# INTERNATIONAL INTERCONNECTION FORUM

# FOR SERVICES OVER IP

# (i3 FORUM)

(www.i3forum.org)

## Source:

## Working Group “Internet of Things”

## i3 forum keyword: IoT

# Internet of Things Whitepaper

# (Release 1.0) April 2017

The purpose of this document is to describe

- The IoT eco-system and the different players involved
- Carriers position and their customers in this eco-system
- Analyze the impact of IoT pertaining to carriers today and tomorrow (with a focus on the business potential)

This document does not intend to duplicate other existing specifications or documents related to the Internet of Things. It is to complement it with the perspective of the International Carrier members of i3 forum.

**EDITORIAL TEAM**

| COMPANY | NAME | ROLE |
|---|---|---|
| Telefónica Business Solutions | **Enrique Wong** | IoT WG Chair and Chief Editor |
| Deutsche Telekom ICSS | **Christian Wollner** | Editorial team member |
| Deutsche Telekom ICSS | **Markus Balasus** | Editorial team member |
| iBasis | **Paul Tommassen** | Editorial team member |
| Orange International Carrier | **Nick Sampson** | Editorial team member |
| Tata Communications | **Alan Tai** | Editorial team member |
| Telefónica Business Soluitons | **Alejandro Hernandez** | Editorial team member |
| Telefónica Business Solutions | **Juan de la Cruz Berlanga** | Editorial team member |
| Telenor Global Services | **Ola Korsmo** | Editorial team member |

## EXECUTIVE SUMMARY

The Internet of Things (IoT) is the use of connected devices and systems that delivers data gathered by embedded systems consisting of sensors and communication modules in machines and other objects like cars, containers, meters etc. IoT is expected to increase rapidly in numbers of devices over the coming years and we will see new services that improve the quality of life of consumers and productivity of enterprises. This is what the GSMA refers to as the 'Connected Life'.

For consumers, the IoT has the potential to deliver solutions that dramatically improve efficiency, security, health, education and many other aspects of daily life. For enterprises, IoT can help to improve decision-making and productivity in insurance, manufacturing, retail, agriculture and other sectors.

Machine to Machine (M2M) solutions - a subset of the IoT – already use wireless networks to connect devices to each other and the Internet, with minimal direct human intervention, to deliver services that meet the needs of a wide range of industries. In 2013, M2M connections reached the number of 195 million connections through multiple networks.

The IoT ecosystem is composed by:

- IoT Devices, which perform specific actions requested by IoT applications located in an IoT Platform or from smartphones and other kind of personal systems. Normally, the IoT Devices produces an event, which vary from a simple status update to sending a full motion video. These devices are smart objects and are composed of smart components such as SIMs, sensors, transponders, etc
- IoT Platform Providers. Devices are the end-edge that perform the final action such as collecting data like temperature, humidity, light and position activating/deactivating lights, heating and cooling systems, up/down the blinds, securing doors and etc,. These devices, however have to be managed and controlled by other instances such as personal devices (laptops, smart phones) and/or the Platform Providers.
- Connectivity Providers, are responsible for IoT devices that are connected and communicated with other end platforms such as data collection platforms, central metering systems, location tracking systems, logistic platforms, and etc,. The IoT Platform Providersalso enable communication between the IoT devices and applications in the personal devices (laptops, web, smartphones, etc).
- International Carriers, the IoT Platforms might not always be located in the same country as the IoT devices. International carriers plays an important roles to facilitate communication between them.

Today, international carriers are providing a set of services in the IoT ecosystem, most of them as an international connectivity services based on Capacity, MPLS, Internet Transit and IPX Transport, but also Voice and SMS are services that carriers provide.

Additionally, roaming services are also carriers services are providing today, as: roaming signalling (Sigtran and LTE Diameter), Data Roaming (GPRS, 3G and S8), Voice and SMS.

With the rapid growth of IoT ecosystem, and also the creation of new technologies and services in the market, international carriers can provide more than the existing connectivity and roaming services. These new international carrier services are based on the following areas: transport for IoT; hosting/data center services; local access - connectivity hub; data collection and analysis - big data; and finally security services. International carriers can explode their value in the IoT ecosystem based in these areas.

As the IoT technology gaining more and more space in the market, a set of problems appears by this uncontrollable growth. Some of those problems are presented in this whitepaper such as: signalling storm that affects the MNOs and carriers, undefined inter-carrier service level agreement, real-time communication, network redundancy and coverage, and business case.

**Table of Contents**

# 1. Scope and objective of the document

Several analysts have forecasted that in 2020 there will be approximately 26 Billion devices connected to the Internet. As part of its networks 2020 program, the GSMA is working to establish common capabilities among mobile operators to enable a network that supports value creation for all stakeholders. These capabilities include security, billing and charging and device management, all of which can enhance the Internet of Things by enabling the development of new services. Through the provision of these value added services, operators can move beyond connectivity and act as a trusted partner for their customers. Operator capabilities need to be tailored for the emergent M2M business model, building a trusted infrastructure that all stakeholders can rely on – and profit from.

The explosion of the number of connected objects might have impacts on carriers interconnections and roaming models both on the technical side and on the business side.

As a first analysis, the scope of this document is to:

- Give an overview of the IoT ecosystem and players: Customers (end-users and enterprises), Devices, Service Providers, Connectivity Providers and International Carriers.
- Analyze the impact of IoT to International Carriers for the existing services used as Data Roaming, Messaging, Signalling, etc, and new services that Carriers can develop in the Transport, Application and Security Layer.
- Give some examples of (potential) issues raised in the communication market due the explosion of IoT, and the impact on the players.

# 2. Symbols and Acronyms

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| E2E | End to End |
| ENUM | E.164 NUMber Mapping |
| ETSI | European Telecommunications Standards Institute |
| FNO | Fixed Network Operator |
| GPRS | General Packet Radio Service |
| GRX | GPRS Roaming eXchange |
| GSM | Global System for Mobile Communications |
| GSMA | GSM Association |
| IEEE | Institute of Electrical and Electronic Engineers |
| IETF | Internet Engineering Task Force |
| IMS | IP Multimedia Subsystem |
| IoT | Internet of Things |
| IoT-PP | Internet of Things Platform Provider |
| IPX | IP eXchange |
| IPX P | IPX Provider |
| ITU | International Telecommunications Union |
| LORA | LOng RAnge |
| LPWA | Low Power Wide Area |
| LTE | Long Term Evolution |
| M2M | Machine to Machine |
| MNO | Mobile Network Operator |
| NB | Narrowband |
| NB-IoT | NarrowBand for Internet of Things |
| NGN | Next Generation Network |
| OneM2M | International organization for standardization of M2M |
| OTT | Over The TOP |
| PSTN | Public switched Telephone Network |
| SMS | Short Message System |
| SP | Service Provider |
| SS7 | Signalling System 7 |

# 3. References

[1] The Internet of Things presents new signalling concerns for mobile operators, as the number of devices and subscribers needing to join the network escalate, by Robin Kent. Connect World 2015.

[2] Mobile networks prep for the Internet of Things, by Stephen Lawson, Computerworld February 2015

[3] Security Takes Center Stage, by Richard Borge, Computerworld 2015.

[4] GSMA, IoT Device Connection Efficiency Guidelines, Version 1.1, 30 January 2015

[5] ETSI, Workshop M2M, Standardized Service Layering for IoT in oneM2M, December 2015

[6] OVUM. The IoT Landscape. Defining and dimensioning the Internet of Things for the telecoms industry by Jamie Moss. 14 Aug 2015

[7] Hot Telecom and Xona Partners. International Carriers' path to the IoT Gold Mine, 1 October 2015

[8] What is IPX's role in the IoT ecosystem, by Christian Wollner, IPX Summit 2016

# 4. Ecosystem

The Internet of Things (IoT) refers to the use of intelligently connected devices and systems through wired or wireless communications to leverage data gathered by embedded sensors and actuators in machines and other physical objects, allowing the human being to do things more efficiently. This is based on the GSMA Connected Living Program definition. The IoT allows organizers to work more efficiently, it automates manual task, monitors instances, collects data, and generates reports.

Different analysts predict more than 26 billion of new devices, e.g. the GSMA Connected Living Program and Gartner, communicating with each other independently of human interaction by 2020.

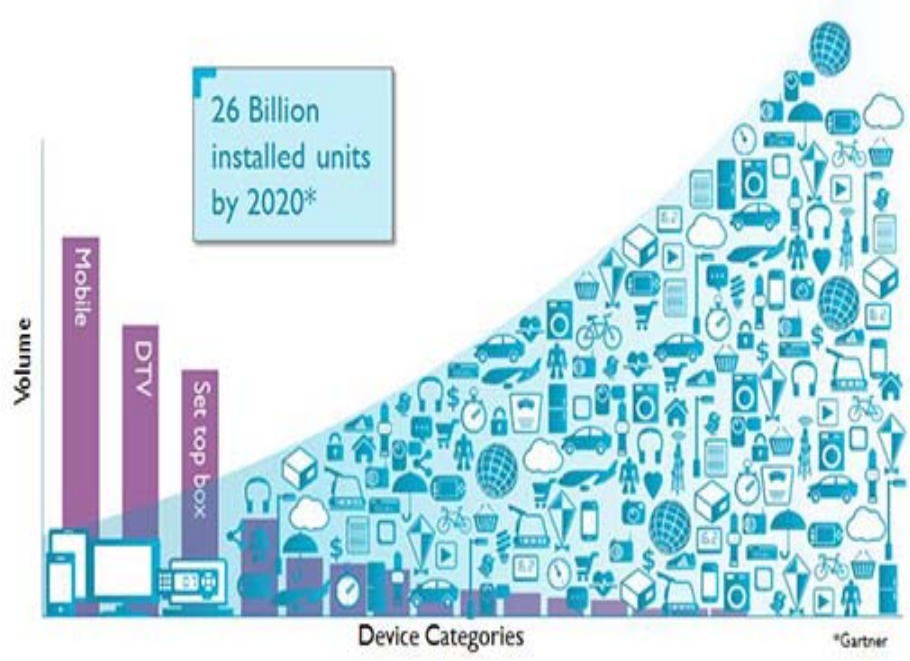


**Figure 1. Evolution of IoT Devices by Gartner.**

A high number of devices are indicating new revenue opportunities for the whole value chain starting from device manufactures, connectivity providers, ISPs, carriers, platform providers and unimaginable new business opportunities.

In telecommunication environment, the business models have been well established for E2E Open Access standards, enabling more than 6 billion “telephony devices” to interact and interoperate among each other via 2G, 3G, and 4G. However, the IoT ecosystem is still to be determined.

From marketing point of view, the IoT market is already categorized and grouped into different segments or verticals. This categorization has also led to different technologies trying to achieve the same solutions.

From technology point of view, different verticals could be served by one technology solution but in fact the solutions have become quite fragmented, and thus prevent economy of scales of IoT devices.

Even though there are already global standards for various different access technologies and protocols in the market, which can be used for IoT, but most IoT solutions are still lacking in following a standardized end-to-end approach like telephony according to 3GPP.

Some initiatives have been kicked off in the past. Those initiatives primarily start of the so called home domain, e.g the AllSeen Alliance (https://allseenalliance.org) or the Interconnect Consortium (http://openinterconnect.org/). However, from technological point of view the most comprehensive set of functions and elements for a standardized and interoperable ecosystem, addressing the technological need of various verticals is the global partnership program formed by oneM2M.

OneM2M can be understood as the organization enabling for IoT, what 3GPP has enabled for Mobile wireless IP broadband access systems and telephony.

OneM2M is also building the bridge between various already existing devices families or industry standards and is thus increasing the number of interoperable devices for the IoT market.

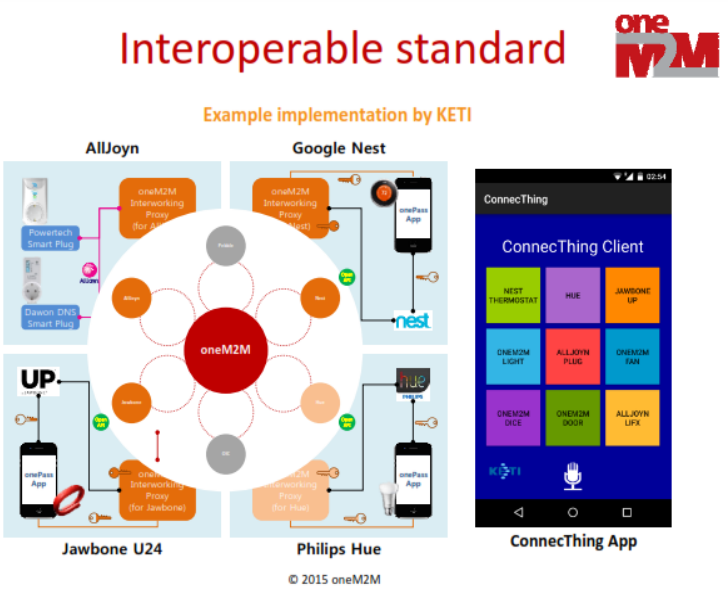


**Figure 2. Example implementation of interoperable devices following different existing "standards" respectively product families**

Thus, oneM2M is a good candidate to building up the economy of scale for the IoT market, like 3GPP did for telecommunications and mobile broadband.

IoT ecosystem can be viewed differently depending on the industry. This document does not pretend to give a broad description and analysis for all industries, so it will be simplified in four players: Devices, IoT Platforms Providers, Connectivity Providers (Fix, Wifi, Cellular, LORA, NBIoT, LPWA), and International Carriers, and especially in the International Carriers role for the IoT ecosystem.

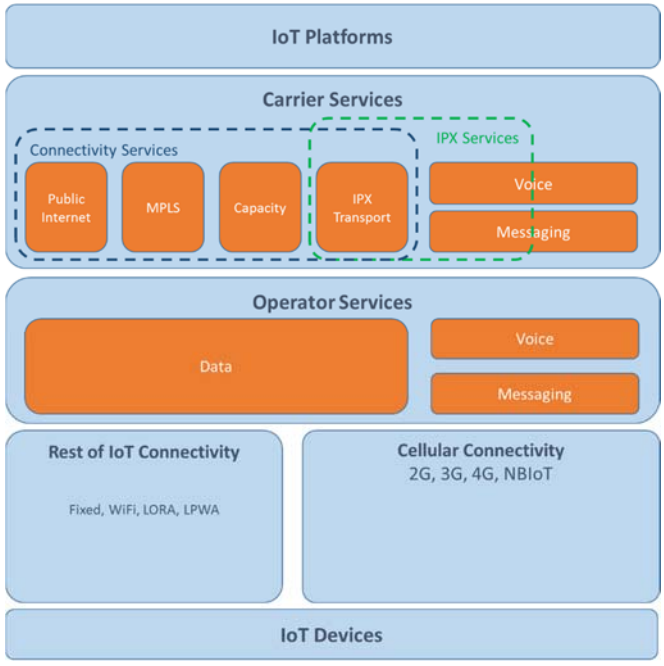


**Figure 3. Carrier services in the IoT ecosystem**

## 4.1. Devices

IoT devices may be found across application domains, such as smart farming, automotive, smart city, smart home, assisted living, future manufacturing and smart wearables.

The IoT device does specific actions requested by IoT applications located in an IoT Platform or from smartphones and other kind of personal systems. Normally, the IoT Devices produces an event, which vary from a simple status update to sending a full motion video. These devices are smart objects and are composed of smart components as SIMs, sensors, transponders, etc.

The wide range of use cases for these applications results in a rich set of requirements for the smart objects.

Some object will remain fixed in place for much of their focus on the international IoT value chain, however, all smart objects are assumed to be mobile at some point in time and will require to be assessed wherever they are. Additionally, the data the IoT devices generate will need to be transported back to the data centers – in case of international IP interconnections, this will happen via carrier borders – where it will be stored and analyzed.

Some examples of IoT devices are:

- Consumer and Home: wireless printers, smart TVs, etc.
- Smart Infrastructure: home appliances, heater control, door and windows control, etc.
- Security and surveillance: video security systems, presences, etc.
- Healthcare: blood pressure measurements, heart monitor, etc
- Transportation: positioning and tracking, traffic monitor, etc
- Retail: inventory management, payments systems, traffic flow, etc.
- Industrial: remote monitoring and control, process control, etc.
- Others: climate information, Agriculture Appliance, etc.

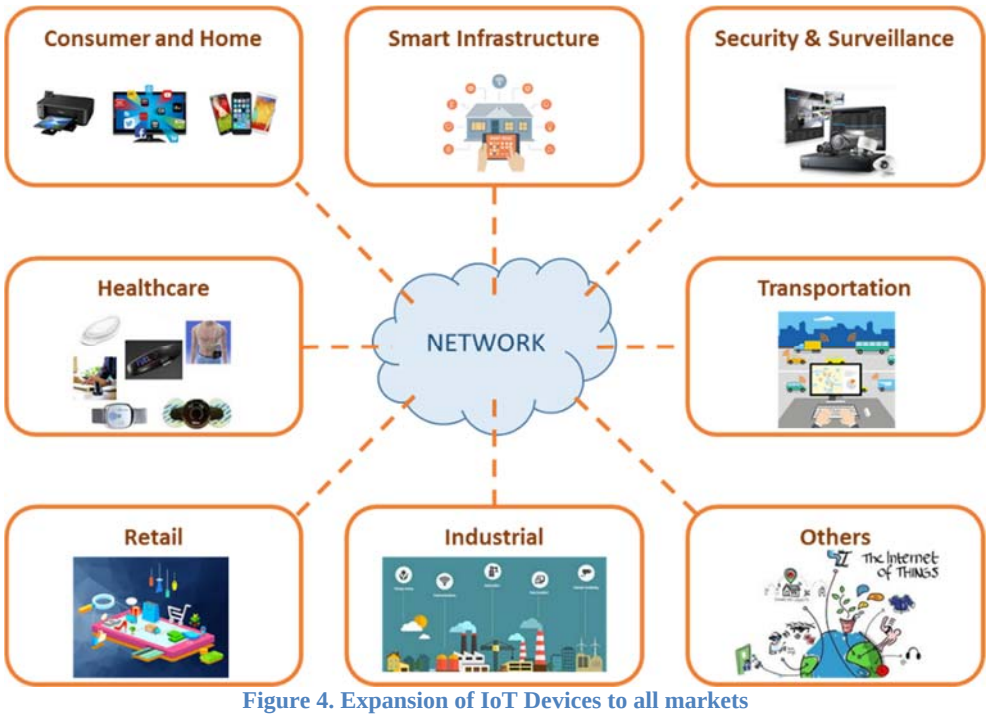


Figure 4. Expansion of IoT Devices to all markets

## 4.2. Platform Providers

The IoT devices are at the edge that perform actions such as collecting data, activate/deactivate certain functions. The types of data collected could be but not limited to, temperature, humidity, brightness location, heart rate, transactions, household appliances, etc. Examples of actions that could be

activated/deactivate but not limited to are lights, heating/cooling systems, up/down the blinds, and door locks. These devices are managed and controlled by other instances that could be the personal devices (laptops, web, smartphones, etc) or the Platform Providers.

The IoT Platform Providers (IoT-PP) are centralized platforms that manage the IoT Devices for the enterprise market, and also allow users to control and manage IoT devices from their personal devices in the consumer market.

Platforms (and its applications) are developed by specialized IoT vendors and sold or licensed to enterprises and to connectivity providers that wanted to create their own IoT business. These Platforms can be unique for a specific function or broader to support multiple functions such as:

- Connectivity management providing intelligent connectivity features such as enterprise self-service, data encryption, compression, and etc.
- Device management that provides interaction with end-edge to perform real-time actions such as self-diagnostics, software update, service provisioning, and etc.
- Application management platforms providing a set of development tools, libraries and a set of functions and software that allows the communications and management of IoT devices.
- Application-specific management dedicated to a certain task, and it is emerging to the IoT ecosystem a set of specific functions that evolves from traditional analytics to Big Data platforms.

The platform is an important part of the IoT equation, because it is the source to generate new value-added revenues for vendors and carriers, and it is an open arena that everybody can play. Platform interacts with the IoT devices collecting data, generating specific actions and improving processes and reducing costs in enterprises or allowing enterprises to create new products and services for customers.

## 4.3. Connectivity Providers

Connectivity Providers are responsible for IoT devices that are connected and communicated with the other end of the data collection platforms such as central metering system, location tracking systems, logistic platforms, and etc. The IoT platform providers, can also enable communication between the IoT devices and the applications thru personal devices (laptops, web, smartphones, etc).

The Connectivity Providers can be Fixed, Cellular, WiFi, LORA, LPWA, NB IoT, Satellite, or proprietary/alternative radio networks built with access and core network equipment to supply a data transport, Voice and SMS services for IoT applications allowing the connection between IoT Devices and IoT Platform Providers.

The connectivity layer is fundamental in the IoT ecosystem, and it is a collection of protocols supporting the rollout of hardware, software, and IoT services. It is composed mainly by WiFi connectivity provided by or based on DSL, cable and WiFi Networks or other non-cellular providers, and in a smaller extend, cellular connectivity. Thanks to the vast installed base of Wi-Fi –and Bluetooth-enabled consumer electronics- devices guarantees their future relevance to the IoT, but new proprietary local area bearers are emerging as ZigBee and Z-wave, and proprietary wide area bearers like Weightless, SIGFOX, and LORA.

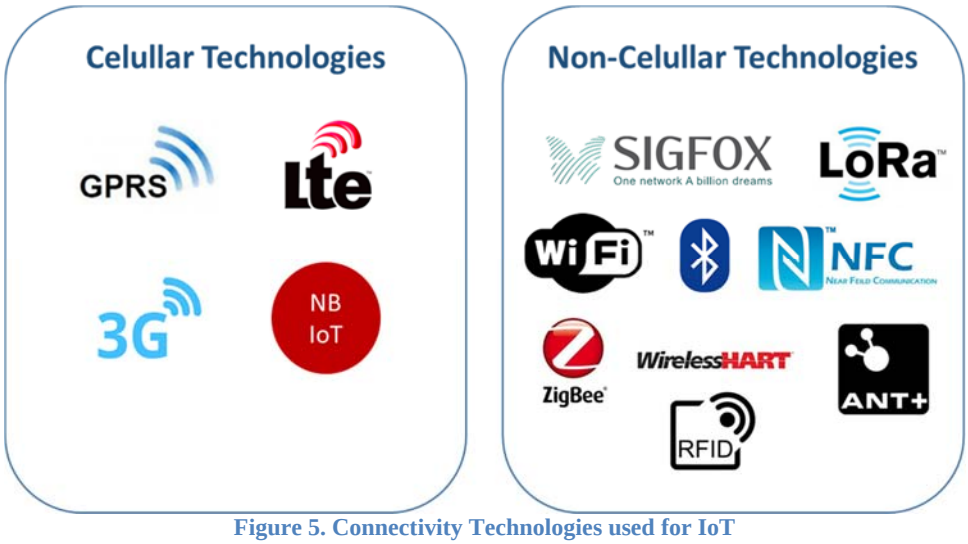


Figure 5. Connectivity Technologies used for IoT

| Technology | Usage |
|---|---|
| Wi-Fi | 72% |
| Fixed (PSTN, ISDN, Cable, DSL, Fibre) | 15% |
| 2G, 3G, 4G | 12% |
| LPWA (SIGFOX, LoRa, NB-IoT) | <1% |
| Satellite | <1% |

Table 1. Distribution of technologies used for IoT [Berg Insight]

If the provision of IoT devices grows as expected, the traffic generated will represent a significant part of the total data traffic, and could trigger a fight for network resources. A separated connectivity network only for IoT devices is something that does not sound feasible.

Although the 5G specification has not been finalized yet, e.g. 3GPP Rel. 15 is planned to be ready by mid-2018 and Rel. 16 by end of 2019, 5G promises a.o. increased data rates, reduced latency and improved coverage. This opens the door for several (new) IoT applications, e.g. automotive (self-driving cars) and interactive mobile games. Also the concept of smart cities will take advantage of 5G as an unified framework for seamless connections, over a mixture of several technologies (e.g. cellular, plus Bluetooth, UWB, RFID, etc.). Currently first field trials with 5G are taking place and commercial deployment is expected by 2020. With that a massive volume of data can and will be generated which need to be analyzed and often react upon quickly. 5G, IoT and Big Data Analysis go ‘hand in hand’.

## 4.4. International Carriers

We have described the importance of the devices, connectivity providers and platform providers in the IoT ecosystem, and how they interact with each other, but another important player that is not always mentioned are the international carriers.

When we said that devices interact with platform providers using data transport layer of connectivity providers, we have not mentioned that platform providers are not necessarily located locally in each country.

For global IoT services, the platform provider are typically located centralized locations, or in the Cloud based redundant data centers located in different countries to provide global services more efficiently.

The global connectivity from the centralized locations of the platform providers to the connectivity providers are supported by international carriers.


**Figure 6. i3forum members in 2016**

Deeper analysis of international carrier role will be cover in the next chapter.

# 5. Carrier Services

International Carriers are always in the game, and all the time are gaining more relevance with the evolution of the technology.

International Carriers provides Internet access to Connectivity Providers, Data Centers for the Service Providers, etc., but do not necessarily provide a IoT service. Basically, they provide an International Transport Service, based on Internet Transit, MPLS or International Connectivity with QoS and Security like IPX.

The IoT ecosystem open new business opportunities, in the consumer and enterprise market and also in the International Carrier market. New business based on new services or existing services that enlarge their business in the IoT ecosystem, provide more value than the Transport layer such as services in the Application Layer, in the Data Analytics layer or in the Security Layer

Providing services to enterprises of all types and complexity is also one of the key opportunities. International Carriers can leverage their existing relationships and local presence to provide a multinational service platform offering a number of applications in the industrial and commercial sectors.

## 5.1. IPX

The IPX is a technical network architecture and an ecosystem model elaborated by the GSMA to allow mobile operators, and to any Service Provider, to interconnect their IP services in a secure and guaranteed quality environment.

Typical services provided by Carriers over the IPX are: Data Roaming, VoIPX, Roaming Signalling (Sigtran and LTE Diameter) and Transport, but the market and the services are still growing and new services will come up.

The current role of IPX in the IoT ecosystem consist of providing a set of services to allow communication and interaction between IoT Platforms and IoT Devices, especially the following services:

- IPX Transport to provide connectivity between IoT Platforms Providers and Enterprises as part of a Carrier service.
- Voice and Messaging over IPX that allows specific interaction between the IoT Device and the IoT Platforms, and also to provide specific information to persons.
- When the IoT Device is in roaming scenario, a set of mobile services are used and most of them are based on an IPX service (Data Roaming, SMS, Roaming Signalling, etc).

## 5.2. Existing Carrier Services.

A set of services are currently provided by the Carriers, for both Non-Roaming scenarios and Roaming scenarios.

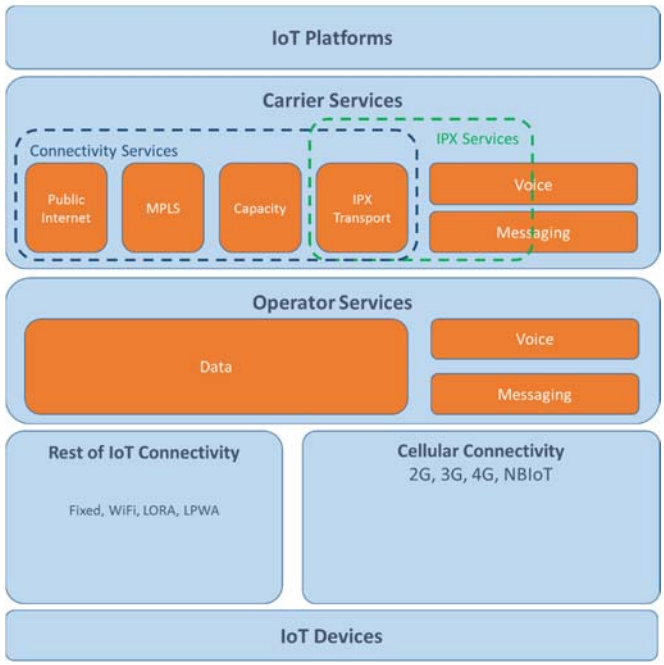


Figure 7. Existing Carrier services used for IoT communications

### 5.2.1. Connectivity Services (Capacity, MPLS, Public Internet and IPX Transport)

The carrier services required by player in the IoT ecosystem is a connectivity service, and this connectivity can be provided by Internet Transit, IPX Transport, MPLS and Capacity, where the two services are not commonly used.

Choosing one connectivity service from the other is a matter of preference, security, technical requirements and cost, but basically all of them provide the connectivity that the IoT Platforms and Enterprises and IoT Devices requires.

The most common usage are:

- MPLS and Capacity: Used to provide secure and private connectivity between the IoT Platform and different locations of an Enterprise, where the IoT Devices are located in remote locations as offices, factories, etc.
- IPX: It is commonly used to provide connectivity between the IoT Platform and the MNO, even when the MNO is contracting it as PaaS (Platform as a Service) or it is located in a Data Center, but also it is used to provide connectivity between the IoT Devices and the IoT Platform through the MNOs.
- Internet Transit: It is considered the most common service used to connect IoT Platforms, IoT Devices, MNOs and Enterprises, because it is accessible by all players and the most economical service, but with no quality assurance and high security risk.

### 5.2.2. Voice

Voice services in the IoT Ecosystems are commonly used to perform calls to centralized call centers (i.e. Vehicle Customer Support) and to perform Emergency calls when an accident occurs automatically, in the Non-Roaming scenario and the Roaming scenario, and in both cases the call is handled in the same way by the International Carriers as any normal call.

Carriers provide International Voice services with global coverage in the standard way, with no specific treatment for voice calls performed by IoT Devices.

### 5.2.3. SMS

SMS messaging was one of the first services used by IoT devices in the very early stage even when M2M and IoT acronyms were not created.

Although this technology is seen as an older technology, is worth recalling some of the advantages compared to other channels. Short messages can be received on any device, does not require Internet connection and it's the only universal direct way to send information that is placed directly in the recipients pocket in the blink of an eye.

While users are overwhelmed by the number of applications needed in their day life, SMS is simple, and doesn't require learning curves or data plan or WiFi connection to transmit information to an IoT device. These benefits makes SMS messaging useful for any IoT solution.

SMS works with no differentiation between Non-Romaing and Roaming scenario, very similar to Voice Services. Probably the only different is the connectivity between SMSCs of the MNOs, that very often are on Roaming Signalling services, and this over IPX.

### 5.2.4. Roaming scenarios

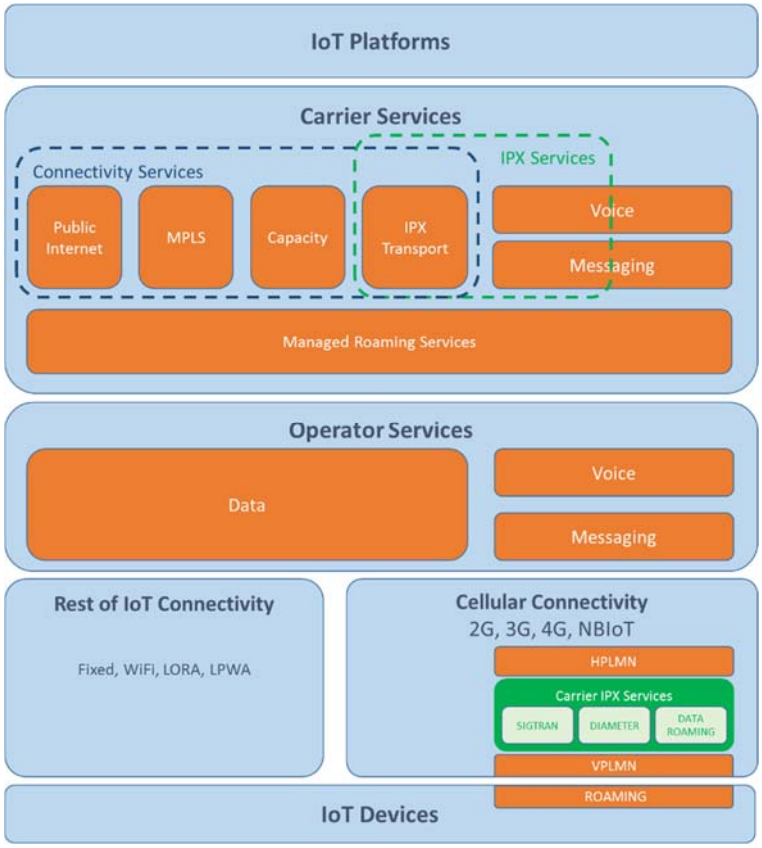


Figure 8. Carrier services in roaming scenarios.

The regular cellular IoT use case consists of a device using the cellular network that owns its IMSI. However, there is also the international roaming case. This means that the IoT device uses a "visited network" (VPLMN) that is different from the network that owns its IMSI (HPLMN). This IoT roaming case has increasing significance in overall roaming (Machina Research mentioned 7% of roaming connections coming from IoT in 2015 with a yearly growth rate of 100%).

The following IoT use cases can lead to international roaming:

1. **Mobility roaming:** When a person travels abroad they can conveniently continue to use mobile services. The same applies to a connected car. When it crosses the border it remains connected.

2. **Permanent roaming:** "permanent roaming" as well plays a significant role in IoT. Some objects equipped with a SIM never see their home country - they remain in a permanent roaming context. There are two main reasons for this:
   a) Global production: It is convenient for manufacturers in their production process to use one home country for their SIMs globally, regardless of the country the product is eventually shipped to. This is comparable to the user manual that contains many languages so that the product, along with its manual, can address an entire region or continent.
   b) Best coverage: In the standard non-roaming scenario, only the network of the original (home) MNO is available. In the typical roaming scenario however, more than one visited network is available. The driver of a connected car equipped with permanent roaming has a vital advantage when he has a serious accident. If this happens in the middle of nowhere, the car could lose network coverage when rolling into a ditch. In the roaming scenario, the SIM will switch to the 2nd or even 3rd operator in the list of preferred networks. The car would still be connected and could place an emergency call.

These scenarios are commercially covered by the existing roaming contracts between MNO's. Also on the technical side MNO's are simply extending the use of existing platforms that were initially conceived for "human" roaming. As such IPX has also become the predominant platform for international IoT roaming as a secure QoS platform providing interconnectivity hub services such as Roaming Signalling and Data Roaming Exchange.

Both Signalling for Roaming and the actual data roaming traffic are being transported between VPLMN and HPLMN via IPX.

#### 5.2.4.1. Roaming Signalling (Sigtran and LTE Diameter)

Sigtran (or in some cases even still TDM-based SS7) signalling is generated in all 2G and 3G IoT roaming scenarios. The same goes for 4G roaming with Diameter Signalling.

Already today IoT generates significant signalling traffic for carriers as all SIM-based IoT connectivity sends at least location updates on a regular basis. This applies even to use cases that generate hardly any data traffic such as, for example, a smoke detector. Its connectivity could be limited to merely stating once per day that it is still active. This generates very little data traffic. As the device remains connected to the network it still sends regular location updates via signalling.

This additional traffic is certainly a good thing for the carrier. MNO's in their role as VPLMN however fear a signalling storm coming from IoT devices that o hardly generate any wholesale revenues (PSD) as their data roaming traffic is almost negligible (cf. Chapter 6.1).

#### 5.2.4.2. Data Roaming (GPRS, 3G and S8)

The standard roaming scenario today includes the home routing of the data traffic. This applies equally to human and to IoT traffic. The different IoT use cases vary tremendously in terms of data volumes (that is to be home-routed if in roaming). The afore mentioned smoke detector example can be found at the lower of the scale, whereas all applications involving video content can be typically found at the higher end of the scale.

#### 5.2.4.3. Voice and SMS

International voice services in roaming scenario does not differ of non-roaming scenarios, enabling IoT Devices to make a voice call to a specific destination as mentioned in the chapter 5.2.2.

Regarding SMS in roaming scenarios, the behavior of the IoT Devices are just as in "human" roaming, SMS are home-routed via the signalling channel. As such they increase the signalling traffic volumes. Once home-routed, the general case described in chapter 5.2.3 is applicable

#### 5.2.4.4. Managed Roaming Services

International Carriers have been creating services to satisfy the roaming needs of MNOs, as Roaming Signalling, IPX Data Roaming Transport, etc, and even creating a Roaming Hub service that include the previous services, Data Clearing House and Dual IMSI, that simplify the process to stablish roaming agreements and activations, and speeding-up the roaming coverage of the MNOs.

All those services are called Managed Roaming Services, and that is the bases where Carriers create M2M Services with the deployment of M2M Platform and agreements with MNOs to get IoT SIMs and special prices for IoT traffic.

#### 5.2.4.5. Rest of IoT connectivity

Cellular-based IoT (incl. NB-IoT) can just use the existing (commercial and technical) roaming infrastructure including carrier services. This is less the case for alternative bearers. Low power wide area networks (LPWAN) based on LoRa technology for example are typically not connected to IPX. They also do not use Sigtran or Diameter Signaling in a way cellular networks do. In Wi-Fi roaming certainly has a long-standing history. But “seamless” roaming between cellular and Wi-Fi is still clumsy. Signaling used in Wi-Fi is traditionally RADIUS-based and the home routing of PSD traffic via an IPX-based is applied not generally. Also commercially most Wi-Fi roaming agreements still use time-based (rather than volume-based) inter operator tariffs.

All of these points are challenges to roaming between networks of different technologies. They explain why ubiquitous roaming is today only available between cellular networks. They would have to be overcome to make roaming between networks of different bearers possible.

## 5.3. New Carrier Services.

In ‘International Carriers’ path to the IoT Gold Mine’ [7] the possible role of the carriers in the evolving IoT landscape is investigated. Five levels of involvement are defined:

- Transport Level
- Hosting Level
- Local Access Level
- Data Collection and Analysis Level
- Security.

The following sections are based on information from the white paper.

### 5.3.1. Transport Level

Many of the international Carriers have already built an IPX network, which could be perfectly used to offer transport of IoT related data because it is a secure network with QoS and SLAs, although the SLAs are not dedicated to IoT type of services (see also Section 6.2 of this document). From a pure transport point of view, carriers are ready to support international customers (MNOs, enterprises) who deliver IoT services, but by offering only transport there is not much gain to be expected for the carrier.

### 5.3.2. Hosting Level - Data Center services

Some International Carriers are exclusively focusing on the transport level as described in the previous section. Ofering Data Center services (e.g. global cloud hosting) can provide a new business opportunity in the IoT space for them, either creating their own service or offering these services in partnership with an existing Data Center provider.

For other carriers, who already offer Data Center services, there is not much that will change because of the introduction of international IoT services, apart from their potential customer base will increase.

### 5.3.3. Local Access Level - Connectivity Hub

Many IoT applications should also work across international borders. For IoT Service Providers it could be a problem to acquire local access in other countries than their home country. Eventually, in combination with the transport service and the data center services, the international carrier could offer a one-stop-shop concept by also offering local access abroad. This could be achieved when the carrier partners with local access providers (MNOs), buys and resells SIMs dedicated to IoT or even launches (data-) MVNOs in countries where necessary.

Carriers providing Signalling and Data Roaming Services or a Roaming Hubbing Service, could also, based on these services, create a sub-service for IoT.

In addition, a Data Clearing Service could be added to offer a full package to the IoT Service Provider.

### 5.3.4. Data collection and analysis Level - Big Data

Even if the carrier only offers a service at the transport level to the IoT Service Provider, since a lot of data is passing through its network, the carrier could collect specific data and do some analytics e.g. to sell/provide patterns and behavior of usage or mobility of the end-users to the IoT Service Provider.
Ultimately, the Carrier could even help the Service Provider to analyze the data collected via the IoT Service in the Data Center e.g. by providing capabilities (e.g. SaaS) from which the Service Provider could benefit.

It is noted here that some problems may arise here regarding privacy of the end-user and permission to use the information might be required.

### 5.3.5. Security

No matter on which of the above levels a Carrier is involved in delivering IoT services, security is key for the whole service provision. When the IPX is used for the transport level, security is already provided, because it is part of all IPX based services.
In case the Carrier also provides Data Center Services, Protection against DDoS attacks becomes important, because the Carrier has to provide secure access for the IoT Service Provider to the hosted platforms.

This DDoS protection is normally part of Data Center services anyhow, and because Data Centers are secured and protected environments, this could be a benefit of using a Data Center instead of locating a Platform in the IoT Service Providers' premise.

In case of the Local Access Level, other security aspects come into the picture e.g. handling of Security Keys of SIMs. And in case of the data collection and analytics level the security and privacy of end user information becomes very important.

Only a few security aspects are mentioned here, but clearly, the Carriers need a complete security framework to cope with all possible security threats related to these services.

# 6. Problems detected

This new technological wave, where everything can be connected and communicating between themselves or to a central service platform, is affecting the current networks and services that are not prepared for this boom.

The impact of more things connected, and the way they are connected and are exchanging information, is generating some problems not expected initially and now the players have to find a solution to address it, from the technical and/or business perspective.

## 6.1. Signalling Storm

### 6.1.1. Problem

The predicted large scale growth of IoT Devices and their associated IoT Device Applications will create major challenges for Mobile Network Operators. One major challenge that Mobile Network Operators must overcome is the risk caused by the mass deployment of inefficient, insecure or defective IoT Devices on the Mobile Network Operators' networks.

When deployed on a mass scale such devices can cause network signalling traffic to increase exponentially which can impact network services for all users of the mobile network. In the worst cases the mass deployment of such IoT Devices can disable a mobile network completely.

This situation also affects the Carrier services provided to an MNO, specifically the Roaming Signalling services, which are designed and implemented based on end-user roamers with average behavior, not on intensive usage by the IoT Devices

#### 6.1.1.1. Technical

A simplified view of a common method for communication between devices and service platform isshown below:

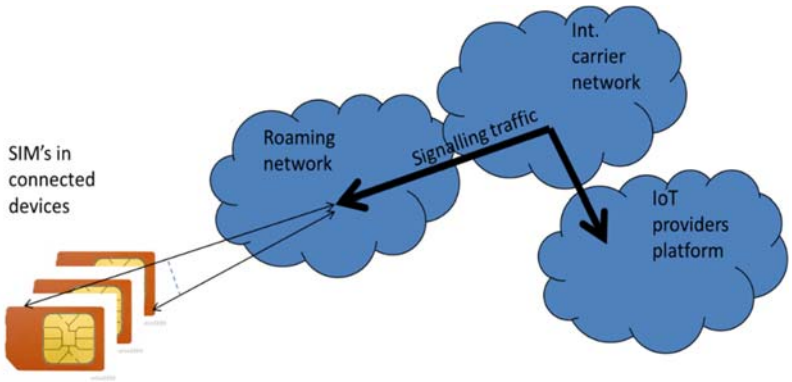


Figure 9. Signalling storm problem.

To ensure that devices always are connected, the IoT service provider often chooses to use SIMs that are roaming. That way, the SIMs will have better connectivity if they are moving. But the downside is that the service provider will not always be able to predict which mobile network the SIMs will be connected to.

An IoT Device overusing the network may lead to problems such as:

- Reducing the lifetime of the (U)SIM card by increasing dramatically the read/write cycles.
- Increased power consumption of the device due to continuous restarts which may also affect the device lifetime.
- Local issues within the Mobile Network Operator's network such as cell congestion.
- Capacity and performance problems within the Mobile Network Operator's core network, such as signalling storms, which result in wide area network disruption.

- Negatively impacting the IoT Service's performance, potentially resulting in delayed communications, degradation of the service quality and even service outages.

IoT Devices overusing the mobile network can affect not only the devices causing the incident but also other devices on the same IoT Service Platform or those devices of other end customers.

### 6.1.2. Players involved

The communication chain consists of the IoT device itself, with its hardware and software, which is the responsibility of the IoT service provider. At the other end of the chain is the IoT central platform with its associated application software and hardware, which is also the responsibility of the service provider.

The communication path between the devices and the central platform may consist of several mobile operators and telecommunication carriers, depending on the distance and the way the service is configured. Normally there is the roaming operator in the country where the IoT devices are located and a national operator in the country where the service platform is located. Then there might be one or more international carriers in between.

All those players might be affected if a signalling storm occurs.

The storm effects can also apply to the device authentication processes, for sample in a Radius network. This critical point must be also assured in order to guarantee the attaching of the IoT devices into the network.

### 6.1.3. Possible Solutions

#### 6.1.3.1. Service provider.

In IoT scenarios, IoT Device firmware and software play a significant part in determining the overall performance and behavior of the IoT Service on the mobile network. With no human intervention to fall back upon, the mechanisms that manage recovery from IoT Service failure need to be built into IoT Devices.

Good design is essential to ensure that IoT Device performance is optimized and to prevent failure mechanisms creating runaway situations which may result in network overload. In situations where many IoT Devices of the same type may be deployed on a single mobile network, the cumulative effect may have a detrimental impact on overall network performance. Poor design of IoT Device Application to IoT Service Platform communications, which disregard the mobile network and IoT Device status, may result in inefficient use of network and device resources, affecting the IoT Service experience end-to-end.

IoT Device Applications should be designed to ensure that network activity is not concentrated at specific times and is tolerant of geographical loading problems. Especially reboot of devices can be critical and it is important that not all devices try to boot at the same time.

#### 6.1.3.2. Mobile operator.

Network signalling resources are dimensioned assuming an overall device usage profile with a sensible balance between traffic and signalling needs. This is not always the case with IoT devices and operators should monitor their traffic to get a good picture of the traffic and signalling trend in their network.

Controlling the capacity of the network access links used to connect the IoT Platform with the roaming network in real time can also help to prevent congestion. Alarm system can warn if a peak in the capacity is happening because a signalling storm, being key in critical situations to react.

Key network components should have sufficient capacity to handle the traffic imposed on them, even when abnormal situations arise, like the increased reconnections after a network downtime, or an increased number of roamers, for example when another mobile network in the same country is down and end user devices try to move to your network.

Steering mechanism also should be considered in order to avoid the connectivity of the device to a network where a capacity incident is happening. Redirecting the traffic to a working operator through network steering or directly through the IoT device configuration can also help with the problems of lack of capacity during a signalling storm or other network incidents, as a workaround until the normalization of network of the main operator.

Long term, the network operators should also look at how Diameter could be improved, and particularly the underlying transport protocol, SCTP, to handle the number of connected devices, whether it be smartphones, tablets or IoT enabled devices.

Short term, mobile operators need to scale up their networks in line with the growing number of connected devices. This also includes the redundant links, which must always exist and have enough capacity to support a peak of traffic if one is lost.

The possibility of using additional channels different to the data ones in order to avoid network issues can be also evaluated for some scenarios during the solution design. A sample of this can be the SMS or voice channels. SMS is frequently used as 'wake-up' system for devices in order to avoid battery wastage. Using voice channel or SMS also as a redundant data channel to avoid problems in the network can also help with critical applications which request redundancy and low data volume to transmit the information.

#### 6.1.3.3. Cooperation between mobile operators and IoT service providers.

It is desirable that mobile operators and IoT service providers cooperate when new IoT services are being deployed with mobile networks as the communication vehicle, and when large numbers of new devices are being deployed in a mobile network. The areas of cooperation could be: planning of service rollout, testing, device rollout forecast and fallback scenarios. It should also be noted that GSMA has released a document "IoT Device Connection Efficiency Guidelines which describe a number of guidelines and 3GPP features to protect mobile networks in two principle situations:

1. When an IoT Service (associated many IoT Devices) causes a large number of IoT Devices to communicate over a mobile network at the same time; and/or
2. When many IoT Devices are roamers and their serving network fails, then they all attempt move onto a local competing network, and potentially overload this network.

It should be noted that both the IoT Device and the Mobile Network must implement these features for them to be of benefit to the IoT Service Provider and Mobile Network Operator.

Typically an IoT solution involves several kinds of technologies and network frames. This means that in order to provide a solution when an issue jeopardizes the network capacity a quick diagnosis and notification to the proper responsible network team is requested. The root cause of the capacity problem must be involved in the IoT devices, the IoT Platform and its internal network or in the roaming framework between the devices and the Platform.

Processes and communication models which support fast detection of the problem location and how to properly manage the incident information is key to getting a solution, especially for critical services as e-health or vehicles. Avoiding too many steps in the communication flow can also help to expedite the solution.

#### 6.1.3.4. Device Certification before deployment.

Another solution is the creation of a device certification program to ensure that the devices that are going to be deployed don´t have an aggressive behavior with the signalling network
Currently, the tests that must be performed are being standardized in the GSMA working group IoT Device Connection Efficiency Guidelines.

## 6.2. Inter-Carrier Service Level Agreement for M2M Service

For global deals, operators use global SIMs working in permanent roaming in those countries where is not forbidden.

Continuous connectivity is needed for some IoT uses so it is very important to ensure that connectivity is not lost in these cases.

The global using of IoT devices through many countries is frequent and necessary for many services such as fleet control, wearables devices or vehicles. Due to their nature, these devices are often in international roaming scenarios.

### 6.2.1. Problem

The main problem is that there are no SLAs included in the interconnection agreement between the different GRX providers, nor in the roaming agreement between different roaming partners.

So when there is a connectivity incident that is caused by a GRX incident, there is no commitment to resolve it. So:

- Customers cannot have a target date to resolve the incident
- It takes a long time to get first feedback about the incident.

In the case of critical services like eCall for vehicles, e-health for patients or industrial environments this is a serious threat.

#### 6.2.1.1. Technical

The above problem is explained in the following figure it:

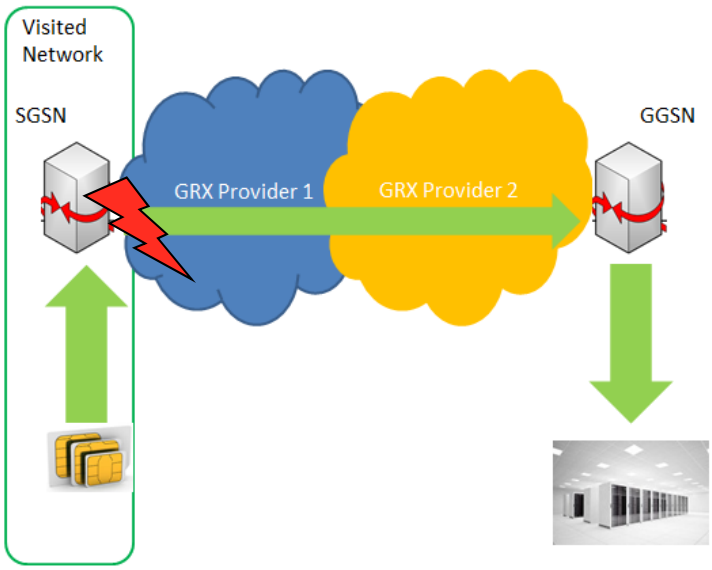


Figure 10. InterCarrier SLA situation in M2M

### 6.2.2. Players involved

The players affected are:

- Customers: As they have loss of service, and little information about the incident…
- Operator: As it does not have any SLA to guarantee this part of the service.

### 6.2.3. Possible Solutions

Solution 1: SLAs cascading in interconnection agreements between the different stakeholders:

Visited Network -> GRX Provider 1 -> GRX Provider 2 -> Home Network

Solution 2: Inclusion of a KPI for Service Availability for M2M traffic in the different roaming agreements between the different roaming partners

Solution 3: Use of the GTP Proxy mechanism can also permit, through the DNS resolution, that the GGSN output is the one of the home operator. In this way we discard GRX traffic in Provider 2. This is a possible solution for partnerships between operators.

Before the “ready for service” status, strict end-to-end quality testing must be also performed in order to agree the necessary quality of service and fulfill the preproduction user acceptance test. Some solutions related to video or tethering request LTE throughput and validation to detect and remedy problems in any network frame is necessary, especially in the ones which involve third parties.
Direct connection between home operator and visited operator is always advisable in order to guarantee SLAs and fast resolution in the case of critical services.

It is also important to limit the number of intermediate carriers between the home and visited network in order to avoid incremental risk.

## 6.3. Real-Time communications and redundancy as an important requirement of IoT

Real time requirements to communicate information to the IoT Platform and the customers’ Business Support System BSS can be also a constraint. For many services it is not only important to have enough availability, but also receive the information with a narrow schedule.

Network information about traffic consumption, device location or device traffic sending status must be required to have in real time in customers’ BSS in order to have flexible and quick decisions.

Knowing the location of a device, in a fleet control service for sample, or its data behavior in order to avoid fraud or limit the traffic throughput can be a necessary scenario critical for some business.

### 6.3.1. Technical

Traffic and network information are sent to the IoT Platform through special links which could be associated to SMSCs (SMS), signalling systems (Voice) or GGSNs (Data) in a mobile network.

Special connectivity, ad hoc, is typically deployed to assure this information sharing between the Home network and the IoT Platform using special links.

### 6.3.2. Players involved

- Mobile operators: to provide in real time this information forward the IoT provider
- IoT Platform Providers: to collect this information and apply the necessary formats in the presentation layer or process it in some useful way for the customers
- Customers: their BSS are going to be the final platform to manage this network information and progress decision taking.

### 6.3.3. Possible solution

An approach to this is be the use of quality-assured networks (IPX networks) which guarantee no-delay or jitter in the information. The utilization of real-time protocols instead of CDR-type technology can also help with the solution.

Protocols such as Radius or Diameter, which permit the sharing of roaming information about traffic consumption in real time can also meet this requirement. Protocol variations such as TCP Radius can also guarantee the reception of information. The capacity of the network should be also considered for this last scenario.

## 6.4. Alignment between business case and coverage necessity

### 6.4.1. Problem

Another problem is how to align the roaming impacts in the business case and the necessity of coverage in roaming scenarios for the IoT device.

The necessity of the customers for a low data cost could mean the restriction of operators, this means that for some solutions only a single operator may be accessible in a country. That will mean that the coverage of the IoT device and possible redundancy in case of a network problem can be non-existent. This situation must be considered when a SLA or KPI is agreed in a new service launching.

### 6.4.2. Technical

In order to block the more expensive operators because roaming agreements typically a block is applied at HLR level, avoiding the registering in the network, or a SIM level, disabling the PLMN list of the SIMs in order to start the registering process with some operator.

In lack of coverage from other operators this means a probable loss of service.

### 6.4.3. Players involved

- Mobile operators: in order to get the best roaming agreements and managing HLR or SIM configurations
- IoT Platforms: establish blocking mechanisms with the operators
- Swaping platforms manufacturers: create the infrastructure in order to get swap between SIMs of different operators.
- vSIM manufacturers. This technology would solve the issue in any device where it is embedded.

### 6.4.4. Possible Solutions

eSIM and swapping technologies can help to offer a good quality/cost to the IoT providers in order to solve this last case. Different mobile operators with different roaming agreements can offer a common solution which increases the coverage across different countries keeping an attractive price.

A technology improvement must be considered in the architecture in order to get this last point through swapping/eSIM platforms and a system which guarantees the Over-the-Air (OTA) operations to switch between operators. Through this architecture it is possible select one or other operator according to the coverage, pricing, etc.

# 7. Potential topics for further discussion

This whitepaper has provided an analysis of what is the role of the Carrier in roaming and non-roaming scenarios, new Carrier services opportunities and some problems detected, but also open the door of potential topics for further discussion as:

- Liability. Usage of IoT devices in different areas is growing rapidly, and also improve and change the way they work in areas as Health and Security. But this situation generate a doubt of who is liable when something goes wrong. For example, if a doctor is doing a surgery remotely and the connectivity is going slow or drop, who in the service chain is liable?, the IoT Device, the Connectivity Provider, the Carrier, who?. When IoT devices comes in more and more areas and it will be part of our lives, liability will be a topic that has to be defined.
- Special services for IoT. As mentioned in the chapter of Service Level Agreements problem and with the rapid growth of IoT platforms and devices, the traffic and revenues that this ecosystem generate is a strong reason to provide a better quality for this traffic and to differentiate it from the normal traffic, creating specific services for IoT and setting SLAs.
- IoT Platforms. The possibilities to evolve the IoT Platforms to cover all the needs of the enterprise market, is something that was not explored in this document. Enterprise market has large possibilities to growth and get revenues for IoT, and that possibilities can be realized if the IoT Platforms can evolve and adapt as fast as the enterprise require.