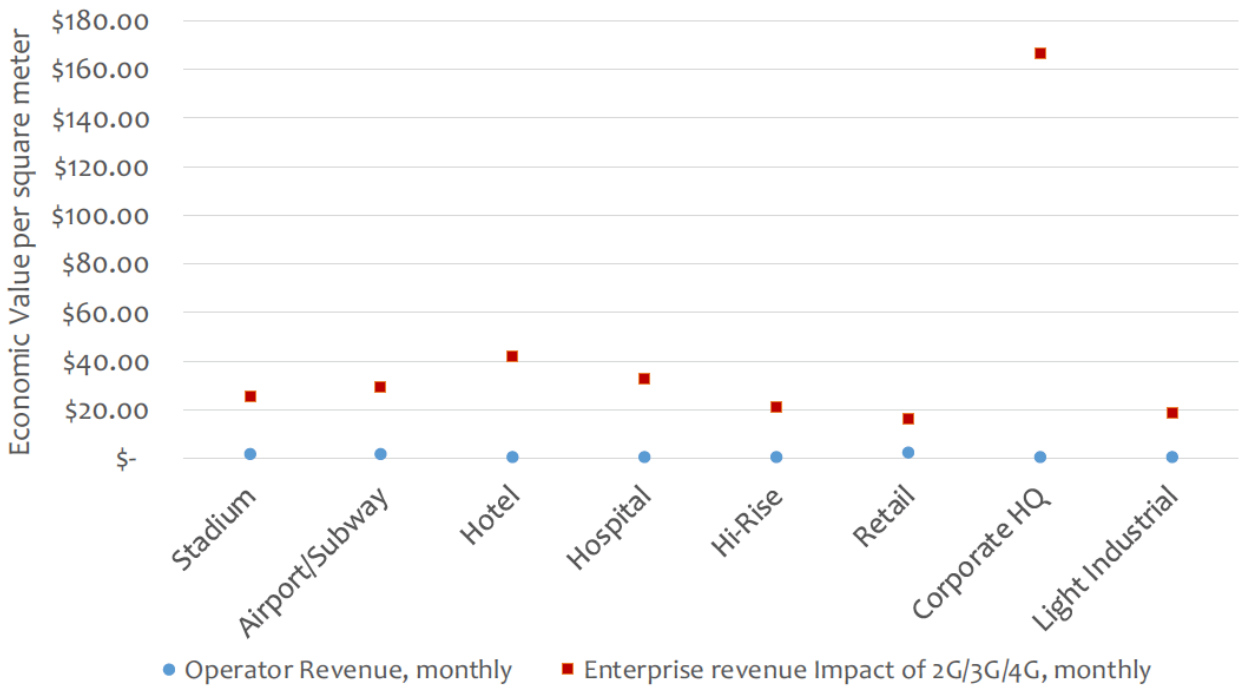


Figure 4-6: Value of Wireless Coverage, by Enterprise Type (Source Mobile Experts)

This situation means that, whereas an Identity Provider for an IoT Thing will need to be involved with the authentication of the IoT Thing within the enterprise environment, because connectivity may be being provided as a courtesy and the deployment monetized by alternative means, there will unlikely be requirements associated with billing for enterprise IoT connectivity.

4.4.2 Use of Enterprise Acceptable Use Policies and Liability Disclaimers

Today's solution for supporting on-boarding of non-enterprise devices is to use web-redirect to a guest portal. Whilst delivering a poor on-boarding experience, the web redirect does enable the enterprise to ensure that users have accepted the terms of service together with any policy and liability disclaimer before receiving Internet access.

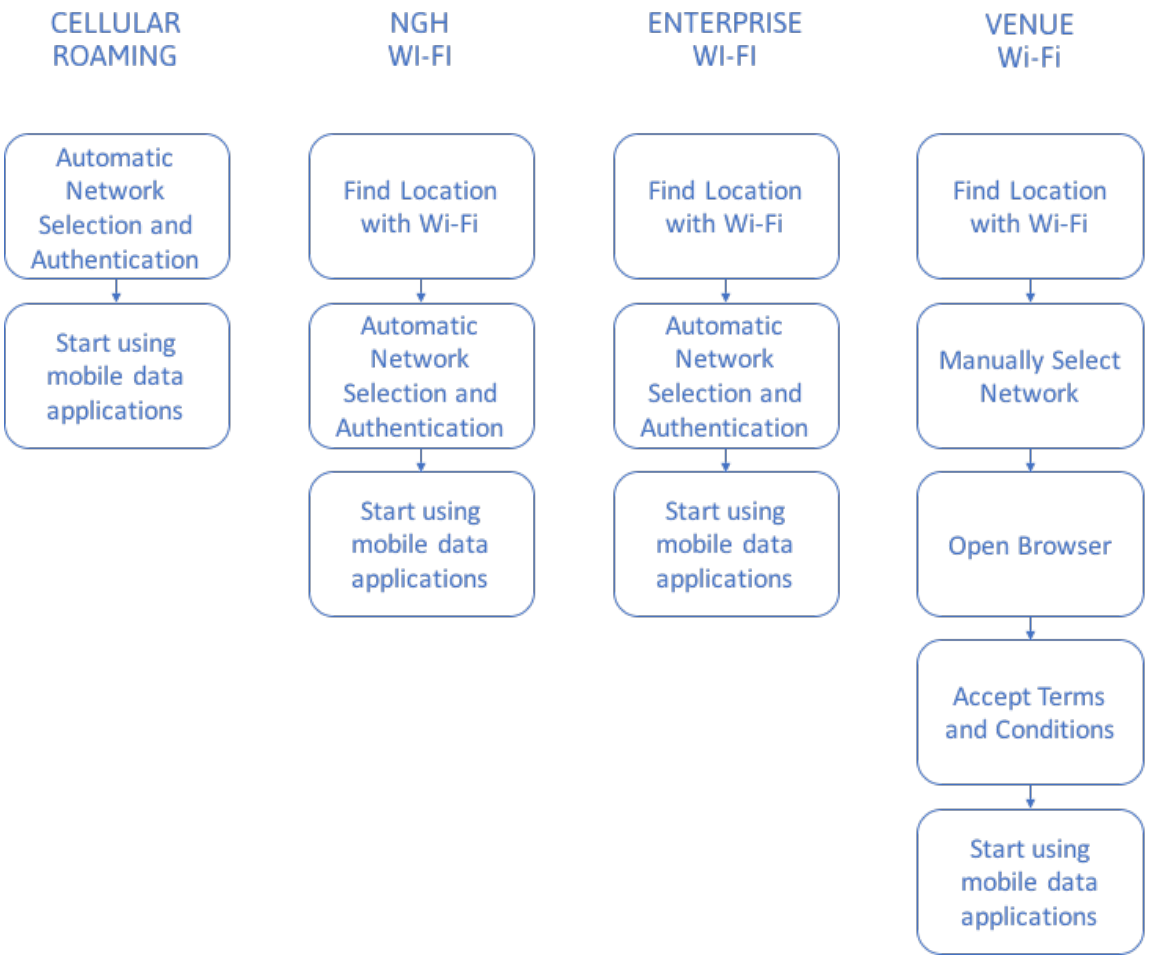


Figure 4-7: Contrasting user experience in different mobile data environments.

In contrast to this fragmented view of enterprise specific terms of service and acceptable use policies, WBA's Next Generation Hotspot systems are built on a foundation of Terms of Service that have been agreed to by a subscriber with their Home Service Provider, obviating any need for agreements to be made between the user and the Visited Network Provider.

It is evident that this inherent capability of WBA's roaming architecture can be a key differentiator, and may trigger further analysis of whether WBA's roaming concepts and Passpoint provisioning can be re-applied to the enterprise IoT environment.

5 Baseline WBA Technical Framework to Address Roaming

5.1 Intro to generic roaming Functions

As described in section 3.1, a Wi-Fi Roaming Service is the Wi-Fi Network Access Service provided by the visited network provider (VNP) to a Customer using the VNP's Wi-Fi Network(s) and the home service provider's (HSP's) customer relationship to access the Internet. The roaming process is normally performed between two operators when at least one of them operates a network and the second has users who are willing to use the Wi-Fi services of the first operator. This process can be divided into two major activities:

1. The technical interconnection between networks either directly or using an intermediary hub, where all real time activities such as authentication and accounting are performed
2. The activities that are related to the commercial background aspects of roaming, such as billing, charging and tariffs.

For Wi-Fi roaming services, the VNP and HSP must have interoperability mechanisms between them. For Next Generation Hotspot service, the visited network provides the connectivity to the client devices, but signals authentication of the roaming client devices to the home network AAA servers, typically via a RADIUS client being implemented on the Access Controller.

Operators may have different approaches when developing a roaming strategy. It is relevant to point out that there are two main scenarios available for operators to interconnect their networks, either through a direct connection or by using a third party to facilitate that interconnection. For this last scenario, there are alternative deployment models, ranging from both operators using the same hub or just one operator using a hub provider.

Much work in the roaming space has been applied to help Wi-Fi operators standardize the approach to ensure the best roaming experience for WBA wireless network users, and to promote the rapid set up of roaming agreements between operators using the WBA's standardized financial and technical approaches based on WRIX.

5.2 The WRIX Framework

As the dominant unlicensed wireless technology, Wi-Fi adoption has experienced phenomenal growth in recent years. Not just a huge growth in number of operator deployed hotspots being deployed by several operators, but also new players emerging in the ecosystem (cities, venue owners, retail brands and specific vertical market service providers) and new value-added services being deployed (Wi-Fi Calling, Location Based Services). NGH expansion to incorporate IoT services as a feature under the WRIX-N framework would allow operators the value-added benefit of enablement of their customers IoT devices.

Carrier grade Wi-Fi platforms, Next Generation Wi-Fi, Wi-Fi roaming and Passpoint have enabled the Wi-Fi ecosystem to develop new services for consumers and enterprises and to develop new

monetization strategies and business models (e.g. Wi-Fi First operators, advertising, location based services).

The WBA has been a leader in the promotion of Wi-Fi Roaming and has harnessed this opportunity 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

The WBA has developed a technical framework to address the requirements for roaming between network partners. This framework constitutes the best practices to simplify the interactions between partners.

The extension of the WRIX frameworks to include the special requirements of the IoT devices and consequentially, the increase of User Data Records (UDR) will be addressed and taken into consideration in this document. The best practices for UDR handling cover possible optimization of WRIX procedures that can be adapted to address the large amounts of potential records stemming from the massive amounts of low cost IoT sensors. This document will discuss alternative approaches and recommendations in order to ensure that the WBA stakeholders are best positioned to support the broadest range of IoT deployments.

One of the main aims of WRIX is the interoperability of wireless networks. The best practices are described in the following documents maintained by the WBA:

- WBA WRIX Umbrella Document
- WBA WRIX for Network (WRIX-n)
- WBA WRIX for Radius Interconnection (WRIX-i)
- WBA WRIX for Clearing (Data and Financial Clearing) (WRIX – d/f)
- WBA Location Feed Format & File Exchange Standard (WRIX-L)

These documents are intended to help operators avoid some of the network configuration pitfalls and to standardize the approach between operators to ensure the best roaming experience for users, and to promote the rapid set up of roaming agreements between operators using standardized financial and technical approaches based on the WRIX framework.

5.3 Overview of WRIX Interfaces

The following figure shows the main entities in this WRIX model:

A separate WRIX may be considered for every kind of **interaction**, then:

- WRIX-n – Is an organization that operates and manages the network for the VNP
- WRIX-i – Is an organization that performs and manages the interconnection between a VNP and HSP.
- WRIX-L – is the organization that facilitates the exchange of hotspot location information between roaming partners.
- WRIX-d – is the organization that provides the exchange of session information needed to support wholesale billing validation, reconciliation and settlement (Data Clearing) between the VNP and HSP.
- WRIX-f – the organization that manages the exchange of invoices, payments, and foreign exchange between the VNP and HSP.

According to this model, WRIX entity/role/functionality/module (implemented either in-sourced or outsourced) is always considered as the end points for the specific interface implementing the corresponding kind of interaction, while VNP entity represents just the network provider role and HSP represents the role for retail service to the end customer/user.

The following diagrams depict the role and function of the various areas:

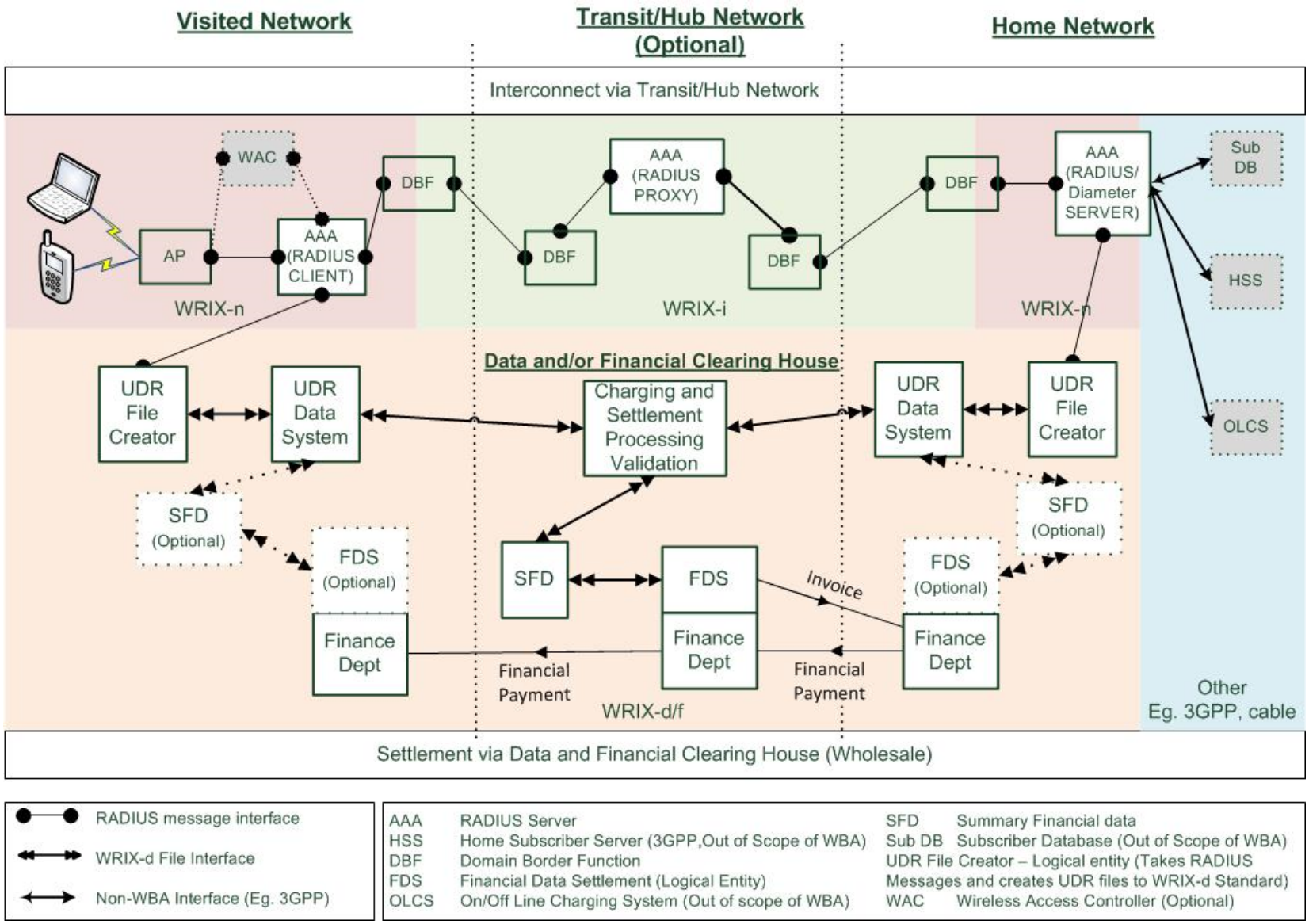


Figure 5-1: WRIX Functionality with interconnect via a Transit/Hub and settlement via Data and Financial Clearing House

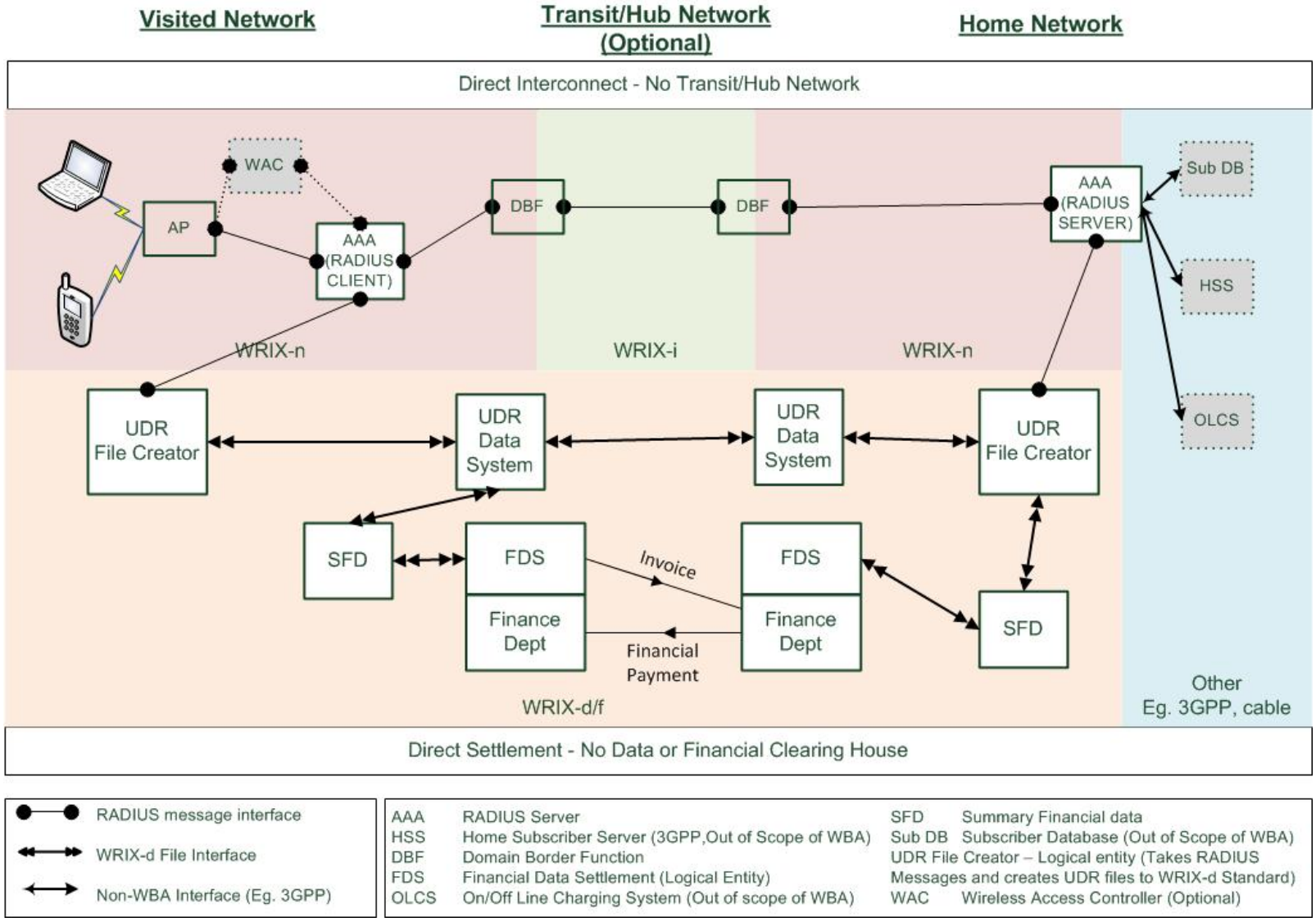


Figure 5-2: WRIX Functionality with Direct Interconnect and Direct Settlement

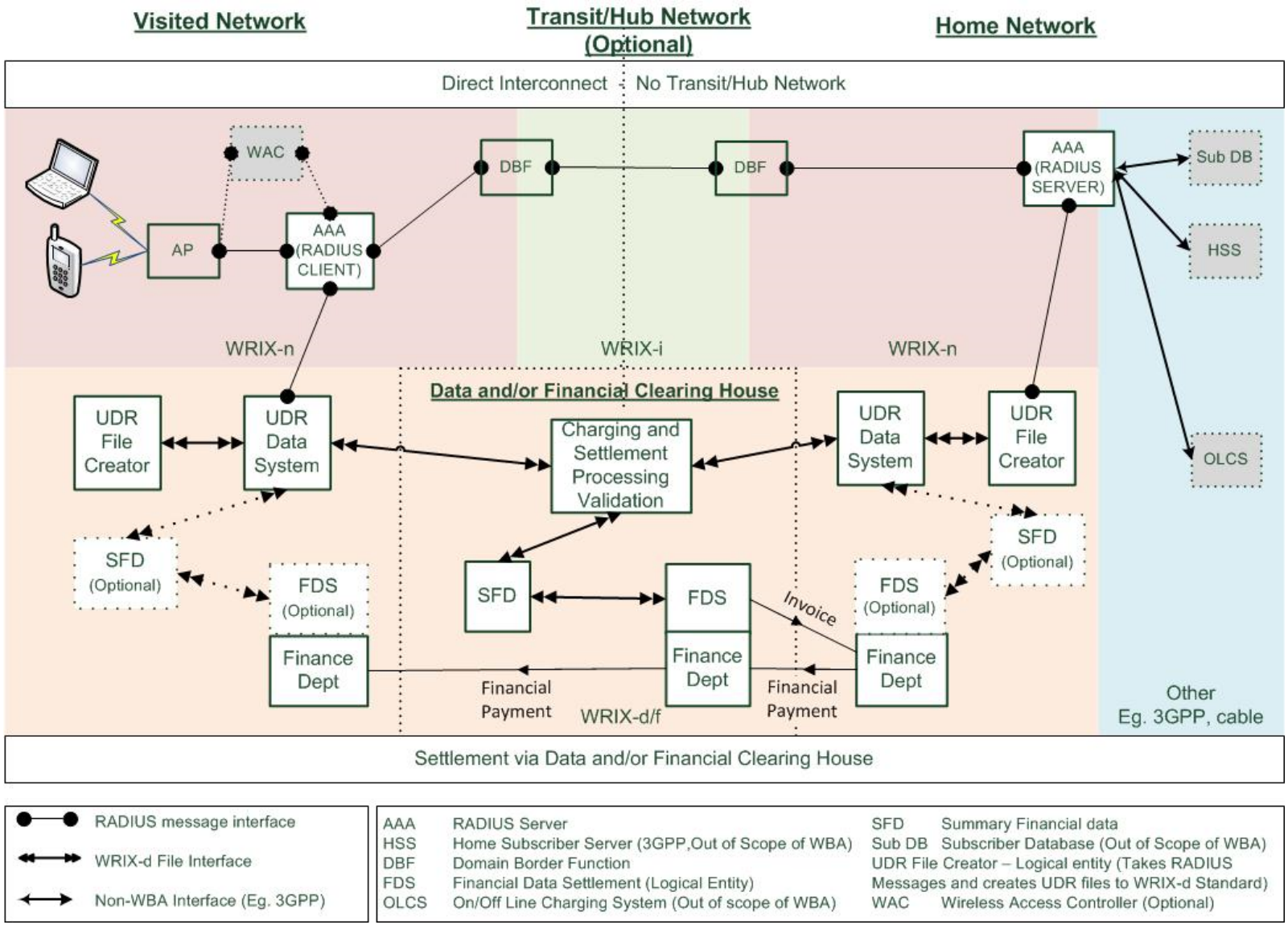


Figure 5-3: WRIX Functionality with Direct Interconnect and Settlement via Data and/or Financial Clearing House

5.4 Functional Activities by WRIX Module

Here below is a summary / high level view of the WRIX modules Functional Scope:

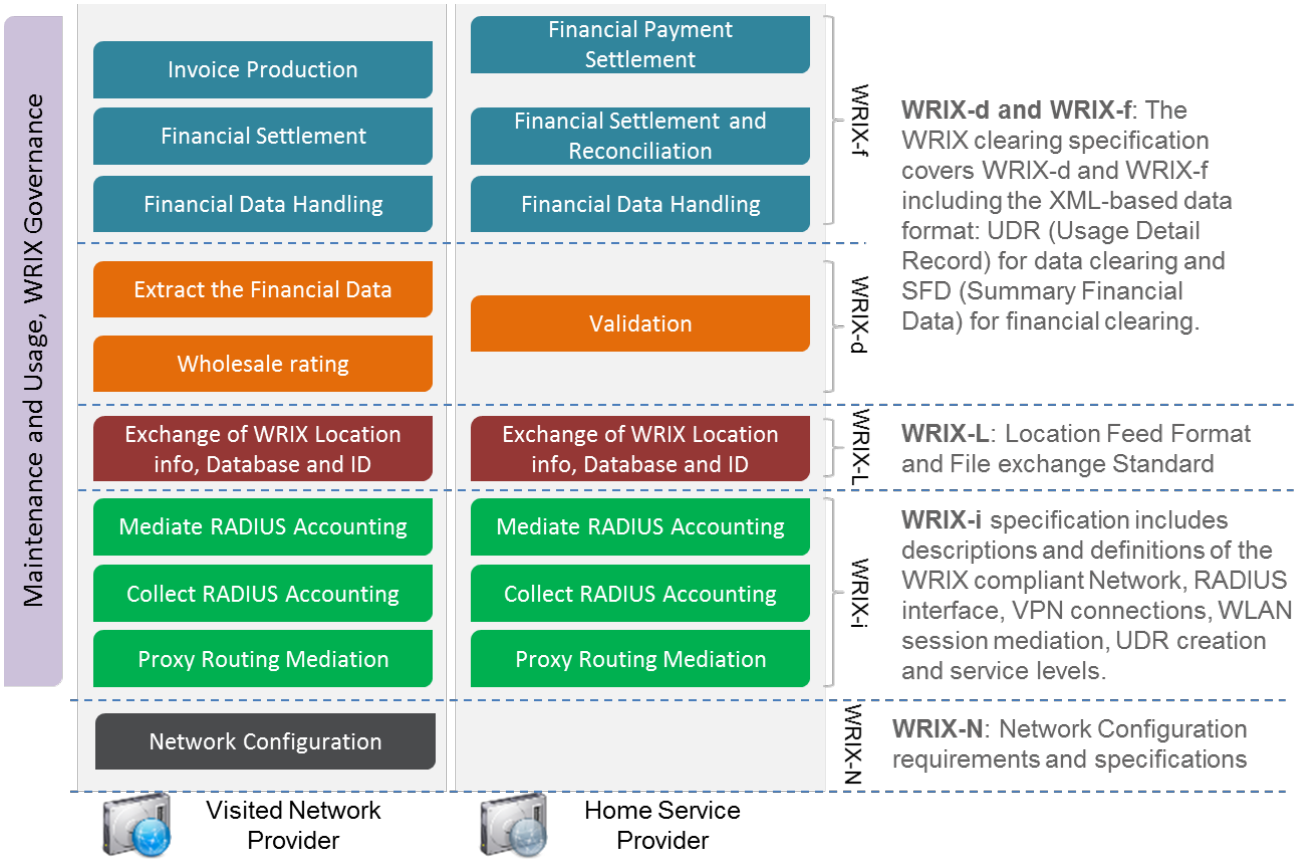


Figure 5-4: Summary of WRIX module functionality

WRIX-i (VNP):

- 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 (VNP)

WRIX-i (HSP):

- 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)

WRIX-L (VNP)

- Provides a location file
- Distributes to roaming partners

WRIX-L (HSP)

- Receives location file
- Uses the location file in connection client software distributed to subscribers

WRIX-d (VNP):

- Receive the mediated records for wholesale billing from the WRIX-i (VNP).
- Rate the received mediated records for wholesale billing using the IOT as specified in the bilateral roaming agreement;
- Send the rated wholesale records to the appropriate WRIX-d (HSP)
- Extract and send the Financial Data to the WRIX-f (VNP)

WRIX-d (HSP):

- Receive rated wholesale billing records from the WRIX-d (VNP);
- Validate those records and potentially trigger reconciliation mechanism.
- Perform data reconciliation

WRIX-f (VNP):

- Receive Financial Data sent by the WRIX-d (VNP)
- Send Financial Data to the WRIX-f (HSP)
- Reconcile the financial settlement together with the WRIX-f (HSP)
- Calculate and create invoices for each HSP
- Send invoices to the WRIX-f (HSP)
- Jointly administers financial settlement with the WRIX-f (HSP)
- Provide support for dispute resolution.

WRIX-f (HSP):

- Receive Financial Data sent by the WRIX-d (VNP)
- Reconcile the financial settlement together with the WRIX-f(VNP)
- Receive invoices sent by each WRIX-f (VNP) of the respective HSP´s roaming partners
- Jointly administers financial settlement with the WRIX-f (VNP)
- Provide support for dispute resolution

5.5 WRIX Security

The WRIX architecture is based on static security associations between peers. Figure 5-5 illustrates a WRIX deployment supporting the deployment of Next Generation Hotspot. The WRIX-N based Visited Network Provider (VNP) routes RADIUS messages based on pre-defined REALM routing policies that identify the next RADIUS server. Security of RADIUS uses pre-shared secrets that are statically configured and agreed as part of the VNP/HUB agreement. This agreement is also used to agree the pre-shared keys involved in deriving the IPSec security association for further protecting the WRIX signaling.

The same bi-lateral agreements can be used to protect the security of signaling between WRIX-I hub providers and between WRIX-I hub providers and the Home Network Provider.

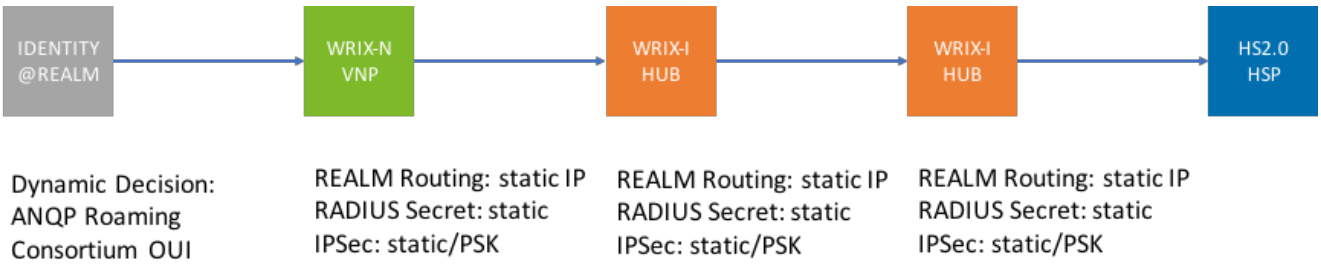


Figure 5-5: Statically defined WRIX Security/RADIUS Hierarchy

6 Enhanced functionality that may be used to support additional IoT roaming requirements

6.1 Flexible Framework for IoT Authentication

The use of EAP as a flexible authentication framework by Wi-Fi networks has facilitated their support of a wide variety of use cases with different authentication mechanisms, ranging from enterprise access, through to carrier Wi-Fi. Moving to IoT, the same reasoning has led researchers to advocate the use of EAP within an IoT environment [33], claiming another key advantage of EAP is that it operates at the data link layer and introduces lower communication overhead in comparison to different authentication mechanisms.

As an example of the adoption of EAP by an IoT ecosystem, the Wi-SUN alliance has defined the use of EAPOL over 802.15.4 systems [34], where the FAN node implements the Supplicant role and the FAN Border Router implements the Port Authenticating Entity. Also, moving forward the 5G Core Network has defined a new Authentication Server Function (AUSF) to enable support of the EAP authentication framework within the 5G system [35]

However, whereas the WBA may be motivated to encourage all IoT ecosystems to adopt EAP and benefit from its advantages, there will always be examples of IoT systems that define the use of other non-EAP authentication frameworks. On example of such is the LoRa Alliance that has defined its own PSK based join procedure, highlighted that the IoT roaming system will also need to support other non-EAP authentication methods.

6.2 IPv6

WBA's earlier analysis of IPv6 [36] identified a number of gaps, and in particular, related to roaming, calling out the need for roaming interconnections to support IPv6 related AVPs and VSAs. The Internet of Things and the rapid increase in number of devices connected to the network can only accelerate the need to address the scalability limitations of conventional IPv4 deployments, specifically as it relates to IoT device addressing.

The adoption of IPv6 by IoT deployments will likely trigger the removing of the conventional Network Address Translation (NAT) functionality that has been typically used in Carrier Wi-Fi deployments; where Carrier Wi-Fi devices are allocated addresses from the private IPv4 address space. The use of NATs obviated any requirements for WBA's roaming infrastructure to support the signaling of the user's IP address in WRIX signaling exchanges. Specifically, the signaling of the framed-IP attribute in RADIUS exchanges has not been defined.

With the increasing adoption of IPv6 for device addressing and the associated removal of NAT functionality, it will be increasingly the case that IoT devices and carrier Wi-Fi users will be allocated globally routable IPv6 addresses. In such cases, the home network provider may be able to derive benefit from knowing the IPv6 address allocated to their subscriber's equipment and so WBA's Roaming Sustainment Group should consider introducing the Framed-IPv6-Address attribute into WRIX signaling exchanges.

6.3 Re-Use of WRIX d/f by non-RADIUS based IoT systems

Operators of IoT systems that are not based on RADIUS and/or EAP, e.g., LoRa Alliance, may decide to leverage existing WBA defined WRIX system for data clearing and settlement for supporting IoT roaming. This section highlights possible enhancements to those systems to enable them to leverage the WRIX framework.

6.3.1 Generalized UDR for IoT Data Clearing

There may be cases where the IoT system wants to leverage the existing WRIX defined Usage Data Record Format for IoT data clearing. However, the current WRIX UDR includes various fields that either assume a RADIUS based authentication or are specific to Wi-Fi usage. The following analysis examines different fields in the UDR and discuss whether equivalents exist in a non-RADIUS LoRa environment.

- **Visited Network provider (String16)**

In LoRa, a 24 bit NetID is used to identify the roaming partners Network Server

- **Home Service provider (String 16)**

In LoRa, a 64-bit JoinEUI is used to identify the Home Network

- **Cause for Termination (From RADIUS attribute 49)**

In Lora, there is no defined signaling exchange to trigger the exit/de-activation procedure.

This means there may be no formal way of closing a charging record.

One approach, if LoRa Alliances wishes to re-use the UDR exchange, is to recommend that LoRa alliance defines a maximum duration (e.g., 24 hours) before records are closed. All LoRa UDRs will then use “Session Timeout” termination cause.

Note, GSMA BA.27 defines 24 hours for the maximum duration of a partial record.

- **Venue Class/Location Name**

LoRa does not define venue classes and because of the wide area nature of coverage, this attribute does not seem to apply to the LoRa use case.

- **User Name – NAI for Wi-Fi**

In LoRa, the user-name is equivalent to the 64 bit DevEUI

- **Chargeable User ID** – transferred in Access Accept RFC 4372

In LoRa there is no concept of a Chargeable User ID.

One approach, if LoRa Alliances wishes to re-use the WRIX-defined UDR exchange is to recommend that LoRa alliance defines such a field in their Join Accept message signaled between JS-to-NS.

- **Device ID** – Wi-Fi MAC Address.

The Device ID is equivalent to the 64 bit DevEUI

6.3.2 Generalized Summary of Financial Data for IoT Financial Clearing

There may be cases where the IoT system wants to leverage the existing WRIX defined procedures for IoT financial Clearing. The following analysis examines different data structures in WRIX defined Summary of Financial Data (FSD) file.

- **Visited Network provider (String16)**

In LoRa, a 24 bit NetID is used to identify the roaming partners Network Server

- **Home Service provider (Sting 16)**

In LoRa, a 64-bit JoinEUI is used to identify the Home Network

- **Number of Sessions**

In Lora, there is no defined signaling exchange to trigger the closing of a session. This means there is no formal way of defining a session.

One approach, if LoRa Alliances wishes to support session based financial clearing is for the LoRa alliance to define a session from a financial clearing perspective. For Example, a LoRa session for financial clearing purposes could be defined as whenever LoRaMAC traffic associated with a unique DevEUI is signaled within any 24 hour period.

- **Total Charged Duration**

In Lora, there is no defined signaling exchange to trigger the closing of a session and hence determine the duration of any charging interval. An implied session idle time can be used, e.g., based on the definition of when a session is ended.

6.4 Billing and Charging impacts on IoT roaming

In CLP-08 [37] GSMA analyses the impact of IoT on billing and charging. The document discusses new scenarios that may arise in IoT environments. These include:

- Split billing, driven primarily by the automotive sector.
- Demand billing, driven by utilities or smart city sensing markets.
- Batch billing, applying predominantly to enterprise IoT / M2M services
- Data pooling, applying to consumer services.

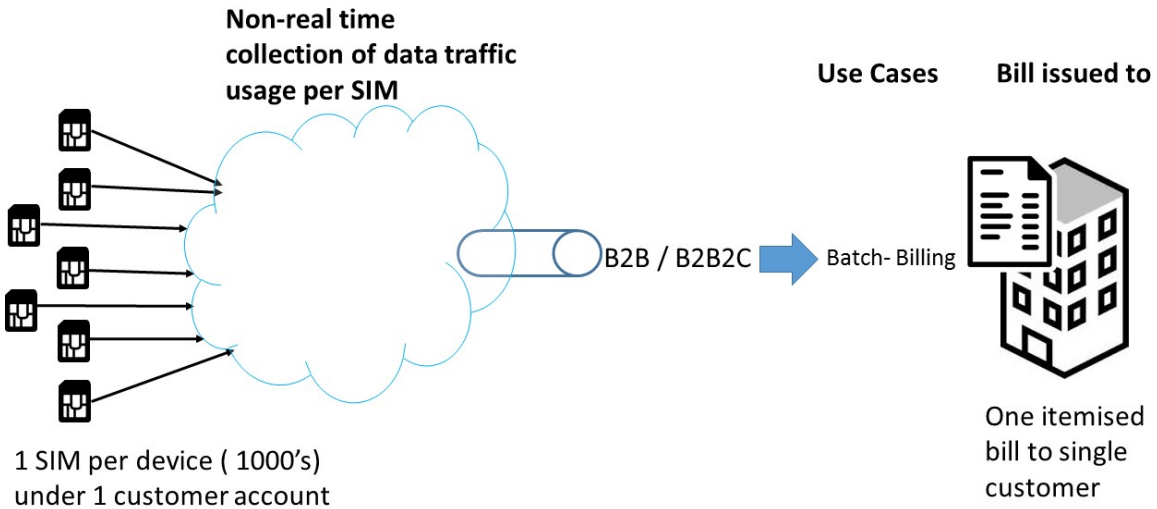


Figure 6-1: Batch Billing [Source GSMA CLP08 [37]]

6.4.1 Split Billing

In terms of split billing, in the cellular environment this can be achieved by using multiple Access Point Names (APNs). CLP-08 describes alternative approaches, including splits based on IP destination address, URL, and interactions with external policy servers.

6.4.2 Batch Billing

Existing support for wholesale contracts typically utilize batch billing, where a single bill is produced for a large number of devices.

6.4.3 Aggregated Usage Reporting

AuRs are new record types able to be exchanged using Transferred Account Procedures. Compared with existing business requirements that only permit usage in any 24-hour period to be included in a record, these records include start and end dates for the reported usage, as well as unit type plus charged units and the aggregated usage charge. Aggregation types supported include IMSI-level aggregation, APN-level aggregation and Rating-group-level aggregation.

6.4.4 Bulk Data Reporting

Within the cellular community, there has been recent discussion regarding roaming and the evolution towards wholesale billing. In particular volumes of CDRs are rising rapidly, whilst their incremental value is falling. Bulk Data Roaming is one approach being positioned as an alternative for supporting IoT roaming.

BDR leverages the fact that that usually in cellular roaming, traffic is tunneled back to a home P-GW/GGSN that is able to generate CDRs to feed a retail billing system. This allows BDRs to be used to signal aggregated records, e.g., daily totals. Initial indication from GSMA indicate that a shift to bulk wholesale model will reduce data processing by 200-300% for the case of IoT roaming.

The Bulk Data Report contains:

- Mandatory fields for the reconciliation as well as for wholesale calculation and invoice production, including visited network, served party MCC/MNC, date at which session are aggregated, number of distinct sessions are aggregated, number of distinct IMSIs within the session date, aggregated usage per session
- Optional fields supporting threshold charge models, either per day or per day and per IMSI
- Optional records of grouped types when the bulk usage is grouped by third “dimension” parameters which are considered in the wholesale charge models or requested for the purpose of reconciliation, such as APN, QCI, or RAT type

6.4.5 Possible Enhancements to WRIX

Compared with GSMA's recently defined AURs and BDRs, WRIX already supports exchange of summarized reports with its exchange of Summary Financial Data (SFD) records, see Table 6-1. This capability leverages the fact that end-to-end RADIUS signaling is still available for the Home Service Provider to generate retail billing for the Wi-Fi usage. Using SFDs there is one record generated per roaming partner per defined period.

Field name	Source	HBT	Description	Format
VNP	Wi	B	Inherit from UDR	Inherit from UDR
HSP	Wi	B	Inherit from UDR	Inherit from UDR
BillingMonth	Wi	B	Inherit from UDR	Inherit from UDR
Currency	Wd	B	Inherit from UDR	Inherit from UDR
BatchTotalNumberOfSessions	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalUsedDuration	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalUsedVolumeDownLink	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchToatalUsedVolumeUpLink	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalChargedDurationAmount	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalChargedDuration	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalChargedVolumeAmount	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalChargedVolume	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalSessionAmount	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR
BatchTotalTaxAmount	Wd	B	Inherit from the trailer of the UDR	Inherit from UDR

Table 6-1: WRIX SFD Content [38]

Compared with GSMA TAP records that are encoded using ASN.1, WRIX records are encoded using XML. It is claimed that the verbosity of XML increases RAM usage, bandwidth requirements, and operating costs [39] and therefore the scaling requirements of the Internet of Things may motivate WBA to investigate alternative record encoding techniques.

With capabilities to optimize data record handling already defined in WRIX, the final aspect covered by GSMA's analysis is split billing. One of the example use cases for split-billing is that of the connected car, where a single IMSI is used to support communications for car telematics as well as user infotainment. Because the end-to-end RADIUS signaling used in WRIX to generate billing is not able to differentiate between Wi-Fi usage for different applications, then there are clear challenges in being able to use WBA's currently defined roaming architecture to support such use cases. Approaches to enable such split retail billing to be supported would seem to necessitate the additional tunneling of user plane traffic between the Visited Network Provider and the Home Service Provider, enabling the HSP to differentiate between the traffic destined to different services, e.g., based on destination IP address. Such an approach would obviate the need for the visited network provider to be aware of such differentiation.

Because of such limitations, WBA's Business Working Group may wish to monitor the market adoption of split retail billing as it relates to IoT deployments and to understand whether WBA needs to trigger the definition of enhanced capabilities to support such within a carrier Wi-Fi roaming environment.

6.5 Automating WRIX Security

6.5.1 Automated Peer Discovery

As described in section 5, the current WRIX architecture is based on RADIUS with its particular requirement for security based on pre-shared keys which are uniquely tied with the IP address of the RADIUS server. This has restricted the use of dynamic discovery by the AAA client of the next-hop AAA server.

This scan be contrasted with the wide scale adoption of DNS to enable dynamic discovery of peer entities, e.g.,

- The inter-PLMN DNS is used to support user plane portions of cellular roaming where DNS is used to resolve an APN into a gateway address [40]
- DNS is used for discovering the "next hop" Diameter agent [41]
- The dynamic discovering of the MME using DNS resolution of the TAI-FQDN [42]
- The LoRa Network Server discovers the address of the LoRa Join Server using DNS [43]

DNS based discovery of RADIUS servers has been specified by IETF in RFC 7585 and is associated with the use of RADSEC. In particular, as the peer has been dynamically discovered, new procedures

are required to enable the client to verify that the discovered peer is authoritative for the NAI realm. These issues are addressed in more detail in the following section.

Automated peer discovery avoids the manual configuration of RADIUS clients and servers and the configuration of shared secrets that require additional administrative effort to manage.

The defined discovery mechanism is very similar to the approach used by the Diameter protocol, where DNS is used to match the NAI realm to a Naming Authority Pointer (NAPTR) record.

Adding automated peer discovery capabilities to the current RADIUS based WRIX-I framework may enhance the longevity of those systems, as dynamic peer discovery has been claimed to be one of the key advantages motivating the adoption of Diameter based AAA roaming.

Whereas Dynamic Peer Discovery for RADIUS does permit the RADIUS client to identify and directly connect to the RADIUS home server, RFC 7585 describes the benefits that roaming brokers/clearing houses can still provide in a dynamic environment, including:

- Where the roaming hub acts as a gateway for multiple back ends
- Where the roaming hub is used to normalize RADIUS messages
- Where a server has not been enhanced with dynamic peer discovery/RADSEC capabilities
- Where a home server does not want to receive request from un-configured peers

6.5.2 Automated security

The shared secret based RADIUS security can add significantly to the burden of administrating a RADIUS system. Furthermore, the use of MD5 to provide per-packet authentication and integrity checks has known weaknesses. Moving forward, the use of these pre-configured shared secrets is incompatible with the adoption of scaling techniques based on dynamic peer discovery.

These limitations can be addressed by the use of secured communications between RADIUS peers, using either TLS [44] or DTLS [45]. This approach obsoletes the use of IP addresses and shared MD5 secrets to identify other peers, enabling the use of alternative trust models, e.g., based on X.509 certificates.

Where the server has been dynamically discovered, the certificate can be used to verify that the peer is authoritative for the NAI realm. RFC 7585 describes a scenario where one or more specific root Certificate Authorities can be defined as issuing certificates for the specific purpose of establishing RADIUS trust and the use of a new X.509 certificate property "SubjectAltName:otherName:NAIRealm" that can be included in the certificate and when present contains the NAI realm(s) for which the server is authoritative.

Adding RADSEC capabilities to the current WRIX-I framework will likely enhance the longevity of those systems, as Diameter's security support has been claimed to be one of the key advantages motivating the adoption of Diameter based AAA roaming.

6.5.3 Automated Revocation

The use of certificates to automate security comes with the additional administrative task of how to deal with revoked certificates. This is not a new issue. Indeed, the Passpoint[tm] deployment guidelines [46] cover certificate revocation:

> "*CAs revoke OSU Server Certificates using OCSP. A revoked certificate will have its status pushed out to the CA's OCSP Server. OSU servers can obtain Hotspot 2.0 OSU Server Certificate status information by querying the issuing CA's OCSP server using the certificate's serial number and relay this information to mobile devices during TLS setup (aka OCSP stapling). OCSP locations are specified in the certificate's Authority Information Access field*."

This same OSCP stapling defined in RFC 6961 can be used to automate the revocation of the certificate used to establish trust between RADIUS peers. RFC 7525 which defines best practice for secure use of TLS and DTLS, recommends that servers support:

- OSCP (RFC 6960)
- OCSP stapling (RFC 6066)
- Status request extensions v2 (RFC 6961)

6.5.4 Different Scenarios for Deploying Automated WRIX Security

The enhanced capability delivered by the combination of RADSEC and DNSROAM can be deployed in different scenarios.

Deployment Option #1: RADSEC to secure WRIX interfaces.

One option is to enhance WRIX definitions to enable RADSEC to replace current RADIUS security. In particular, its deployment may be focused on protecting HUB-to-HUB signaling links, where the scaling challenges are less likely to be evident (e.g., because of the limited number of inter-HUB provider links that need protecting).

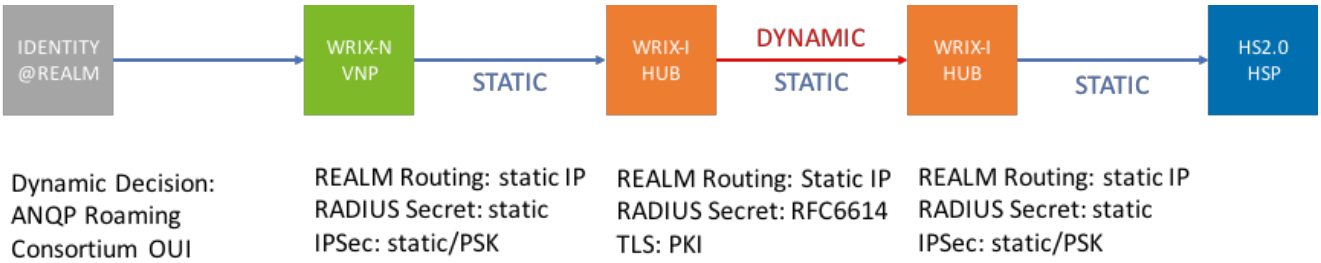


Figure 6-2: Introduction of RADSEC to secure interfaces between WRIX-I HUB providers.

Deployment Option #2: RADSEC and DNS ROAM used to secure WRIX interfaces.

An evolution of Option #1 is to additionally deploy DNSROAM capability to now support dynamically automated security between the WRIX-I based HUB providers.

Instead of relying on static realm based routing, DNS can be used to dynamically discover a RADIUS peer with the HUB's certificate indicating that it is authoritative for a particular realm.

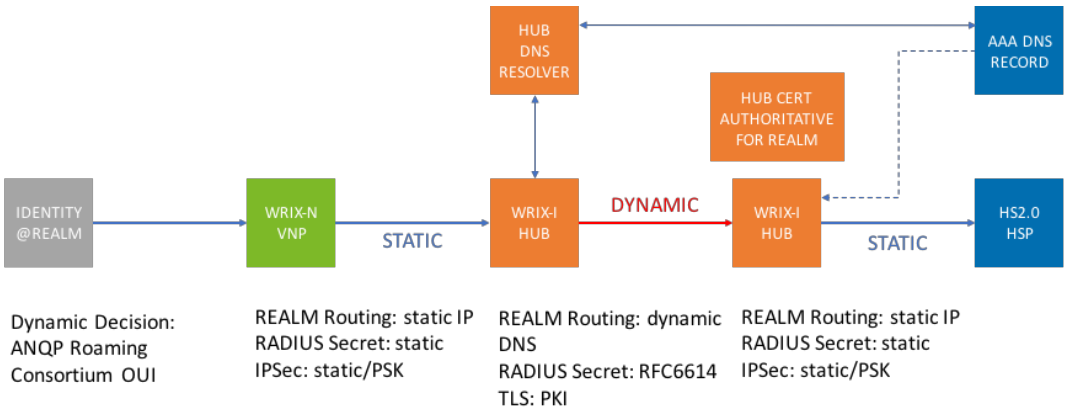


Figure 6-3:Using a combination of RADSEC and DNSROAM to automate the security between WRIX-I HUB providers.

Deployment Option #3: Automating security of the WRIX-I hub-to-HNP interface.

With some anticipating IoT deployments will see a dramatic increase in the number of identity providers, the same core capability can be used to automate the security between WRIX-I hub providers and home network providers/identity providers.

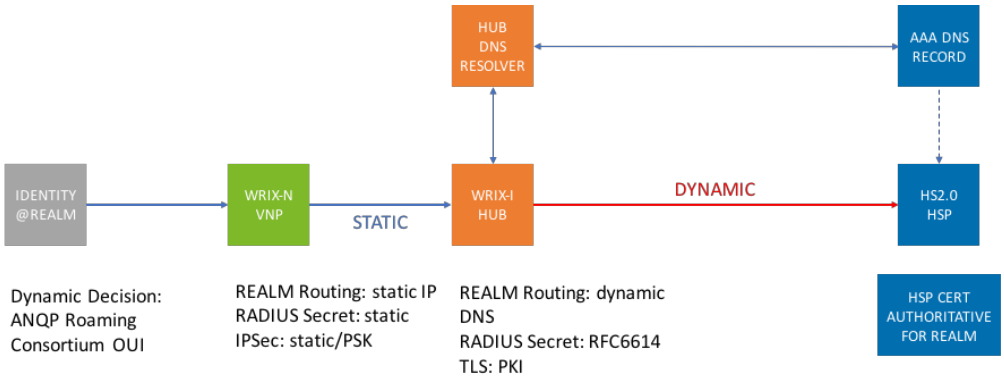


Figure 6-4: Automating the security between WRIX-I hub and HNP

Deployment Option #4: Automating security of the VNP-to-WRIX-I hub interface.

The same core capability can be used to automate the security between VNP-to-WRIX-I hub providers, for example to facilitate the rapid increase in access networks that may in the future want to offer WRIX based courtesy access to users.

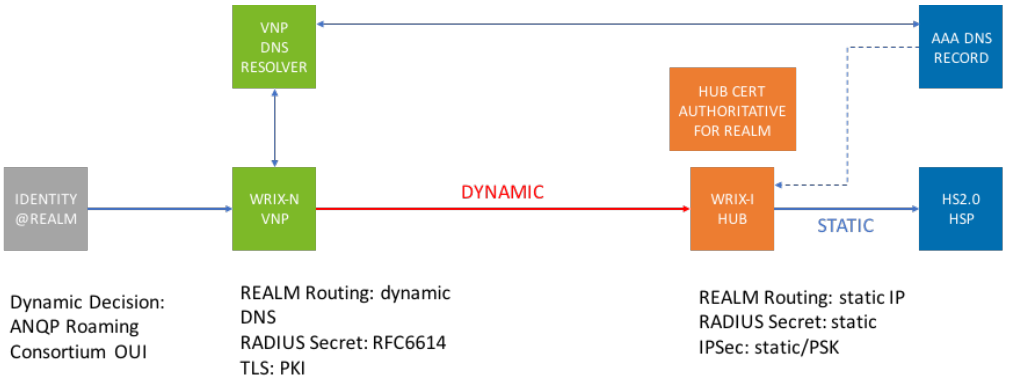


Figure 6-5: Automating the security between VNP and WRIX-I hub

6.6 IoT Application Security

The scale of the IoT applications exacerbates the necessity to manage exponentially more identities than traditional Wi-Fi-based systems do. Moreover, the migration to cloud architectures means that these IoT applications will likely be increasingly hosted within third party cloud provider environments. However, these externally hosted applications still require credential management. Instead of simply duplicating identity management capability in each application, an approach that is increasingly being used is so use ideneity federation to solve the above challenge.

Within the Internet's brower based environment, SAML has emerged as the dominant standard for enabling the secure exchange of authentication and authorization information between security domains [47]

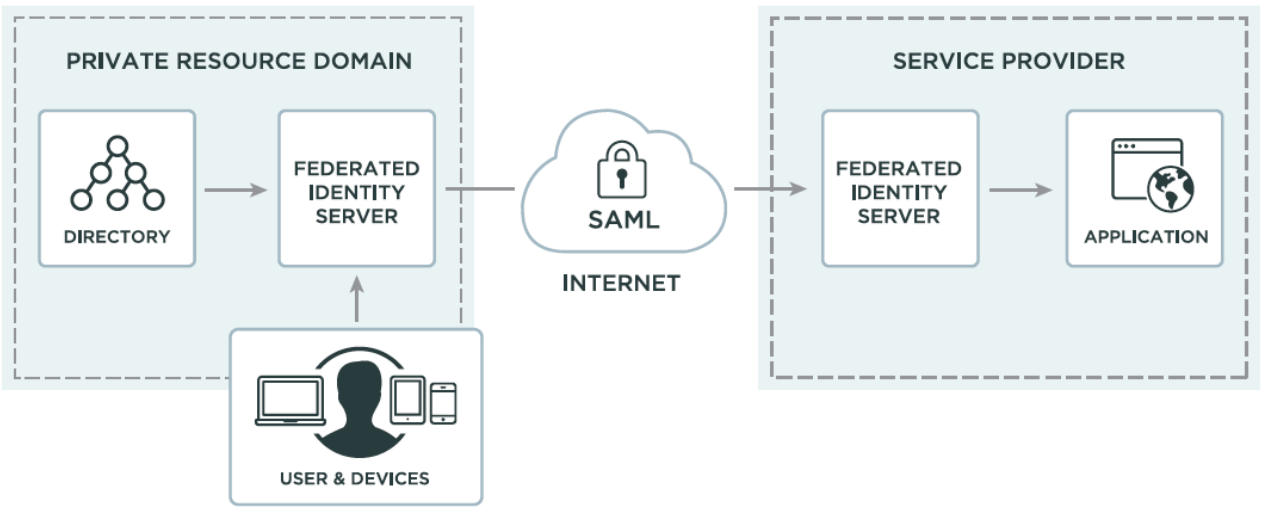


Figure 6-6: Federated identity translates the user's local identity into a SAMLassertion [47]

Leveraging SAML to enable these use cases provides the following benefits [47]:

- User passwords never cross the firewall, since user authentication occurs inside of the firewall and multiple web application passwords are no longer required.
- Web applications with no passwords are virtually impossible to hack, as the user must authenticate against an enterprise-class IdM first, which can include strong authentication mechanisms.
- "SP-initiated" SAML SSO provides access to web apps for users outside of the firewall. If an outside user requests access to a web application, the SP can automatically redirect the user to an authentication portal located at the IdP. After authenticating, the user is granted access to the application, while their login and password remains locked safely inside the firewall.
- Centralized federation provides a single point of web application access, control and auditing, which has security, risk and compliance benefits.

Compared with the browser-centric SAML based single-sign-on, the Simple Authentication and Security Layer (SASL) and the Generic Security Service Application Program Interface (GSS-API) are application frameworks to generalize authentication. In particular, RFC 6595 specifies a SASL mechanism and a GSS-API mechanism for SAML 2.0 that allows the integration of existing SAML Identity Providers with applications using SASL and GSS-API. In contrast to re-using username and password credentials within a SASL/GSS-API application environment, RFC 7055 specifies a GSS-API mechanism for supporting EAP based authentication. This means that the previous restriction limiting the used of EAP for network

access authentication has been removed, permiting the use of EAP in (IoT) application authentication.

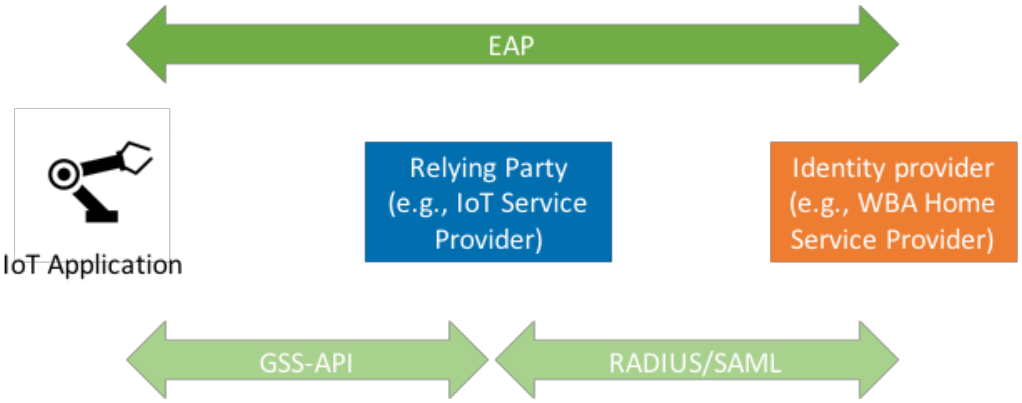


Figure 6-7: IETF's Application Bridging for Federated Access Beyond web architecture

6.7 Automated Settlement

Investigations are on-going into using new technology to address clearing and settlement, driven primarily by the banking sector. As identified by Santander [48] IoT is one of the drivers for the streamling of the contractual process, advocating the use of digital platforms that govern and verify smart contracts.

In particular, the use of distributed ledger (also referred to as blockchain) technology is receiving much attention in the financial technology (FinTech) sector to revolutionize transaction clearing. Within the Fintech environment, the near-instantaneous clearing and settlement achievable with distributed ledgers is targeted at increasing accuracy of trade data and to reduce settlement risk. Distributed ledgers can be open, even enabling anonymous entities to participate and so clearly scaling to support the dynamic discovery and operations described previously. Alternatively, they can be closed, requiring all entities to be identified and be participants in a common network.

7 Summary of gaps identified and recommendations

7.1 Framed-IPv6-Attribute and Framed-IPv6-Prefix support

With the increasing adoption of IPv6 for device addressing and the associated removal of NAT functionality, it will be increasingly the case that IoT devices and carrier Wi-Fi users will be allocated globally routable IPv6 addresses.

WBA should introduce the Framed-IPv6-Address and Framed-IPv6-Prefix attributes into WRIX signaling exchanges.

7.2 Generalized UDR for IoT Data Clearing

WRIX d/f systems are currently defined to support Wi-Fi based use cases, using fields derived from RADIUS based authentication.

WBA, in co-operation with LoRa Alliance, should consider enhancing current WRIX definitions to allow other IoT use cases to be supported. Topics to be addressed include how to signal LoRa specific information, including NETID, JoinEUI and DevEUI, as well as session definition, chargeable user identity and record handling.

7.3 WRIX Record Encoding

WBA should consider the possible decreases in WRIX record handling costs (and corresponding increases in scalability for IoT handling) associated with a new record encoding techniques.

7.4 Monitoring Split Billing Adoption

WBA's Business Working Group may wish to monitor the market adoption of split retail billing as it relates to IoT deployments and to understand whether WBA needs to trigger the definition of enhanced capabilities to support such within a carrier Wi-Fi roaming environment

7.5 Adoption of RADSEC between WRIX Hub providers

WBA should enhance its WRIX definitions to enable RADSEC to be supported. WBA should work with Certificate Authorities to understand the requirements necessary for supporting RADSEC between hub providers. Any proposal should cover off comparisons between current IPSec and proposed RADSEC approach.

7.6 Adoption of DNSROAM for automating HUB-to-HSP Connectivity

The wide scale adoption of IoT may be characterized by devices using many different credential types and be supported by a wide range of identity providers being required to be supported. In order to accommodate such a scenario, WBA should analyze any HUB-to-HSP scaling limitations associated with current realm routing functionality.

According to the output of such analysis, WBA may consider enhancing its WRIX definitions to enable enhanced scalability via dynamic discovery of HSPs.

Note: This functionality can be defined to coexist with existing WRIX functionality, for example, only relying on DNSROAM where no static realm route already exists.

7.7 Adoption of DNSROAM for automating VNP-to-HUB Connectivity

The proliferation of IoT devices connecting to Wi-Fi networks can impact the definition of a Visited Network Provider. If IoT devices effectively roam onto Enterprise networks, there will be a dramatic impact on the scaling requirements for VNPs. In order to accommodate such a scenario, WBA should analyze any VNP-to-HUP scaling limitations associated with current realm routing functionality.

According to the output of such analysis, WBA may consider enhancing its WRIX definitions to enable enhanced scalability for increased numbers of VNP/Enterprise networks.

7.8 IoT Application Security

WBA should continue monitoring the adoption of EAP/GSS-API and the possible re-use of WRIX and GSS-API for securing IoT Applications.

7.9 IoT Ease of Use

Whereas roaming agreement based approaches ensure that terms and conditions are agreed a priori and thus do not impact the user experience, the current fragmented approach to acceptable use policies and liability disclaimers for isolated Wi-Fi hotspots, where individual networks define their own policies necessitating acceptance of those by a browser based interaction, severely impact user experience and will prohibit headless IoT devices from accessing the network.

WBA should consider, as part of its WRIX evolution strategy, how to facilitate the adoption of roaming by providers of isolated Wi-Fi hotspots.

7.10 WRIX enhancements for MulteFire Alliance Support

The MulteFire Alliance has adapted the 3GPP defined approaches for Trusted and Un-Trusted Wi-Fi integration for enabling Neutral Host Network deployments of MulteFire technology.

WBA should consider enhancing its WRIX specifications and systems to enable authentication via the MulteFire Alliance defined Neutral Host MME, e.g., to cover deployment in 5GHz and/or CBRS-based 3.5 GHz band.

7.11 5G Non-3GPP Subscription Identifiers

Although 3GPP documents indicate that roaming scenarios are precluded for 5G's non-3GPP subscription identifiers, WBA and GSMA capabilities already permit roaming based on non-IMSI identifiers.

WBA should, in co-operation with GSMA, consider how to facilitate roaming for devices with 5G non-3GPP subscription identifiers.

7.12 Impact of automated clearing and settlement

WBA should continue monitoring evolutions in the automation of clearing and settlement and understand the implications of such on its existing WRIX based roaming systems.

8 Next steps for the WBA

8.1 Dissemination and implementation of the framework

The new framework will be trialed by WBA leveraging on the experience acquired with previous end-to-end interoperability trials such as Next Generation Hotspot.

The execution model will involve gathering relevant members, both operators and vendors, to define the scope, architecture and timeline. A set of test cases will be defined so that a test plan can be built.

Industry collaboration will also help evolving WBA roaming framework by being applied in additional use case scenarios. The immediate collaboration opportunities are listed in the following section.

8.2 Industry Joint work

WBA is discussing the development of a roaming framework for specific IoT technologies similar to the WRIX approach for Wi-Fi Roaming. Currently there are ongoing discussions with industry alliances such as:

- LoRa Alliance
- MulteFire Alliance
- eduroam

The scope of the collaboration is planned to include:

- Outline different technologies requirements, features and capabilities.
- Identify the most relevant use cases that require interoperability & roaming
- Define interoperability scenarios, architectures, protocols that will support the roaming framework
- Research on charging models and Inter-operator tariffs
- Develop the roaming framework specs and associated documentation (guidelines / templates)
- Execute interoperability trials

These are planned to kick-off within the calendar year timeframe and industry is invited to participate.

For more information please contact: pmo@wballiance.com

REFERENCES

[1] WBA 2020 vision, http://www.wballiance.com/resource/vision-2020/

[2] WBA: “IoT New Vertical Value Chains and Interoperability”, https://www.wballiance.com/wp-content/uploads/2017/03/IoT-New-Vertical-Value-Chains-and-Interoperability-v1.00.pdf

[3] http://www.gartner.com/newsroom/id/3598917

[4] https://machinaresearch.com/news/press-release-the-inexorable-rise-of-m2m-roaming/

[5] https://machinaresearch.com/report/a-balanced-view-on-extra-territorial-use-of-e164-numbering-permanent-roaming/

[6] https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#1b7df3e292d5

[7] http://www.fiercewireless.com/wireless/comcast-expands-lorawan-based-iot-network-to-12-cities

[8] https://www.multefire.org

[9] https://www.fiercewireless.com/tech/nokia-alphabet-qualcomm-take-cbrs-to-race-track

[10] https://www.networkworld.com/article/3196191/lan-wan/wifi-s-evolving-role-in-iot.html

[11] http://www.cvt-dallas.org/IOT-Nov15.pdf

[12] https://www.wi-fi.org/discover-wi-fi/specifications

[13] https://www.wballiance.com/resource/interoperability-compliance-programme-icp-business-benefits/

[14] “GSMA. Internal roaming explained”, Retrieved from GSMA: http://www.gsma.com/latinamerica/wp-content/uploads/2012/08/GSMA-Mobile-roaming-web-English.pdf

[15] http://portal.lora-alliance.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=1080

[16] MFA TS MF.202 “Architecture for Neutral Host Network Access Mode, Stage 2”

[17] https://www.slideshare.net/multefirealliance/multefire-endtoend-architecture-neutral-host

[18] www.3gpp.org/DynaReport/23402.htm

[19] https://www.eduroam.org/2017/11/05/2016-a-record-breaking-year-for-eduroam/

[20] https://wiki.geant.org/display/H2eduroam/eap-types

[21] http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5755-berec-report-on-enabling-the-internet-of-things

[22] http://www.sigidwiki.com/wiki/SIGFOX

[23] https://www.semtech.com/Press-Releases/2017/semtech-announces-industrys-first-disposable-lora-enabled-nano-tag-for-internet-of-things-(iot)-applications.html

[24] http://www.rfidjournal.com/articles/view?15779

[25] https://www.ipass.com/press-releases/ipass-and-armada-partner-to-improve-supply-chain-visibility-via-ipass-global-wi-fi-network/

[26] https://techcrunch.com/2017/09/20/target-rolls-out-bluetooth-beacon-technology-in-stores-to-power-new-indoor-maps-in-its-app/

[27] http://wise-iot.eu/wp-content/uploads/2016/12/D1.1-Use-Cases-PU-V1.0.pdf

[28] https://enterpriseiotinsights.com/20170418/internet-of-things/20170418internet-of-thingsairbus-iot-asset-tracking-tag23

[29] https://venturebeat.com/2017/09/26/sigfox-introduces-dramatically-cheaper-iot-module-to-catalyze-adoption-of-connectivity-for-any-object/

[30] 3GPP TR 22.891, “Study on New Services and Markets Technology Enablers”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2897

[31] 3GPP TR 33.899, “Study on the security aspects of the next generation system”, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

[32] “Enterprise Mobile Infrastructure 2016”, Mobile Experts, April 2016

[33] Compact Extensible Authentication Protocol for the Internet of Things: Enabling Scalable and Efficient Security Commissioning, https://www.hindawi.com/journals/misy/2015/506284/

[34] Wi-Sun alliance, Technical Profile Specification, Field Area Network

[35] WBA, “The Role of Wi-Fi & Unlicensed Technologies in 5G”, https://www.wballiance.com/resource/5g-networks-the-role-of-wi-fi-and-unlicensed-technologies/

[36] WBA, “IPv6 for Carrier Wi-Fi: Wi-Fi Operator Guidelines”, https://www.wballiance.com/resource/ipv6-for-carrier-wi-fi-wi-fi-operator-guidelines/

[37] GSMA “CLP Billing and Charging Analysis”, CLP-08

[38], WRIX Clearing, WBA

[39] https://www.cs.fsu.edu/~engelen/SACpaper.pdf

[40] GSMA IR.67, “DNS and ENUM Guidelines for Service Providers and GRX and IPX providers”

[41 GSM IR.8, “LTE and EPC Roaming Guidelines”

[42] 3GPP TS 29.303, “Domain Name System Procedures”

[43] http://net868.ru/assets/pdf/LoRaWAN-Backend-Interfaces-v1.0.pdf

[44] RFC 6614, “Transport Layer Security (TLS) Encryption for RADIUS”

[45] RFC 7360, “Datagram Transport Layer Security (DTLS) as a Transport Layer for RADIUS”

[46] Wi-Fi CERTIFIED Passpoint™ (Release 2) Deployment Guidelines, https://www.wi-fi.org/file/passpoint-release-2-deployment-guidelines

[47] https://www.pingidentity.com/en/lp/saml-101.html

[48] http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

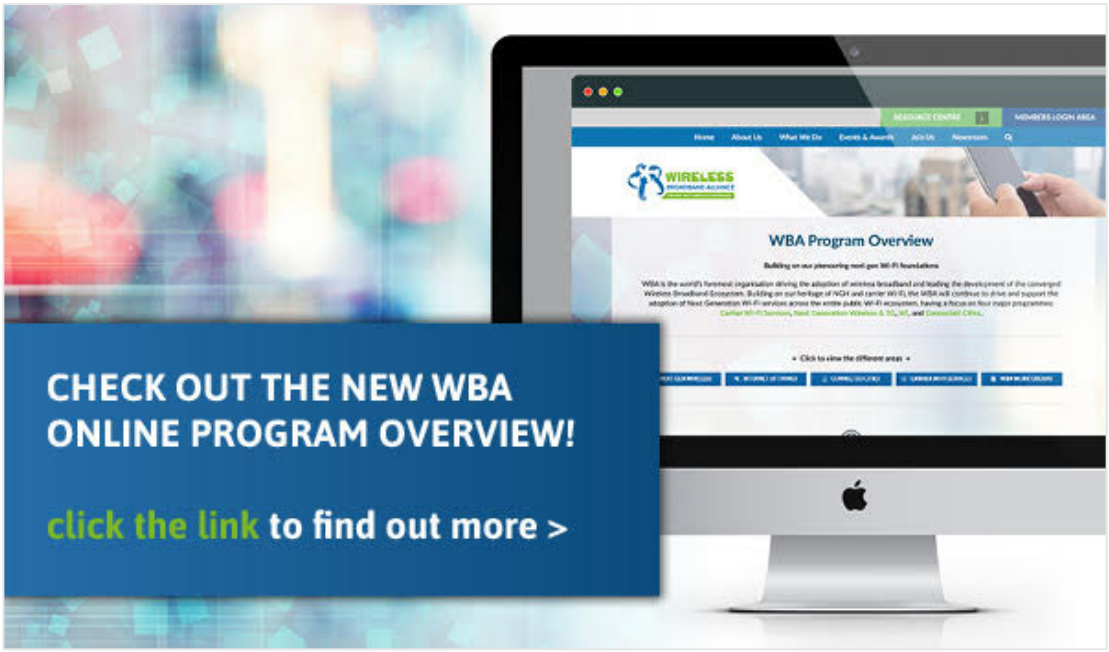
ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
AAA	Authentication, Authorization and Accounting
APN	Access Point Name
AUSF	Authentication Server Function
AVP	Attribute Value Pair
BDR	Bulk Data Report
CBRS	Citizens Broadband Radio Service
DNS	Domain Name System
DTLS	Datagram Transport Security Layer
EAP	Extensible Authentication Protocol
EUI	Extended Unique Identifier
GSMA	GSM Association
HSP	Home Service Provider
ICP	Interoperability Compliancy Program
IdP	Identity Provider
IoT	Internet of Things
IMSI	International Mobile Subscriber Identity
LP-WAN	Low Power Wide Area Network
MME	Mobility Management Entity
NAI	Network Access Identifier

NAPTR	Naming Authority Pointer Record
NAT	Network Address Translation
NGH	Next Generation Hotspot
NHN	Neutral Host Network
OCSP	Online Certificate Status Protocol
OSU	On-line Sign Up
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PSK	Pre-Shared Key
SFD	Summary Financial Data
SSID	Service Set Identifier
TAP	Transferred Accounts Procedure
TLS	Transport Layer Security
UDR	Usage Data Records
VSA	Vendor Specific Attribute
VoLTE	Voice over LTE
VNP	Visited Network Provider
WBA	Wireless Broadband Alliance
WGC	Wireless Global Congress
WRIX	Wireless Roaming Intermediary eXchange
WWD	World Wi-Fi Day™

PARTICIPANT LIST

COMPANY	NAME	ROLE
Syniverse	Dan Klaeren	Project Leader
Cisco	Mark Grayson	Project Co-Leader & Chief Editor
BSG Wireless	Betty Cockrell	Project Co-Leader
Boingo Wireless	Brian Shields	Project Co-Leader
BT	Steve Dyett	Editorial team member
Intel	Bahar Sadeghi	Editorial team member
UL	Mick Conley	Editorial team member
WBA	Bruno Tomas	Editorial team member



For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please get in contact:
Click Here >

READ MORE