WHITE
PAPER

# PREPARING FOR THE INTERNET OF THINGS REVOLUTION

## Document No. 1 – Mapping out the challenges

7 November 2016

DGE DIRECTION GÉNÉRALE DES ENTREPRISES

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

ANFR AGENCE NATIONALE DES FRÉQUENCES

MINISTÈRE DU LOGEMENT ET DE L'HABITAT DURABLE

ANSSI

FRANCE STRATÉGIE

arcep autorité de régulation des communications électroniques et des postes

# EDITORIAL

*"**Arcep** identified the Internet of Things as one of the priorities of its strategic review. Because this cross-cutting subject involves a great many authorities, Arcep wanted to create a partner-based approach in the public sector."*- www.arcep.fr/iot

*"At a time when connected objects are collecting a host of personal data, including people's most intimate information (lifestyle, health), **CNIL** wanted to ensure that these innovations developed in a way that respects users' privacy."*- www.cnil.fr

*"**France Stratégie**, the organisation responsible for shedding light on the future and preparing tomorrow's public policies, is interested in the Internet of Things from a forward-looking perspective, to characterise its transformative potential, to help define the paths for its development and to identify the positive actions that public authorities can take."*- www.strategie.gouv.fr

*"**ANSSI** wants to contribute to the development of the Internet of Things by encouraging stakeholders to take security into account when designing connected objects. Computer incidents as well as attacks on people, data and the networks will thus be avoided."*- www.ssi.gouv.fr

*"The Internet of Things constitutes a tremendous source of wealth for businesses whose processes will benefit from innovative solutions, while ensuring data are protected. Under the New Industrial France (NFI) initiative, **DGE** supports the development of solutions that meet users needs, that are sustainable and cost efficient."*- www.enterprises.gouv.fr

*"When it comes to the Internet of Things, **ANFR** works to ensure that spectrum is available to enable innovation, thanks to international harmonisation and the right technical conditions. It monitors how spectrum is used and deals with cases of harmful interference."*- www.anfr.fr

*"The Internet of Things is being deployed in every city department and changing the way that cities operate and are managed. **DGALN** is participating in the IoT initiative to better understand, anticipate and support this development in urban projects."*- www.developpement-durable.gouv.fr

# PREPARING FOR THE INTERNET OF THINGS REVOLUTION
# WHITE PAPER
# DOCUMENT NO. 1 – MAPPING OUT THE CHALLENGES

## Introduction

The Internet of Things (IoT) has attracted the attention of consumers and businesses alike. And rightly so: the promise of a world populated by connected objects opens up countless opportunities and possibilities, as much for users as for service providers.

A great many studies are predicting that the number of connected objects being used worldwide is set to explode between now and 2020. IDATE[1] forecasts 80 billion connected objects by 2020, CISCO[2] is forecasting 50 billion while Gartner[3] predicts 26 billion. Even if we need to be careful how we interpret these figures, given the sizeable disparities in their definitions of the IoT's scope, all confirm a trend of massive deployment for connected objects.

The very notion of what constitutes the Internet of Things is subject to interpretation, and warrants clarification. For the purposes of this report a broad interpretation of the term "Internet of Things" will apply, corresponding to a set of physical connected objects that communicate via multiple technologies with diverse data processing platforms, in tandem with cloud and big data solutions.

Data and how they are utilised are indeed at the heart of the Internet of Things. Extracted from a vast array of devices and sensors, these data make it possible to inform users in real time about how their environment is changing. In addition to simply providing information, aggregating this plethora of data collected from heterogeneous sources makes it possible to quantify the connected environment, to then pinpoint trends, enhance existing applications and devise new ones. Thanks to the Internet of Things, the user – whether an individual or an enterprise – gains the ability to take action in their environment in real time, either manually or automatically, and to optimise processes (e.g. optimising traffic flows or logistics chains in real time).

Public authorities want to facilitate the adoption of the Internet of Things and lift any possible barriers so that French and European businesses are part of the ecosystem now taking shape at the global level. The IoT's emergence raises a multitude of issues that need to be considered, and requires coordination between many institutions. Arcep was thus committed to joining forces with its public sector partners most directly concerned by the Internet of Things: France's National Frequency Agency (ANFR), the National Network and Information Security Agency (ANSII), French data protection authority CNIL, the Directorate-General for Planning,

---

[1] *Internet of Things - A key pillar of the digital transformation,* IDATE research, October 2015

[2] *The Internet of Things - Vertical Solutions,* Cisco, February 2015

[3] http://www.journaldunet.com/ebusiness/le-net/previsions-gartner-objects-connectes-1213.shtml

Housing and Land Management (DGALN), the Directorate-General for Enterprise (DGE) and France Stratégie. If we break down the different facets of the Internet of Things, it becomes clear that connectivity and networks are underpinned by scarce resource management, while also giving rise to security issues proper to the different types of object, the networks that carry them and their destination, along with trust issues proper to the new kinds of data being collected and which impact several user categories, and development issues for French and European businesses.

## ALREADY CONCRETE APPLICATIONS OF THE INTERNET OF THINGS

The potential applications for the Internet of Things translate into a great many concrete uses – either new or improved – that will have a significant impact on the daily lives of people, businesses and local authorities. The expected potential benefits are facilitating their adoption by this disparate group of users. Several sectors, or key markets, in particular stand out:

- Smart regions are a central focus for local authorities' projects and should help optimise the process of managing intelligent infrastructures (transportation, energy, water, etc.) to provide residents with better service, while meeting regional sustainable development objectives;
- Thanks to the Internet of Things, homes and workplaces become more comfortable, easier to manage and less costly to run. Smart buildings, which include smart homes, provide solutions for controlling energy consumption, incorporating security systems and greater comfort;
- Industry 4.0 (i.e. using the Internet of Things to improve the means of production) is developing steadily. Collecting information is the first phase. Feedback and remote operation are more complex phases to implement in certain areas of activity;
- Connected cars, for which the first applications have already been introduced, have also moved past the first step of reading data thanks to on-board electronics which have been around for some time. Today, automotive sector players are working to develop new business models to capitalise on these new possibilities, while grappling with emerging questions over responsibilities;
- Connected health, which includes well-being, is one of the applications that consumers are most aware of, not least because of wearables. Data privacy aspects are a main focus of attention as these applications involve private sector players collecting new and very personal, and often health-related, information, and because of the issues bound up with their utilisation, notably by certain services. The way in which technologies shape how healthcare is organised, along with healthcare workers' level of involvement is another key area of concern. The changes enabled by the evolution of technologies, which are often more rapid than social and regulatory changes, makes this sector harder to grasp and more complex;
- Agricultural businesses have already incorporated the Internet of Things into their production processes. Farmers are employing more and more connected tools in their daily work: using sensors that monitor the status of crops, livestock or the environment,

farming equipment with built-in sensors, tools that help with decision-making or with operating machinery.

## STIMULATING THE FRENCH ECONOMY, AND A ROLE TO PLAY FOR PUBLIC AUTHORITIES

Beyond the sectors listed above, the Internet of Things has a very vast potential range of application, capable of having a positive impact on every sector of the economy. The IoT can thus be considered as a new, cross-cutting sector unto itself – one that generates revenue and creates jobs.

France is proving especially dynamic across this entire ecosystem that is currently taking shape. Buoyed up by this successful start, public authorities want to accelerate the availability of these services, to benefit businesses and citizens, and facilitate national enterprises' ongoing European and global development.

Arcep made the Internet of Things one of the priorities of its strategic review[4]. The Authority's aim is to help further the ecosystem's development by identifying and anticipating possible structural decisions that need to be made to enable its self-organisation. To this end, it initiated a collaborative approach with other public institutions that are concerned with the emergence of this new sector. The goal above all is to fully explore, understand and facilitate the Internet of Things revolution.

This approach translated in some 30 interviews[5], and later a series of workshops[6] on the high-potential sectors mentioned earlier. Arcep and its public sector partners were thus able to gather input from the ecosystem's stakeholders on the core issues at hand, and to produce this state of the art.

At the same time, Arcep is publishing its own roadmap for accompanying the emergence of the Internet of Things.

Parallel work on the Internet of Things is also being performed by a range of institutions, and particularly by the European Commission, the Body of European Regulators of Electronic Communications (BEREC) and the European Radio Spectrum Policy Group (RSPG). This document is an integral part of the European work programme, and Arcep's purpose here is to help further the work being done on a subject that is transnational by nature.

[4] Conclusions of the Arcep strategic review, Arcep, January 2016 - http://www.arcep.fr/larceppivote/larcep-presente-les-conclusions-de-sa-revue-strategique/

[5] The list of interviews can be found in Annex 1

[6] The list of workshop participants can be found in Annex 2

# 1 THE INTERNET OF THINGS ECOSYSTEM

The Internet of Things will be equally capable of allowing devices and appliances in the home to communicate information to users, as allowing vehicles to communicate with one another and with the smart regions through which they are travelling. It is also thanks to IoT solutions that certain individuals will be able to monitor their health, and manufacturers will be able to optimise their production processes. The meetings with stakeholders served to reveal the tremendous diversity of the IoT ecosystem, whose equally diverse applications paint a very broad spectrum of requirements in terms of technologies (low-speed, high-speed), security (data and network integrity), coverage and business models.

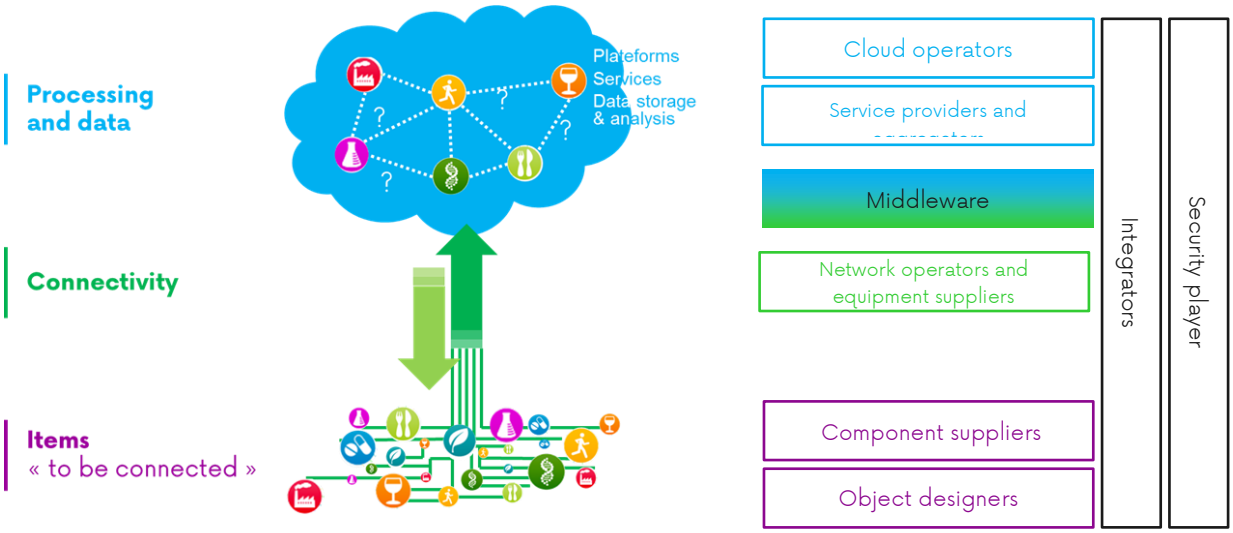
One aspect that is specific to the Internet of Things is that it mobilises consumer issues as much as those that affect the world of business, industry and services. The business models that have been or are being developed, and the resulting value chains, are as much B2B and B2B2C as B2C, which has considerable consequences on the ecosystem's structure and on who earns the revenue from the applications tied to the different economic sectors.

## 1.1 A LARGE ECOSYSTEM, ENCOMPASSING OBJECTS, COMMUNICATIONS AND DATA PROCESSING

The Internet of Things is at the confluence of the computing and electronic communications sectors, where every object communicates, can be queried, sends information and interacts. In 2012, the International Telecommunication Union (ITU) defined the Internet of Things as "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies*".

From a more practical perspective, the Internet of Things corresponds to a set of connected objects, communications and the internet, which combine with cloud computing and big data solutions:

- Physical objects possess technologies with built-in sensors, intelligence and connectivity, enabling them to communicate with other objects;
- Electronic communication networks provide the means for relaying the data generated by the objects;
- More or less distributed computing provides the tools for the storage, correlation and analysis of these data. It is often in the cloud that the decision-making processes capable of retroacting with the physical objects are located.




Different aspects of the Internet of Things to considerer

The nebula of the Internet of Things is made up of a multitude of players from different sectors, and working together to constitute this new facet of economic activity:

- The designers and manufacturers of the objects to be connected;
- The manufacturers of the module components that provide the objects with connectivity via embedded hardware and software components. They include electronics companies, semiconductor manufacturers, makers of sensors and the developers of the embedded software that ensures connectivity;
- Network operators and equipment manufacturers for the networks that connect the objects and cloud services. This segment includes veteran electronic communications players, i.e. telecom carriers, that already have networks which they are adapting for new, dedicated IoT uses, along with their traditional equipment suppliers. This segment also includes other players that have traditionally been less involved in electronic communications, such as utility and energy companies that make their infrastructure available for deploying new communication technologies, or companies born of the Internet of Things that are developing their own dedicated networks;
- Cloud computing companies, which primarily provide raw data storage and processing solutions. In this segment, veteran Internet and server companies are having to compete with new players that are deploying their own computer infrastructures;
- Suppliers of the middleware that enables the different objects to communicate. This includes traditional software companies;
- Integrators that orchestrate all of the previous building blocks by assembling the different physical layers first – objects and sensors – to design the final product, which can then be relayed via the networks to the cloud where it will managed, and where the data are stored and analysed to then be utilised. This segment includes classic IT integrators;

- Service providers and data aggregators that exploit the user data generated by the objects to meet their needs. Classic digital platform operators are positioned in this segment;
- Security specialists are present on every link on the chain, from object design to services. In the best case scenario, these IT security specialists work closely with all of the other players along the chain. Some are even taken over by Internet of Things players.

The series of meetings with stakeholders revealed an ecosystem where the players are still working to establish their position in the market. Some are exploring mergers or partnerships in the different building blocks that make up the Internet of Things.

This will to cover the entire value chain can be attributed to a desire:

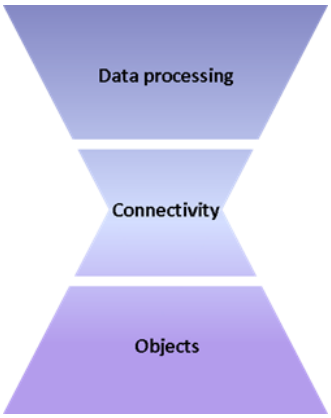
- To stand out from the competition, and so persuade users to adopt their solutions;
- For a larger market share, by offering complete end-to-end solutions;
- To be positioned in the segment where most of the value resides.

All of the players listed above sell products that users incorporate into their daily lives. There are three main user categories: enterprises, local authorities and individuals. Some users, local authorities or businesses, develop their own electronic communications infrastructure or position themselves as trusted third parties – in the arena of data protection and network security – for new service rollouts.

## 1.2 DATA DRIVING THE VALUE OF THE INTERNET OF THINGS

The value of the Internet of Things is rooted in three main aspects, as defined earlier: the objects, connectivity and data processing.

Connectivity – in other words the networks and their equipment – appears to be the most advanced IoT layer. Connectivity is already part of the daily lives of users who have an interface for interacting with the Internet of Things, via their smartphones and tablets: in France, 58% of population use a smartphone[7]. This connectivity is structured around a multitude of networks that make it possible to cover the country on both a local and national scale. The emergence of a vast array of networks and applications makes connectivity an especially competitive aspect of the IoT. But two more levels of competition are yet to come: between market players and between standards.




The objects layer is still in transition. One on the hand, technological developments over the past several years have made sensors both more powerful and less expensive. To give an example, the price of sensors has been cut in half over 10 years[8], and is expected to continue

[7] Source: CREDOC, Survey of "Living conditions and Aspirations"

[8] According to the report, "*Internet des objets, les business models remis en cause* ?" (Will the IoT challenge business models?), Oliver Wyman (2015)

to decrease. On the other hand, technical solutions still need to be developed to satisfy more complex needs, in many instances requiring faster speeds or better quality of service, such as connected cars and certain critical manufacturing processes.

Lastly, in the area of data processing, which will need to underpin the intelligence associated with the Internet of Things, everything remains to be organised for market players whose positions have not yet stabilised. The series of meetings held by Arcep and its partners revealed a relatively broad consensus that the bulk of the IoT's value, in terms of revenue, will reside in this last aspect, in other words data processing that results in the production of services. Innovation could be concentrated in this top layer where much remains to be done: new services for industry players, local authorities but also consumers. Even if it is not yet clear how revenue will be distributed, data-related activities are likely to be the biggest earners in the medium term. A study conducted by A.T. Kearney[9] confirms this expectation, and places future IoT revenue in the top layers. According to this study, activities related to data processing (services, data aggregation and systems aggregation) are forecast to generate close to €56 billion by 2025, notably by cloud computing companies and integrators, while revenue generated by connectivity is forecast to total €15 billion, and the objects layer, i.e. components, is slated to earn €10 billion.

This breakdown of the revenue generated by the Internet of Things places data at the very core of the IoT economy. Data could be monetised on two levels: first, with each user for collecting and directly utilising that data – notably for enterprises – and, second, through the massive exploitation of data that would enable the supply of intelligent solutions, by aggregating and correlating data belonging to multiple users. Data will increase in value when contextualised and interacting within an environment that will initially enable them to communicate with other data generated by different objects belonging to the same user, and later for them to communicate with similar data on other users.

With these future scenarios in mind, we can distinguish two business models for monetising data: selling the data directly or monetising them by selling a service. In the first instance, the data could be sold to economic players, whether users or not. Some players may be interested in obtaining raw data which they would than analyse themselves, while others would be interested in data that have already been processed. One example could be insurance companies that want to acquire and utilise data to better target their products, and calculate the risks involved. Another example could be IoT solution providers that collect data to then offer users free services, which include targeted ads, for instance, or adopt a freemium model wherein basic features are offered for free, but users need to pay for more advanced ones. In this second instance, the Internet of Things economy could be built around services that are sold directly or more efficient production processes. In which case, the data would be directly monetised through the end user.

[9] *The Internet of Things: A new path to European prosperity*, A.T. Kearney

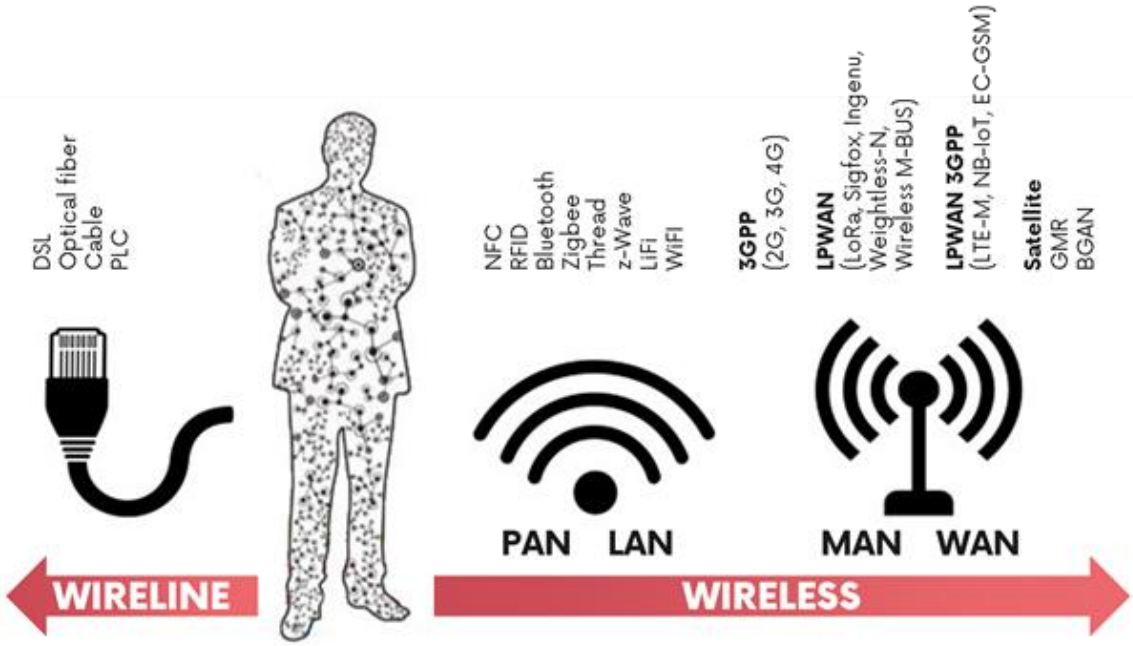
# 2 CONNECTIVITY INFRASTRUCTURES

The IoT's development depends on having access to networks of very disparate objects. The full spectrum of communication technologies is mobilised to achieve the many uses attached to these objects. This gives rise in particular to a growing need for mobility and coverage for objects that consume little power, which stimulates the development of new connectivity technologies, which in turn enable new applications.

## 2.1 A PLETHORA OF TECHNOLOGIES

If some fixed objects can be connected by wired networks, the IoT's growth will no doubt be driven largely by the use of wireless and mobile technologies. There are many and various wireless connectivity technologies, and the choice of which one to use is often based on the range of the network to be employed. Some uses also require a combination of wireless and wired technologies to connect the equipment to wide-area private networks or to the Internet.

One particular highlight of current technological developments around the Internet of Things concerns the disruption of the classic dichotomy in the world of frequencies between, on the one hand, short-range technologies, of which there is often a plethora and deployed by users themselves, operating in unlicensed bands and, on the other, long-range technologies operating in frequency bands that require a licence, and deployed by a small number of operators. The build-out of low-speed and long-range networks, using unlicensed bands, is driving a host of initiatives and developments.




A plethora of technologies to satisfy a multitude of connectivity needs

### 2.1.1 LOCAL AND ULTRA-LOCAL OPERATOR-FREE NETWORKS

For short-range wireless applications, such as PAN (Personal Area Network) and LAN (Local Area Network), Wi-Fi and Bluetooth technologies stand out, and notably the latter's Low Energy version (BTLE), but also Zigbee[10], Thread[11], z-Wave[12], RFID UHF and NFC, all of which operate in unlicensed bands[13]. A large portion of Internet of Things applications will be underpinned by this type of connectivity technology, and particularly those aimed at consumers, whose numbers are already growing (wearables, home automation, etc.). Other technologies could also develop, such as Li-Fi that uses very high frequencies in the visible light portion of the electromagnetic spectrum.

Most of these local area networks, notably those in residential users' homes, are not run by an operator. It is typically the user who acquires the network equipment (routers connected to a network box, for instance) and who are responsible for the local network's configuration and operation. These networks enable very limited mobility, albeit perfectly suited to home or individual use.

However, these above-mentioned, largely LAN and PAN technologies, do not provide wide-area connectivity on a national or international scale, contrary to MAN (Metropolitan Area Network) or WAN (Wide Area Network). These different categories of network, which supply partial geographical coverage but satisfy different needs, can be combined and used to complement one another.

### 2.1.2 WIDE AREA OPERATED NETWORKS

Among the wireless technologies deployed over a large radius, such as MAN or WAN, the main ones include:

- Classic cellular networks (3GPP[14]): 2G, 3G and 4G, most of which are deployed on frequencies under exclusive licence;
- LPWAN (Low Power Wide Area Network): LoRa[15], Sigfox[16], Qowisio[17], Ingenu[18], Weightless-N[19], Wireless M-BUS[20];
- LPWAN solutions on cellular networks (3GPP[21]): eMTC[22] (also called LTE-M), NB-IoT[23], EC-GSM-IoT[24];

[10] http://www.zigbee.org/

[11] https://www.threadgroup.org/

[12] http://z-wavealliance.org/

[13] The definition of "unlicensed frequencies" can be found in Section 3.1

[14] http://www.3gpp.org/

[15] https://www.lora-alliance.org/

[16] http://www.sigfox.com

[17] https://www.qowisio.com/

[18] http://www.ingenu.com/

[19] http://www.weightless.org/about/weightlessn

[20] http://www.m-bus.com/info/mbuse.php

- Existing satellite solutions (e.g.: Inmarsat, Iridium, Globalstar) and solutions in the process of being deployed (ex: O3b, OneWeb), operating in licensed frequencies.

In most instances, the use of an operator[25] is required to ensure the installation and operation of these networks on a large scale. Hence the term operated networks[26], which include most long-standing cellular networks deployed almost exclusively using 3GPP technologies (2G, 3G and 4G).

Here, some of the Internet of Things' new requirements – which largely run against the tide of the race for ever greater performance that has spurred mobile networks' development – have fostered the emergence of new mobile connectivity technologies. These technologies make it possible to achieve very low terminal costs and very low energy consumption, and are often grouped together under the umbrella of LPWAN (Low Power Wide Area Network). Several LPWAN technologies are taking hold on a global scale, including Sigfox, LoRaWAN, Qowisio, Ingenu, Weightless-N as well as Wireless M-BUS. It is essentially the first two that have developed on a significant scale in France, in addition to having been born in this country:

- Sigfox offers a vertically integrated model. The operator ensures international coverage by employing its own deployments or partnerships with local (national) operators. The technology for the development of connectivity modules is open source, but devices and terminals must be Sigfox certified and only the Sigfox cloud can be used[27];
- LoRaWAN is a communication protocol developed cooperatively by a number of players within the LoRa Alliance, whose members in France include Bouygues Telecom, Orange, Actility and Qowisio. This model, which is open to the coexistence of several of the alliance's member operators in the same geographical area, leads naturally to the development of an interoperable standard, enabling LoRa objects to function on various internationally deployed networks, both public and private. If the protocol remains open, there are only a very small number of decoding component suppliers, however.

---

[21] http://www.3gpp.org/

[22] http://www.gsma.com/connectedliving/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/

[23] http://www.gsma.com/connectedliving/narrow-band-internet-of-things-nb-iot/

[24] http://www.gsma.com/connectedliving/extended-coverage-gsm-internet-of-things-ec-gsm-iot/

[25] According to Article L. 32 para. 15 of France's Postal and Electronic Communications Code (CPCE), "*operator means any physical or legal person operating a public electronic communications network public or providing an electronic communications service to the public*".

[26] For the purposes of this document "operated network" is synonymous with "public electronic communications network*".*

[27] http://makers.sigfox.com/

Regarding cellular technologies, operators and mobile telephone equipment suppliers, working together to develop 3GPP standards, are collaborating on adapting existing network and equipment standards, notably 4G LTE, to satisfy the need for low-speed and very low-power systems. This work is expected to result in several solutions in the near future: Narrow Band IoT (NB-IoT), EC-GSM and LTE-M. For mobile operators, all of them will have the advantage of employing existing equipment and, in most instances, requiring only software updates.

3GPP members are also working on 5G standardisation which is due to take into account all of the Internet of Things' requirements from the outset (density, energy consumption, asynchronicity, terminal costs...).

As concerns satellite technologies, operators and equipment suppliers are working together within ETSI on adapting terrestrial network standards to the demands of satellite systems, notably 2G, 3G, 4G and future 5G related standards. This work will facilitate the integration of satellite technologies and satellite-terrestrial convergence.

### 2.1.3 PROFESSIONNAL MOBILE RADIO

Businesses also have the option of deploying an independent network dedicated to their own IoT applications. This is the route taken by a number of utility companies and municipal service providers such as Veolia, Suez Environnement and GrDF, which operate their own networks to be able to have greater control over their quality and security, or because they use their own technology, which can be based on an existing standard.

### 2.1.4 WIRED NETWORKS

A great many fixed objects are connected to traditional operators' wired networks. Copper, optical fibre or coaxial cable networks are also widely used, particularly for all applications that have significant bandwidth requirements (CCTV cameras, video advertising panels, etc.) or controlled low latency needs (machine tools, telesurgery, etc.).

Innovative applications may thus emerge, notably with the rise of multiple smart city and smart street lighting projects. In its current public consultation[28] Arcep raises the question of reusing optical fibre deployments outside buildings for the Internet of Things.

Powerline carrier (PLC) technologies can also be used via power companies' networks, but are confined largely to short distances for applications that are less demanding in terms of bitrate (controlling street lamps, meter reading, etc.).

[28]http://www.arcep.fr/index.php?id=8571&no_cache=1&tx_gsactualite_pi1[uid]=1874&tx_gsactualite_pi1[annee]=&tx_gsactualite_pi1[theme]=&tx_gsactualite_pi1[motscle]=&tx_gsactualite_pi1[backID]=26&cHash=2a6abd1f8efe62c7f9cfd0d64291632d

## 2.2 OBJECTS' CONNECTIVITY NEEDS INCREASE THE SET OF DEMANDS ON NETWORKS

The massive deployment of connected objects is forcing a review of networks' coverage and quality requirements. Regarding the need for wide-area networks, the Internet of Things economy will only develop if networks are available in a large portion of every country, at the very least on a Europe-wide scale.

Operators also need to guarantee the resilience – i.e. a system's ability to overcome a crisis triggered by a critical incident – of their own network, to be able to meet the needs of their users, who may want to ensure the resilience of their own connectivity systems thanks to multisourcing, or by being highly compatible with multiple systems (multi-network roaming).

### 2.2.1 GROWING NEED FOR MOBILITY AND COVERAGE

Stakeholders are aware of the challenges inherent in achieving the wide, continental-scale coverage needed to create a sufficiently vast market, to generate economies of scale and bring down the price of terminals and connectivity. This transnational coverage will also be imperative for certain applications, such as connected cars and tracking merchandise.

Traditional cellular networks have had agreements in place for some time that enable SIM card roaming the world over. Across Europe, these agreements are governed by obligations resulting from European Union laws, which include both technical and economic provisions. The EU entrenched its commitment to creating a single market for electronic communications with the publication of new roaming regulation[29] on 25 November 2015. This regulation lays down the conditions for wholesale access to public mobile communication networks for the purpose of providing roaming services. It aims to eliminate the gap between national access prices and roaming prices inside the European Union, by setting maximum roaming tariffs for wholesale and retail markets.

The Body of European Regulators of Electronic Communications (BEREC), of which Arcep will assume the chairmanship in 2017[30], published a report on 12 February 2016 called *Enabling the internet of things*[31], in which it concludes, based on its interpretation of the roaming regulation, that the way in which IoT services employ mobile electronic communications networks generally falls within the scope of this regulation, and are thus also subject to its access and price supervision obligations. However, on the matter of permanent roaming, BEREC asserts that a case-by-case approach is required. It concludes that the regulation should not apply when "*the connected device (e.g. smart meter, sensors) is used on the basis*

[29] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance)

[30] And the vice-chairmanship in 2016 and 2018

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

*of permanent roaming but is not travelling at all*". Here, BEREC calls for future work to bring further clarification to cases of permanent and transitory roaming in the IoT context.

Also worth noting is satellite technologies' usefulness is expanding coverage to the remotest parts of the planet (sea, desert), to those locations not covered by existing networks and those where roaming agreements are not possible (conflict areas).

### 2.2.2 CERTAIN APPLICATIONS REQUIRE HIGH AVAILABILITY

Arcep has ascertained a demand, chiefly from economic players from the private and public sectors, for high availability mobile services capable of handing over from one mobile network to another when needed (multi-roaming) – a demand that French operators can only partially satisfy today.

Solutions that are currently used to satisfy this demand often employ circumvention mechanisms, based on international roaming agreements: they transit over networks belonging to foreign operators that have access to roaming agreements with several French operators.

A national solution that incorporates secured handover between mobile networks requires a mobile network sharing scheme be established between French operators. This type of solution is already in place for emergency calls. In addition to economic players from the private sector, the natural users of such a product would be certain critical public services or machine-to-machine communication applications that require a special level of security.

If Arcep has stressed[32] that, in theory, it is unlikely that this type of product will become available to the entire market, it has also stated that providing high availability mobile services could be a good solution to meet certain specific needs. It thus invited operators interested in doing so to contact the Authority.

Mixed solutions, combining satellite and terrestrial technologies, are another possibility for guaranteeing a high degree of availability, while eliminating geographical borders to some degree.

### 2.2.3 NEW LPWAN ALSO OPEN UP COMPLEMENTARY REDUNDANCY POSSIBILITIES

Neither the users nor the manufacturers of connected objects are required to meet resilience obligations[33]: they are considered merely purchasers of connectivity from an electronic communications operator, on operated networks. However, certain objects, websites and critical applications have been using redundancy mechanisms (multisourcing) for many years, particularly in the business market. Dual connectivity solutions, with or without automatic handover to another network in the event of a power cut, with more or less strong security

[32] Arcep guidelines on mobile network sharing, May 2016 (section 3.3.2.a)

[33] It must nevertheless be noted that, in accordance with CPC Article L. 34-9, terminal equipment that is to be connected to a public network must be assessed for compliance with essential requirements, which can include network protection imperatives.

guarantees (dual physical or logical connection), have made it possible to satisfy redundancy requirements by combining networks belonging to different operators and/or different technologies (fibre, copper, cable, cellular, satellite, Wi-Fi, other). The birth of new LPWAN network technologies, such as LoRa or Sigfox, usher in complementary possibilities for providing redundant access.

LPWAN connectivity services cost little to produce, are energy autonomous and deliver good indoor coverage performance. In particular, the fact of being very low power, which means they can be battery-powered, makes power cuts a non issue. These features make back-up connection one of key target markets for LPWAN connectivity services: an object can be connected using a "high-speed" fixed or mobile network as its main source of connection, and hand over to a back-up LPWAN connection if the main network fails in some way. To give an example, Securitas Direct has chosen to connect 1.2 million alarms to the Sigfox network in Spain and France. However, the low speeds associated with LPWAN forced the company to use certain types of solution for their back-up links, or to adopt an approach of relaying only certain critical streams that consume little data.

## THE MAIN CHALLENGES

The interviews proved that a plethora of technologies – both wired and wireless – is necessary and must be encouraged, to meet the multifarious application and connectivity needs created by the Internet of Things. Short range wireless networks are typically managed by users themselves, whereas long-range networks (which include 3GPP and LPWAN) typically require an operator.
Another challenge, this time at the European level, concerns the terms and conditions of permanent roaming for objects, since a portion of connection objects are designed to operate outside their country of production.
Lastly, resilience is central to IoT technologies. Operators need to guarantee their own network's resilience, while users may also want to ensure their own connectivity system's resilience through inter-technology redundancy (multisourcing) or the high availability of multiple technologies (multi-network roaming). Today, solutions for satisfying the need for high availability fall short, and the question of national roaming (under restricted conditions) could be considered to remedy the situation. The properties of LPWAN (wide area coverage, low-power, low connectivity cost) make them ideal candidates for adding complementary options for redundant connection.

# 3 SCARCE RESOURCES REQUIRED FOR THE IOT'S DEVELOPMENT

The ability to provide the connectivity solutions described earlier often requires two types of resource: frequencies and IP addresses. These resources, which are already considered to be scarce, will become all the more so as the number of connected objects is expected to grow exponentially.

## 3.1 DIFFERENT FREQUENCY AUTHORISATION SYSTEMS TO ADDRESS DISPARATE REQUIREMENTS

The frequency bands that can be used by the Internet of Things include:

- Frequencies whose use is based on a system of general authorisation, requiring users to comply with certain technical conditions. These are referred to as unlicensed frequencies and are used, for instance, by Sigfox, Qowisio and LoRa Alliance members for LPWAN;
- Frequencies that require an individual licence:
    - Frequencies used to operate public mobile networks (2G, 3G or 4G and later 5G);
    - Frequencies used to operate professional mobile radio (PMR) networks;
    - Fixed service frequencies (wireless local loop, broadcasting);
    - Frequencies for satellite services.

As their name implies, unlicensed frequencies require no prior individual authorisation, and users do not have to pay a licensing fee. They must, however, comply with certain technical restrictions attached to these bands whose purpose is to ensure users can all coexist on the spectrum. Despite the existence of these rules, it must nevertheless be said that there is a small, but not zero, probability that interference will occur as other users are able to employ the same frequency. A certain number of these frequency bands, whose technical terms and conditions of use are set by Arcep, are employed by low-power devices, such as devices that use Wi-Fi, but also by the Internet of Things, notably the following bands: 13.56 MHz, 169 MHz, 433 MHz, 863 – 870 MHz, 2400 – 2483,5 MHz, 5150 – 5350 MHz and 5470 – 5725 MHz[34].

Regarding frequencies that require an individual licence, the licensing process makes it possible to ensure that two entities are not using the same frequency in the same location. This means that, in theory, aside from cases of unlicensed use or the use of non-compliant equipment, interference is never an issue on these frequencies. With very few exceptions, users must pay a fee to be able to employ these frequencies. GSM, UMTS and LTE access technologies, which are used by public mobile networks, already enable IoT applications

[34] The regulatory framework that sets out the conditions for short-range devices' use of radio frequencies is set by Arcep Decision No. 2014-1263 of 6 November 2014 on frequency use: http://www.arcep.fr/uploads/tx_gsavis/14-1263.pdf

which will be further facilitated by the above-mentioned 3GPP release 13. The frequency bands allocated to mobile operators in Metropolitan France[35] are: 700 MHz, 800 MHz, 900 MHz, 1800 MHz, 2100 MHz and 2600 MHz.

In addition to the system of authorisation, which determines how easy it is to access the spectrum resource, the choice of whether to use one frequency band rather than another will depend on operational requirements:

- Volume of data to transmit and exchange;
- Uninterrupted communication or intermittent use;
- Real time communications (e.g. for operating/control applications) or delayed communications (e.g. for collecting information);
- Bandwidth use (high or low bitrates);
- Coverage (local use or wide-area coverage, indoors or outdoors);
- Power consumption.

So depending on their business model or planned applications, market players will tend to opt either for unlicensed bands or bands that are allocated by exclusive licence (notably using mobile operators' consumer networks). It must also be stressed that hybrid licensing systems may exist, for instance by authorising several entities to use the same frequency band: this reduces the risks of interference by controlling the number of users, while eliminating the constraints of a system of exclusive use by a single license-holder. The meetings revealed that, for some players, often the smallest ones, the use of unlicensed frequencies provide a means for testing their business models at little cost, compared to the use of licensed bands.

Using unlicensed bands can enable innovation without having to obtain permission, for applications that are compatible with the more or less stringent technical conditions attached to these bands, but without protection against interference. The meetings also provided stakeholders that lacked certain information with an opportunity to query Arcep on the legal framework governing the use of licensed bands to conduct trials, as those bands may the most suitable in certain other cases.

Here, Arcep is keen to stress that, in accordance with Article L. 42-1 of France's Postal and electronic communications code (CPCE), it already grants individual frequency licences to conduct trials. The provisions designed to facilitate experimentation were introduced by the Digital Republic Act. Under certain conditions, Arcep could define an experimental framework aimed at supporting a given actor in the development of a technology or service that is innovative from a technical or commercial standpoint. To this end, when it allocates individual frequency and numbering resources "*for experimental purposes*", Arcep could lift certain obligations attached to the use of these resources, to engaging in the business of operator, or to operating an independent network, for a maximum duration of two years.

[35] The frequency allocation table for the four mobile operators in Metropolitan France is available on the Arcep website:
http://www.arcep.fr/fileadmin/reprise/dossiers/mobile/Repartition_des_frequencies_-_decembre_2015.pdf

## 3.2 ANTICIPATE MEDIUM-TERM FREQUENCY AVAILABILITY

In the short term, available frequencies do not appear to be an obstacle to the IoT's deployment, and multiple options are already available, as the recent CEPT[36] workshop revealed.

The growth outlook which forecasts an Internet of Things that will be connecting more than 50 billion objects[37] by 2020, nevertheless requires some forward-planning. CEPT has thus undertaken several concrete actions to develop frequency ranges that can be mobilised. Arcep is helping to prepare the French position, under the aegis of National frequency agency (ANFR), under whose purview this issue falls. On the one hand, it is working to identify paths to harmonisation of general authorisation uses in the 800 - 900 MHz band in the short term. It is also assessing whether the technical conditions governing the use of mobile operators' bands are compatible with The Internet of Things.

### 3.2.1 IN BANDS SUBJECT TO GENERAL AUTHORISATION, AKA UNLICENSED BANDS

In its approach to the use of unlicensed frequency bands, the first step for Arcep was to hold a public consultation[38] in late 2014 whose purpose was to deepen its strategic foresight on the future use of and need for these bands, particularly within the context of the IoT's development. The findings of this public consultation coincide with those of the more recent interviews and confirm, in certain contexts, some limits to the use of unlicensed frequency bands. A strong increase in applications and traffic on certain frequency bands could hamper the operation of an application or the service provided to end users. It is therefore vital to meet demands for access to frequencies created by new applications and coming from the industry, to be able to address more complex or more bandwidth-hungry applications, if necessary, and to keep pace with the predictable increase in the density of connected objects. The cooperation process between ETSI and la CEPT is an asset for Europe in this regard.

In addition, it emerged from the meetings that the quality of the use of these bands can be disturbed by interference, notably due to certain equipment's non-compliance with harmonised standards, or with the conditions set for using these frequencies. Moreover, the rules of use designed for specific applications may need to be adapted to the Internet of Things' new requirements. The technical terms and conditions of use for unlicensed frequency bands can be relatively restrictive to allow for their uncoordinated use by a large number of systems. In some instances they may be limited to a specific application to reduce the risks of interference. However, the exponential increase in the density of objects that every forward-looking study is predicting, could ultimately justify the identification of new harmonised resources, taking into account new rollout scenarios and terms of use, such as increasing power levels and rates of use, to keep pace with the sector's growth. Stakeholders thus took advantage of the meetings to confirm the need for more relaxed conditions for the

[36] http://www.cept.org/ecc/cept-workshop-on-machine-to-machine-communications-m2m/

[37] Source: Cisco

[38] The summary of the public consultation (in French) is available here: http://arcep.fr/fileadmin/uploads/tx_gspublication/Synthese_-_Consultation_bandes_libres.pdf

863 - 870 MHz band, and for opening up part of the 870 - 876 MHz and 915 - 921 MHz bands. These potential changes had been formulated in the Ministerial report of March 2014 entitled, *Dynamic spectrum management for innovation and growth*[39]. Following this report's submission, the Minister of State for the Digital Sector tasked ANFR with studying "*the technical and regulatory conditions that would enable the development of low-power devices in the 870-876 MHz, 915-921 MHz and 862-870 MHz bands, to contribute to the development of connected objects".* This assignment was reprised in the ANFR Objectives and performance contract for 2015-2017[40]. Work began in 2015 and a public consultation was held from 3 June to 18 July 2016.

Frequency harmonisation at the global level is an important condition, particularly for players planning on international deployments. French and European companies' growth on the international stage depends in part on their ability to generate economies of scale, to be able to supply technological solutions at a low cot by relying on systems using the same frequencies.

On this matter, the 863 – 870 MHz, 870 – 876 MHz and 915 – 921 MHz frequency bands were identified at the European level for several low-power applications (RFID, smart metering, smart grid, smart cities, home automation, alarms, hearing aids). French authorities are currently working on relaxing the conditions governing the 862 – 870 MHz band and on opening up the 870 – 876 MHz and 915 – 921 MHz bands for the Internet of Things. This is in keeping with a push for European and, as much as possible, international harmonisation. On 3 June 2016, Arcep and France's National frequency agency (ANFR) launched a public consultation[41] aimed at obtaining stakeholders' observations on new opportunities for using the 862 - 870 MHz, 870 - 876 MHz and 915 - 921 MHz bands. The aim is to open up new frequency bands and study the technical and regulatory conditions that would enable the development of low-power devices in these bands, to help steer national and European work that is currently being done on facilitating the development of the Internet of Things.

### 3.2.2 IN BANDS SUBJECT TO INDIVIDUAL LICENCES

The meetings did not reveal any specific demand for the allocation of new bands subject to individual licences. The stakeholders who expressed themselves on this point, and particularly mobile operators which already have licences to these frequencies, are above all awaiting the arrival of the EC-GSM, LTE-M and NB-IoT standards which should be compatible with the bands that have already been assigned and, further down the road, with 5G which is already being worked on, with a view to making new frequency bands available or adapting the technical conditions in bands that are currently harmonised for mobile networks.

As a complementary measure, discussions are taking place at the European and national levels to examine and amend if necessary the technical and regulatory framework, ultimately

[39] Original title: *Une gestion dynamique du spectre pour l'innovation et la croissance.*

[40] http://www.anfr.fr/fileadmin/mediatheque/documents/Publications/COP_ANFR_VF_2015-11-23.pdf

[41] The public consultation ran until 18 July 2016 and is available here: http://www.arcep.fr/uploads/tx_gspublication/consult-arcep-anfr-iot-frequencies-030616.pdf

with a view to allowing operators to use all of the bands assigned to cellular networks for M2M. Harmonised provisions for using the 700 MHz, 800 MHz, 2.1 GHz, 2.6 GHz and 3.5 GHz bands are based on the principle of "power masks" without referring to any technologies in particular. In the 900 MHz and 1800 MHz bands, however, harmonisation measures are tied to specific conditions of coexistence between GSM, UMTS, LTE and WiMAX systems. CEPT has begun the work of assessing the compatibility of these regulatory frameworks with the solutions envisaged for the Internet of Things in these bands. It plans on publishing its findings in March 2017.

## 3.3 MULTIPLICITY OF ADDRESSING SCHEMES

In an environment where several billion objects are due to be connected, the scarcity of addressing resources is one of the major challenges. Several systems are used to identify connected objects in the networks:

- Open identifiers: mobile phone numbers, SIM card identifiers, IP addresses (in their IPv4 or IPv6 variants), MAC addresses, ITU OID (Object IDentifiers), EPC, UID...
- Proprietary identifiers: non standardised formats.

The main challenge is to avoid a dearth of open identifiers as the volume of connected objects continues to grow exponentially. It may also be necessary to establish a better interplay between the IoT market's global scale and the management of numbering resources on a national scale. Moreover, issues surrounding addressing schemes overlap with those surrounding fluidity and interoperability, which will be examined in the next chapter.

### 3.3.1 CELLULAR NETWORKS

Regarding mobile networks: the 3GPP standards (GSM/UMTS/LTE) stipulate that an MS-ISDN mobile telephone number compatible with the ITU E. 164 standard[42] will be assigned to each mobile access line. These MS-ISDN numbers are also used to identify connected objects in a mobile network operator's information system. But the object typically communicates with a business application using communication protocols such as IP, situated in one of the top network layers[43].

However voice and SMS communication protocols, employing the MS-ISDN number as the addressing identifier, are used as part of certain dedicated applications, or to "wake up" machines (which spend most of their time in sleep mode to maximise their autonomy) to initiate a data exchange. This is notably the case for remote metering actions controlled by a central system.

Arcep assigns these MS-ISDN numbers to operators, which then assign them to their subscribers. In 2012, to avoid a dearth of mobile numbers, Arcep decided to create a range

[42] Public telecommunications numbering plan defined by the International Telecommunications Union (ITU). ITU is the United Nations specialised agency for information and communication technologies: https://www.itu.int/rec/T-REC-E.164-201011-I/EN

[43] As per the OSI model

of special expanded 14-digit mobile numbers for Metropolitan France, starting with "0700", to enable mobile lines dedicated to machine-to-machine (M2M)[44] communications, and so not be a burden on the 10-digit mobile numbers pool. M2M communications have thus been excluded from using 10-digit mobile numbers since 1 January 2016 (operators were able to request special dispensations from Arcep to use these numbers until 30 June 2017)[45]. It should also be noted that, in accordance with the national numbering plan[46], these numbers must be assigned to users living in France, and are therefore not intended to be used in a permanent fashion outside the national territory. Some international operators that were included in the meetings nevertheless expressed a desire to see these terms relaxed, to streamline access to the global market using the resources of their country of origin.

Each SIM card is also identified by an IMSI code whose format is defined by ITU recommendation E. 212[47]. The International Mobile Subscriber Identity is composed of three parts:

- MCC: Mobile country code: assigned to countries by ITU (208 for Metropolitan France);
- MNC: Mobile network code: assigned to operators by Arcep[48]. 100 MNC are available per MCC;
- MSIN: Mobile subscription identification number: assigned to customers by their operator (a non public number used for internal network purposes, different from the subscriber's telephone number).

Given their mobile network identification function and their scarcity, MNC are only assigned to operators which, because of their infrastructures and their contracts, are capable of operating them. In practice, today this includes mobile network operators (MNO) and mobile virtual network operators (MVNO).

### 3.3.2 LPWAN

Regarding Low Power Wide Area Networks (LPWAN), there is currently no standardised and unified numbering plan in place. These networks use private identifiers, with proprietary formats, to identify sensors. If this does not seem likely to be problematic in the immediate future, identification could become a standardisation challenge in the long run (cf. paragraph 4.2).

---

[44] Arcep Decision No. 2012-0855 of 17 July 2012

[45] Arcep Decision No. 05-1085 of 15 November 2005, as amended by Decision No. 2015-1295 of 22 October 2015

[46] Arcep Decisions Nos. 05-1084 and 05-1085 of 15 December 2005.

[47] The international identification plan for public networks and subscriptions defined by ITU - https://www.itu.int/rec/T-REC-E.212/EN

[48] The list of MNC assigned by Arcep is available online at: https://extranet.arcep.fr/portail/LinkClick.aspx?fileticket=etHdgos5yN4%3d&tabid=217&portalid=0&mid=850

### 3.3.3 RFID AND NFC TAGS

Today, a great many objects have an identifier thanks to RFID or NFC technologies. It is made up of several sub-identifiers (SUID) that are built into the chipset's memory during the production stage, or used by the operator. Given the multiplicity of the objects that use RFID and NFC, having unique identifiers is a crucial challenge.

A registration authority – currently the ISO – thus ensures overall consistency and assigns codes to a plethora of organisations which are responsible for managing the supply of certain sub-groups of identifiers to users. ISO recently published the ISO/IEC 29161[49] standard which establishes a unique identification scheme for IoT applications. Another standard, ISO/IEC 30141, is in the process of being published and will propose an Internet of Things reference architecture, enabling information to be exchanged between different applications.

### 3.3.4 IP ADDRESSING

Lastly, a portion of objects need to be directly accessibly on the Internet, and must therefore have public IP addresses (one address per object or per network of objects), which increases demand for IP addresses. At the global level, it is the Internet Corporation for Assigned Names and Numbers (ICANN) which is responsible for managing IP addresses. ICANN parcels out IP addresses in blocks to the different regional Internet registers (RIPE NCC, Réseaux IP Européens – Network Coordination Centre, for Europe and the Middle East), which are in charge of assigning IP addresses locally.

On 14 September 2012, RIPE NCC announced that it had begun distributing the last block of IPv4 addresses (the version of the protocol defined in 1981) it had been assigned, thus warning against a possible dearth and calling for the necessary migration to the new addressing system, IPv6. Version 6 of the Internet protocol was finalised by IETF in 1998, and will make it possible to directly identify all objects connected to the Internet around the world with no risk of running out, thanks to the use of longer addresses providing virtually unlimited addressing space. The Minister of State for the Digital Sector, Axelle Lemaire, asked Arcep for a status report on the deployment of the IPv6 protocol in France in early 2016.

Arcep submitted its report on 30 June 2016, and made it available to the public on 30 September. This report proposes a government action to plan to guarantee users' freedom on the internet and to increase France's influence over the global digital community.

[49] ISO/IEC 29161 standard: "Information technology -- Data structure -- Unique identification for the Internet of Things", 2016

### THE MAIN CHALLENGES

Two key challenges emerged during the interviews, linking scarce resources to the IoT's deployment. The first challenge pertains to frequencies, and the second to object identification issues.

Two frequency-related challenges have been identified:

- It is imperative that resources be available for all players, including unlicensed frequency bands, for IoT solutions to be deployed. The frequency availability challenge is closely bound up with European and international harmonisation of the resources required for IoT players' global rollouts. Work on the matter is already underway, notably by Arcep and ANFR in the 862-870, 870-876 and 915-921 MHz bands;
- The conditions governing the use of certain unlicensed bands could be adapted to new IoT requirements, albeit by imposing conditions capable of minimising the risks of interference in these bands. This issue is also covered by the above-mentioned work being done by Arcep and ANFR.

Regarding the identification of objects, two challenges have been identified:

- Managing the scarcity of these resources is a challenge involving several addressing systems used to identify objects in the networks. For cellular networks, a range of 14-digit numbers was made available specifically for M2M. By the same token, some operators today want to have access to permanent worldwide roaming using national numbering resources from their country of origin.
- The transition from IPv4 to IPv6 is a challenge that public authorities are already working on, as it addresses the scarcity of identifiers at the outset, and then promotes interoperability in the bottom layers (cf. next section). In its report to the Government on the deployment of IPv6, Arcep assesses the risks of a dearth of IPv4 addresses and the potential negative impact of a late deployment of IPv6, notably on IoT.

# 4 OPENNESS ON THE INTERNET OF THINGS

For connected objects to be able to organise themselves into a network, and keep the promises associated with the expression "the Internet of Things", there will need to be more or less interoperability between the objects, which can be established at different levels.

The meetings helped distinguish two main levels of interoperability:

- interoperability in the bottom layers, in other words at the information delivery level;
- interoperability in the top layers corresponding to a dialogue between applications, for processing data.

## 4.1 THE OPENNESS AND INTEROPERABILITY CHALLENGE

The inherent implications of a system's degree of openness have already been the focus of economic analysis devoted to markets that are characterised by intense innovation and large network economies. In its 2014 report entitled, *The economics of open and closed systems*[50], the Competition Authority postulates that the pros and cons of an open system[51], compared to a closed system, need to be assessed on a case-by-case basis. First, it notes that both an open and closed system can have a positive impact on competition: while the first seeks to promote competition within a single system, the second encourages competition between systems. Next, it underscores that openness would foster compatibility between systems, which is good for users and maximises network effects. It also notes that a closed system, on the contrary, could help encourage innovation while avoiding standardisation. These analyses can apply to the Internet of Things.

The development of the Internet of Things depends on previously unconnected objects gaining access to networks. For this to happen, the full array of communication technologies[52] will be used, to satisfy users with multifarious needs. This diversity of connectivity solutions demonstrates strong innovation, and goes hand in hand with the emergence of a number of players, but could be challenged as the market matures. The market's development thus raises the question of the right degree of openness, which can be posed at different levels (objects/sensors, data, connectivity, addresses and protocols, etc.). In this case, openness can be measured on the basis of interoperability and in terms of fluidity in general.

The question of interoperability refers to the compatibility that exists between objects and between applications. Interoperability translates into two economic effects. First, interoperability bolsters a market's fluidity, which is vital for competition to flourish since it gives users a choice of IoT solutions with no impediments to switching between technologies, hence between providers. Second, once a certain degree of competition is achieved, it makes it possible to maximise network effects. By making the objects compatible, it enables users to enhance the range and number of new objects that can be connected to the ones they are already using. This in turn helps enhance products and stimulates the emergence of new applications. So interoperability can, in theory, improve users' welfare.

However, because it can create constraints for manufacturers and force them to be interdependent (albeit to degrees that can vary depending on the level at which interoperability comes into play), interoperability can limit the capacity to differentiate oneself from the competition and to innovate. When a market is still only nascent, forcing interoperability runs the risk of slowing, and possibly preventing, innovation: this in turn would limit monetisation possibilities for innovative players who would struggle more to keep their

---

[50] Report published jointly in December 2014 by the French Competition Authority and the British Markets Authority

[51] A system defined by Hazlett et al (2011) as "'*collections of two or more components together with an interface that allows the components to work together*" qualified as "open" when the interface is accessible to all players, and not just its owner.

[52] See Part II, "Connectivity technologies"

customers. In the specific context of the Internet of Things, imposing total and general interoperability could also have a physical impact on the objects, while manufacturers are already having to deal with considerable technological imperatives, such as size, memory, autonomy and power consumption.

In the very short term, interoperability does not appear to be manufacturers' chief consideration: technological solutions are not yet mature, usage is often still local, restricted to a limited geographical scale or within the same entity, and involves only metering in many instances, particularly in an industrial context. The many suppliers are thus tending to develop their objects independently of one another, which is resulting in a plethora of siloed products. For users, interoperability is not a priority in the short term, particularly for certain manufacturers and a few local authorities that are still testing the solutions available to them on a small scale, and which they can then incorporate after the integration stage, before considering a large-scale rollout.

Internet of Things stakeholders are, however, aware that in the medium term the value of every connected object will be measured by its ability to communicate with an ecosystem. For instance, in the case of smart homes, the situation of residential users having to deal with a multitude of connectivity systems should be avoided, by selling objects that speak the same language, and so sparing users a steep learning curve and additional expenditures on controlling their devices and appliances. Local authorities, which are in charge of a multitude of connected objects, will need to streamline their inventory of equipment to decrease costs and cross-reference the collected data. In the case of connected cars, it will be crucial that vehicles be able to talk to one another, and with the smart regions they travel through. A lack of interoperability could thus prove an impediment to the IoT's deployment. Some stakeholders are already concerned that the lack of interoperability could result in a fractured market. A lack of clarity on interoperability efforts could eventually result in a wait-and-see attitude to large-scale service rollouts.

## 4.2 A STANDARDS WAR IN THE BOTTOM LAYERS

We can identify two targets for interoperability in the bottom layers: communication protocols and object addressing.

We are still some way from interoperability in terms of communication protocols: the search for very low-cost connectivity modules imposes a simplicity which, for now, makes it very hard to deliver multi-protocol connectivity. Some players are, however, joining forces to promote standards on a global scale.

By complying with the common LoRa standard, members of the LoRa Alliance are working to achieve a form of interoperability between member operators' networks. Meanwhile, members of the Wi-Fi Alliance, which are already active around the world, support the HaLow standard for satisfying IoT needs for low power consumption. By the same token, ZigBee Alliance members are developing a common standard on the communication protocol, and have formed a partnership with the Thread consortium to achieve interoperability that goes right to the top layers.

Meanwhile Sigfox is singlehandedly supervising the deployment of its proprietary standard, and managing the Sigfox Network Operators (SNO) alliance which issues exclusive local rollout agreements to its partner members. In this particular case, interoperability is a way to increase Sigfox technology's footprint.

Mobile network operators rely on 3GPP standards, which enable high interoperability since devices are natively compatible with all of the networks belonging to operators that comply with these standards.

Object identification also raises interoperability questions. As we saw earlier, manufacturers have chosen a variety of addressing systems for objects (mobile phone numbers, SIM card identifiers, IP addresses in their IPv4 or IPv6 variants, and non standardised proprietary formats). In this respect, because it will not suffer from the dearth issues experienced with IPv4, the deployment of IPv6 could be a boost to interoperability. This protocol could act as a universal language to the extent that, in a great many cases, communication does not take place directly between objects but rather through intermediate network elements that provide the translation between disparate networks and protocols.

## 4.3 ANOTHER STANDARDS WAR IN THE TOP LAYERS

If interoperability seems difficult to achieve in the bottom layers, certain stakeholders appear to be positioning themselves in the top layers to structure the market at the applications level, erasing disparities in the physical layers. These practices adopt one of two systems, either through collective governance or around a single player.

In the first case, it is an alliance that champions a standard. The AllSeen consortium – whose members include Qualcomm, Microsoft, LG, Panasonic and Huawei subsidiary, HiSilicon Technologies – is working to develop common communication standards using AllJoyn technology, which has the added feature of being open source.

In the second case, a single player acts as the gateway between objects. This player can play a more or less compulsory role with the makers of connected objects. The role of gateway can be relatively unobtrusive, when it serves simply as a translator. Such is the case, for instance, of the IFTTT (If This Then That) platform which has established a large number of partnerships to ensure interoperability between objects by sharing APIs: for instance with Netatmo for the smart home. Its role can, on the contrary, be very wide-reaching, as is the case with Apple which has developed the HomeKit protocol, or Google and its Weave protocol: both of these protocols are directly integrated into household objects. In this second case, the intermediary's role may also increase when data must be relayed over its platform.

## 4.4 FLUIDITY CHALLENGES

If switching from one technological solution, or from one supplier to another, typically generates switching costs, this can dampen the incentive to switch and have an impact on fluidity and on incentives to compete in the marketplace.

The meetings made it possible to identify, at this stage, three main categories of potential switching costs for the Internet of Things.

First, switching costs may be incurred when changing connectivity provider. This may include the cost of completely replacing an object, when technologies are not interoperable, or the cost of switching out SIM cards in the case of interoperable cellular technologies. With these technologies, switching operators requires the physical SIM card to be changed, which entails sizeable switching costs for the user. However technologies that make it possible to reprogram SIM cards over-the-air are being developed, hence the ability to modify the contents of the SIM card to replace one operator's security keys and IMSI with another's remotely, with no need to intervene physically on the devices. In the case of cellular networks, this solution would seem to help limit, at least partially, connectivity providers' ability to lock-in customers. Their proper development, under efficient conditions and which are open to all cellular connectivity providers, is a very current challenge.

Next, switching costs could be incurred due to a lack of transparency in the marketplace, resulting from a very limited ability to compare available information on the different existing networks, in terms of coverage and quality of service. The observed disparities, for instance, in how indicators are defined can detract from the ability to understand each supplier's advertised performance, and stifle users' desire to switch vendors.

Lastly, data or content portability systems can also generate switching costs for users, if changing systems means the total or partial loss, or at least an alteration, in user data. Future revisions to the national and European legal framework[53] should facilitate the portability of the personal data supplied by users, by allowing them to recuperate that information in a structured format, which is widely used and machine-readable.

## THE MAIN CHALLENGES

The IoT's emergence is going hand in hand with the emergence a multitude of technologies. Today, the Internet of Things is structured around a large number of walled garden ecosystems, despite standardisation initiatives.
As a result, analysing the market's openness is a two-step process. First, when the market is still only nascent, innovation trumps all, and stimulates competition, often between standards. Later, when the market is more mature, the issue of openness, via that of interoperability, will become more pressing, to ensure the welfare of users and the large-scale rollout of IoT solutions.
At this stage of the Internet of Things' deployment, openness appears to organise itself naturally, without any need to intervene in a way that could hamper innovation. However, it is important to remain attentive to the overall level of openness on the Internet of Things, as a lack of openness could handicap the market's development and create regulatory problems if it results in users being locked in.

[53] Article 48 of the Digital Republic Act and Article 20 of Regulation 2016/679 of 27 April 2016, referred to as the General Data Protection Regulation, which will come into effect in May 2018.

# 5 TRUST AT THE HEART OF THE INTERNET OF THINGS

The Internet of Things is at the core of business models based on producing, supplying and utilising data. The meetings with stakeholders confirmed the role that these data play in the development of IoT ecosystems: if no trust is established amongst consumers and the companies that produce data, the Internet of Things will only be adopted on a limited scale.

This trust can be broken down into several facets, which will be explored in more detail below, and include:

1. Trust in the accuracy, reliability and integrity of the data being exchanged;
2. Trust in the data's protection and in their processing, which often occurs in a centralised fashion;
3. Trust in the security, resilience and performance of connected objects and the networks that underpin them.

## 5.1 DATA'S IMPORTANT ROLE

Applications based on collecting and processing data represent a tremendous opportunity for the future, whether in saving lives thanks to e-Health systems that automatically alert emergency services, or having the ability to optimise the management of traffic on the roads or energy supply across a city in real time.

Data constitute the ecosystem's raw material. Whether personal data[54], data from an enterprise or a local authority, trust is a major challenge that will determine whether users adopt the Internet of Things.

### 5.1.1 BUSINESSES' OWNERSHIP OF DATA AND PROTECTING PRIVACY

For IoT market players, data ownership, integrity and confidentiality are often held up as key imperatives for establishing trust across the entire value chain.

#### Enterprises and data ownership, utilisation and monetisation

With the advent of the Internet of Things, enterprises will become producers of unprecedented volumes of data, whether extracted from objects dedicated to their own means of production, or from B2B, B2B2C or B2C finished products. While the business models associated with the Internet of Things will be in large part B2B and B2B2C, the ownership of the data (aside from personal ones) – and particularly technical and commercial data – produced by enterprises, as well as the rights of use attached to them, are not governed by the same laws as physical people. The IoT's ubiquity in all businesses will also depend on trust. It is vital to ensure that businesses, including those that have limited negotiating power with their IoT suppliers, remain the owners of the non personal data they

[54] Personal data means any information relating to an identified or identifiable natural person, or who can be identified directly or indirectly. Article 2 of the Data Protection Act (*Loi "informatique et libertés"*).

produce, and that they have they ability to make them available in a secure contractual and legal framework.

### Personal data: responsibilities with respect to how they are processed and individual rights

Regarding personal data, the main problem posed by recent IoT developments concerns individuals' ability to have actual control over the data that pertain to them. It can be complicated to provide users with clear information on the data collection process, and the data's destination if the objects do not have a screen.

In addition to problems tied to the sensitive nature of certain data (e.g. those relating to health), certain sensors or connected objects produce a new kind of data that are on the (fuzzy) borderline between health and well-being. Pertaining to a person's body or immediate environment, these data – even the apparently most innocuous ones – can reveal intimate details about their lives.

First, the data being collected in this manner have never been collected on such a scale or by this type of company. For instance, there has never been a database of the number of steps taken by, or a weight curve for thousands of people over several years, controlled by private sector players. On these points, European data protection regulation recognises widespread acceptance of health-related data.

Second, big data creates the ability to cross-reference many different types of data, which could seem innocuous when taken separately, but the correlation of which could make it possible to deduce trends or behaviours that can reflect users' private lives. The issue here is not only protecting personal data as such, but also the interconnections between the different databases: this point will be addressed further on.

## 5.1.2 DESTINATION AND SECONDARY USE OF DATA

In a situation where the rate at which data are collected is intensifying, the type of data being captured and the associated challenges vary depending on whether the process is taking place close to the person, to their body (wearable), how the data are used (quantified self), the immediate environment (home automation) or, on the contrary, more distant environments over which the person, in theory, has less control (connected cart, smart city). It is essential that users have the ability to be informed when they are likely to be involved in different data capture processes (type of data collected, processing time, the data's destination, etc.).

The aggregation and processing of data culled from disparate sources is at the very core of the Internet of Things. One major source of concern is the potential ability to stray from the original purpose of the collected data. Individuals provide information about themselves for a specific purpose: these data must not, for instance, be kept in an identifying format once they are no longer needed. The plethora of data attached to a user may well generate a secondary application that is far removed from their original purpose. This may include deducing intimate information from apparently innocuous data (e.g. a person's physical condition based on the number of steps she or he takes every day), or enabling the ability to profile people by cross-referencing initially isolated pieces of information.

Questions thus emerge over the transparency of, and ultimate use that is made of data, the methods for reusing them and possible transfers of the data, as do questions over the anonymisation methods that may be put into place to limit users' exposure. The General Data Protection Regulation[55] introduces the notions of data protection by design, data protection by default and data protection impact assessment. These general provisions, which pertain notably to IoT industry players, will come into effect on 25 May 2018.

## 5.2 COMPLEX SECURITY CHALLENGES THAT ARE STILL DIFFICULT FOR STAKEHOLDERS TO GRASP

The meetings revealed an uneven and only partial understanding of the IT security issues surrounding connected objects. The measures taken to secure objects, networks and data storage methods may not be strong enough compared to the risks to which users are exposed. Some objects content themselves with default configurations, which leave them vulnerable to hackers. But security challenges can differ depending on the application. The same degree of security will not be required for a temperature sensor and an insulin pump, for instance. Restrictions tied to users' computing and interface resources do not encourage the safeguarding of objects, or the deployment of possible updates, nor do those resulting from products' short design cycles.

A connected object must be seen as the tip of the iceberg of a complete information system that includes the collection, processing, storage and restitution of information generated by these objects, but also the management and administration of the objects and the system. Several security-related factors need to be taken into account for a connected object:

- Its function: moisture sensor for crops, a wearable, a smart grid element, a self-driving car, industrial process automation system, etc.;
- Its destination: consumer object or designed for business purposes;
- Its capacities: simple sensor or an object likely to perform processing or receive instructions;
- Its connection mode: directly to an electronic communications operator's network through an intermediate device (network box, smartphone, smart city equipment), over a dedicated network, possibly low speed and which may or may not be connected to an operator's network through a technical gateway, etc.;
- Its possible interaction with other connected objects;
- The type of information it handles: sensitive, personal data, medical data;
- The object's ownership model: the user may rent or own the object, or merely subscribe to a service;
- The reuse of the embedded system building blocks, widely used or not.

[55] Articles 25 and 35 of (EU) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, published on 4 May 2016 and repealing Directive 95/46/EC: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

All of these risks need to be analysed systematically, and broken down at the object level: a compromised connected object can in turn contribute to compromising the network on which it relies, or that of other information systems. The risks to be taken into consideration are those that are typically covered by risk assessments performed for information systems' security:

- Availability-related risks*:* the intentional or unintentional compromise of a connected object by malicious code can make it inaccessible to its user or its use for malicious purposes, for instance to incorporate the object into a network designed to provoke distributed denial of service (DDoS) attacks, and so impair the availability of other IT resources;
- Confidentiality-related risks: the information transmitted by a connected object can be intercepted during the collection, transmission, processing or storage process, the object's functions can be diverted from their original purpose (e.g. a microphone used to answer calls could, for instance, be used to eavesdrop on the object's environment);
- Integrity and authenticity-related risks: compromising a computer system can alter how the object operates, alter its functions, its trigger conditions or the information transmitted.

These risks need to be taken into account during the connected object's entire lifespan, and keep pace with changing threats. So maintaining security is as important as building security into the object's initial design and development. Failing to take IT security sufficiently into account during the design, development or use of connected objects can have serious consequences: loss of human life, violation of privacy or property, loss of competitiveness, disturbance of daily lives, breaches of security or national defence. These challenges must be considered with respect to the object's criticality, to achieve the right balance between the need for security and implementation costs. To give an example, the risks surrounding a temperature sensor are clearly not the same as those attached to an autonomous car. Here, the Network and Information Security (NIS[56]) directive, which is due to be transposed into law on 10 May 2018, specifies requirements in terms of security and the notification of incidents for the security of digital service providers' networks and information systems.

In addition to the issues tied to the security of the objects themselves, the security of the networks that interconnect these objects must be given utmost attention. Obligations in terms of security and resilience are governed by national law, and apply to all operators of public electronic communication networks including, when applicable, dedicated IoT network operators. The security of operator-free networks, however, in other words those that are managed directly by the user, may constitute a weak link in the security chain, as their management is handled by the user (Wi-Fi hotspot, Bluetooth, etc.). By the same token, the intelligence of a great many objects will lie solely in a sensor linked to a unique identifier

[56] Article 16 of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

(e.g. NFC or RFID). They will have very limited authentication means, which could pose a problem in terms of the integrity of the collected data. In these types of circumstances, the question of the objects' security remains to be addressed by the makers of connected objects and the services associated with them.

### THE MAIN CHALLENGES

The IoT's adoption will be shaped by the ability to secure the trust of users and data producers.

Users, which include consumers, businesses and local authorities, need to be able to retain control over the data that pertain to them. It is also vital to ensure transparency with users to avoid an unknown, secondary use of the data that is outside the scope of the initial purpose for which the data were supplied.

The security of objects and of the networks is another essential ingredient in establishing trust. The degree of security required needs to be measured with respect to the criticality of the object in question and the data it collects, to achieve the right balance between the need for security and implementation costs. The General Data Protection Regulation and the NIS directive – which will come into effect in May 2018 and expected to be transposed into national law – will provide a clearer framework for data protection and network security matters.

## 6 A TRANSITION PERIOD FOR IOT STAKEHOLDERS

Several user categories will benefit from the Internet of Things:

- Enterprises, whose business processes will be modernised and their production and logistics tools optimised; they will have a better understanding of their products' lifecycle, and could be brought to rethink their business model;
- Local authorities, and regions in general, which will incorporate digital technologies in traditional city planning initiatives, new urban services, economic development and citizen-participation schemes;
- Individuals who will incorporate a multitude of connected objects into their daily lives;
- The different players along the IoT supply chain, and particularly the manufacturers of objects and modules, equipment suppliers, operators and application providers that will seize the Internet of Things as an opportunity to develop their business, products and services.

### 6.1 THE IMPORTANCE OF CONTINUOUS DIALOGUE BETWEEN PUBLIC AUTHORITIES AND IOT INDUSTRY PLAYERS

The period devoted to meeting with stakeholders underscored the desire for ongoing dialogue between public authorities and the players that are helping to build the Internet of Things. The process that Arcep and its partners initiated for this purpose was very well received. There are two aspects in particular to this process:

- the dialogue with public authorities over the regulatory framework that applies to new uses based on Internet of Things technologies;
- and networking national and European stakeholders involved in the IoT value chain, with a focus on competitiveness and supporting the sector.

This first dialogue between Arcep, its partners and the companies that attended the meetings helped shed light on the regulatory framework's lack of clarity. New uses (connected cars, drones, connected health, industry 4.0, smart grid, smart city, etc.) to emerge from the Internet of Things affect a great many sectors, and are at the intersection of several regulations – data privacy, electronic communications, including net neutrality, platforms' good faith, and other sector-specific regulations that are hard for some players to fully grasp. Market players are calling for ongoing dialogue between public authorities and the entire ecosystem, to clarify the perimeters of the regulatory environment to which IoT solutions are subject, without necessarily moving towards the implementation of a dedicated framework, as regulation that is introduced too hastily runs the risk of hampering the deployment of the still only nascent Internet of Things.

In addition to establishing a dialogue with public authorities, the meetings also confirmed the need to bring together players along the value chain, to engage in a dialogue amongst themselves. Initially, by encouraging them to share their experience on issues such as security or interoperability, to help the players get a handle on the different challenges surrounding connected objects and the networks on which they rely. Next, some of the companies at the meetings also expressed a desire for simpler and accelerated relationships between start-ups, SMEs and large corporations to initiate and encourage partnerships between enterprises, in which local authorities can also be involved, to boost the Internet of Things in France. This is a role that is currently played by schemes such as the French Tech initiative and business clusters, by simplifying interactions, making it easier for companies to make contact with one another and encouraging meetings, but also by helping French businesses to expand their footprint in global markets, as proven by the presence of French connected objects companies at the Consumer Electronics Show (CES), under the French Tech banner.

## 6.2 THE DESIRE FOR CONCRETE IOT APPLICATIONS

If the expected upsurge of the Internet of Things does not yet appear to be a reality, it is because market players prefer to focus initially on proofs of concept rather than large-scale applications. The meetings with stakeholders revealed that this trial period is coming to a close, and that they are beginning to roll out actual services for businesses, local authorities and consumers, and entering into an industrialisation stage for large-scale offerings.

Businesses are the first IoT users to deploy the first concrete applications. While a great many of the solutions being sold to businesses are data collection or smart metering on a local scale, some are targeting more complex applications for the near future, such as remote control, before planning for an industrial rollout of their solutions. Consumers are also taking advantage of concrete IoT applications, while a number of local authorities, if they have not deployed their own solutions, are very open to industry demonstrators to test the different configurations and study how new regional services can be organised. These trials provide local authorities which an opportunity to define the requirements (security, confidentiality, etc.) they want to incorporate into the services whose management they will outsource.

## 6.3 FRANCE AND EUROPE'S INTERNATIONAL POSITIONING

In addition to having the right regulatory framework that allows applications to develop and be deployed, for the stakeholders that were interviewed it is important that public authorities enable national and European players involved in the IoT value chain to network with one another, in the interests of competitiveness and to foster an industrial cluster.

The IoT's deployment extends beyond France's borders, and is unfolding on the European and international stage. The players are asking public authorities to help secure a strong position for France and Europe amongst Internet of Things actors, compared to China and the United States, and to introduce a harmonised regulatory framework across Europe.

As part of the work being done by the New Industrial France initiative, the "Smart Objects" solution is helping to develop a national French strategy and create a sectoral structure, to carry out coordinated actions for developing French smart objects businesses by bringing together the interested enterprises. Work is also being done on consolidating France's position on the smart city, in connection with the Sustainable City solution.

Fostering the development of French start-ups is another challenge: they need to be given the means to finance themselves, to structure their business (in terms of marketing, HR, product line and making the most of their investment capital) and to develop their products.

European players are very present in global industrial alliances and standardisation bodies engaged in standardisation strategies for future, concrete IoT applications. Such is the case, for instance, with the LoRa Alliance whose members include European operators and global players, working to achieve greater standardisation for the Internet of Things. AFNOR[57] created the National Commission on the Internet of Things (CN IoT) in 2016, to defend French interests during ISO international projects. ETSI is also contributing in the creation of the partner-based "OneM2M"[58] project, rooted in the same model as 3GPP and dedicated to standardisation in the service layer of M2M equipment and connected objects. Regarding

[57] *Association française de normalisation*/French standardisation association.

[58] OneM2M covers a large portion of the ecosystem with partners in the area of standardisation and global industrial consortia [ARIB (Japan), ATIS (USA), CCSA (China), ETSI (Europe), TIA (USA), TSDSI (India), TTA (South Korea), TTC (Japan), Broadband Forum, CEN, CENELEC, GlobalPlatform, New Generation M2M Consortium (Japan) and Open Mobile Alliance (OMA)] along with more than 200 members.

smart cities, the National Commission on Sustainable and Resilient Development (CN ADR) addresses the issue of smart city services.

## THE MAIN CHALLENGES

The transition phase in IoT solutions' deployment is a subject that was addressed during meetings by both users – local authorities and manufacturers – as well as players on the supply side of the Internet of Things. Two distinct and complementary aspects emerged.

The main message is the need for ongoing dialogue with public authorities who must maintain contact with IoT industry stakeholders, both those helping to build it and those that are using it, including consumers, to sustain a detailed knowledge and understanding of developments as they unfold, and to ensure the clarity and suitability of the regulatory framework.

In the different but complementary interests of competitiveness and of fostering an industrial cluster, support will also be needed to enable French companies to maintain a strong position on the international stage.

# ANNEX NO.1 – LIST OF MEETINGS HELD

| MEETINGS | COMPANY/ORGANISATION |
|---|---|
| Thursday, 12 November 2015 | Actility |
| Thursday, 12 November 2015 | Intel |
| Tuesday, 17 November 2015 | Connecthings |
| Wednesday, 25 November 2015 | Commission de régulation de l'énergie (Energy regulation committee) |
| Wednesday, 25 November 2015 | IDATE |
| Wednesday, 02 December 2015 | Huawei |
| Thursday, 03 December 2015 | Numéricable-SFR |
| Tuesday, 08 December 2015 | Adeunis RF |
| Tuesday, 08 December 2015 | Polytechnique "Internet of Everything" Chair |
| Thursday, 10 December 2015 | Bluelinea |
| Thursday, 10 December 2015 | ERDF |
| Monday, 14 December 2015 | IBM |
| Thursday, 07 January 2016 | Qowisio |
| Monday, 11 January 2016 | Google |
| Wednesday, 13 January 2016 | Ericsson |
| Tuesday, 19 January 2016 | Sequans |
| Tuesday, 19 January 2016 | Optiflows |
| Wednesday, 20 January 2016 | Kerlink |
| Wednesday, 20 January 2016 | Nest |
| Thursday, 21 January 2016 | Cisco |
| Thursday, 21 January 2016 | STMicroelectronics |

| | |
|---|---|
| Tuesday, 26 January 2016 | Bouygues Telecom |
| Tuesday, 26 January 2016 | Sigfox |
| Thursday, 28 January 2016 | Qualcomm |
| Tuesday, 02 February 2016 | Sagemcom |
| Tuesday, 02 February 2016 | Legrand (construction) |
| Thursday, 11 February 2016 | Orange |
| Tuesday, 16 February 2016 | SNCF – Digital Affairs Dept. |
| Thursday, 18 February 2016 | Eutelsat |
| Thursday, 18 February 2016 | Samsung |

# ANNEX NO. 2 – WORKSHOPS HELD

| WORKSHOP | DATE | PARTICIPANTS |
|---|---|---|
| Smart industry & Transportation | Monday, 23 May 2016 | Blue Solutions |
| | | Hub One |
| | | Mission Transport Intelligents |
| | | Renault |
| | | RTE |
| | | SNCF |
| | | Thalès |
| | | Transdev |
| Smart buildings & cities | Thursday, 23 June 2016 | AFNOR |
| | | AVICCA |
| | | Enedis |
| | | Ijenko |
| | | JC Decaux |
| | | M2ocity |
| | | Nokia |
| | | Oledcomm |
| | | Sigfox |
| | | Suez |
| | | Vertical M2M |
| Connected Health | Monday, 27 June 2016 | AFNOR |
| | | Altran |
| | | ASIPS |
| | | DGCCRF |

| | | |
|---|---|---|
| | | INRIA |
| | | Korian |
| | | Medappcare |
| | | Nokia |
| | | Orange |
| | | Telecom ParisTech |

# Annex No.3 – Contributors to the public consultation that ran from 19 July au 16 September

| CONTRIBUTORS | | |
|---|---|---|
| AFNIC | Enedis | Qualcomm |
| AFNOR | Eutelsat | Qwant |
| AFNUM | Fédération française des telecoms (French telecoms Federation) | Renault |
| Airbus Defence and Space Division Space System | FIEEC | Rennes Métropole |
| Airbus DS SLC | Huawei | SFIB |
| AVICCA | Intel | SFR |
| Bouygues Energy | Mr Jean-Paul BON | Sierra Wireless |
| Bytel Objenious | La Loi des Parties | Sigfox |
| Carrefour de l'internet des objets | Mr Lionel RUDANT | Syntec numérique and the firm A Lefèvre |
| Cerema | Microsoft France | Syntec numérique cyber securité |
| Cisco | Mobivia Groupe | Syntec numérique |
| Conjonction numérique | Mr LAUNAY | Towercast |
| M. David DORVAL | Nokia | Transatel |
| EchoStar | Oracle | Verizon |
| EDF | Orange | Qualcomm |