Internet of Things

New Vertical Value Chains & Interoperability

Source: Internet of Things Working Group
Author(s): WBA Members
Issue date: March 2017
Version: 1.00
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 accelerate global leadership for enabling of wireless services that are seamless, secure and interoperable. Building on our heritage of Next Generation Hotspot (NGH) and carrier Wi-Fi, WBA will continue to drive and support the adoption of Next Generation Wireless services across the entire public Wi-Fi ecosystem, including IoT, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Charter Communications; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel.

The WBA Board includes AT&T, Boingo Wireless, BT, China Telecom, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO, Orange and Ruckus Wireless. 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

http://www.linkedin.com/groups?mostPopular=&gid=50482

https://plus.google.com/106744820987466669966/posts

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

Tables

Figures

1 Introduction

The WBA's 2020 vision describes a future 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.

The industry is just starting to explore the business cases for IoT and how the revenues will be shared between the various contributors within the IoT value chain. There is a consequential opportunity to define the evolution of the Wi-Fi platform and broader unlicensed ecosystem so as to enable the evolution of the business cases for Wi-Fi service providers. However, with certain IoT applications sending only a few bytes of data per day, there will likely be novel approaches to the evolution of access charging and associated impact on established roaming capabilities.

Hence, it is likely that IoT deployments will drive monetization by non-traditional approaches based on big data capabilities, etc., that allow the investments in un-licensed technology to be recouped in new and innovative ways, with the service being cross-subsidized by alternative value chains.

In this context, the diverse range of IoT vertical segments can easily dilute focus, and therefore, WBA members are engaging to set priorities on a specific set of IoT use cases, which are more prominent. Acknowledging value is migrating away from access towards the IoT application, focus is on evolution of core WBA competencies associated with network connectivity, identity and service management.

WBA is conducting analysis on the evolution of existing value chains and the future role of evolved Passpoint/NGH based roaming to accelerate the deployment of those services (unlicensed technologies, monetization/revenue, roaming capabilities).

Overall, WBA objective is to focus on delivering a new perspective to the IoT space facilitating the definition of identities, which in the near term will result in broad interoperability and roaming capabilities.

This whitepaper focuses on the following key blocks to drive the industry forward –

It aims at defining vertical markets and respective unlicensed access technologies, by exploring its use cases, business models and opportunities (related to vertical) for WBA members.

It evolves then to outline the baseline of IoT environment: Enablement platforms, capabilities and IoT identities which impact WBA Members, taking into consideration interoperability between technologies (IoT verticals interoperability).

In addition, eventually, the cornerstone is reached by analysing the evolution of existing value chains and the evolution of existing roaming models based on Passpoint/NGH based roaming to accelerate the deployment of IoT services. The whitepaper concludes with the identification of gaps and next steps for the industry and the WBA.

2 Definition of vertical markets and respective un-licensed access technologies

2.1 IoT Market Segmentation

The "things" in IoT cover a very wide range of devices; small devices like temperature sensors to personal devices to large industrial equipment. Similarly the IoT applications are diverse and span many industries and markets. [2] has divided the IoT market into the following nine categories:

- Buildings, including commercial and industrial
- Energy, including supply & demand, alternative energy, and oil & gas
- Consumer and home, including infrastructure, awareness & safety, and convenience & entertainment

- Healthcare, including care, in vivo/home, and research
- Industrial, including distribution, converting/discrete, fluid/processes, and resource automation
- Transportation, including transportation systems, vehicles, and non-vehicular
- Retail, including stores, hospitality, and specialty
- Security & public safety, including emergency services, public infrastructure, tracking, equipment and surveillance
- IT & Networks, including enterprise and public

However, the development of these market segments have not been at the same pace; not all market segments are IoT enabled and not all grow at equal speed. Even within a market segment, some subcategories and specific applications may grow much faster than the others. For example, IoT applications in healthcare, industrial, buildings, home, and energy segments exist more dominantly and hence these segments have experienced a more rapid growth compared to the other segments. Table 2-1 provides an example list of existing IoT applications in the five categories mentioned above.

Market Segment	Applications
Healthcare	Patient monitoring Home healthcare Medical imaging
Industrial	Sensor/actuator networks for process control Automation Monitoring Maintenance Asset tracking
Buildings	Heating ventilation air conditioning Lighting Surveillance
Home	Smart lighting Thermostat control Security systems Smart appliances Smart entertainment
Energy	Smart metering Outdoor lighting

Table 2-1 Example of applications for select market segments

A direct result of diversity of IoT applications is diversity of the enabling requirements for these applications. As evident by the examples listed in Table 2-1 the communications requirements for these applications can be very different. For example, smart metering requires city-wide coverage; while home applications require indoor coverage within a house; while medical imaging requires transporting large amount of data, the actuator control requires very short data transfers. Some devices, like sensors require long battery life, whereas smart appliances are plugged in to the power.

There are different wireless technologies to address the requirements for different market segments and applications. Next, first, an overview of the alternative unlicensed wireless technologies is provided and then requirements and applications are mapped to each wireless technology.

Importantly, from the WBA's perspective, recent research [3] 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.

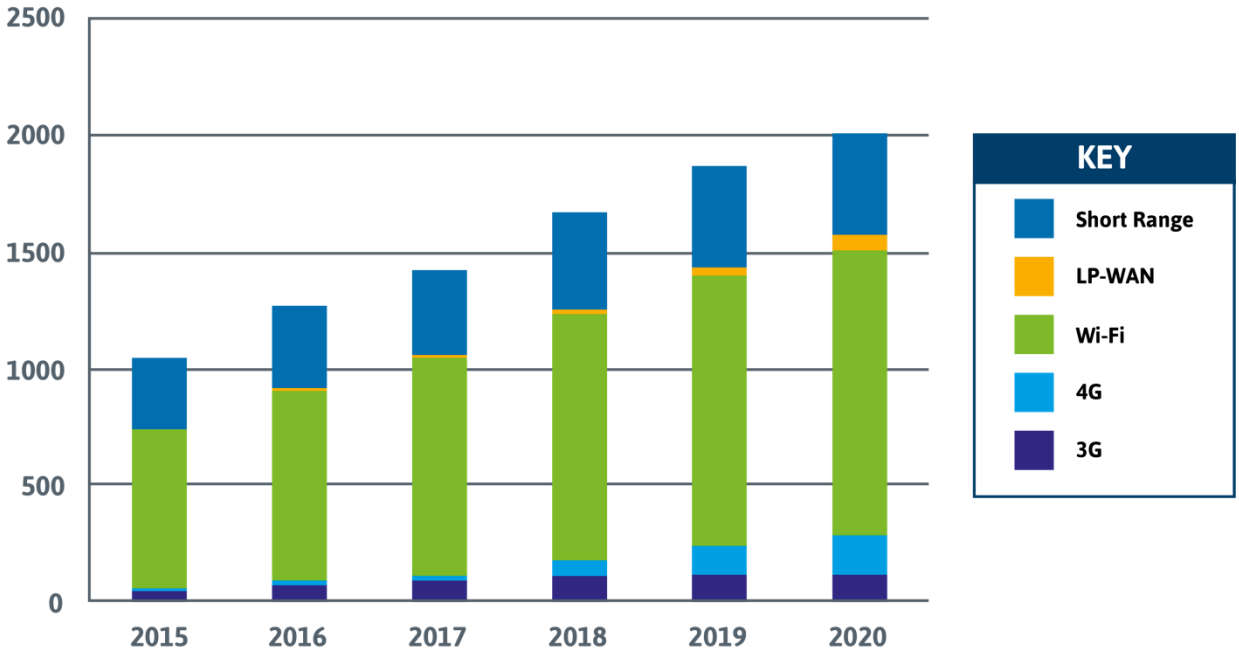


Figure 2-1: North America M2M/IoT Connections (Millions)

2.2 Alternative Unlicensed Access Technologies

The unlicensed access technologies addressing IoT are here divided based on their typical transmission range, to short range, medium range, and long-range technologies.

2.2.1 Short Range

The wireless access technologies in this category have traditionally been used for Personal Area Networks (PANs). However, mesh capability has enabled them to expand their coverage area significantly by multi-hopping. Growth in this category is reported as being driven by consumer electronics, home automation, smart city and smart buildings.

- IEEE 802.15.4
    - IEEE 802.15.4 is a standard that specifies the physical and MAC layers for low-rate wireless personal are networks (LR-PANs) [4]. LR-PANs are used to provide connectivity to devices with very low power requirements, operating in a *personal operating space* of around 10m. IEEE 802.15.4 operates primarily in 2.4.GHz ISM band and is the basis for ZigBee, and Thread specifications, among others.
- Bluetooth
    - Bluetooth is a wireless technology standard for exchanging data over short distances using the un-licensed 2.4 GHz band [5]. While traditionally it has been used for audio applications, Bluetooth Low Energy (BLE) has been introduced to expand into IoT applications including healthcare and home entertainment. To further improve the applicability and use of Bluetooth technology, the Bluetooth SIG is in process of definition of a long range version of Bluetooth as well as enabling Bluetooth mesh.
- Zwave
    - Designed to provide reliable, low latency, and low data rate communication, Zwave's target application is home automation. It operates in sub 1GHz ISM band. Similar to the previously listed PAN technologies, Zwave also can be used to cover a larger area by use of mesh.
- IEEE 802.11ad (WiGig)
    - Operating in 60GHz ISM band WiGig enables communication at very high data rates. Given that the 60GHz signal typically cannot penetrate through walls, the WiGig network is confined to a room. The large channel bandwidth of WiGig enables delivery of signals at a very low latency, making it a good candidate for mission critical industrial applications.

2.2.2 Medium Range

Wi-Fi is the only medium range wireless technology capable of providing single hop connectivity in a local Area Network (LAN). As illustrated in Figure 2-1, from a North America perspective, Wi-Fi is expected to provide the majority of connectivity to IoT devices. Wi-Fi, however, comes in different variations depending on the band in which it operates.

- Wi-Fi
    - The traditional Wi-Fi operates in 2.4GHz and 5GHz ISM bands and comes in two flavours of Infrastructure Wi-Fi where devices connect to the Access Points (APs) primarily for accessing the Internet and Wi-Fi Direct which enables peer-to-peer communication among devices without need of an AP.
- Wi-Fi HaLow
    - Wi-Fi HaLow, which is currently under development in the Wi-Fi Alliance, will operate in sub 1GHz ISM band. Wi-Fi HaLow is based on IEEE 802.11ah which provides longer range, lower power operation, and lower throughput compared to other Wi-Fi technologies and hence is suitable for sensors and IoT devices distributed in larger areas. Non harmonized spectrum globally is identified as a contributing factor for slow adoption of Wi-Fi HaLow in the industry.

- IEEE 802.11p
  - IEEE 802.11p defines enhancements to Wi-Fi required to support Intelligent Transportation Systems (ITS). IEEE 802.11p operates in 5.9GHz band (700MHz in Japan). IEEE 802.11p enables delivery of high throughput data with low latency which is required for ITS safety applications.

2.2.3 Long Range

The Wide Area Networks (WAN) operating in unlicensed bands primarily target IoT applications. These technologies are also managed and are in direct competition with their licensed counterparts, i.e., Cellular IoT solutions. Using the numbers illustrated in Figure 2-1, LP-WAN connections are rather low in absolute numbers, but growing at a compound annual growth rate of 53%.

[6] provides a detailed comparison of the following unlicensed Low Power Wide Area Networks (LP-WAN) technologies:

- LoRa:
  - 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.
- SigFox:
  - Using an Ultra Narrow Band physical layer, the SIGFOX system is designed for infrequent sending of small messages that characterizes many IoT use cases.
- Wi-SUN:
  - The Wi-SUN alliance is an initiative under the National Institute of Information and Communications Technology defining the technical specifications for short-range wireless communications based on IEEE 802.15.4/4g PHY layer and IEEE 802.15.4/4e for the MAC layer [7].
- Ingenu:
  - Ingenu promotes the use of Random Phase Multiple Access (RPMA) in the 2.4 GHz band to address IoT communications.
- DASH-7:
  - The DASH7 Alliance fosters the development of the DASH7 protocol specification, operating in the 433 MHz, 868 MHz and 915 MHz unlicensed ISM bands for supporting IoT communications.
- Weightless:
  - The Weightless Special Interest Group advocates the use of Weightless technology for delivering wireless connectivity for low power, wide area networks. Weightless can operate in both sub-1GHz license exempt and licensed spectrum.

2.3 Mapping of alternative access technologies to market segments and applications

The applicability of different access technologies to different applications is determined based on the application requirements and the ability of the access technologies in addressing those. The following are the main requirements of IoT applications.

- Coverage
  - Some IoT applications, e.g., Industrial applications, require a wide coverage area, whereas Home applications, for example, require a small coverage area. A large coverage can be

provided by use of multi-hopping, a technique ZigBee utilizes to extend its coverage area; or can be achieved by longer range transmissions, as provided by Wi-Fi for medium range coverage or LP-WAN technologies for wide area coverage.

- Scalability
  - The ability of an access technology to scale to large number of nodes with high efficiency is another determining factor for its applicability for a particular application. Bluetooth for example, is capable of supporting small-sized networks, whereas ZigBee easily scales to very large networks.
- Power
  - A major requirement for IoT sensors is low power operation and a multi-year long battery life. There are other IoT devices, for example in Industrial applications, which are ac-powered. And there are different devices with different battery life expectancies in between. A related parameter to power is the form factor; the form factor of a battery powered device determines the type and size of battery it contains and hence how low power the operation of the device needs to be. Other related parameters impacting power requirements are required throughput and traffic patterns as well as the determinism of access.
- Throughput and traffic patterns
  - While sensors typically require very low throughput to transmit collected data at low frequencies, e.g., reporting measured temperature every hour, other IoT devices, for example surveillance cameras, require higher throughput for long durations of time. There are actuators that typically only receive data and there are sensors which only report data, and there are many different types of devices that both transmit and receive on a regular basis.
- Reliability
  - Some applications require high reliability communications. All wireless access technologies that operate within a fading environment provide probabilistic reliability, i.e., there will typically always be a finite possibility that the wireless channel is suffering from an extreme fade. Furthermore, wireless access technologies that operate in unlicensed spectrum need to operate in an environment with un-coordinated and un-controlled sources of interference and hence inherently cannot provide guaranteed reliability; however, higher levels of reliability is achievable with implementing efficient medium access mechanisms and operation in low interference environment.
- Determinism
  - Mission critical applications require determinism to be provided by the access technologies. While unlicensed technologies in general do not provide guaranteed timely access to the wireless medium, in special scenarios, for example in an isolated industrial field, determinism can be achieved especially for short-range and high-bandwidth communication technologies like WiGig.
- Cost
  - Unlicensed communication technologies enjoy lower cost in general compared to cellular communications. Among unlicensed technologies, the cost the complexity of the technology and the size of existing ecosystem impact the cost.
- Security

- Secure communication is required for many IoT applications and becomes more critical for longer range access technologies.

Access Technologies	Requirements							
	Coverage	Scalability	Power	Throughput	Reliability	Determinism	Cost	Security
IEEE 802.15.4	√ (mesh)	√	√	√	√	√	√	√
BT & BLE	√	√	√	√	√	√	√	√
ZWave	√ (mesh)	√	√	√	√	√	√	√
WiGig	√	√	√	√ √	√	√	√	√
Wi-Fi	√	√ (HaLow)	√	√ √ (11ac)	√	√	√	√
LP-WAN	√ √	√	√	√	√	√	√	√

Comparative Support	
√ √	Strongest
√	Strong
√	Some
√	Limited

Table 2-2 Mapping of Access Technologies to IoT Requirements

- Different access technologies by design focus on addressing different IoT requirements, and the developers and providers of IoT solutions would choose the appropriate access technology based on the specific requirements of the IoT application. The table above presents a mapping of access technologies to IoT requirements. While for each application there can be more than one candidate access technology, which would address its requirements, from the analysis above a few clear conclusions can be drawn:
- IEEE 802.15.4 is best applicable for IoT applications where large number of devices form a network and low throughput, low cost, and low power are the main requirements, e.g., home automation,
- BT and BLE are best suited for networks with small number of nodes where high reliability and low throughput (as well as low cost and low power) are needed, e.g., home healthcare.
- WiGig is the technology of choice for applications that require very high throughput, and low latency and determinism (due to minimal interference), e.g., industrial control and machine vision systems used for robotic guidance.
- For high throughput applications, Wi-Fi is currently the only choice with reasonable coverage, however, at a higher cost and power consumption.
- For any wide area network coverage with high scalability, e.g., smart city applications, LP-WAN technologies would be the right fit. Table 2-3 lists the most applicable access technologies for the IoT market segments identified in Table 2-2. Traditionally, Wi-Fi has not been used in market segments where low power is the primary requirement, however, the emergence of new applications that require higher throughput combined with the development of Wi-Fi techniques providing low power operation, has positioned Wi-Fi to play a more significant role in the future for a majority of IoT market segments.

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 2-3 Mapping of Access Technologies to Market Segments

2.4 WBA members survey – status and priorities

A global WBA members' survey was conducted to gather priorities, recent industry developments and latest trends. The target audience were operators, vendors, hubs and testing labs, resulting in a total of more than 25 companies responding. The most represented profile of the respondents ranged from strategy & development to R&D.

The following key takeaways were extracted from the survey:

- **Deployments evolution**
  - During the last year more than 85% of the companies have increased the priority level of IoT on their roadmap or focus areas
  - Main reasons pointed out are the increased understanding (including top management), strategic support and increased product availability / deployments and use case scenarios which can generate revenue for the companies
  - Significant number of operators (60%) already deployed or plan to deploy until the end of 2017

- **Technology roadmap & roaming**
  - Access technologies currently being preferred to support IoT deployments are Wi-Fi (and its HaLow variation) and LP-WAN, followed by 3.5 GHz, NB-IoT and ZigBee.
  - More than 90% of the companies consider that inter-network roaming in IoT is important, for certain application areas, such as smart city and automotive in dense environments
  - Most companies are currently studying the best framework/platform, whereas devices/chipset does not seem a focus area at this stage

- **Market and application areas prioritization**
  - The top three market areas are 1) Consumer and home, including infrastructure, awareness & safety, and convenience & entertainment, 2) Transportation, including transportation systems, vehicles, and non-vehicular and 3) Energy, including supply & demand, alternative energy, and oil & gas.
  - In general the applications are more relevant are, 1) Automotive, 2) Asset tracking, 3) Fleet management and 4) Security systems. Moreover, for Wi-Fi specifically, smart trilogy (appliances, entertainment and lighting) were indicated as the most relevant
  - WBA members conclude that for IoT to grow exponentially the key actuation areas are the development of 1) operator guidelines, 2) standardization and 3) field trials together with industry advocacy.
  - For more information and detailed results please consult the Appendix – WBA Members Survey.

3 Use cases, business models and opportunities (related to vertical) for WBA members

"In the next century, planet earth will don an electronic skin. It will use the Internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies--even our dreams." - Neil Gross 1999

3.1 IoT Use Cases

Given the breadth of IoT use cases, the following are included as representative examples covering the various different market segments introduced in Section 2. Furthermore, the specific "value" of information being passed over the IoT access network may influence the type of access connectivity employed.

- **Connected Product Quality Analysis**
  - ***Use Case:*** *Continuously analyze data with sensor-equipped products or systems to meliorate root cause analysis and corrective actions, product quality, reliability and safety, preventative maintenance, and service.*
  - In a 2013 survey conducted by Enterprise Management Associates Inc. and 9sight Consulting [8], 38% of the nearly 600 big data projects being pursued by the 259 respondents involved machine-generated data, up from 24% in a similar survey a year earlier. In another survey conducted in 2013 by The Data Warehousing Institute, 47% of 188 respondents with big data management experience said machine data was part of their deployments.
  - Continuously analyzing data can be a challenge with sensor-equipped products. The volume of machine-generated data can create a lot of noise that will need to be filtered out. Separating the digital wheat from the chaff is one of the highest priorities and requires specialized data analysts paired with parsing tools that can exclude the noise and focus business on the important details. This type of setup can allow operators to base decisions in real-time, or near-real-time. For more detailed analysis downstream, predictive analytics, data mining and big data analytics tools all have possible

roles to play. Generating predictive models that can be applied for preventative maintenance and service would follow as a natural response.

- Data capture and storage can be achieved many ways, but two standard patterns could evolve that have benefits and drawbacks of their own that could have an impact on pre-auth infrastructures that require AAA:

  1) Centralized data communication, processing and storage. This method requires a network connection to enable secure interaction with an API, e.g., using Hadoop big data storage, but it has the benefit of enabling data to be transferred back to the sensor.

  2) Batch log file processing using tools such as Splunk or Loggly. This method leverages the controlling system log files and requires no pass-throughs, thereby, removing the additional dependency of additional network transport. Account privileges and role-based control can be used to avoid exposing sensitive data to unauthorized third parties.

  Because of the nature of the wireless networks, IoT QoS would require additional network layer analysis to be applied in order to ensure clear transport of sensor data and to ensure that SLA's are adhered to. For more information, refer to the WBA's QoS project:

  http://extranet.wballiance.com/apps/org/workgroup/qos/

- **Operations Asset and Material Tracking**
  - ***Use Case:*** *Locate and monitor key assets (e.g. raw materials, luggage tracking, and containers to optimize logistics, maintain inventory levels, and detect theft.*
  - The latest number of IoT devices in use is at 6.4 billion in 2016, up 30 percent from the 2015. It's anticipated that this number will hit around 21 billion by 2020. That kind of traction implies that the need for location and tracking of "things" will be an imperative for purposes of logistics, inventory, and theft detection.
  - Some of the emerging ways that IoT technology can help operations include: equipment optimization and energy efficiency, safety, materials tracking and lifecycle product traceability.
  - Technologies could include leveraging tagged assets, e.g., using RFID and/or Wi-Fi, that are monitored by installed sensors to track location of items such as luggage for airport travellers. This would improve baggage-handling logistics and improve customer experience ratings.

- **Real-Time Asset Health Monitoring**
  - ***Use Case:*** *Minimize downtime, locate spent assets, avoid mission-critical equipment failures through detailed monitoring of condition and operating parameters to automatically trigger alerts and proactively initiate response from maintenance teams when problems are detected.*
  - In August 2015, Forrester conducted an online study that found Asset management tops IoT reasons for IoT deployments [9]. Two-thirds of the 366 polled companies are currently using, or plan to implement asset management solutions such as fleet management, industrial asset management, and predictive maintenance.
  - IoT can help facilitate data collection from assets throughout the value chain. If a tracked asset starts to perform at a suboptimal level, it can report an issue to a central system where maintenance teams can see it and put in a work order for repair before the asset fails completely.

- This predictive maintenance can use an array of embedded monitoring tools. Assets can consistently communicate the state of their properties, levels, and other key indicators of health. This data helps management teams spot deficiencies before they lead to unscheduled downtime.
- Other benefits would include:
    1) Tracking important parameters such as mean time to repair (MTTR) and mean time between failure (MTBF)
    2) Holistic view of assets and equipment
    3) Resource monitoring
    4) Archive historic maintenance data to formulate preventative maintenance strategies
    5) Automatic spare part replenishment

- **Industrial Process Automation**
    - ***Use Case:*** *Production processes may use a significant amount of constituent resources. Optimization of process integration can be used to integrate complex field devices, such as pumps and mass flow controllers, with industrial control systems.*
    - Multiple, simultaneous, real-time control loops can be implemented and uptime is maximized through diagnostic and condition monitoring by plant asset management systems. In one case, a manufacturer was able to reduce resource usage by 10% while being able to produce unique product formulations in response to market demand [10].

- **Smart Outdoor Lighting**
    - ***Use Case:*** *Remote control of street and roadway lighting can be used to provide visibility as to how much energy is being used as well as real-time control to save energy. Furthermore, instrumentation of the lighting infrastructure can be used to cut maintenance costs with real-time fault monitoring.*
    - The global outdoor lighting market is growing, due to government support, drivers for enhanced energy efficiency, together with the continuous replacement of traditional outdoor lighting. A shift towards light emitting diode (LED) lighting and high intensity discharge (HID) lamps can be seen in the outdoor applications, due to government support and longer lifetime offered by these technologies.
    - The outdoor lighting segment is expected to exceed USD 8 billion by 2020, growing at a CAGR of 30%, with countries across the globe looking for the possibilities of efficiently implementing smart lighting in public infrastructures such as roads, airports, railway stations, and subway stations [11].

- **Smart Heating Ventilation and Air Conditioning (HVAC)**
    - ***Use Case:*** *IoT enabled HVAC systems enable real time monitoring of conditions and system operations. The information provided can be used by HVAC system managers to provide predictive maintenance and remote diagnostics. Consumers can be offered detailed control of their systems. By linking HVAC control systems with on-line weather forecasts and sensor derived occupancy levels, the process of HVAC control can be automated to improve comfort and energy efficiency.*
    - Grand View Research estimates that the global smart thermostat market was valued at USD 785.4 million in 2015, and is expected to expand at a CAGR of 18.7% (in terms of revenue) from the year 2016 to 2022 [12]. Wireless technologies enable thermostats to be connected to home automation systems, with key technologies identified as including Wi-Fi, ZigBee, Power Line Communications, NFC and Bluetooth.

3.2 Device Characterization

One of the key characteristics of the IoT is the breadth of application behaviours that are anticipated to be required to be supported. Indeed, this breadth of application behaviour, coupled with the different use cases and access network characteristics will see IoT systems needing to support everything from streaming real-time high definition video from mains powered “things”, to the other extreme, of “things” that send only a few

bytes of data a day. The latter which are powered by simple coin cells and expected to last several years when deployed in the field.

Whereas the former group of applications are well understood as being able to be supported by end-points with fully functional IP stacks, the latter is causing the definition of new "constrained devices".

RFC 7228 [13] describes 3 classes of constrained devices:

- **Class 0: << 10 KB RAM, <<100 KB Flash**
  - Very constrained sensor-like motes that are severely constrained in memory and processing capabilities that most likely they **will not** have the resources required to communicate directly with the Internet in a secure manner

- **Class 1: ~10 KB RAM, ~100 KB Flash**
  - Quite constrained in code space and processing capabilities, such that they cannot easily talk to other Internet nodes employing a full protocol stack such as using HTTP and Transport Layer Security (TLS). However, they are capable enough to use a protocol stack specifically designed for constrained nodes (such as the Constrained Application Protocol (CoAP) over UDP) and participate in meaningful conversations without the help of a gateway node.

- **Class 2: ~50 KB RAM, ~250 KB Flash**
  - Fundamentally capable of supporting most of the same protocol stacks as used on notebooks or servers.

However, whereas RFC 7228 concentrates on the constraints associated with the device, it is more often bandwidth limitations that dominate the drivers towards Class 0 devices. In particular, the 4 Byte CoAP header and 4 byte 6LoWPAN can contribute towards a significant proportion of the overall LP-WAN frame that may be able to transport very much less than the 81 bytes that can be carried in an 802.15.4 sensor based network [14]. For example, with 51 bytes available using an EU version of the LoRaWAN protocol, a minimum 15% of the bandwidth and possibly battery consumption will be used in transmitting the IP headers.

As a consequence, architectures are evolving to address such issues by supporting Non-IP Data Delivery (NIDD) for supporting constrained devices and/or avoiding bandwidth expansion, with 3GPP's NB-IoT, LoRa, Sigfox together with legacy 802.15.4 based sensor networks all supporting non-IP based data delivery.

3.3 IoT Application Characterization

The breadth of IoT use cases mean that it is difficult to define a standard model for characterizing IoT applications. Some of the most important criteria that lead to divergence between IoT application behaviour and conventional "human-driven" applications include: [15]

- Environment interaction: Because IoT devices typically interact with their environment, the resulting traffic characteristics can be expected to be driven by the dynamic nature of that environment. A typical consequence is that IoT devices may exhibit very low data rates over a large time scale when their sensed environment can be considered as quasi-static, but can have very bursty traffic when something changes their environment.
- Energy: The energy supplying an IoT device may be scarce and hence energy consumption may be a key consideration in defining IoT application behaviour. In extreme cases, the power used to transmit IP headers may contribute a significant percentage to the overall power budget, which may motivate the use of compressed IP headers, e.g., 6LoWPAN that has been defined to enable IPv6 to be supported over constrained message lengths experienced in IEEE 802.15.4 based networks, or Non-IP Data Delivery (NIDD) that enables binary IoT messages to be transported over low power networks, including IEEE 802.15.4, LoRaWAN and 3GPP NB-IoT.
- Dependability and QoS: IoT applications span the widest of ranges when it comes to aspects associated with reliability, with some IoT automation applications requiring deterministic service qualities that ensure information is received, processed and actioned in a matter of milliseconds, to others that send occasional messages that may be able to be delayed for minutes or even hours.

3.4 Security Aspects

There is consensus that security issues may become a significant inhibitor to the deployment of IoT services. GSMA in its CLP.11 document [16] describes 4 security challenges:

- Ensuring secured connectivity between Endpoints and their respective services
- Identity: Authenticating Endpoints, services, and the customer or end-user operating the Endpoint
- Privacy: Reducing the potential for harm to individual end-users
- Security: Ensuring that system integrity can be verified, tracked, and monitored

Addressing these in turn, from a Hotspot 2.0 perspective, WBA has already shown how it can deliver an equivalent level of security to modern cellular systems. There may be an opportunity to broaden HS2.0 approaches to ensure newer LP-WAN based access systems together with gateway based capillary systems for integrating sensor networks are equivalently secured, enabling the broadest range of communication protocols can be supported, e.g., sensor and/or network triggered, information push and/or pull.

From an identity perspective, WBA has not only encompassed 3GPP concepts of identity with EAP-SIM and EAP-AKA, but has broaden support to include PKI based security as well as On-Line Sign-up capabilities that facilitate the on-boarding of SIM-less devices. There is an opportunity for WBA to broaden HS2.0 approaches to address on-boarding use cases for IoT devices.

From a security perspective, moving on from HS2.0 that focuses on securing the 802.11 radio interface, what capabilities need to be defined to couple device based access authentication with IoT service-based authentication and security?

3.5 Mobility and Roaming Requirements

As introduced in section 2, IoT Applications can be characterised by their coverage criteria. Furthermore the use cases introduced in section 3 include those that look at operations asset and material tracking. It is evident therefore, that mobility and roaming requirements need to be addressed.

The IoT-Architecture is a European FP7 project that has defined an IoT Architecture Reference Model [17] which can be used to provide insight into a range of different Mobility requirements:

- Because of mobility and multi-homing, the IoT device's identity needs to be distinguished from its network location. Indeed where a device can change access networks, a device's permanent identity should be decoupled from the access network.
- Due to the mobility of physical entities, an IoT application may require continuity of service such that the IoT device needs to be able to change between similar networks without losing on-going connectivity.
- Due to the heterogeneity, dynamicity and mobility of the Internet of Things, the IoT device may change access network type. Alternatively, different endpoints may be used.

As it relates to roaming, recent research published by Starhome-Mach, a global provider of roaming services [18] indicates that the number of cellular roaming registrations attributable to IoT devices had doubled over 12 months and in 2015 now represented 7% of all roaming connections.

Further research published by Machina [19], estimates that 25% of all M2M SIMs deployed in Europe are roaming. However, whereas the growth predicted by the Starhome-Mach data indicates that there is a possibility of "as many machines as people roaming by 2020", Machina also notes that increasingly M2M providers will use embedded UICC subscription management (as described in section 4) to localize the SIM card identity onto a domestic network and so avoiding any complexities associated with IoT roaming.

3.6 QoS Aspects and optimization for IoT

The IoT Architecture Reference Model [17] provides an insight into a range of different QoS requirements. The use cases and market segments highlight the wide range of different deployments and corresponding QoS attributes associated with different IoT systems, with healthcare and industrial automation providing examples of high reliability and time criticality IoT communications. More broadly:

- IoT supporting life critical systems will require the system to ensure the device can send and/or receive time critical messages
- Not all IoT services are equivalent; the IoT system needs to assure that support of time-sensitive services can be prioritized
- Service reliability may be an issue and resiliency options may be needed to ensure those requiring (and paying for) such capabilities do not suffer service outages.
- While congestion avoidance is an important topic on conventional IP networks, its importance can be magnified when operating on low bandwidth networks.
- The IoT systems should ensure real-time, event-triggered data with high time resolution can be delivered with a high priority.

3.7 IoT Value Chains

One of the key characteristics of the Internet of Things is the increasingly diversified and complex value chains when compared to the conventional network connectivity focused value chains that apply to mobile broadband type service. Figure 3-1 illustrates the value associated with IoT increasingly migrating towards the vertical applications. Moving forward we can anticipate the increasing adoption of IoT will see a refocusing from criteria such as raw throughputs onto the evolution of network connectivity value propositions. Indeed, using one example use case from section 2, it is evident that the value in the connected product quality analysis use cases is around being able to use IoT data analysis to enable increased efficiencies through preventative maintenance and improved product quality.

Specifically, while the network connectivity of carrier Wi-Fi, the identity management of Passpoint/NGH, the self-service portals of On-Line Signup and the billing and settlement capabilities of WRIX all play an important role in supporting IoT, there will also be the emergence of M2M application enablement, device management and analytics platforms, so called “IoT middleware” as a critical capability for accelerating IoT adoption.

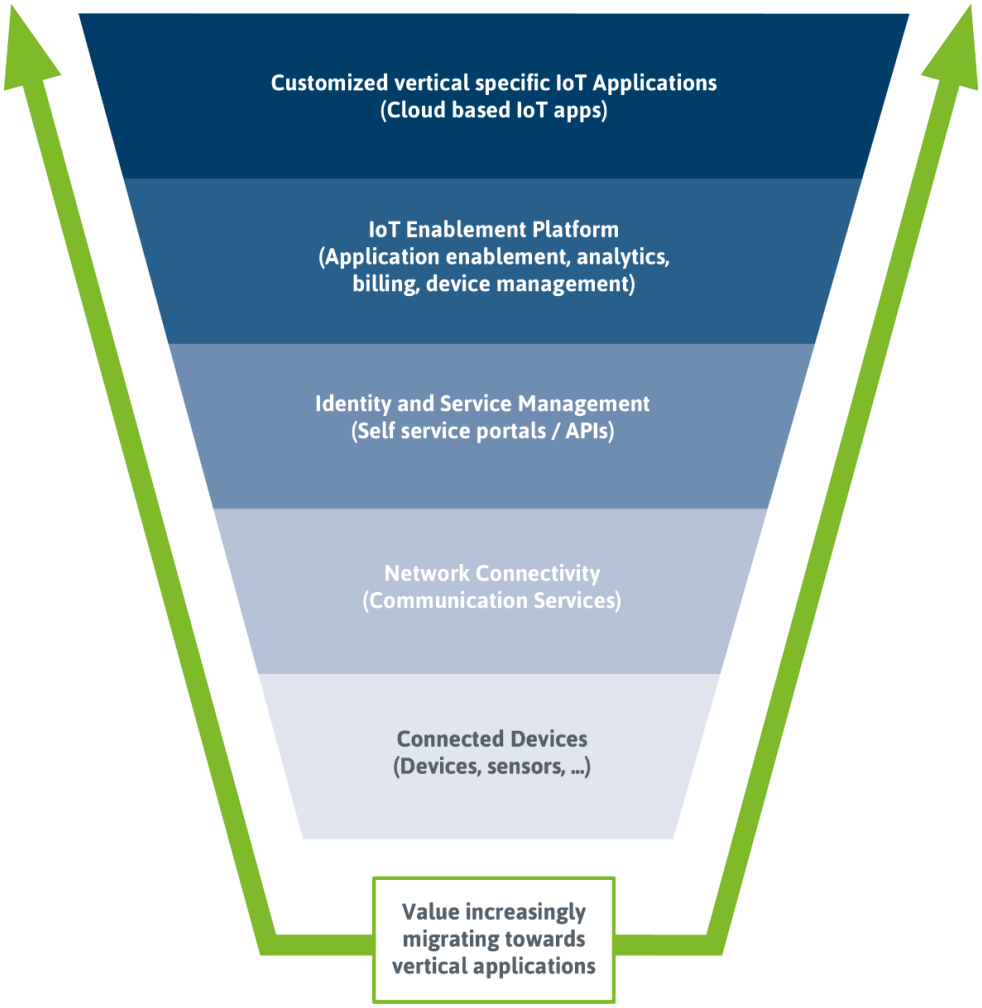


Figure 3-1: IoT Value Chain

Note, this migration of value from coverage and connectivity, to more vertically focussed, is evident in the IoT use cases introduced earlier in this section, where value is associated with increased asset utilization, decreasing resource wastages, increasing energy efficiency, etc.

3.8 Monetization and Charging aspects

There are at least four different models that are emerging as to how the Internet of Things will be monetized [20]:

- Hardware Based: This is the most basic form of monetization and involves adding network connectivity to an existing or new product. This connectivity will typically be coupled with a web based tool, typically cloud based, for providing basic management of the network connected device.
- Service Based: In this model, traditional product offerings are transformed into a recurrent service offering. Importantly, this transforms the customer relationship and their associated lifetime value to the business by allowing continued engagement over the lifetime of the service offering.
- Data Insight Based: Instead of the business to consumer service revenue, data revenue is focused on the business to business opportunity whereby businesses can generate revenue by monetizing the suitably aggregated and anonymized data gathered from the Internet of Things.
- Ecosystem Model: Where focus is not on the end-to-end product or service offering, but rather on delivering a shared platform to enable other ecosystem partners to monetize their unique capabilities.

- These alternative monetization strategies can be supported by different pricing models [20]:
  - **One-Time Charges:** Typically associated with hardware based monetization, the customer makes a one-off payment for the offering.
  - **Subscription model:** Recurrent payments enable the customer to tailor the duration of service to their needs.
  - **Pay-as-you-go:** Delivers enhanced capabilities compared to conventional subscription based, where customers only pay when the service is used.
  - **Pay-for-Results:** An outcome based payment model which enables clarity in terms of the return on investment for the customer.
  - **Freemium models:** Whereby customers are attracted to the basic IoT service which is provided for free with the provider additionally charging for enhanced services
  - **Transaction based:** Used by platform providers to monetize access to their services.

4 Baseline of IoT environment: Enablement platforms, capabilities and IoT identities which impact WBA Members

4.1 Enablement platforms

As presented in Section 2, there are many different IoT market segments growing at different pace; some markets have existed for a while and some are new. Additionally, as the nascent markets are created, there are specific solutions developed to address the early and specific use cases. These solutions and devices catering to specific markets, while numerous and diverse, have been developed in silos; as a result, different solutions do not necessarily interwork and in most cases are not scalable as the market grows.

Such fragmented solutions hinder the realization of the true economic value of IoT where billions of devices with variable levels of capability, connect and communicate with one another regardless of the device manufacturers, band, operating system, chipset, or physical transport used. Indeed, whilst most initial IoT services are “vertical” in nature, some analysts predict that the market will accelerate when the application work “horizontally”, leveraging cross-domain architectural frameworks to share their information between conventional silos.

To enable collaboration and interworking (interoperability) among devices and services developed for the same different market segments a standardized connectivity middleware is required which provides a common method for discovery, service interaction and a common data model for all device types, irrespective of underlying physical transport..

The Open Connectivity Foundation (OCF), a consortium of companies from all major IoT verticals, provides a common connectivity framework for IoT devices in the form of both specification and open source. The framework targets all device types, regardless of how simple or complex and capable they are, or what market segment they belong to, and enables interoperability between the devices. OCF specifies both a request-response and a pub-sub cloud-native architecture enabling flexible and eminently scalable IoT deployment among all market segments.

Figure 4-1 depicts the scope of OCF where not only local and remote control of IoT devices via the cloud are covered, but also the server to server communication among different service domains is also in scope.

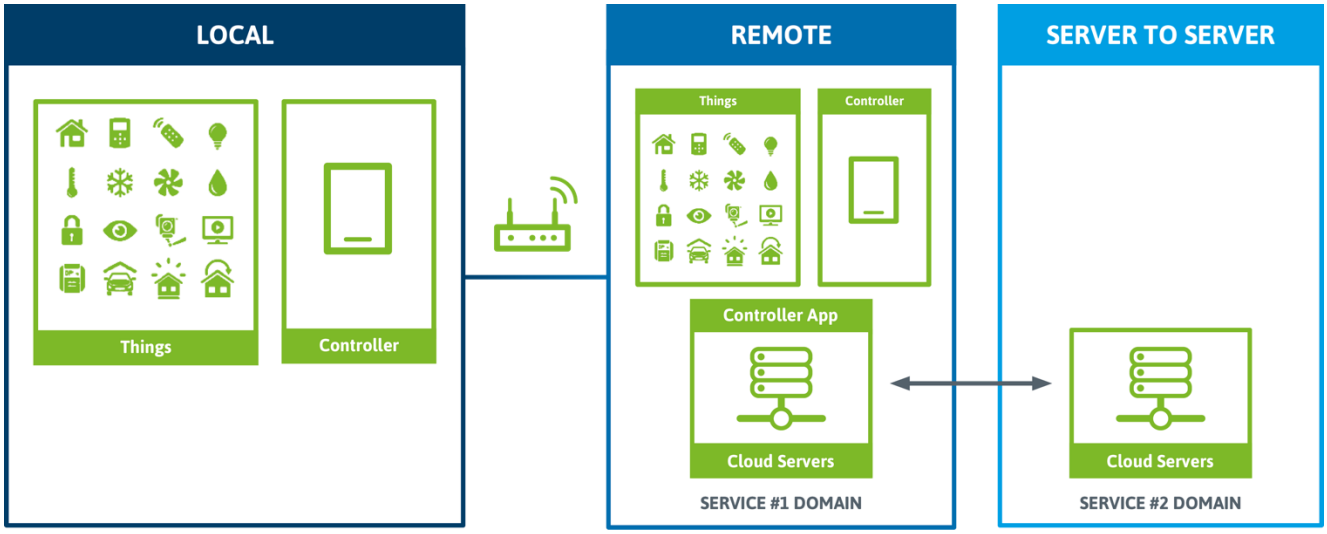


Figure 4-1: Scope of OCF

OCF framework as depicted in figure 4-2, works with any transport and supports different network protocols and topologies. OCF specifies a specific resource model, data and protocol agnostic interaction model that can map down to many different transport protocols, e.g., CoAP, HTTP, etc.

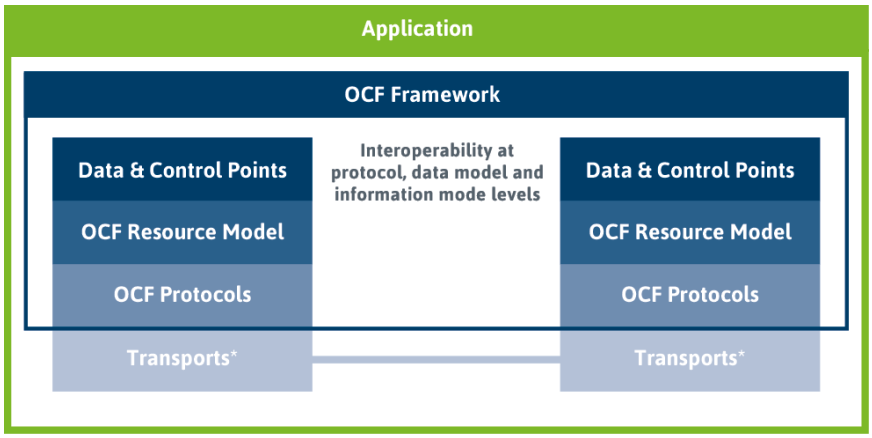


Figure 4-2: OCF Framework

While specification of the transports are not in scope of OCF, any transport capable of carrying IP traffic can be used and Wi-Fi with native support for IP traffic fits well with OCF framework.

OCF achieves interoperability among protocols by mandating a particular protocol stacks while still supporting others; the current mandated stack is depicted in Figure 4-3.

Figure 4-3: OCF protocol stack

OCF defines an expansive information model through which the data and control points on the devices are accessed and manipulated. The information model is resource oriented, follows a RESTful architecture and abstracts the physical entities of the device.

Security is a first class citizen in the OCF framework, and is designed to ensure only authenticated users have access to the devices, the data is secured and encrypted, and access to the specific resources is only granted to authorized applications and users.

OCF also funds an open source project called IoTivity which is a gully certified open source implementation of the OCF specifications. IoTivity is hosted by the Linux Foundation and is licensed under a standard Apache 2.0 open source license. This full reference implementation of the OCF specification serves to enable developers, OEM's, brands etc. to quickly bring their fully interoperable IoT products to market.

4.2 Interoperable Metadata

Hypercat is an open, lightweight JSON-based hypermedia catalogue format for exposing collections of uniform resource identifiers (URLs) for exposing information about IoT assets over the web (http://www.hypercat.io/standard.html). Using HTTPS, REST and JSON, each Hypercat catalogue may expose any number of URIs, each with any number of resource description framework-like (RDF-like) triple statements about it. Hypercat allows a server to provide a set of resources to a client, each with a set of semantic annotations. Implementers are free to choose or invent any set of annotations to suit their needs [21].

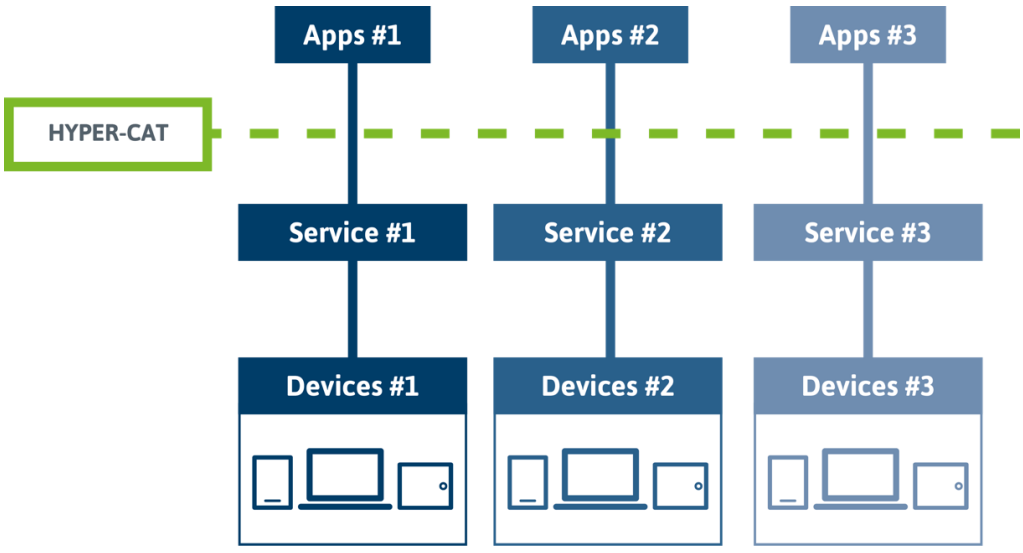


Figure 4-4: Hyper-cat IoT Interoperability

4.3 IoT Identities

Triggered by the broadening of the value chains associated with IoT is a broadening of the concepts associated with identity, as illustrated in Figure 4-5. Whereas previous WBA deliverables have concentrated on solutions that support equipment identities (e.g., signalling Wi-Fi MAC-48 addresses in the RADIUS Calling Station ID attribute) and subscription identifies (e.g., signalling IMSI in the case of EAP-SIM/AKA/AKA' based Passpoint/NGH based authentication), the IoT Centric device will typically have an identity associated with its application as well as possibly an Embedded UICC Identity. Importantly, there may be use cases where providers of these different identities correspond to different entities.

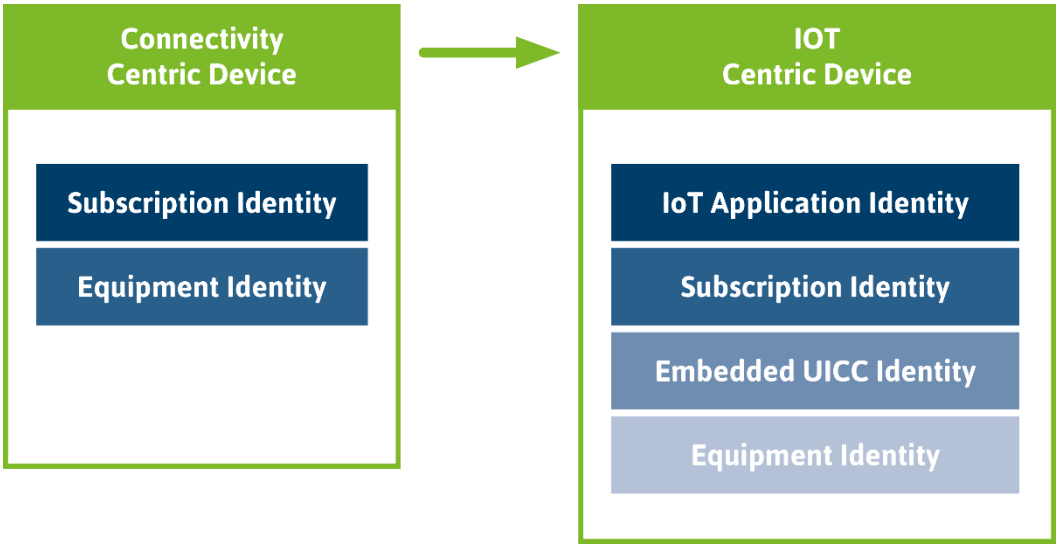


Figure 4-5: Broadening of Device Identity concepts

The following sections will review the different identities defined to support a range of IoT use cases.

4.3.1 802.11 Passpoint/NGH Identities

Established Passpoint/Next Generation Hotspot solutions support a range of different EAP authentication mechanisms with their respective identity definitions.

EAP-SIM, EAP-AKA and EAP-AKA' based authentication re-use the International Mobile Subscriber Identity (IMSI) configured in the USIM application for identifying a subscription. The IMSI conforms to E.212 numbering standard [22] that comprises of the concatenation of a Mobile Country Code (MCC), a Mobile Network Code (MNC) and a Mobile Subscription Identification Number (MSIN). When used within an EAP method, the IMSI is embedded within a Network Access Identifier (NAI), wherein the IMSI is used to encode the "user" portion and the MNC and MCC are used to encode the "realm" portion.

EAP-TLS enables re-se of the TLS-protocol exchange that may already be used for protecting the end-to-end IoT communication. From an IoT perspective, such re-use enables sharing of components between network access security functionality and the TLS functionality needed for securing IoT application-layer traffic.

4.3.2 Embedded SIM Card Identities

Previous WBA architectures that have focused on Network Connectivity centric value chains have looked to leverage conventional cellular approaches that couple access identities with the provision of network connectivity, for example, with conventional SIM cards being used to store credentials including the identity of the access network provider (i.e., MNC and MCC). These established procedures are being challenged by the emerging IoT use cases that are driving two new capabilities:

- The definition of a new M2M embedded SIM form factor, MFF2 [23] that enables direct soldering onto a IoT device PCB
- decoupling of the (transient) access identities from the permanent eUICC Identity, enabling the remote (re-) provisioning of an IoT device with new access identities and credentials [24].

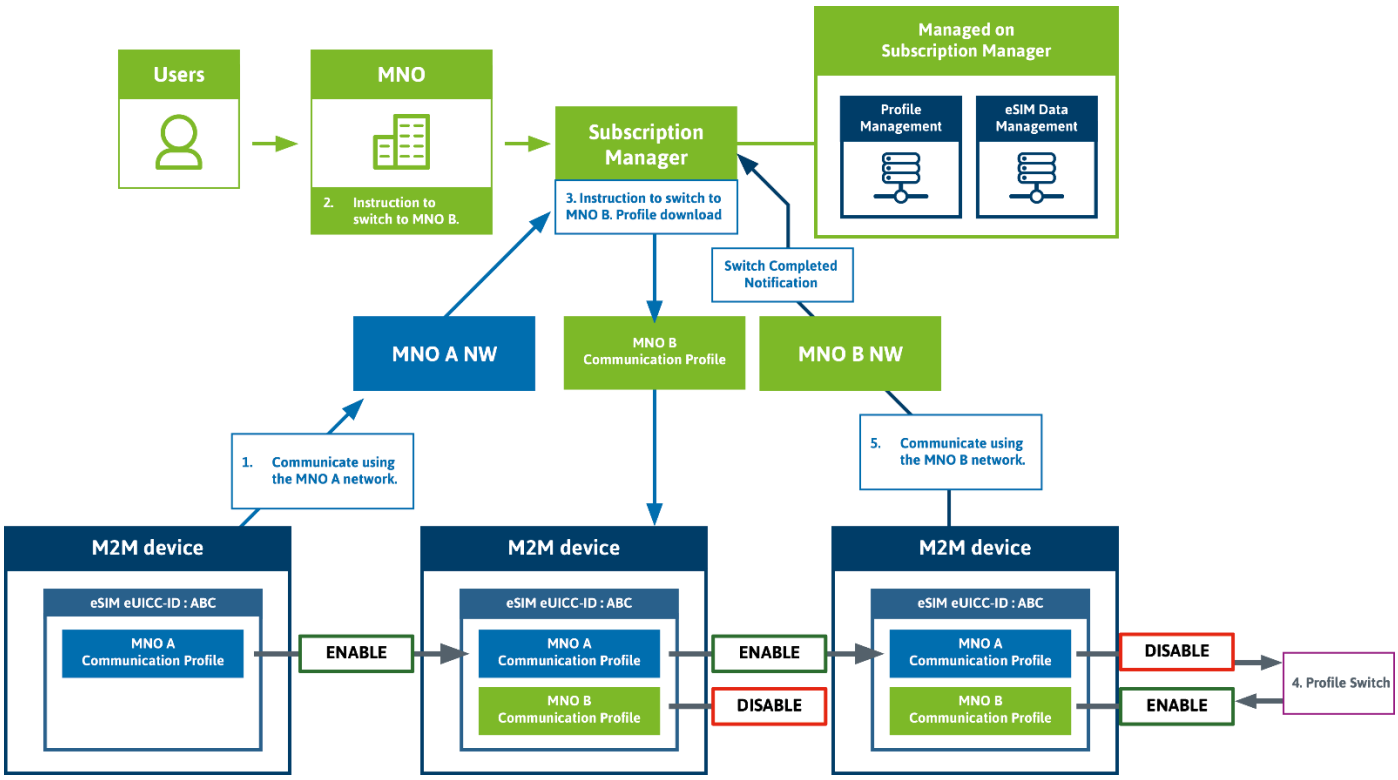


Figure 4-6: Embedded UICC for Switching SIM Profiles [25]

Whereas with conventional SIM card, an Integrated Circuit Card Identifier (ICCID) is used to internationally identify a SIM card, in the embedded SIM card architecture the ICCID is used to identify one of a number of different profiles. A new permanent identity has been defined, the eUICC-ID which is used as the unique identity of the embedded SIM card.

Devices that integrate embedded UICC functionality can ship with a default provisioning profile, enabling it to communicate with a Subscription Manager that is then able to provision new profiles and trigger the switching of active profiles by the M2M device.

4.3.3 OneM2M Identities

From an IoT Service perspective, the oneM2M security architecture framework [26] defines a framework for securing M2M communications, enabling the establishment of a security association between a field domain deployed (IoT) entity and an infrastructure domain entity. Different identities are defined within the oneM2M architecture framework, including:

- Application Entity Identifier: a globally unique identifier used to identify the Application Entity resident on a particular M2M Node, and of format {M2M-SP-ID}{SP-relative-AE-ID}
- Application Identifier: used to identify a particular IoT application, and of format R{authority-ID}.{reverseDNS}.{applicationName}
- M2M Node Identifier: A globally unique identifier that is pre-provisioned in the node hosting the M2M Application Entity. One example of such is an IMEI.

- M2M Service Subscription Identifier: used internally within the IoT service provider to bind various identifiers to a particular IoT service subscription, but which is not exposed over any IoT interface.

4.3.4 LoRa Identity Definition

The LoRa alliance is developing a LoRaWAN specification for supporting low power wide area capabilities with specific functionalities to support low-cost IoT applications [27]. LoRaWAN re-uses the IEEE-defined 64-bit Extended Unique Identifier (EUI-64) [28]. The device EUI-64 is used to uniquely identify an end device. The application EUI-64 is used to uniquely identify the application provider (i.e., owner) of the end device.

The EUI-64 identity is formed by the concatenation of an Organizationally Unique Identifier (OUI) value assigned by the IEEE Registration Authority and an extension identifier assigned by the organization with that OUI assignment.

4.3.5 Wi-SUN Alliance

One particular focus of Wi-SUN is the specification of Smart utility Networks, defining a mesh-enabled Field Area Network (FAN) between smart meters. Wi-SUN has adapted IEEE 802.1X and EAP-TLS for mutual authentication and establishment of a secure 802.15.4g link between a FAN node and its Border Router [29].

4.3.6 IEEE 802.15.4

All IEEE 802.15.4 devices include a unique EUI-64 universal address. IEEE 802.15.4 networks are identified using a 16 bit PAN identifier that is selected by a PAN co-ordinator to ensure that overlapping networks do not share a common identity.

4.3.7 Bluetooth

Bluetooth specifies the use of IEEE EUI-48 addresses. The EUI-48 identity is formed by the concatenation of a 24 bit Organizationally Unique Identifier (OUI) value assigned by the IEEE Registration Authority and a 24 bit extension identifier assigned by the organization with that OUI assignment

4.3.8 DASH-7

DASH-7 devices all have a fixed-length Unique ID which is a 64 bit EUI-64 value that is unique to every device.

4.3.9 Weightless

Weightless uses a 128-bit unique identifier for each weightless terminal. The 128-bit length of UUIDs is intended to permit independent generation of unique identities with negligible chance of collision. UUIDs must be registered with the Service Provider Data Base (SPDB).

4.4 IoT Security Architecture

From an IoT Service perspective, the oneM2M security architecture [30] defines a framework for securing M2M communications, enabling the establishment of a security association between a field domain deployed (IoT) entity and an infrastructure domain entity, as illustrated in Figure 4-7. This security architecture supports a number of different security options, including:

- Symmetric Keying based security framework
- Certificate-based security framework, and
- Generic Bootstrapping Architecture (GBA) based security framework

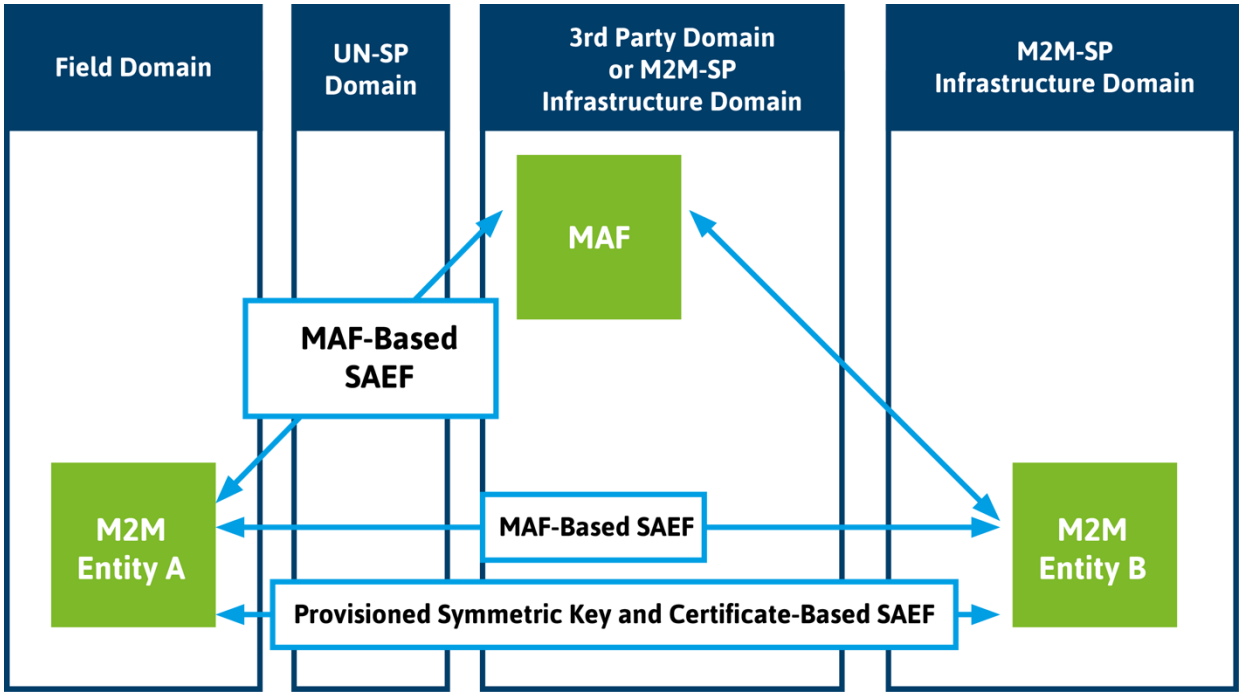


Figure 4-7: oneM2M Security Association Establishment Framework [26]

Figure 4-7 illustrates the role of the Mobility Authentication Function (MAF) that is used for supporting all security options, together with the Mobility Enrollment Function (MEF) and the Generic Bootstrapping Architecture Bootstrapping Server Function (GBA BSF) that are additionally used to support the derivation of master credentials in certificate based security and SIM based GBA security respectively. (In the case of pre-shared symmetric keying, the master credentials are assumed to be pre-provisioned in the MAF.)

In all cases, the keying material generated during remote provisioning is then used to protect the IoT application communications, e.g., using TLS or DTLS with appropriate cipher suites.

Note, whereas the oneM2M security architecture provides for securing the communications link between a field domain deployed IoT device and an infrastructure deployed IoT server, there are other security aspects that need to be considered, for example, including

- avoiding default username/passwords,
- using trusted secure boot and trusted secure storage,
- supporting true random number generation,
- disabling test and debug ports,
- securing firmware update procedures.
- IoT and Identity Ownership

The introduction of remote re-provisioning capabilities associated with devices that include an embedded UICC together with the use of permanent LoRa identities that are associated with the IoT application provider are recognition that the identity models that have been successfully used over the last 25 years of cellular deployment need to be enhanced to optimally support the Internet of Things.

Furthermore, the shift in monetization and charging aspects introduced in Section 3 may further lead to disruption in the identity management. In particular, for service based monetization models, the title of a particular IoT device associated with an identity may remain with the manufacturer who then offers the

service to the user. In other hardware based models, the user may represent the owner of the device who bought the product but the ownership may change over time. These important aspects of ownership and identity relationship have an important impact on security related procedures such as authentication and authorization.

Importantly, the current identity and roaming models have delivered foundational capabilities associated with authentication, authorization, charging, settlement and fraud management. However, these have been based on the assumption that the identity is owned by the telecom service provider and hence the conventional roaming domain has been successfully used to address the N^2 scaling problem where N=O(100) and where brokers can be used to address some scaling issues.

The emergence of IoT will likely see new identity providers emerge, and so systems will need to scale to the level of "an enterprise" being an identity provider and where an enterprise can be a city, a thing manufacturer, a Wi-Fi service provider or a traditional telecoms operator. Hence, the foundational capabilities should enable scalable services that are able to support N=O(>10,000) identity providers.

5 Interoperability between technologies (IoT verticals interoperability)

5.1 Automated/Seamless Authentication

The Internet of Things is set to trigger a diversification in terms of the endpoints being connected to the wireless network. Compared to earlier mobile broadband tailored offers where devices are assumed to have some display and user input capabilities, many of the constrained devices used in Internet of Things will have limited Input/Output capabilities such that conventional web based authentication and/or splash page acknowledgement of terms and conditions will inhibit IoT connectivity solutions.

Consequently, the work the WBA has delivered from a Passpoint/Next Generation Hotspot perspective in terms of automated authentication is directly applicable to the Internet of Things. However, the current definition of the on-boarding solution in terms of On-line Signup Service and its reliance on displaying OSU providers and manual user selection looks to be poorly suited to IoT use cases.

5.2 Emerging Standards for IoT Roaming

The LoRa Alliance is defining an end-to-end system for supporting the LoRaWAN based air interface and is currently defining back-end interface specification that will deliver a standardized secured and authenticated interface between the various core components [31].

Figure 5-1 below shows a representation of the back-end 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.

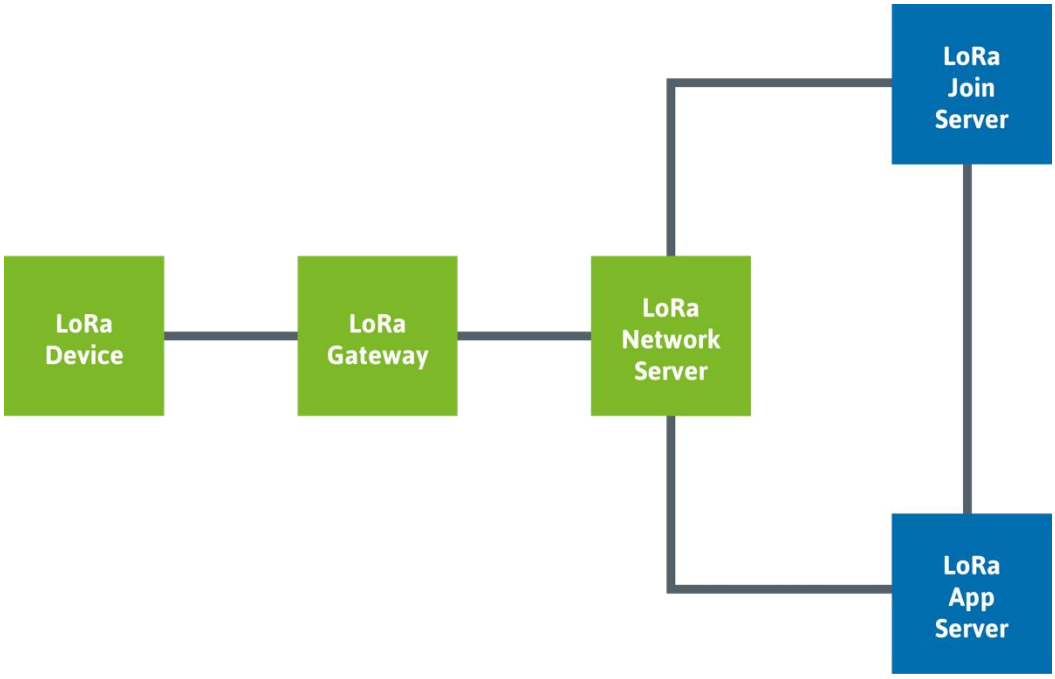


Figure 5-1: LoRa End-to-End System Components

One of the more recent developments has been to start to define new RADIUS attributes for supporting the join procedure between the LoRa NS and JS [32]. In a similar fashion to how RFC 3579 specifies how to transport EAP messages over RADIUS, the above reference proposes an encapsulation of the LoRa Join Request/Join Accept messages with RADIUS, together with the delivery of appropriate LoRaWAN keying material in the RADIUS Access Accept.

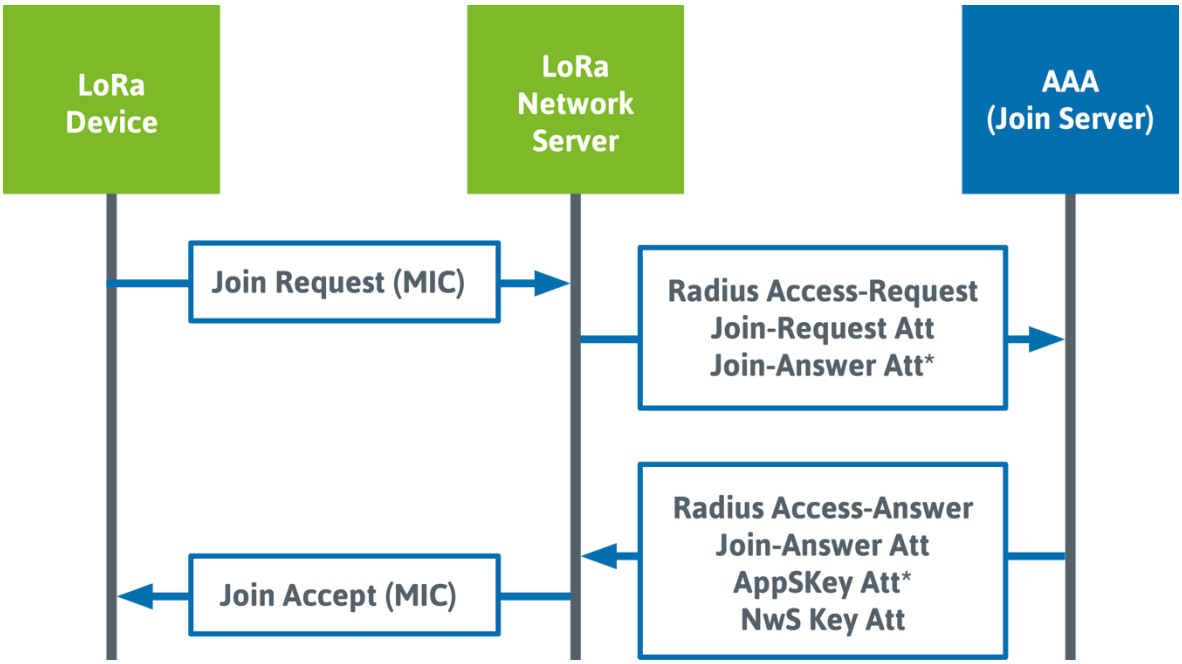


Figure 5-2: Proposed RADIUS Support of LoRaWAN Join Exchange

In addition to supporting the AAA interface for roaming users, 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 5-3.

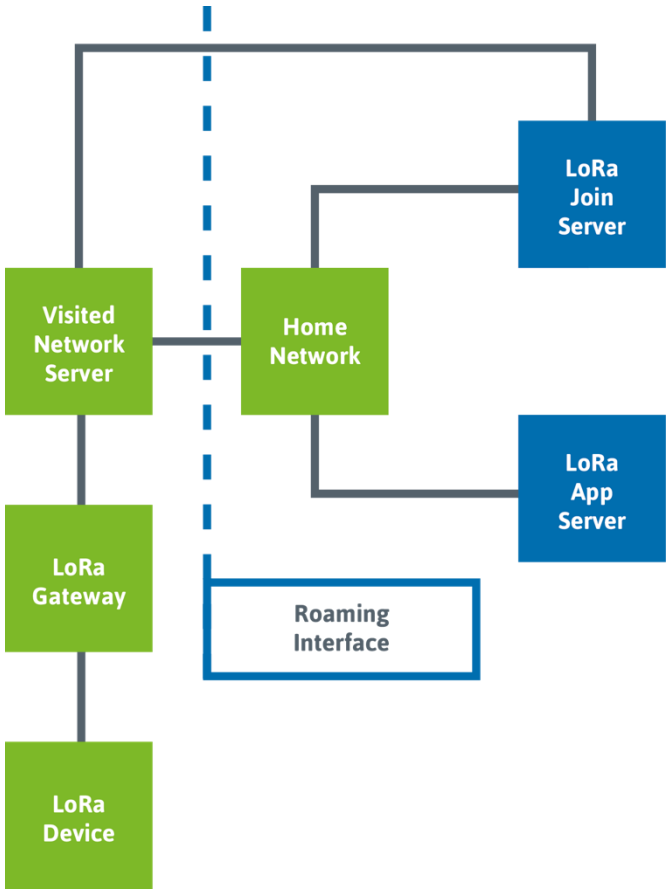


Figure 5-3: LoRaWAN Roaming Back End Interfaces

5.3 Interoperability challenges for IP and Non-IP data

When developing an end-to-end IoT service, the majority of effort is focused on development of the applications. However, often these applications require common functionalities and rather than develop each from scratch, common libraries can be leveraged to enable effort to be focused on the differentiated IoT capabilities.

For non-IP data deployments, there are several application stacks that are already commonly used in markets such as ZigBee, Wireless M-Bus, Modbus, KNX, etc. These stacks have already specified interoperable capabilities that can be leveraged by IoT application developers.

As an example, the ZigBee Cluster Library (ZCL) defines a common means for (non-IP) applications to communicate. It defines a header and payload that sit inside the ZigBee Protocol Data Unit (PDU) used for messages. For example, the Basic ZigBee Cluster includes support for commissioning activities, e.g., including remote factory reset capabilities, and the Over-The-Air (OTA) Upgrade cluster provides the facility to upgrade (or downgrade or re-install) application software on the ZigBee device.

For IP-data deployments, there are several specifications that can be leveraged by IoT application developers. Most notably, oneM2M (www.onem2m.org) develops technical specifications for supporting a common M2M service layer. Further, Lightweight M2M is a client-server specification for IoT device management.

5.4 Interoperability using Application Gateways

Concerning gateways, ETSI's Machine-to-Machine Functional Architecture [33] defines two modes of operations:

- Direct Connectivity mode: where the M2M devices connect to the Network Domain via the Access network. The M2M Device performs the procedures such as registration, authentication, authorization, management and provisioning with the Network Domain.
- Gateway as a Network Proxy: where the M2M Device connects to the Network Domain via an M2M Gateway. M2M Devices connect to the M2M Gateway using the M2M Area Network. The M2M Gateway acts as a proxy for the Network Domain towards the M2M Devices that are connected to it. Examples of procedures that are proxied include: authentication, authorization, management, and provisioning.
- These two alternatives are illustrated below.

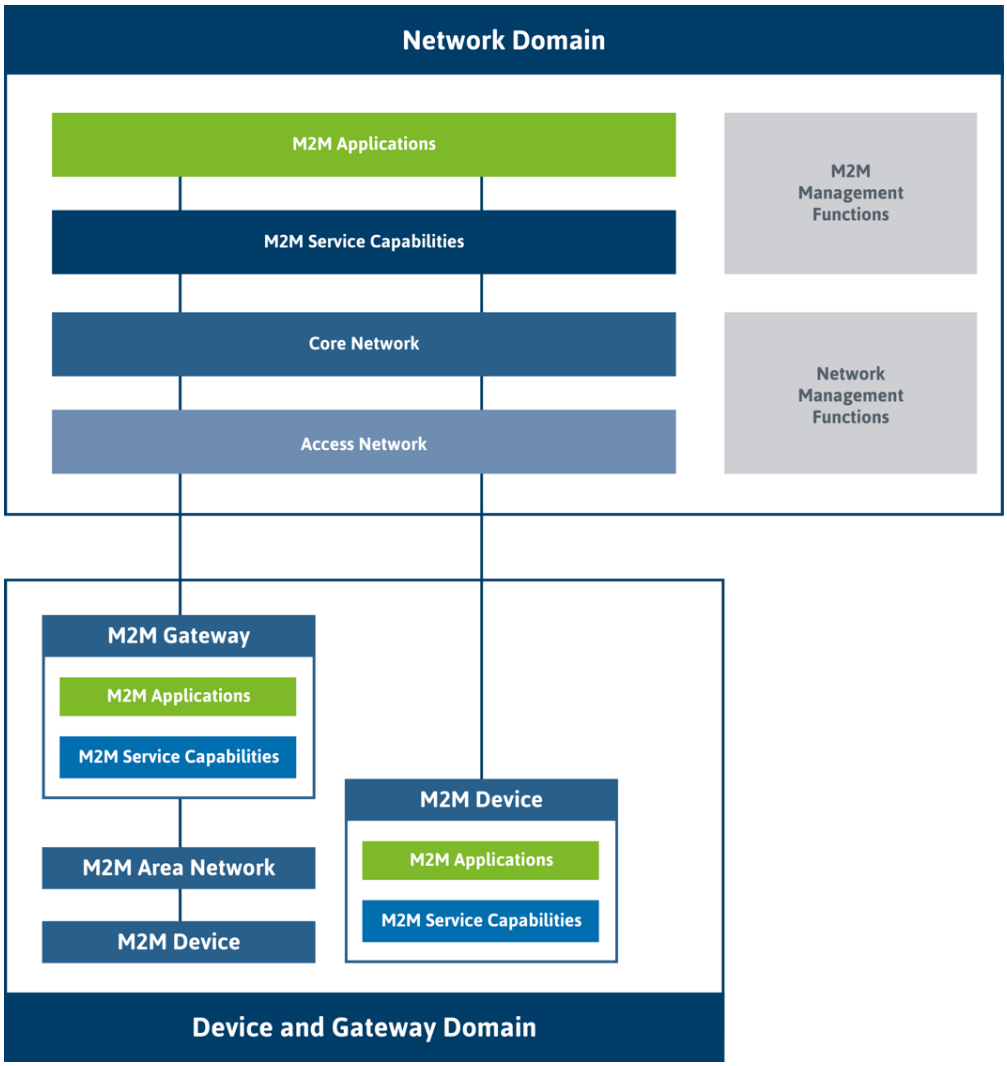


Figure 5-4: High level architecture for M2M

- The Gateway as a Network Proxy approach is necessary when non-IP data IoT devices need to communicate with back end M2M services/applications. The gateway model may also be used to support IPv6 only IoT devices when the network domain only supports IPv4.
- *As illustrated above, the gateway model requires application software running on a local gateway device which then acts as an intermediary between the M2M device and the M2M Service*

Capabilities/Applications in the network domain. (Note, RFC 7452 [34] warns that M2M approaches that include the use of application-layer gateways will, in general, lead to a more fragile deployment.)

- An evolution of this gateway approach is the "hub" model where the gateway can additionally bridge the interoperability gap between the IoT devices themselves. For example, the Samsung Smartthings hub (www.smarthings.com) supports Wi-Fi as well as Z-Wave and Zigbee wireless technologies.

5.5 Back End Data Sharing and Interoperability

This model refers to an architecture where IoT data back-end data is shared. Compared to architectures where IoT application data exists in silos, a back end data sharing approach enables the user to suitable authorize the sharing of uploaded data with third parties.

Furthermore, as described in [35] an effective back-end data sharing architectures will allow users to move their data when they switch between IoT services and between IoT service providers, breaking down traditional data silo barriers. Figure 5-5 illustrates such an architecture, highlighting the importance of standardized APIs for interoperable data sharing.

Such a federated, cloud IoT service requires not only standard protocols to eliminate data silos, but also common information models, to enhance the interoperability in the Internet of Things at the application layer. This can be contrasted to the current state of the market that can be characterized by the use of inconsistent information models [36]. Accelerated adoption of back end data sharing requires information models to converge. These schemas need to be fully decoupled from underlying communications protocols, architectures, and access specific identity and security mechanisms.

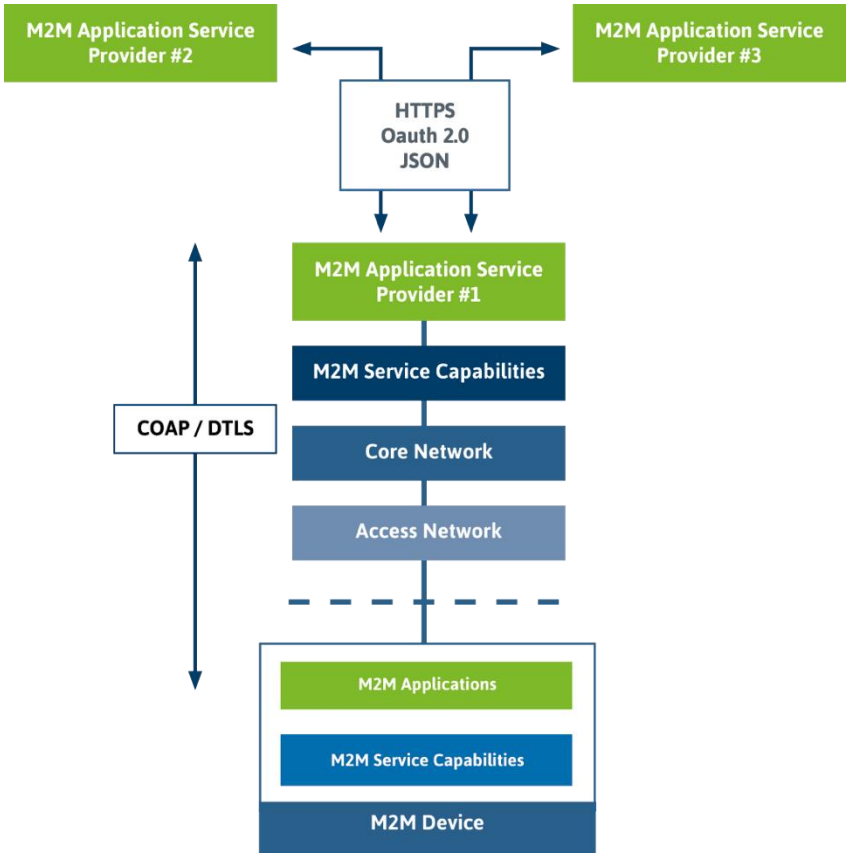


Figure 5-5: Back End Data Sharing Architecture

6 Analysis of the evolution of existing value chains

6.1 IoT Value Chains

Compared with the capacity and/or coverage centric value chains of conventional Carrier Wi-Fi deployments, IoT brings with it a diverse set of value chains, including [37]

- Phase 1 - Operational efficiency: Looking to optimize asset utilization, deliver operational cost reduction and/or worker productivity
- Phase 2 - New Product and services: including taking traditional products (e.g., a car) and delivering value added services (e.g., connected car, infotainment, remote engine diagnostics, etc.), that are software based and consumable on a pay-per-use basis.
- Phase 3 - Outcome based offerings: Applying advanced analytics to a broad range of data derived from IoT systems as well as external systems, companies will be able to gain a better understanding of interactions and causality among a set of observed data variables, and to determine what it takes to manipulate the variables in order to achieve a desired outcome.
- Phase 4 - Autonomous Pull Economy: Defining closed loop systems that are continually self-optimizing for optimized resource utilization

Phases 1 and 2 are likely to represent near term opportunities that drive the initial adoption of IoT.

6.1.1 Value Chains Based On Operation Efficiencies

With internal productivity and efficiency being cited as the primary driver for IoT adoption, this section looks at network wide functionality aimed at facilitating adoption of such value chains.

As efficiency is the primary motivator, understanding of key issues associated with costs around delivering the IoT service will be required .These costs include [38]:

- On-going operational costs
- Operational cost savings
- The time it will take to achieve ROI

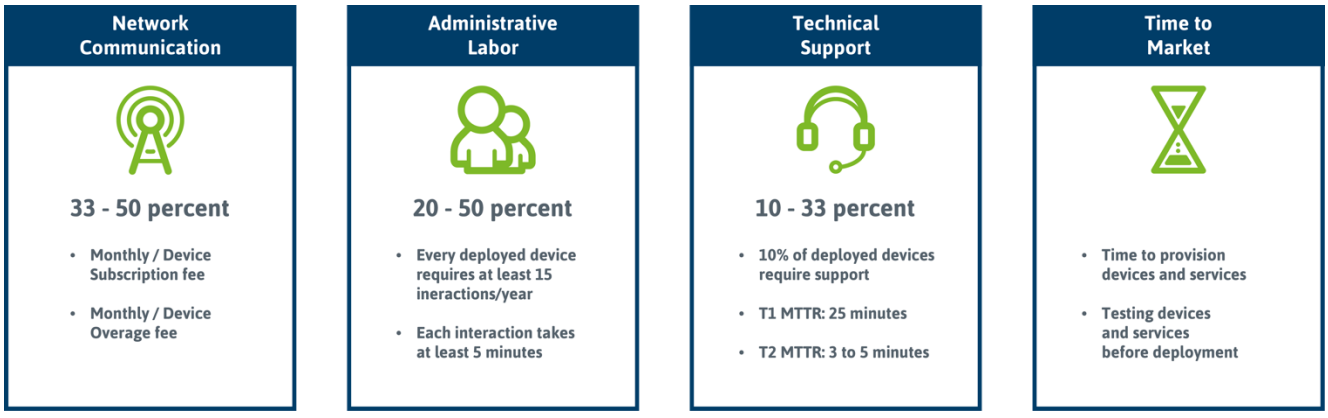


Figure 6-1: Operational Expenses for an Industrial IoT deployment

In particular, as it relates to network connectivity, data averaged over a deployment of 100K networked devices within an industrial IoT environment [38], indicate that average utilization was

2MB/device/month of data and 19KB/device/month of messaging traffic, equating to an average spend of $1.25/device/month on cellular connectivity. However, these averages masked wide scale differences in network connectivity requirements, with some IoT devices using as little as 25 Kbytes/device/month and other using up to 1GByte/device/month.

Because network communications can contribute up to 50% of the overall operation expense of deploying the IoT service, key criteria related to network access needs to be understood; monthly access fees, data plans, overages, roaming fees, usage report rounding, flexible allocation of consumption to devices with bucket plans as well as taxes and surcharges, are all important factors to consider.

6.1.2 Value Chains Based On New Services

The second phase of IoT adoption focuses on the transformation enabled when every product offers ubiquitous connectivity, enabling new opportunities in the interactions with existing customers. This will trigger a value chain shift in the industries adopting IoT, moving from product-centric value offers to service-centric value, delivering continuous updates to existing products and services.

Key challenges for successfully deploying IoT value chains based on new services include: [39]

- Device provisioning and on-boarding along with a set of usage policies
- Service performance monitoring and optimization
- Remote diagnostics as well as problem resolution
- Service monetization and cost management

6.2 IoT Usage Based Reporting

As there is not a one size fits all for characterizing IoT services, there will not be a single size when it comes to aspects related to connectivity charging. Indeed, there will certainly be “IoT” services that consume equivalent amounts of bandwidth compared with today’s smartphone users and so in such scenarios, there should be no difference in usage based reporting requirements. Indeed, analysis of existing cellular IoT services indicate that connection fees, including monthly access fees, data plans, overages and roaming, account for 33-50 percent of the overall OpEx spend for delivering IoT services [40].In particular, it is reported that some service providers limit the amount of time that an IoT device can be connected to the cellular network, with sessions typically lasting four hours before a device is disconnected to free up resources for other devices on the network. Importantly, when the four-hour session ends, usage is generally rounded up the nearest KB.

However, IoT will also see the emergence of new consumption trends where IoT devices only send a few bytes of data over a defined period. These scenarios may drive new usage reporting requirements, in particular where the cost of handling device records needs to be factored into the overall costs of supporting a particular IoT service. For example, commercial rates for managed IoT cloud platforms charge less than $10 for handling 1 million IoT messages [41]. In example pricing, an IoT device generating a message every hour will incur a monthly cost of less than ½ cent associated with IoT message publishing. Compared with the session analysis above, this may mean that 180 charging records are generated over the same 30 day period.

Note, the current billing information used in cellular networks defines that the maximum context duration must not exceed 24 hours [42] meaning that a minimum of 30 (partial) records will need to be generated and processed for supporting the IoT device.

Compared with conventional cellular charging, current on-going definition of the Low Power Wide Area Networks is leading to new low cost charging options. Recently SK Telecom announced its pricing scheme for its national LoRa network with the lowest cost plan offering 100 kB of data for 30 cents/month [43]. This focus on low cost is also reflected in the on-going definition of the backend

systems to support LP-WAN access networks, with proposals for the access network to generate monthly Network Traffic Records, aggregating the traffic generated by IoT users.

Moving forward, it is interesting to note that new innovative rate plans are being introduced on cellular networks. For example, AT&T have recently launched mobile-specific IoT rate plans, with bundles of data and text being valid for up to 2 years [44].

6.3 Monetization of data assets/cross subsidies

There is an increasing recognition that when the value chain for connected products is analysed, there is often more value to be found in the middle, associated with data assets, than there is revenue to be had from the end user [45]. However, compared with the unambiguity associated with monetizing connectivity services, the task of identifying key value points associated with data assets is difficult at best and may vary depending on IoT use case. One example use case for monetizing data assets concerns location data and associated movement analytics. It is reported by Inrix [46] that there are large scale opportunities for monetizing movement analytics. Example use cases include city planning and transportation industries, as well as outdoor advertising, where movement analytics is able to estimate the number of people who have viewed a particular installation.

As noted by Inrix, one of the challenges with monetization data assets is recognizing that this should not be seen as extension of a conventional connectivity proposition, and will require new capabilities in terms of tools and platforms. Possible business models include the access operator providing direct access to its network data, with the access provider looking to establish a revenue share with third parties who utilize the data. Alternatively, the access provider can develop its own data analytics service and market that directly to a new set of consumers.

One example of such is the MK Smart project, formed in collaboration between the Milton Keynes council authority in the UK, BT and the Open University, to launch smart city services using Internet of Things technologies (www.mksmart.org).

BT and partners deployed a network of sensors connected via cellular, Wi-Fi and Low Power Wide Area Radio Network (LoRa), operating across the city to carry data that enabled applications to improve public services.

The aim of MK Smart was to create an Open Data Hub to store and make available the data collected from these sensors to service providers, innovators and in some instances, directly to citizens. BT and the Open University worked together to create a platform whereby data silos were broken down to enable a range of council proprietary and open source data (e.g. weather and temperature) to be shared so that third parties could create useful applications in a number of different domains [47]. Monetization opportunities were expressed in savings through optimisations in water, energy & fuel usage as well as derivatives gained from the data itself.

6.4 Machine learning capabilities and application to optimization and monetization opportunities

Much like the location analytics described above, the availability of real-time sensor data made available by IoT-enabled devices provides new opportunities for on-the-go analysis and programmed decision making. This results in new value creation opportunities that were previously unattainable.

- More generically, IoT data analysis is expected to progress in four stages of maturity [48]:
  - Stage 1: Descriptive analytics. What happened?
  - Stage 2: Diagnostic analytics. Why did it happen?

- Stage 3: Predictive analytics. What will happen?
- Stage 4: Prescriptive analytics. What should I do?

- Using this ranking, it is evident that much of today's location analytics is based on stage 1, merely presenting details of the footfall associated with users and their devices onto coverage maps. However, such visual analytics simply show historical variations, saying nothing about why a particular reported set of events might be occurring. Figure 6-2 below illustrates that these approaches typically require a human to interpret the data and take an action. In many cases, these steps may be costly and so may never happen.

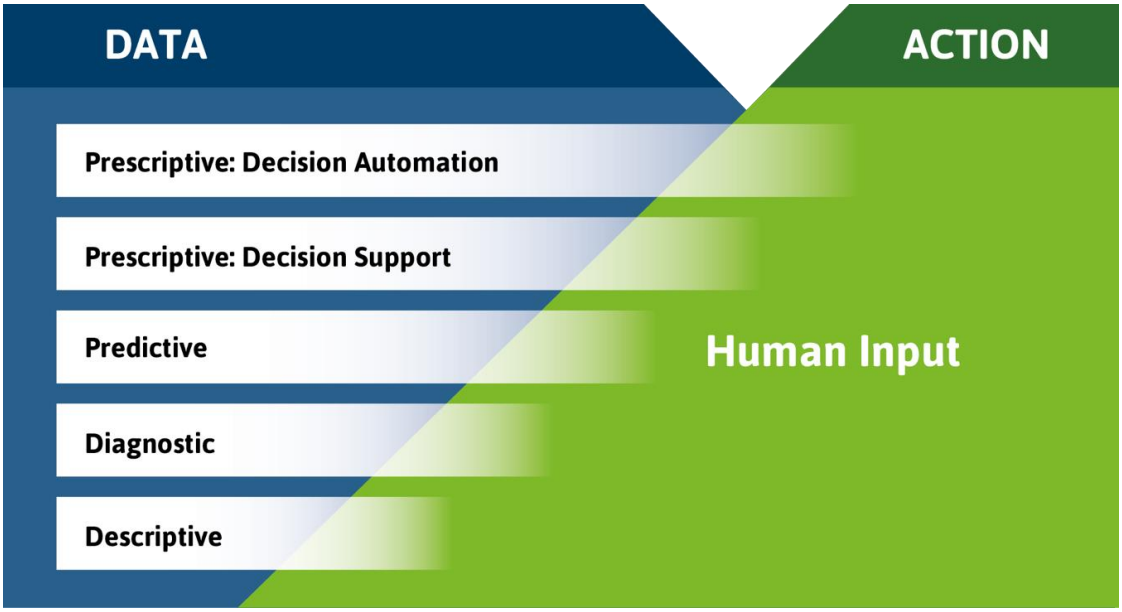


Figure 6-2: Stages of analytics maturity [49]

- Moving to stage 3, IoT data is being used for predicting events. For example, in the industrial automation arena, companies install IoT sensors in equipment and then create system models to learn the correlation between sensor data and associated system problems or failures. In particular, asset intensive industries and organizations are already using IoT to generate large amounts of data that is being used to positive effect [50]
  - A medical device manufacturer was able to leverage data from devices to nearly double availability of its equipment, while reducing cost of maintenance by 20-30%
  - A global producer of cold storage equipment was able to monitor installations in 4500 supermarkets worldwide, analysing thermostats, evaporators, fans and compressors to greatly reduce unplanned failures
  - Elite athletes are now monitored for fatigue and physical load through using wearable IoT sensors, allowing teams to manage player performances in-game by the use of wireless systems.
- Moving forward, companies are investing in suites of product to be able to deliver prescriptive analytics. Building on prediction capabilities that are able to analyse patterns found in historical data, optimization tools look to find the best choice from a variety of alternatives and finally to decide on the best course of action give objectives, requirements and constraints. Research by ABI indicates that growth in prescriptive IoT analytics will initially be targeted at asset-intensive industries in which machinery cost is high, listing opportunities in industrial, manufacturing, field, oil and gas sectors [51].

7 Evolution of Passpoint/NGH based roaming to accelerate the deployment of IoT services.

For the IoT based roaming to flourish existing technologies should evolve and adapt to cope with IoT broad requirements. Wi-Fi has been an industry reference in developing itself to become more secure, seamless and interoperable leveraging on industry consensus. These lessons should be taken into the IoT scope.

Wi-Fi networks, given their nature, evolution and adaptability, can aim at efficiently integrating IoT roaming. One key example is the embedded SIM card (eUICC) which contain the same information as of regular physical SIM cards. All the configuration information needed such as device identity, passwords and network selection can be provided. In fact, this removes the concept of physical authentication element on the device, bringing it closer to other non-physical credential based EAP methods, such TTLS and TLS. As a result, existing NGH/Passpoint authentication procedures are a vehicle to accelerate roaming in IoT.

In the enterprise context it is expectable that a broker will play a key role on massive deployments and control of authentication information (e.g. EAP information, pre-shared keys). Security is still a key aspect to consider in these onboarding mechanisms.

7.1 Provisioning

By norm, configuring each IoT device to be used in the scope of Wi-Fi networks, might involve several steps:

- Service set identifiers (SSID)
- Identities
- Credentials
- Spectrum ranges
- Frequencies

These, in large scale deployments, might be time-consuming and make the system vulnerable to user-entered errors.

Industry consensus around devices configuration should be guarantee and operators should create and support on the IoT platforms a self-configuration tool so the devices are sold and shipped with these set of information.

Provision of pre-shared keys from HS2.0:

- One example of a potential solution is Device Provisioning Protocol (DPP) from Wi-Fi Alliance, it enables new devices to be added to a network via the device of an already-authenticated user. The major advantage of DPP is that it maintains security when adding a new device over Wi-Fi, so that its unique credentials are encrypted and kept hidden from the sponsor (include reference).

Roaming Consortium OI:

- It is expected that the number of players in ecosystem of roaming providers will grow substantially, thus adoption of common Roaming Consortium OI based on HS2.0 is a vehicle to manage these ramifications

Proprietary solutions:

- Operators and vendors have developed as well proprietary solutions to provision multiple devices across a certain footprint within a vertical. These devices credentials should readable from a central system that is capable of interoperate with standard solutions so the ecosystem information can flow smoothly. However, it is recommended that proprietary solutions are avoided and rather focus on industry-driven standards which are key to drive the burgeoning of IoT revolution, they should aim at client-server protocol that clients use to discover and acquire presence information of other clients.

7.2 Authentication

Currently NGH based roaming authentication relies on identities presented on section 4.1.1, the EAP methods (e.g. SIM, AKA, AKA', TLS, TTLS).

IoT growth will leverage the evolution of devices identities on the client and server side, both in terms of provisioning and virtualization. Thus, IoT devices should comply with software modules which can guarantee either support for a digital credential (for EAP-TTLS) or the anticipated roll-out of the embedded UICC (for SIM based authentication).

Passpoint certification is a key enabler for these and the most effective industry process to achieve it. As a result, authentication should be performed according to the seamless network discovery, SSID independent, leveraging on NGH key features, such as enterprises retaining control over network access while avoiding reconfiguration of the sensors (nearly zero-touch).

7.3 Security

In terms of security, current standards should be implemented in IoT devices, with the main recommendation to follow Passpoint certification which includes Wi-Fi Protected Access (WPA or WPA2 enterprise) security type. This should be the standard for IoT devices operating in Wi-Fi networks.

Another angle is the usage of pre-shared keys which need to have security mechanisms in place.

7.4 Evolution of On-line Signup and On-Boarding

The current definition of the on-boarding solution in terms of On-line Signup Service and its reliance on displaying OSU providers and manual user selection looks to be poorly suited to IoT use cases.

7.5 Foreseen evolution building blocks

WBA have been developing trials in the field of Wi-Fi roaming, in the form of Next Gen Wi-Fi end-to-end live trials. Also, the Device Compliance Program (DCP) is focused aimed at testing devices against end-to-end live networks, based on test plans with a strong focus in roaming.

Both programs use cases will evolve in order to align with pertinent range of verticals which can leverage on NGH/Passpoint roaming evolution.

8 Gaps identified

The WBA has analysed the impact of IoT on the evolution of existing value chains and the possible evolution of Passpoint/NGH defined capabilities to facilitate the accelerated adoption of such services using unlicensed based radio technologies.

The results of this analysis demonstrate that there is an opportunity for WBA to broaden HS2.0 systems to incorporate IoT use cases. In particular, whereas current on-boarding procedures assume display and input capabilities, IoT devices will likely be defined without such. Consequently, WBA has the opportunity to augment its on-boarding definition to enable simplified IoT devices to be provisioned with Passpoint/NGH security credentials.

As it relates to current roaming capabilities, there are a number of areas that can be enhanced to facilitate the evolution of current systems to address the broad range of IoT use cases. As a baseline, best practice for using WRIX recommendations as they relate to Usage Data Record handling for IoT can help optimize the ability to support massive numbers of low cost IoT sensors. Broadening the roaming discussions to include non-Wi-Fi based un-licensed systems, it is evident that alternative roaming architectures are being defined that include not only conventional authentication, authorization and accounting services, but also user plane handling, e.g., where the LoRa user plane is always terminated in the home network. This is one example of how WBA can look to evolve its definition of roaming to address such new scenarios.

In parallel, it is likely that adoption of IoT will lead to the broadening of identity provision. In the future, roaming systems may need to scale to the level of "an enterprise" being an identity provider and where an enterprise can be a city, a thing manufacturer, a Wi-Fi service provider or a traditional telecoms operator. Compared with conventional cellular roaming, which is built on an assumption of scaling to an order of 100s of identity providers, there is an opportunity for WBA to enhance its roaming systems to be able to support scaling of the order of tens of thousands of identity providers.

Roaming is also impacted by the evolution of the value chains supported by IoT. Whereas conventional roaming is built to support traditional coverage and capacity value chains, this project has highlighted that adoption of IoT will see value migrate out of the connectivity layer to the new vertical centric value chains associated with IoT applications, big data/analytics, etc. As a consequence, there is an opportunity for the WBA to deliver new roaming capability that supports such value chain evolution, simplifying roaming deployments and accelerating the adoption of unlicensed connectivity solutions by the IoT ecosystem. This may include looking at security perspectives associated with these higher layer services, for example, examining how the WBA can define enhanced capabilities to couple device based access authentication with IoT service-based authentication and security.

From a connectivity perspective, some IoT use cases drive requirements for enhanced service assurance and reliability. Hence, there is an opportunity for the WBA to examine on-going QoS work, and to be able to describe best practice aspects of Wi-Fi system configurations necessary to address support of time critical communications, service reliability and service outage avoidance. From a mobility and multi-homing perspective, enhanced requirements associated with IoT can be addressed by WBA. In particular, although to date WBA has considered cellular-Wi-Fi mobility use cases, IoT may broaden such to include mobility across non-cellular access types.

Finally, from a platform perspective, there is the opportunity for the WBA to advocate a particular ecosystem approach to IoT, where focus is not on the end-to-end product or service offering, but rather on delivering a shared platform to enable other ecosystem partners to monetize their unique capabilities. Moreover, the analysis in this project pointed to the importance of data analytics in IoT use cases. There is therefore an opportunity for the WBA to position on-going and future location based services work within WBA as part of a generic data analytics opportunity, describing current location services as descriptive visualization tools and framing their evolution towards more advanced analytics solutions.

9 Next steps for the WBA

WBA Members see the current momentum as an opportunity to evolve WBA legacy work and aid the IoT world with enhanced practices on the roaming field. Similarly, the case depicted on this document, guide the industry to leverage Wi-Fi existing and evolving capabilities to deliver new services based on IoT verticals.

WBA have recently started a follow-on work focusing on IoT roaming framework and identities – some of the work items include:

- Definition of a technical framework to address IoT roaming
- Integration of AAA infrastructures into LP-WAN
- Evolution of WBA WRIX-i and WRIX-n RADIUS settings adjustment

Moreover, several streams are under discussion to kick-off in the near term:

- IoT gaps standardization:
  - Possibility of including provisioning on IoT standardization related topics, e.g. online sign-up
  - Potentially include as one of the items to address on "NGH Provisioning Standardization" project currently driven by the WBA
- Next Gen Wi-Fi trials to include IoT use cases:
  - Based on the WBA members survey results there are significant number of verticals considered relevant under the scope of IoT and NGH Roaming
  - As a result of the above mentioned work streams, champion worlds' first IoT roaming trial
- Carrier Wireless Services Certification (CWSC) new silos:
  (WBA workgroup: http://extranet.wballiance.com/apps/org/workgroup/cwsc/)
  - IoT services testing to be included as one of the available certification options
  - Enable the industry to test different device types against live unlicensed networks achieving a common baseline of testing to improve time-to-market

WBA invites the industry to join the efforts in making the IoT ecosystem more interoperable and agile regarding service enablement.

LINKS

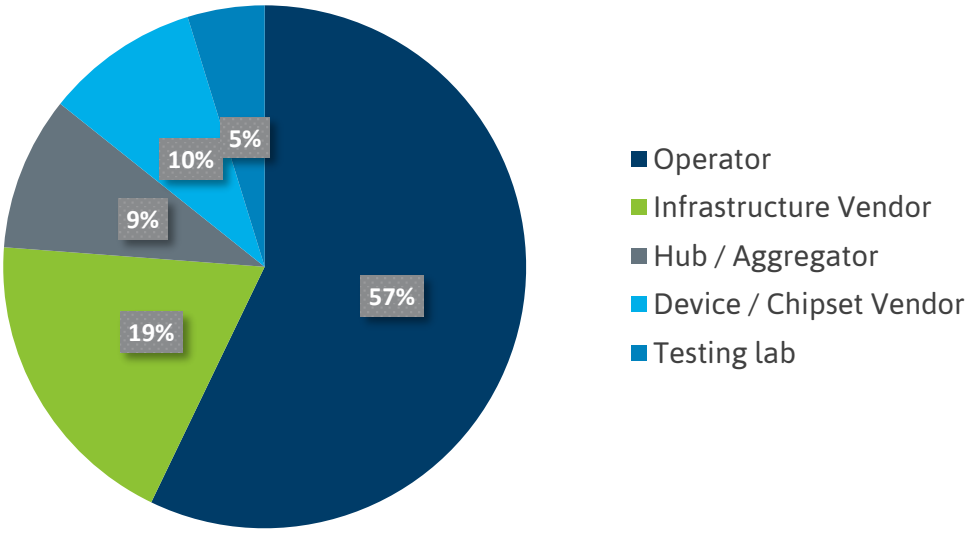
1. WBA 2020 vision, http://www.wballiance.com/resource/vision-2020/
2. "M2M/IoT Sector Map", http://www.beechamresearch.com/article.aspx?id=4
3. "The Internet of Things: Transforming the world we live in", http://www.cvt-dallas.org/IOT-Nov15.pdf
4. http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf
5. https://www.bluetooth.com/specifications/adopted-specifications
6. "LP-WAN Technologies", https://docs.google.com/document/d/1n7cXN4_VuI8imy8MG3-fHjl9FNiNvYfdB4txN4hDQ-w/edit#heading=h.g3u16990965f
7. http://dl.cdn-anritsu.com/ja-jp/test-measurement/reffiles/About-Anritsu/R_D/Technical/E-23/23-04.pdf
8. http://internetofthingsagenda.techtarget.com/feature/Sensors-offer-big-data-users-an-operational-analytics-edge
9. http://go.sap.com/docs/download/2015/08/54f65c37-3b7c-0010-82c7-eda71af511fa.pdf
10. https://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00286R1_ODVA-Optimization-of-Process-Integration.pdf
11. http://www.technavio.com/report/global-lighting-global-smart-lighting-market-2016-020?utm_source=T4&utm_medium=BW&utm_campaign=Media
12. http://www.grandviewresearch.com/industry-analysis/smart-thermostat-market
13. RFC 7228, "Terminology for Constrained-Node Networks", https://tools.ietf.org/html/rfc7228
14. https://www.ietf.org/proceedings/95/slides/slides-95-lpwan-1.pdf
15. "A short survey of wireless sensor networks" http://www.tkn.tu-berlin.de/fileadmin/fg112/Papers/TechReport_03_018.pdf
16. "IoT Security Guidelines Overview Document", http://www.gsma.com/connectedliving/wp-content/uploads/2016/02/CLP.11-v1.1.pdf
17. http://www.iot-a.eu/public/requirements/copy_of_requirements
18. https://machinaresearch.com/news/press-release-the-inexorable-rise-of-m2m-roaming/]
19. A balanced view on extra-territorial use of E.164 numbering (permanent roaming), January 2015, https://machinaresearch.com/report/a-balanced-view-on-extra-territorial-use-of-e164-numbering-permanent-roaming/
20. https://www.capgemini-consulting.com/resource-file-access/resource/pdf/iot_monetization_0.pdf
21. https://drive.google.com/file/d/0B5JKRgbs8OylcmdvMmlGYmtVTU0/view
22. https://www.itu.int/rec/T-REC-E.212/en
23. http://www.etsi.org/deliver/etsi_ts/102600_102699/102671/09.02.00_60/ts_102671v090200p.pdf
24. GSMA Remote Provisioning Architecture for Embedded UICC Technical Specification
25. "Standardization of Embedded UICC Remote Provisioning", NTT DoCoMo Technical Journal, Vol. 2, https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol16_2/vol16_2_005en.pdf
26. oneM2M Security Solutions
27. https://www.lora-alliance.org/For-Developers/LoRaWANDevelopers
28. https://standards.ieee.org/develop/regauth/tut/eui64.pdf

29. Wi-SUN Alliance, “Technical Profile Specification: Field Area Network”
30. oneM2M Security Solutions
31. “The LoRaWAN™ Specification Developments”
32. https://tools.ietf.org/html/draft-garcia-radext-radius-lorawan
33. http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf
34. “Architectural Considerations in Smart Object Networking”, https://tools.ietf.org/html/rfc7452
35. The Internet of Things: An Overview, Internet Society, October 2015, https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf
36. https://www.iab.org/wp-content/IAB-uploads/2016/03/IoT-Information-Model-Interoperability-IAB-Workshop-March-2016-Jean-Paoli-Taqi-Jaffri.pdf
37. http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf
38. http://www.jasper.com/sites/default/files/Cisco-Jasper-Hidden-Costs-of-Delivering-IIoT-Services-White-Paper.pdf
39. http://pages.jasper.com/White-Paper-Capitalizing-on-IoT_LP---Capitalizing-on-IoT-Cisco-Top-Hat.html
40. http://blog.jasper.com/understanding-hidden-costs-iot-part-2-5-network-communication-costs/
41. https://aws.amazon.com/iot/pricing/
42. “Transferred Account Procedure and Billing Information”, GSMA BA.12
43. http://rethink-iot.com/2016/07/08/charge-iot-data
44. http://www.rcrwireless.com/20161005/carriers/att-unveils-iot-pricing-plans-lte-m-trial-san-francisco-tag2
45. http://info.exosite.com/hubfs/Downloadable_Content/Monetization_Strategies_for_Connected_Products.pdf
46. http://inrix.com/wp-content/uploads/2016/02/INRIX-Movement-Analytics-White-Paper_Machina-Research.pdf
47. https://smartcitiesworld.net/news/mksmart-launches-the-mk-data-hub-624
48. http://info.exosite.com/hubfs/Downloadable_Content/Monetization_Strategies_for_Connected_Products.pdf
49. http://info.exosite.com/hubfs/Downloadable_Content/wp_109_data_analytics_for_iot_final_web_reva.pdf?t=1475785567866
50. http://www.datawatch.com/wp-content/uploads/2014/10/Gartner-Industrial-Analytics-Newsletter.pdf
51. “Big Data and Analytics in IoT and M2M”, https://www.abiresearch.com/market-research/product/1024282-big-data-and-analytics-in-iot-and-m2m/

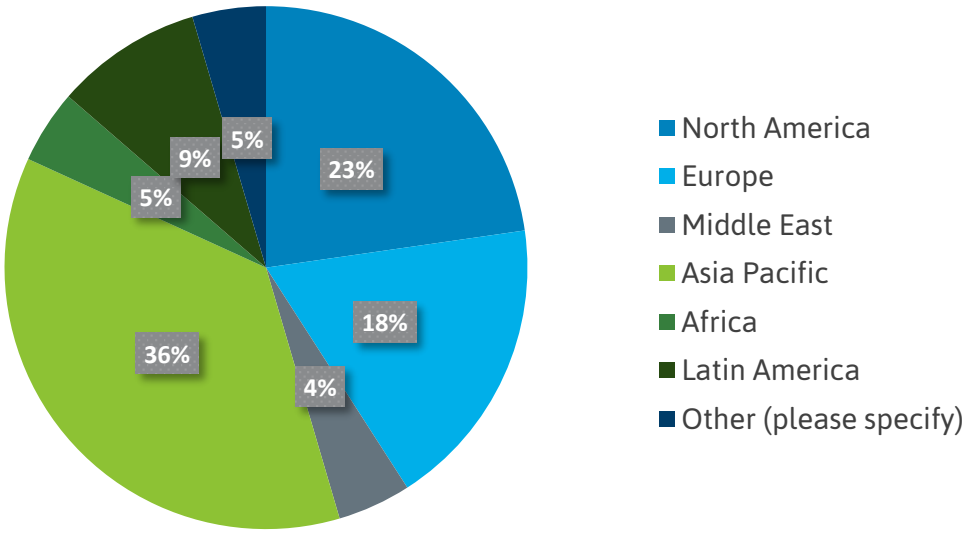
APPENDIX

Detail of the WBA members' survey presented on section 2.4 – The results shared below are direct outputs and were leveraged to extract key takeaways presented on section 2.4:

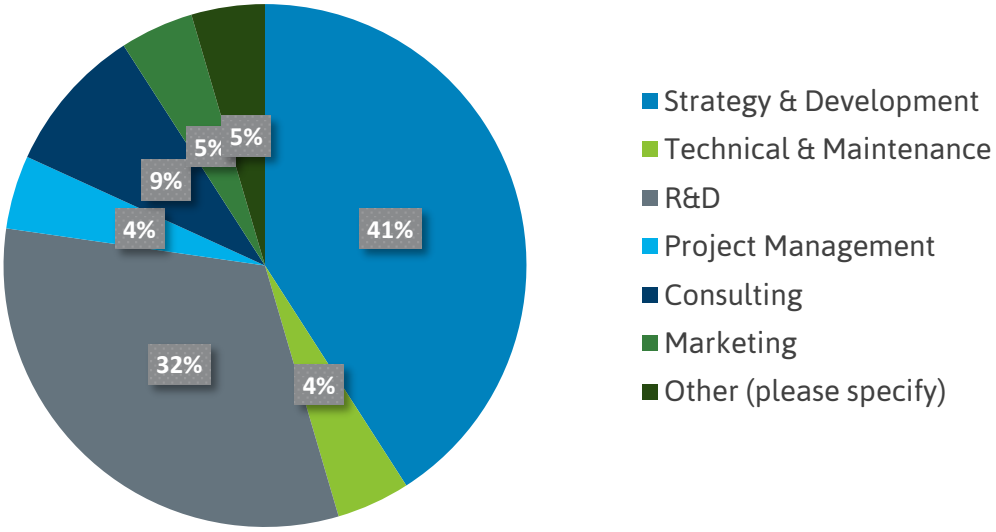
Company type



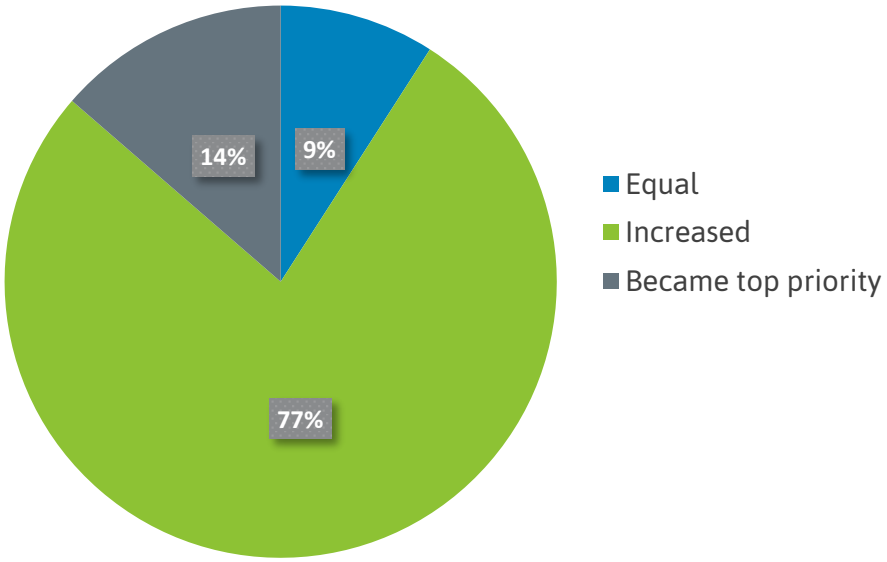
In which region are you based?



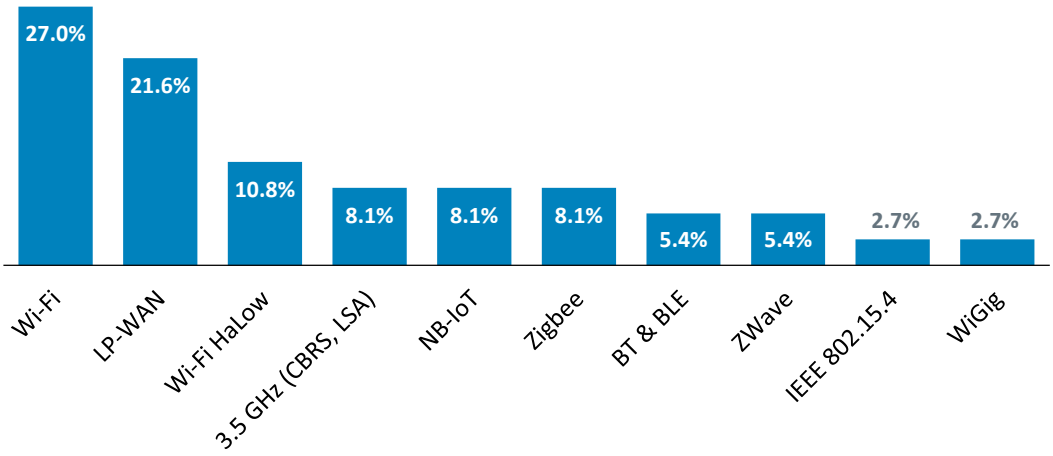
What is your area of work?



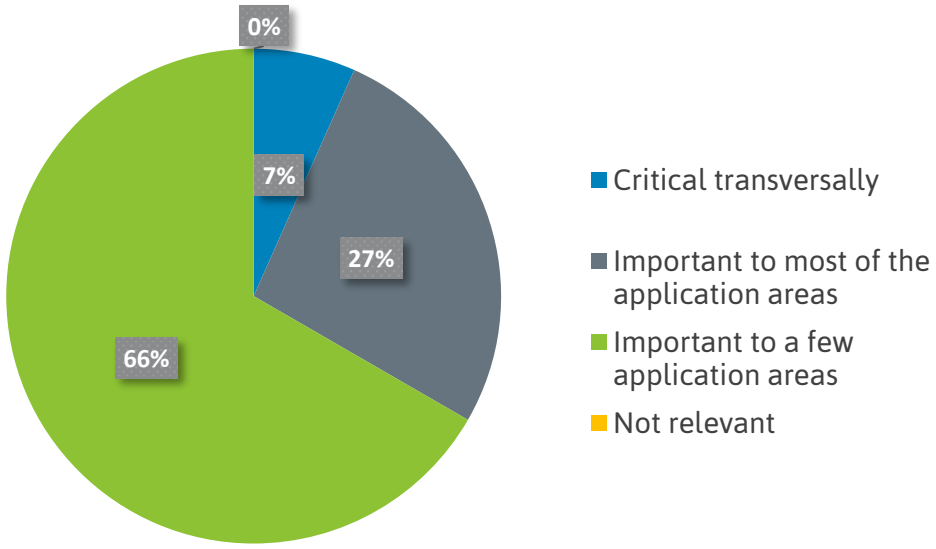
How the priority of IoT services evolved within your company compared to 1 year ago?



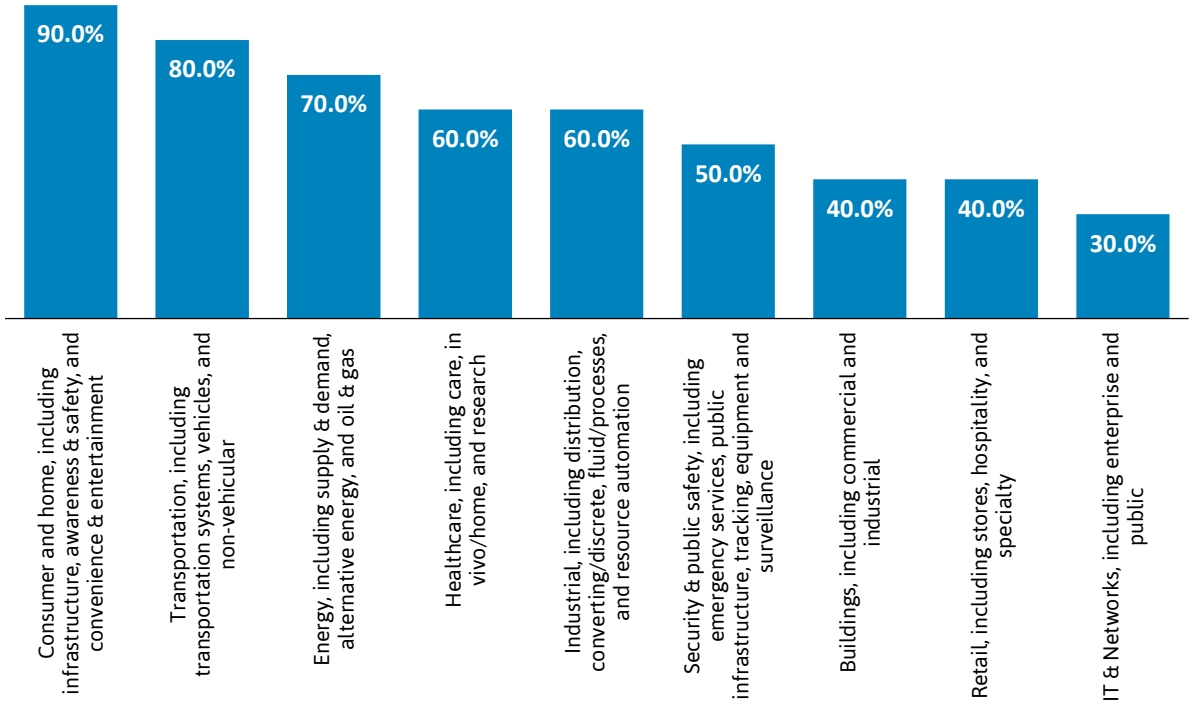
Which access technologies you consider more relevant to IoT?



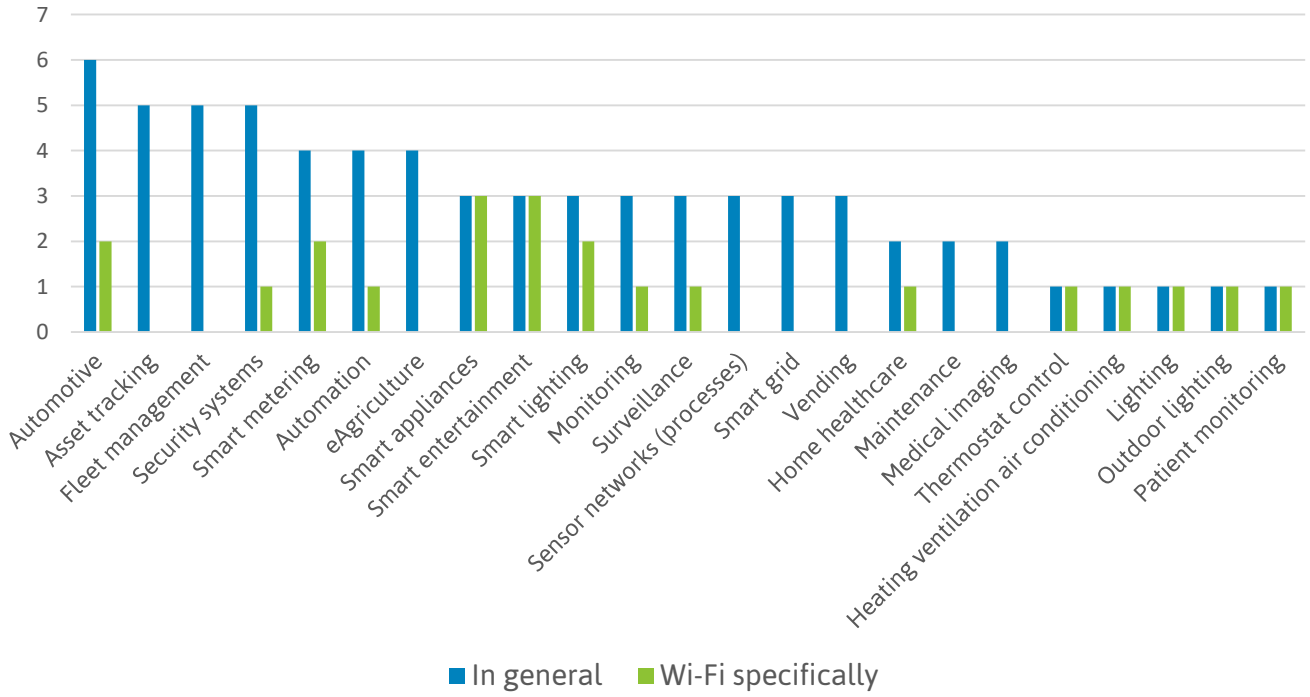
How relevant is roaming for IoT solutions ?



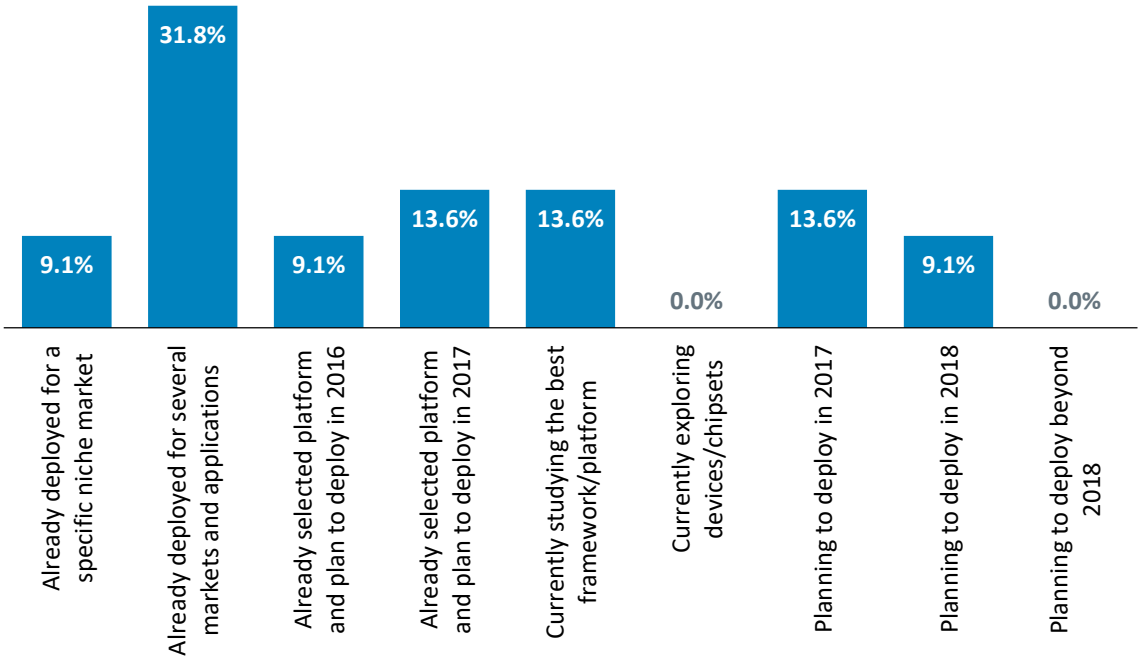
Which IoT market categories you consider more relevant?



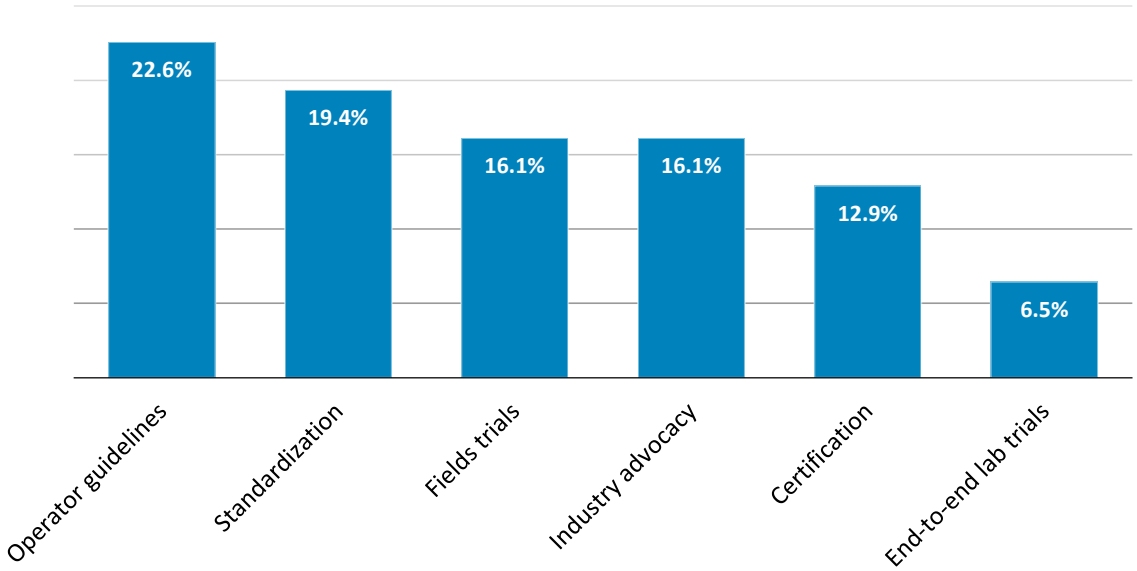
Please mark the application areas you consider more relevant to your company business?



What are your deployment plans regarding IoT?



What should be the major focus areas to make IoT grow exponentially?



EDITORIAL TEAM

COMPANY	NAME	ROLE
Boingo Wireless	**Brian Shields**	Project Leader & Editorial team member
Cisco	**Mark Grayson**	Project Co-Leader & Chief Editor
iPass	**Blaz Vavpetic**	Project Co-Leader & Editorial team member
Boingo Wireless	**Derek Peterson**	Editorial team member
BT	**Steve Dyett**	Editorial team member
China Telecom	**To Guojia**	Editorial team member
Intel	**Bahar Sadeghi**	Editorial team member
UL	**Mick Conley**	Editorial team member
WBA	**Bruno Tomas**	Editorial team member

PARTICIPANT LIST

COMPANY	NAME
Accuris Networks	**Eamonn O'Kane**
Accuris Networks	**Finbarr Coghlan**
Aruba Networks	**Peter Thornycroft**
AT&T	**Erinn Hall**
Boingo Wireless	**Derek Peterson**
Boingo Wireless	**Kishore Raja**
Boingo Wireless	**Brian Shields**
BT	**Steve Dyett**
Charter Communications	**Umamaheswar Kakinada**
China Telecom	**To Guojia**
Cisco	**Mark Grayson**
Fon	**David Valerdi**
Intel Corporation	**Necati Canpolat**
Intel Corporation	**Bahar Sadeghi**
iPass	**Blaz Vavpetic**
Liberty Global	**Stephen Kelly**
Nokia	**Max Riegel**
Orange	**Nigel Bird**
Rogers	**Edward O'Leary**
Smith Micro Inc.	**Dzung Tran**
Syniverse Technologies	**Dan Klaeren**
Tata Teleservices	**Srinivasa Rao**
UL	**Mick Conley**
WBA	**Tiago Rodrigues**
WBA	**Bruno Tomas**