COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 29.9.2008
SEC(2008) 2516

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Future networks and the internet

Early Challenges regarding the "Internet of Things"

{COM(2008) 594}
{SEC(2008) 2507}

TABLE OF CONTENTS

1. INTRODUCTION

The phrase "Internet of Things" heralds a vision of the future Internet[1] where connecting physical things, from banknotes to bicycles, through a network will let them take an active part in the Internet, exchanging information about themselves and their surroundings. This will give immediate access to information about the physical world and the objects in it – leading to innovative services and gains in efficiency and productivity. The productivity and efficiency improvements rendered possible by this Internet of Things and the services it will convey will definitely contribute to improvements in European living standards. So citizens and society will benefit. But there are also important policy issues, especially in the areas of privacy and data protection.

The Internet of Things lies in the future. But RFID[2], one of its key technologies, is already being deployed. Policy issues related to RFID, which must be tackled now, should give insights into the wider policy issues which the Internet of Things will bring. Section three of this document describes RFID based developments and the policy challenges they raise.

This Staff Working Document is a contribution to an important, ongoing public debate. Concerned stakeholders are invited to send comments on the issues addressed here. Concrete suggestions of possible actions or initiatives that should be taken are particularly welcome. Once these have been assessed, the Commission intends to present a Commission Communication on the Internet of Things in 2009.

2. THE INTERNET OF THINGS

The Internet has adopted many new technologies as it evolved to meet the changing needs of Industry and Society. This flexibility has been a factor in its growth, and today's Internet spans the globe and brings voice and video, data and information to billions of people. Converging fixed and wireless technologies help make the Internet a ubiquitous infrastructure, always accessible and always on, supporting a wide range of activities.

The next jump in the growth of the Internet will come from seamlessly integrating physical things into information networks. The phrase "Internet of Things" covers the overall infrastructure (hardware, software and services) supporting this networking of physical objects. And these objects will be active participants in business and information processes, exchanging data including their identities, their physical properties and information 'sensed' about their environment.

Developments in several technologies are bringing us closer to the Internet of Things. Identification technologies like RFID allow each object to have its own unique identifier (rather than one identity number for each product type, like with today's barcodes), which can be read at a distance. This allows automatic, real time identification and tracking of individual objects. Wireless sensor technologies allow objects to provide information about their environment and context – so a car tyre could warn if its pressure were too low, or if the road were icy. Smart technologies such as robotics and wearable computing will enable everyday objects to become "things that think and communicate". Nanotechnology and energy

---

[1] See http://www.future-internet.eu/home.html

[2] Radio Frequency Identification Technologies: see http://en.wikipedia.org/wiki/RFID

scavenging technologies are packing more processing power in less space, so that networked computing can be woven into the fabric of things around us. These technologies will progressively create an almost invisible infrastructure, with far-reaching capabilities organized into global systems that serve society as a whole and our information and decision-making needs in adaptive and dynamic ways.

The key feature of this new phase of the Internet will be innovation in services relying on information related to the identity, status and possibly changing location of objects. New opportunities will be created and new needs will be met, bringing about potentially disruptive business models, and new societal services that will improve the quality of life. The Internet – or the future network into which it will one day evolve – will have to deal with an increase in traffic as today's off-line objects are brought online to make industrial processes more efficient with higher degrees of productivity.

As the technologies needed for the Internet of Things become available, a wide range of applications will be developed. These can support policy in areas including transportation, environment, energy efficiency and health. Huge benefits will come not only from faster productivity growth, but also in many other ways: increasing efficiency in material handling and general logistics, efficiency in warehousing, product tracking, efficiency in data management, reducing production and handling costs, speeding the flow of assets, anti-theft and quicker recovery of stolen items, addressing counterfeiting, reducing mistakes in manufacture, immediate recall of defective products, more efficient recycling and waste management, achieving CO^2 reductions, energy efficiency, improved security of prescription medicine, and improved food safety and quality.

The first visible signs of these new developments are linked to the arrival on the market of two new technologies: RFID and NFC[3] (Near Field Communications), which promise – respectively in the fields of retail and logistics and mobile-based micro-payments – to revolutionise the way business is conducted in their areas and to create tremendous economic opportunities.

Some potential applications of these technologies are described below. Behind the simple, visible functionalities illustrated in these examples lies an invisible but complex web of networked connections and smart systems, which capture information, process it, transmit it and store it. It is these invisible elements, the way in which they are identified and are connected, the scope of their actuation capabilities, the databases where information is stored and securely consulted, the spectral properties of the communication devices etc. that raise a number of important policy challenges.

A retail example

Using a mobile phone as a credit card, a travel pass or to automatically get information from the Internet about products in a store is becoming possible. The underlying NFC technology, which allows networking over a few centimetres, is increasingly found in new mobile phones. Predicted to be in more than one billion phones by 2015, NFC should open up a large market for consumer services.

Fully automated warehouses, where items will be checked in and out and orders passed on to the suppliers automatically, may be coming soon as RFID technologies are deployed. This

[3] http://www.nfc-forum.org/home.

will improve asset management and make supply chain management more efficient and proactive. Goods will be transported from producer to consumer with less need for human intervention, and manufacturers will have a real time view on the market's needs. In this way, production and transportation needs can be adjusted dynamically, saving time and energy and being more environmentally friendly.

An e-health example

The use of RFID and sensing technologies will allow real time monitoring of patients, leading to earlier diagnosis. Vital parameters such as heart rate, breathing rate and blood pressure can be measured by lightweight, intelligent sensors, worn by the patient without interfering with daily activities. These wearable networked monitoring systems can acquire, process and transmit data on multiple health parameters, letting medical professionals make better informed decisions. Automatic alerts can be immediately sent to medical staff to warn of deterioration in patients' condition.

A medication example

Smart networked devices could help address the challenges of our ageing society. For instance, using tags on pharmaceutical products could allow monitoring to check that an ageing patient takes the right mix of drugs. Networked sensors could be used to help and monitor the behaviour of people with special needs; e.g. sensors might automatically select the right shower temperature, thus avoiding the risk of scalding, or could report unexpected behaviour that might require medical intervention.

An energy example

The use of networked temperature and lighting sensors will allow intelligent houses to reduce energy consumption without compromising comfort, by dynamically adjusting room temperature and lighting conditions. Remote monitoring of home or office energy consumption will allow for better planning of energy needs.

An environment example

The Internet of Things will have a profound effect on the way traffic, weather, particles in the air, water pollution, and the environment can be monitored and statistics collected.

3. RFID APPLICATIONS AS A FIRST EXAMPLE OF THE INTERNET OF THINGS

As indicated in section two, a new series of developments is leading to the situation described by the phrase "Internet of Things". However, at present we are confronted with some new policy challenges resulting from the implementation of one specific technology – RFID – and its applications.

3.1 The Existing Architecture of RFID Applications

To help identify the main policy challenges, this section describes how current RFID applications operate and what their evolution in the near future – 5 years or so – is likely to be.

Looking at the development of the RFID applications, one can notice that in the past few years RFID has been especially successful in more intelligent applications (smart cards) used in public domain settings such as identity cards and public transport. Also the logistic and retail sector has, so far, been a main driver of the RFID application architecture. RFID tags, associated with objects or goods, are used to follow them through the retail value chain. The tags themselves do not store much information; essentially each tag just provides a unique identifier. This can be used to look up additional information about the product from a large, distributed network of databases, potentially located around the globe.

As an illustration, consider the different steps a product goes through in moving from manufacturer to retailer. The manufacturer ships the product in bulk to a distributor, who dispatches it to a number of retailers, possibly located in other countries. If it crosses the borders of the European Union, then customs must be cleared. Each actor in this chain has a database, used to record the events happening to each product. The information in these databases can be private, or might be available to other actors in the value chain, depending on the chosen access policies.

The architecture that makes possible the gathering of this information, its transmission and storage, as well as the search for particular events and particular products (including their tracking) is, to a large extent, based on what is referred to as an overlay architecture of the Internet and as such uses many of the Internet's core features. It is built around:

- A naming system, needed to define and address an object or a sensor, possibly complemented with information related to the object;

- An event reporting and storage system used to register the information related to a change occurring in the real world, either to the object or as monitored by a sensor/embedded processor. Several storage systems may exist under control of different entities depending on the number of players that participate in the overall value chain;

- A look up and routing system, enabling the linking of an object/sensor name with the address of the database where event information pertaining to that object/sensor is located;

- A discovery system, enabling the discovery within the accessed database of the relevant event information that corresponds to the originating query and to the rights associated to the authenticated query originator.

3.2 Policy Challenges in RFID Architectures

Drawing on the experience gained from the development of RFID applications in recent years, a number of policy challenges needing consideration can be identified:

- Security;

- Privacy and Data protection;

- Control of Critical Global Resources and Subsidiarity;

- Identity Management, Naming and Interoperability;

- Fostering Innovation;

- Spectrum;
- Standardisation.

3.2.1 Security

RFID applications use the existing Internet, and therefore, are subject to the security issues confronting it – SPAM, Denial of Service attacks, identity theft, etc. The user perception of new technologies will require security regimes that are commensurate with the sensitivity of the transactions supported by these technologies. Only if the Internet of Things can earn the trust of its users, over time larger deployment will take place.

Attention must be given to potential new security aspects, as specific new issues are likely to emerge:

- To keep data confidential, reliable solutions are needed to restrict access to information stored on tags associated with objects.
- Information exchanged through the Internet or other networks must be protected against unauthorised access or manipulation, perhaps using end-to-end encryption[4] and the use of digital signatures.
- Potential tracking, identification or profiling of an individual through the aggregation of heterogeneous data, possibly collected from different sources, constituting "personal data" should be avoided for the sake of consumer protection.

Solutions to these confidentiality issues must not limit the interoperability of the participating systems. Achieving this interoperability will require a set of open, interoperable and publicly accessible standards.

In particular, it will be important to address two issues:

(1) The authentication of queries.

In RFID applications, queries can be used to retrieve information from databases or directly from the objects, devices and sensors at the 'edge' of the network. To prevent unauthorised or malicious queries, query originators must be identified through strong authentication mechanisms.

A problem here is the lack of these mechanisms in the current Internet. For example the Domain Name System (DNS), a lookup service giving the network address corresponding to a computer name, does not authenticate the client, the server or the information provided. If DNS is reused in RFID applications, information about a citizen’s assets – or those of an organisation – could potentially be acquired by illicit means.

(2) The integrity of RFID applications architecture

[4] End-to-end encryption refers to continuous protection of the confidentiality and integrity of transmitted information by encrypting it at the origin and decrypting at its destination

How well will the proposed architecture for most RFID applications cope with attack? For example, hackers on the Internet can trick DNS into giving the wrong network address for a computer name. This lets them redirect queries of, say, a bank's website to their own system, and defraud users. Such an attack on an RFID application could let an attacker return his 'own' information about an object, device or sensor, with potentially damaging consequences for the real owner. This means that strong authentication mechanisms are needed from the service or information provider.

And attention should be given to the fact that the risk levels of today differ from those that will challenge the Internet of Things of tomorrow because also the technology available to attackers enhances.

3.2.2 Privacy and Data Protection

The development of RFID applications will allow more extensive and distributed data collection and processing. This leads to new challenges in protecting privacy and data to avoid, for example, the possibility of tracking users without their knowledge. Privacy and security friendly technologies must be designed to ensure that applications respect the fundamental right to privacy and the data protection legislation. The Commission will soon adopt a recommendation on the implementation of the privacy, data protection and information security principles in applications supported by RFID.

While regulation is in place in Europe for the protection of personal data, the application of this regulation to new technological developments poses practical questions and requires more detailed guidance. The objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible, together with the principles of proportionality, purpose limitation and transparency, should serve as a starting point for such guidance. Self-regulation can be an effective tool to provide clarification when practical questions arise, as well as to enhance privacy in a given context. However, specific legislation should not be excluded where self-regulation or interpretation prove insufficient. The Commission will adopt a Communication on Privacy and Trust in the ubiquitous information society, which will address the future challenges in the area of privacy.

From a public policy perspective, the following aspects should be considered, among others:

- What requirements will public authorities have for the authentication of users accessing their data or event repositories?

- What requirements will public actors have for the identity of the service or data providers for their RFID applications?

- The need for a harmonised approach to authentication requirements across the Union.

- Considerations of public policy principles associated to data privacy, information consent, etc. in the context of the first instances of the development of RFID applications where developments are driven by private interests.

- The potential for identification or profiling of individuals through the aggregation of heterogeneous data, collected from different sources, constituting "personal data", in relation to consumer protection.

3.2.3 Control of Critical Global Resources and Subsidiarity

The operation of RFID applications will need governance schemes which are appropriate and proportional to the scale of the network, and at the same time scalable in order to achieve the operational efficiency of a single centralised architecture. The full set of governance rules might not be needed for localised, independent networks. For example, the governance requirements of an isolated household system managing heating, lighting and entertainment are likely to be different from a network which links international logistical chains involving many different firms, or those of a town centre security and surveillance system in which personal identification and processing of personal information may be involved.

Global naming and routing control architectures are currently in place for RFID applications. Control of look up and discovery services is global and centralised, without delegation to national or regional levels. Concerns have been expressed that a fully centralised critical resource control may not be appropriate and that some form of resource control at national or regional level should rather be the rule. Another concern is that reliance on a single, out-of-country service provider, possibly under non-European jurisdiction, may not be compatible with business continuity needs, especially considering that overly resource centralisation naturally creates single point failure. Therefore, over-centralisation of critical RFID application resources raises potential concerns both from sovereignty and subsidiarity aspects and from the operational business viewpoint.

A consultation involving Member States, national data protection authorities and the private sector should be planned in order to define the minimum level of visibility and control of critical resources that must be provided to national authorities for safeguarding public policy interests. These include economic interests (how far the retained architectures are compatible with business transaction confidentiality), competition rules (how far the retained architectures prevent other architectures to emerge), and protection of personal data and privacy (how far the retained architectures are compatible with user data confidentiality and access restricted to the right party only).

RFID applications use the today's Internet, and this reinforces the need to ensure openness, security, access, diversity and adequate management of critical Internet resources, identified by policy makers in the context of the Internet Governance Forum.

3.2.4 Identity Management, Naming and Interoperability Requirements

Identity management and naming are critical parts of the proposed RFID application architecture. Correct definition, specification and implementation will drive their economic potential and their adherence to public policy principles.

Key issues here are identity allocation, authentication, access control, privacy, data protection and security, and the capability to generate audit trails. Just as individuals may have multiple digital identities, so will devices or objects, depending on their context, location and movements.

Furthermore, the current proliferation of identity codes such as 2D barcodes, alphanumeric codes, hybrid codes, and RFID tags (both passive and active), means that attention must be paid to the identification technologies themselves.

It may be necessary to create different name spaces to meet the specific demands of different applications, in which case questions arise on the interoperability requirements and the design

and control of gateways between different name spaces. This is already happening with various regions, notably Japan, which have defined their 'local' variant of identity and naming functionalities.

This means that Standardisation Organisations (SDOs) should be issued a mandate to define, with the support of public entities, the functional requirements that identity and naming schemes should respect, in order to comply with principles of general interest. SDOs should also define the global interoperability requirements across identity/naming schemes.

3.2.5 Fostering Innovation

There is a need to ensure adequate competition at all levels in the development of the architecture for RFID applications. As with all other areas of the digital economy, competition is needed to facilitate consumer choice, generate competitive pricing and provide sufficient incentives for innovation.

In particular, open architectures should be defined for distributed software and service platforms (middleware) that are required to "control transactions and events". These software architectures are at the core of the potential innovation, and their control and degree of openness will, to a large extent, influence the access of new actors to this emerging market. Openness should become a driving requirement, to let smaller actors access this global market without any unreasonable IPR constraints. This is in particular crucial to offer prospect of innovative SME development in Europe, which can also capitalise on the important academic expertise available in Europe.

Similarly, at device level, the services accessible from devices or sensors should be governed by architectures with open interfaces, to facilitate use of the device across multiple applications and enable economies of scale and of scope, whilst favouring adoption by older or people with disabilities.

Innovation-friendliness also depends on the policies applied to govern critical control resources. As an example, it is today widely accepted that a key success factor of the Internet was that centralised DNS transactions are free. There are no guarantees that this would be true for an Object Naming System built around a centrally controlled look up service, especially if under private management outside public control.

Opportunities for market entry might help to offset a tendency for a de facto monopoly to arise from a centralised architecture. However, if this happens, interoperability across multiple control systems would need to be ensured to maintain their global nature. This could be facilitated through open standards.

As innovation is directly related to competition, it is necessary to avoid architectural approaches that:

- Favour a de facto monopolistic operation of one single system world-wide;
- Lead to a multiplicity of incompatible systems, with 'RFID islands' developing, probably structured across economic/application sectors;
- Lead to closed proprietary standards with high IPR access costs.

Facilitating transparent and non-discriminatory conditions is essential to ensure European industry can offer competitive and innovative services and gain market share in what is expected to be a significant (and lucrative) global market. A 'true' market – based on open standards and interoperable interfaces – at all levels is hence necessary. This will in particular provide appropriate entry conditions for small- and medium-sized enterprises (particularly in the enterprise software market and the upcoming Internet of Things services).

3.2.6 Spectrum

The Internet of Things will, to a large extent, be based on the wireless connectivity of tagged objects, sensors and other smart devices, and the assessment of future spectrum requirements for these devices is important.

The European Commission has already harmonised several spectrum bands used by 'IoT-devices'. The SRD Decision is an example of such harmonisation (Commission Decision 2006/771/EC as amended by Decision 2008/432/EC), it harmonises various frequency ranges used by various 'short-range devices' which are likely to be considered 'IoT-devices'. It is the intention of the Commission to regularly update this Decision in response to market developments[5]. The Radio Spectrum Decision (676/2002/EC) provides the basis for these actions. The need for additional harmonised spectrum, as a result of technological and market developments, can be addressed under the existing policy mechanisms if such use of spectrum is considered to be of optimal benefit to the European economy. These policy mechanisms can support the availability of harmonised spectrum for the various wireless devices that will interconnect through the Internet.

To the extent that spectrum for 'IoT devices' falls within the scope of the regulatory framework for electronic communications services it will benefit from the increase in flexibility and increasing ease of access as currently proposed under the review of that framework, including the development of pan-European IoT applications.

The necessity for and possibility of globally harmonised spectrum for 'IoT-devices' shall also be considered in bilateral contacts with the EU's trading partners and through the International Telecommunications Union.

3.2.7 Standardisation

A more European-centric approach to the development of standards for RFID-based applications would be beneficial to all European stakeholders and in particular those who are closest to its technology and service dimensions. Standards are vital to European competitiveness as they will provide a level playing field for industry, enabling companies and service providers to compete in European and global markets.

The European Commission, notably through its R&D programme, has already launched a number of actions which allow for improved coordination and provide a forum for input to standards bodies. While much is being done, worldwide efforts are still quite fragmented and decisions are sometimes taken by ad-hoc organisations which do not necessarily follow the principles guiding EU standards organisations.

---

[5] Notably via the permanent Mandate of the Commission to CEPT regarding the annual update of the technical annex of the Commission Decision on the technical harmonisation of radio spectrum for use by Short Range Devices (5 July 2006).

Matters that require concrete attention by standards bodies include all networking layers of the future Internet of Things infrastructure, including the functionality and interfaces for Internet of Things devices, data formats and information codes, naming, addressing and identification issues, middleware aspects and interoperability needs meeting the requirements of the global market place. Interoperability is a particularly crucial dimension in that it contributes to the provisioning of affordable end-to-end solutions while reducing the costs of application integration.

Finally, debates and decisions on standardisation matters concerning RFID-based applications must also take place in global settings. This requires close cooperation between regional standards bodies, supported by policy debates and international dialogues with other world regions.

4. THE POLICY CHALLENGES OF THE INTERNET OF THINGS

As we move towards the Internet of Things we will see increases in the number and type of objects being networked, in the types of information being exchanged and in the number and complexity of the underlying technologies. The policy challenges raised by today's RFID based applications will remain, and the policy responses to them will need to be revised for the greater scale and scope of the Internet of Things.

In some cases, moving to the Internet of Things will change not just the scale but also the nature of the policy challenge. For example, the issues of privacy and data protection will take on particular importance in the Internet of Things. To take advantage of the convenience offered, individuals are likely to put more and more of their devices online. Combining the information from all of these devices could allow a complete and invasive picture of an individual to be drawn. It becomes important to ensure that the fundamental rights of individuals/citizens to privacy and data protection, as enshrined in European law, are adequately captured in the design and functioning of the Internet of Things. Therefore, it is necessary that appropriate policies supporting the development of the Internet of Things are conceived to provide the stakeholders and competitors in this new market place, with a predictable level playing field.

Policy issues to be discussed include:

- How to build awareness and trigger action among all stakeholders (consumers, companies, tag and reader manufacturers, developers, researchers, technicians, and indeed all parties intending to make use of Internet of Things technologies)?

- How to make Internet of Things technologies and services affordable, understandable, and accessible to all, in particular to people with special needs or disabilities?

- How to ensure that the fundamental rights of individuals to privacy, protection of personal data and consumer protection, enshrined in European legislation, are adequately captured in the design and functioning of the Internet of Things?

- With a greater deployment of the technology, additional policy issues are likely to appear:

- More electronic materials will become embedded in a range of every day objects and materials and as an example some materials that are currently either biodegradable or easily recyclable can become problematic.

- Assessment should be made if the radiation associated with a continuous exposure to a myriad of highly loaded wireless networks could imply health risks. In this the EU pleads for adopting the precautionary principle[6]

[6] See http://www.rfidconsultation.eu/41/38/264.html

ANNEX I - LIKELY EVOLUTION OF RFID ARCHITECTURES

In the previous sections we looked at issues related to the early development of the aspect of the Internet of Things represented by RFID-based applications. However both the spread of RFID technology beyond the logistic and retail sector, as well as technological progress, will probably result in a number of changes to the currently proposed architecture. In this regard, the following elements can to be noted:

- The tags associated to products, which today are largely passive (e.g. RFID) will progressively be more intelligent and complemented by active tags. As a result, event information may be dynamically stored in the tag itself. This could, for instance, be the case of a tag (such as a smart embedded processor with storage capabilities) which controls the status of a particular element in a vehicle and stores information for maintenance purposes.

- Another scenario predicted in some reports[7] is two separate tracks of development: one into the direction of the very cheap item-level tag and the other in the direction of sophisticated multi-purpose tags putting constraints on the functionality that can be requested, e.g. to enhance security, for these low end devices.

- Sensors and actuators will become addressable and capable of executing service requests. This technological progress will lead to the development of a variety of ad-hoc networks including body-area networks, home automation networks and industrial networks, serving applications ranging from home entertainment and automation to early warning systems for environmental applications.

- The event information which today is stored in databases controlled by professional organisations (the manufacturer of a good, the shipping company, the customs control service, the retailer etc.) may in the future be stored under direct end user control. This means that the field of application of 'Internet of Things related technologies' moves from the professional domain to the domain of end users and citizens, opening the perspective of an 'Internet of My Things' which would mirror the emergence of private 'intranets'.

- A multiplicity of services will be composed from global sources: as an example, an event pertaining to an object could be linked to the location (GPS or Galileo coupling), and generate a command to a local device. So usage scenarios will use multiple sources of aggregated services which might in turn result in a need for increased levels of openness and stronger interoperability requirements.

---

[7] See for an overview of arguments Maghiros, I. Rotter, P, Van Lieshout, M (2007). *RFID-Technologies: Emerging Issues, Challenges and Policy Options*, EN-22770. Sevilla: IPTS-JRC; De Panizza, A., Rotter, P., Lindmark, S. (in press). RFID Item – Techno-economic analysis, Interim report, Sevilla: IPTS-JRC. To be published; Rotter, P. De Panizza, A., Lindmark, S. (in press). RFID for Mass Transportation – Techno-economic analysis, Interim Report, Sevilla: IPTS-JRC, to be published.

ANNEX II - RESEARCH AND INNOVATION FOR THE INTERNET OF THINGS

R&D is by nature a medium- to long-term issue and, as such, should not be covered in this Staff Working Paper. However, for completeness reasons, some mention should be made of the actions and initiatives within the European Union Framework Programmes which are related to the Internet of Things.

Regarding the longer term aspects of the Internet of Things itself, a number of issues are considered in research activities at European level:

- Edge technologies. Further research and development is needed on enabling technologies for sensors and actuators, passive/active identification tags, embedded systems etc. that are attached to real-world objects and that enable them to be networked and participate in Internet of Things applications.

- Networking technologies. Research must also concentrate on fixed, mobile, wired and wireless networks allowing highly available bi-directional communication on different levels, i.e. between real world objects, applications and services that offer functionalities specific to the Internet of Things. Massively distributed computing and storage on objects will raise huge privacy and data protection issues (the data will be stored in the "ambient intelligence" and not at a single and well identified location) but also offer very interesting capabilities, e.g. for reducing energy consumption.

- Middleware systems. Scalable, secure and semantically enriched service-oriented middleware architectures play a key role in putting real world data into the context of various Internet applications. Research has to concentrate on how to bridge gaps that occur due to the usage of heterogeneous device, network, sensors and other technologies.

- Platform services that run in the background have to support a superior management of all involved technical components (i.e. trillions of loosely coupled devices!) in an integrated way, ensuring scalability, high availability, and the safe and secure execution of the requested functionality.

For some applications, a high level of security and perhaps even cryptographic techniques may be needed while for others authentication may be the only requirement. Trade-offs between cost, speed of execution, quality of service and overall exposure to risks need to be considered.

Object mobility renders the security issue more complex. For instance, a high level of security may be needed in one location but not another (e.g. no encryption may be required for someone's communications within his/her company, where the environment is safe, whereas they must be protected at his/her home or in public spaces). This should be determined according to the object's security policy, the environment it is in, and the security policy of the devices it communicates with. Security of the information itself needs to be accounted for, particularly when information flows are of a global nature.

Further to the technical questions above, research test-beds and experimental facilities must be envisaged in order to accelerate the orderly adoption of the Internet of Things in various application domains, notably in those areas where there is a strong public service aspect. This includes the analysis of current and future demands and trends in various industries, public

and governmental organisations, etc, as a necessary step towards the most future proof solutions:

For the application domains of the Internet of Things, a clear role is given to actions at European level with the joint participation and efforts of Member States. It is felt that a critical mass of resources and efforts must be brought together to tackle applications in Energy, Health, Environment, Transport and Safety amongst others.

The Competitiveness and Innovation Programme (CIP) creates opportunities to set in place Europe-wide thematic networks and pilot actions with the support of Member States. Such actions will pave the way towards the development of applications in domains outside the commercial sphere, including for instance environment monitoring, forestry management, and waste management.

Stronger integration and coordination of current and future research and innovation efforts would greatly facilitate Europe's role in shaping the Internet of Things and its future deployment. Creating the right synergies and assembling a critical mass of resources is needed in order to assess what actions will accelerate the diffusion of the Internet of Things and increase its social acceptance.

Measures accompanying research and innovation efforts should be considered to allow better assessment of the impact of the Internet of Things at global and industrial level, as well as at the organisational level. Actions aiming at fostering research and innovation cooperation and partnerships between Europe and other world regions will need to be envisaged as a means to support the early identification of global requirements, where needed, notably as regards naming and addressing, spectrum designations and overall networking design considerations.