Internet of Things in 2020

A ROADMAP FOR THE FUTURE

INFSO D.4 NETWORKED ENTERPRISE & RFID
INFSO G.2 MICRO & NANOSYSTEMS

in co-operation with the

RFID WORKING GROUP OF THE EUROPEAN TECHNOLOGY PLATFORM ON SMART SYSTEMS INTEGRATION (EPOSS)

05 September, 2008

European Commission
Information Society and Media

EPoSS
European Technology Platform on Smart Systems Integration

"We have a clear vision – to create a world where every object - from jumbo jets to sewing needles – is linked to the Internet. Compelling as this vision is, it is only achievable if this system is adopted by everyone everywhere – Success will be nothing less than global adoption".

Helen Duce

Foreword

In the course of the year 2007 the Information Society and Media Directorate-general of the European Commission (DG INFSO) and the European Technology Platform on Smart Systems Integration (EPoSS) followed convergent paths – the former towards a common policy framework for Radio Frequency Identification (RFID) and the latter towards smart systems that are able to take over complex human perceptive and cognitive functions and frequently act unnoticeably in the background. Both initiatives met at a crossroads – the "Internet of Things". On one hand, the Commission, in association with many sector actors, established that RFID was one major vector towards embedded intelligence in things making them smarter that is able to do more than they initially promised. On the other hand, work in EPoSS demonstrated that RFID technology could provide added value to smart systems integration in logistics and many other industrial sectors. Using RFID technology, everyday objects will become 'smart objects' – elderly and disabled people will be supported by intelligent devices; the close tracking and monitoring of goods in the food chain will improve food safety; smart industrial goods will store information about their components and their use; waste disposal management will be switched from today's mass-oriented approach to a more efficient individual recycling process.

At a time when the notion of 'Internet of Things' was still rather undefined and debated mostly in academic circles, DG INFSO and EPoSS realised that they were sharing the same vision of an Internet of Things as the result of several shifts – from systems to software-based services, from passive RFID tags to active RFID tags and wireless sensors, to the mythic Semantic Web, from identification to real-time 'sense and response', from exposure to privacy, and from protection to trust. The rise of ubiquitous services and the integration of the network within the objects of everyday life – each of us is permanently surrounded by some 4000 objects – constitute the next step of the development of the Internet. This evolution towards the Internet of Things raises tremendous opportunities for Europe's industry as Internet of Things related technologies have the potential to drastically transform the sector of production and services altogether, while it also unveils new policy challenges, especially privacy, trust, security, governance, and therefore highlights the need to define and implement policies that respect the principles and values shared by the citizens of the European Union.

Against this background and a shared commitment to trigger a Europe-wide dialogue on the requirements and options relating to the Internet of Things, DG INFSO and EPoSS organised a "founding workshop" in February 2008 – *Beyond RFID – The Internet of Things*. The present report draws the conclusions of the workshop and incorporates the views and opinions of many experts who were consulted over the six months that followed the workshop.

DG INFSO and EPoSS look forward with confidence and enthusiasm to meeting the challenges of the Internet of Things, especially by working together and with all other organisations and experts willing to develop plans to ensure the potential of the Internet of Things for our economies and society can be fully met.

Gérald Santucci Sebastian Lange

Table of content

Executive summary

This report outlines the results of the workshop "Beyond RFID – The Internet of Things". The workshop was initiated and jointly organised by the Commission and EPoSS and more than 80 invited experts with expertise in different fields of related technologies and research attended the event. This report is not confined to summarising the discussions and conclusions of the workshop, but also elaborates on themes identified at the workshop to substantiate what the Internet of Things might become in the future.

Radio Frequency Identification techniques (RFID) and related identification technologies will be the cornerstone of the upcoming Internet of Things (IoT). While RFID was initially developed with retail and logistics applications in mind in order to replace the bar code, developments of active components will make this technology much more than a simple identification scheme. In the not too distant future, it can be expected that a single numbering scheme, such as IPv6, will make every single object identifiable and addressable. Smart components will be able to execute different set of actions, according to their surroundings and the tasks they are designed for. There will be no limit to the actions and operations these smart "things" will be able to perform: for instance, devices will be able to direct their transport, adapt to their respective environments, self-configure, self-maintain, self-repair, and eventually even play an active role in their own disposal.

To reach such a level of ambient intelligence, however, major technological innovations and developments will need to take place. Governance, standardisation and interoperability are absolute necessities on the path towards the vision of things able to communicate with each other. In this respect, new power efficient, security centred and fully global communication protocols and sustainable standards must be developed, allowing vast amount of information to be shared amongst things and people. The ability of the smart devices to withstand any kind of harsh environment and harvest energy from their surroundings becomes crucial. Furthermore, a major research issue will be to enable device adaptation, autonomous behaviour, intelligence, robustness, and reliability. The general organisational architecture of intelligent "things" will be of fundamental importance: whether it should be centralised or totally distributed.

Another central issue of the Internet of Things will be related to trust, privacy and security, not only for what concerns the technological aspects, but also for the education of the people at large. The growing data demand and higher data transfer rates will require stronger security models employing context related security, which in return will help the citizens to build trust and confidence in these novel technologies rather than increasing fears of total surveillance scenarios. The dissemination of the benefits that these technologies can bring to the general public will also be essential for the success of this technology on the market. The real advantages of the IoT have to be shown convincingly, all citizens' concerns must be addressed and taken into account when developing innovative solutions and proposals.

It is therefore expected that the Internet of Things will become a reality over the next 20 years; with omnipresent smart devices wirelessly communicating over hybrid and ad-hoc networks of devices, sensors and actuators working in synergy to improve the quality of our lives and consistently reducing the ecological impact of mankind on the planet.

The Internet of Things (IoT)

It is foreseeable that any object will have a unique way of identification in the coming future, what is commonly known in the networking field of computer sciences as "Unique Address[1]", creating an addressable continuum of computers, sensors, actuators, mobile phones; i.e. any *thing* or object around us. Having the capacity of addressing each other and verifying their identities, all these objects will be able to exchange information and, if necessary, actively process information according to predefined schemes, which may or may not be deterministic.

The definition of "Internet of Things" has still some fuzziness, and can have different facets depending on the perspective taken. Considering the functionality and identity as central it is reasonable to define the IoT as *"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts"*. A different definition, that puts the focus on the seamless integration, could be formulated as "Interconnected objects having an active role in what might be called the Future Internet".

The semantic origin of the expression is composed by two words and concepts: "Internet" and "Thing", where "Internet" can be defined as "*The world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP)*", while "Thing" is "*an object not precisely identifiable*" Therefore, semantically, "Internet of Things" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols".

The set of actions that the future objects should be able to do is a matter of research. Quite understandably, a fundamental enabler would be the identity knowledge, of the "self" and of the others. Enabling the object to know "itself" and its common properties such as creation, recycling, transformation, ownership change, or use for different purposes will allow common objects to interact actively and decisively with the environment. For example, the integration of communication capabilities between RFID tags, sensors and actuators is seen as a very important area which needs to be studied together with the integration of such devices into hybrid wireless sensor networks that are characterised by modularity, reliability, flexibility, robustness and scalability.

While the current Internet is a collection of rather uniform devices, however heterogeneous in some capabilities but very similar for what concerns purpose and properties, it is to be expected that the IoT will exhibit a much higher level of heterogeneity, as totally different objects in terms of functionality, technology and application fields will belong to the same communication environment.

In this vision of the future, is it easy to imagine things that are able to transport themselves: e.g. by consulting global positioning system sensors on its way, instructing conveyor belts for its routing, consulting logistics

[1] Already today many tags operate with a 128 bits address field that allows 340282366920938463463374607431768211456 ($\approx 3.4 \times 10^{38}$) unique identifiers, more than a trillion unique addresses for every square centimetre on the earth.

information databases and decide themselves upon the best route to their destinations; or alternatively the things may consult an external entity like their customers before making decisions that will increase cost or cause delays. There will be fully automated supply networks, autonomous warehouses, and the customers will not only know when a thing passes certain transit checkpoints, but monitor entirely the transport route from the point an object or product leaves the manufacturer.

Obviously, all such devices will need to harvest their own energy. Overcoming the power problem will allow the things not only to communicate for indefinitely long, but also to relay information from other objects. In environments where there will be no fixed access point offering efficient communication for the things, they will form extensive ad-hoc networks routing information towards the infrastructure or their destination node in the formed network. This allows sensors to be placed everywhere, even when the infrastructure is weak or absent, and even if the sensors are mobile.

Recent years have seen the raise of social networks and the virtual worlds with real peoples' avatars enjoying their second life. Anyone "always connected" may twitter their context with those interested and authorised to see the person's whereabouts. With proper authorisation an individual's mobile phone may consult any stationary sensor in the room about its location, the thermometer on the wall about the temperature and the hygrometer about the local weather, and communicate this to the person's friends; and their phones will play their friend's tune when the person is entering the same building. The virtual entity may finally coalesce with a person's physical presence – provided that the person permits.

New innovative applications will emerge from this social and technological context exploiting the connectivity and accessibility of everything. Some can readily be identified above: there will be better and more energy efficient logistic, probably changing completely the retail industry; there will be intelligent buildings, robots, cars, and cities facilitating and assisting our daily lives and thereby increasing our quality of life; social networks will deepen and transcend physical boundaries, and global communities will emerge; yet it is today impossible to envision most of the applications exploring the Internet of Things.

When technology transforms society social tension is unavoidable and will represent political challenges. Economical and legal conditions must nurture the capacity of companies to exploit the new possibilities. Efficiency may create redundancy; new business models may overthrow traditionally strong enterprises. Monolithic corporations may crumble into networks of peers; or trusts and monopolies emerge from the most successful actors in a sector. The legal framework regarding privacy and security must adapt to a new reality. New social networks and organised sub-groups may renew the democracies and challenge existing power structures. It is therefore important that socio-economic research and political debate on the Internet of Things go hand in hand with technological research and advancements.

The workshop and this report have to be considered just as a part of a work in progress, subject to an open, web based consultation process[2].

[2] See http://www.smart-systems-integration.org/public/internet-of-things.

Technology
Wider technological trends

It is possible to identify, for the years to come, four distinct macro-trends that will shape the future of IT, together with the explosion of Ubiquitous devices that constitute the future Internet of Things:

1. The first one, sometimes referred as “exaflood” or “data deluge”, is the explosion of the amount of data collected and exchanged. Just to give some numbers, business forecasts indicate that in the year 2015 more than 220 Exabytes of data will be stored. As current network are ill-suited for this exponential traffic growth, there is a need by all the actors to re-think current networking and storage architectures. It will be imperative to find novel ways and mechanisms to find, fetch, and transmit data. One relevant reason for this data deluge is the explosion in the number of devices collecting and exchanging information as envisioned as the Internet of Things becomes a reality.
2. The energy required to operate the intelligent devices will dramatically decreased. Already today many data centres have reached the maximum level of energy consumption and the acquisition of new devices has necessarily to follow the dismissal of old ones. Therefore, the second trend can be identified covering all devices and systems from the tiniest smart dust to the huge data centres: the search for a zero level of entropy where the device or system will have to harvest its own energy.
3. Miniaturisation of devices is also taking place amazingly fast. The objective of a single-electron transistor is getting closer, which seems the ultimate limit, at least until new discoveries in physics.
4. Another important trend is towards autonomic resources. The ever growing complexity of systems will be unmanageable, and will hamper the creation of new services and applications, unless the systems will show self-* properties, such as self-management, self-healing and self-configuration.

Enablers

Energy

Energy issues such as energy harvesting and low-power chipsets are central to the development of the IoT. There is a need to research and develop solutions in this area, having as objective a level of entropy as close as possible to zero. Current technology seems inadequate for the processing power and energy limitation of the forthcoming future. The development of new and more efficient and compact energy *storage* like batteries, fuel cells, and printed/polymer batteries etc; as well as new energy *generation* devices coupling energy transmission methods or energy harvesting using energy conversion will be the key factors for implementing autonomous wireless smart systems.

Intelligence

Capabilities such as context awareness and inter-machine communication are considered a high priority for the IoT. Additional priorities are the integration of memory and processing power, the capacity of resisting harsh environments, and an affordable security. Furthermore, the development of ultra low power processors/microcontrollers cores designed specifically for mobile IoT devices and a new class of simple and affordable IoT-centric smart

systems will be an enabling factor. The solutions in this respect will range from the use of hard wired or micro programmed finite state machines to the use of microcontrollers. The choice is a trade off between flexibility, programmability, silicon area, and power consumption. The devices require some form of non-volatile storage (EEPROM[3]/FRAM[4]/Polymer), independent of whether this will be laser trimmed at the time of manufacture, one time programmable, or electrically rewritable. Rewritable non-volatile memory is clearly preferred for achieving high throughput during production test, and allows concurrently the benefit of user memory, programmability and storage of sensor data.

Communication

New, smart multi frequency band antennas, integrated on-chip and made of new materials are the communication means that will enable the devices to communicate. On-chip antennas must be optimised for size, cost and efficiency, and could come in various forms like coil on chip, printed antennas, embedded antennas, and multiple antenna using different substrates and 3D structures. Modulation schemes and transmission speed are also important issues to be tackled allowing multi-frequency energy efficient communication protocols and transmission rates. The communication protocols will be designed for Web oriented architectures of the Internet of Things platform where all objects, wireless devices, cameras, PCs etc. are combined to analyze location, intent and even emotions over a network. New methods of effectively managing power consumption at different levels of the network design are needed, from network routing down to the architecture of individual devices.

Integration

Integration of smart devices into packaging, or better, into the products themselves will allow a significant cost saving and increase the eco-friendliness of products. The use of integration of chips and antennas into non-standard substrates like textiles and paper, and the development of new substrates, conducting paths and bonding materials adequate for harsh environments and for ecologically sound disposal will continue. System-in-Package (SiP) technology allows flexible and 3D integration of different elements such as antennas, sensors, active and passive components into the packaging, improving performance and reducing the tag cost. RFID inlays with a strap coupling structure are used to connect the integrated circuit chip and antenna in order to produce a variety of shapes and sizes of labels, instead of direct mounting.

Interoperability

It is a known fact that two different devices might not be interoperable, even if they are following the same standard. This is a major showstopper for wide adoption of IoT technologies. Future tags must integrate different communication standards and protocols that operate at different frequencies and allow different architectures, centralised or distributed, and be able to communicate with other networks unless global, well defined standards emerge.

Standards

Hence, open standards are key enablers for the success of the Internet of Things, as it is for any kind of machine to machine communication. Without clear and recognised standards such as the TCP[5]/IP[6] in the Internet world, the

3 Electrically Erasable Programmable Read-Only Memory.
4 Ferroelectric Random Access Memory.
5 Transmission Control Protocol.

expansion of the Internet of Things beyond RFID solutions cannot reach a global scale. The unique addresses follow two standards today, Ubiquitous ID and EPC[7] Global, and there is quite a big variance in the frequencies used according to the country and the manufacturer. Standards evolution and interoperability will influence the RFID deployments in the near future and the viability of the Internet of Things in the long term. Sustainable fully global, energy efficient communication standards that are security and privacy centred and are using compatible or identical protocols at different frequencies are therefore needed.

Manufacturing

Last but certainly not least, manufacturing challenges must be convincingly solved. Costs must be lowered to less than one cent per tag, and production must reach extremely high volumes, while the whole production process must have a very limited impact on the environment.

Barriers

Absence of Governance

One major barrier for the widespread adoption of the Internet of Things technology is the absence of governance. Without an impartial governing authority it will be impossible to have a truly global "Internet of Things", accepted by states, companies, trade organisations and the common people. Today there is not a unique universal numbering scheme as just described: EPCglobal and the Ubiquitous Networking Lab propose two different, non-compatible ways of identifying objects, and there is the risk to have them competing in the coming future over the global market. There is also the need of keeping governance as generic as possible, as having one authority per application field will certainly lead to overlap, confusion and competition between standards. Objects can have different identities in different contexts so having multiple authorities would create a kind of multi-homing, which can lead to disastrous results.

EPCglobal is, according to its website, a "neutral, consensus-based, not-for-profit organisation" that leads "the development of industry-driven standards for the Electronic Product Code to support the use of Radio Frequency Identification in today's [...] networks". Their roots lie on the work that has been carried by the AutoID centre, a consortium led and hosted by the Massachusetts Institute of Technology. The EPCglobal architectural framework is based on the EPC Information Service, which is composed by information provided by the manufacturer and the different stakeholders in the value/supply chain, and on the ONS, the Object Naming Service, that provides similar functionalities than the Domain Name Service for the Internet. The root directory of the ONS is hosted by Verisign.

According to many experts, this architecture presents an issue. Being a central lookup service, the root of the ONS can be controlled and/or blocked by a single company or a country, unlike the DNS system. The danger of a unipolar system is that the company who controls the ONS has the power of isolating companies or products, and obtaining vital information (for competitors) about the movement of goods.

6 Internet Protocol.
7 Electronic Product Code.

What could be the governance of the Internet of Things, and how different should it be from the governance of today's Internet? It remains an open question if it should be a state-led agency, or a group under the supervision of the United Nations, or an industrial consortium. All parties should convene and work together towards a solution to avoid that a de-facto standard will eventually appear, as, regrettably, in these cases the winning solution is often neither the technically most advanced nor the most socially acceptable one. The guidance of the EU can be crucial to stimulate the emergence of open, global governance.

Privacy and Security

In order to have a widespread adoption of any object identification system, there is a need to have a technically sound solution to guarantee privacy and the security of the customers. While in many cases the security has been done as an add-on feature, it is the feeling that the public acceptance for the Internet of Things will happen only when the strong security and privacy solutions are in place. This could be hybrid security mechanisms that for example combine hardware security with key diversification to deliver superior security that makes attacks significantly more difficult or even impossible. The selection of security features and mechanisms will continue to be determined by the impact on business processes; and trade-offs will be made between chip size, cost, functionality, interoperability, security, and privacy.

The security and privacy issues should be addressed by the forthcoming standards which must define different security features to provide confidentiality, integrity, or availability services.

There are also a range of issues related to the *identity of people*. These must be dealt with in politics and legislation, and they are of crucial importance for the efficient public administrations of the future. Although many of the proposed technologies are based on RFID or smart systems, they will not be discussed in this report whose focus is on *objects* and *things* and the related technological and application challenges.

European strengths

One of the major success stories for Europe in wireless technology is the GSM[8]. This story shows the ability of European institutions and industries to work together towards a common standard, which has become universally accepted. In general, the fact that the European Union is composed by states with very different habits and sensitivities towards technology is also a positive fact. In particular, we can observe that:

1. The different cultural backgrounds that are at the very roots of the European Union allow a fair treatment of privacy and security issues. The capacity of understanding different positions, and the continuous strive for the most widely acceptable compromise are two general European characteristics that enable the addressing of a fair balance between security concerns and privacy issues.
2. Leading regulation on data protection make EU-conceived standards naturally more advanced, more likely to be accepted by a large audience, and more regulation-compliant than other developed in other

8 Originally *Groupe Spécial Mobile*, now Global System for Mobile communications.

areas of the world, with different objectives and different common sensitivity.

3. World-leading standardisation bodies, such as ETSI, and industrial consortia, such as Airbus, are outstanding European organisations that demonstrated in the past the capacity of producing highly successful multilateral collaborative results. These are essential to ensure the diversity and proper governance of the IoT.

Applications

Things on the move

Retail

The first large scale application of the Internet of Things technologies, will be to replace the bar code in retail. The main barriers so far have been the much higher cost of the tag over the bar code, some needed technology improvement for what concerns transmission of metals and liquid items, and privacy concerns. Nonetheless, the replacement has already started in some pilot projects and although one may expect to see co-existence of the two identification mechanisms for many years into the future, advances in the electronics industry will render the RFID tag ever cheaper and more attractive and accessible to the retailers.

The electronic tags offer multiple benefits over the bar code for both the retailers and the consumers. The retailers will have item identification unified from the producer, through the storage, the shop floor, cashier and check out, as well as theft protection. They may also save cost by allowing customers to check out the products themselves and without having to put the bought items on a conveyor belt. The shelves may be intelligent issuing a refill order automatically to the storage as items are sold offering precise delivery from the wholesaler directly to the shelf. Furthermore, the history of any item from production to the shelf can be stored offering increased quality management along the supply chain.

For the consumers this offers the possibility to avoid long check-out lines, and having the product history available will improve food safety and protect consumer rights in case of failing products. Yet, RFID in retail has created major consumer concerns, that led to the creation of groups such as CASPIAN (Customer Against Supermarket Privacy Invasion and Numbering) in the United States. Any item paid with a payment card in somebody's name may be connected to the owner in the shop's database, as the electronic tag could be read post-sale to identify date and location of the purchase. Although those tags could be used to prove rightful ownership and sort out guarantee disputes, the perception by the public has always been mainly negative.

The privacy issues related to RFID and retail can be divided into pre-sale and post-sale. In the first case, retailers have to protect themselves from competitors that may read the stock quantities of products and influence their sales prices accordingly. In the second, the possibility of linking a product to a person may pose a threat to the privacy (in case, for instance, of medical products), and exposes the possibility of illegal use of those information, from simple unwanted advertisement to threats due to religious, sexual or political preferences.

The challenge is to put this into a useful context for the user and to provide the right incentives to increase acceptance, while developments on the technology must avoid privacy intrusion and guarantee the uniqueness of tags. As an example, similar to the way that security equipment in cars gives a discount on insurance, having the capital goods in a household marked with electronic tags makes the illegal sales of the items more difficult, and in case of theft eases the recovery. This could give discounts on the house insurance.

Today almost every phone sold is equipped with some kind of short range radio communication like Bluetooth, or more specifically near field communication (NFC) specifically designed for reading RFID tags. Predictions indicate that there could be as many as 2 billion NFC enabled mobile phones by 2012. Soon the consumer will no longer need to consult a shop floor reader to know the history of a product, and the shopping list can be created as the wrapping of used goods are discarded. This opens for automated warehouses where the shopping list is transmitted when the customer leaves the house to collect a ready made shopping bag already checked upon arrival to the warehouse. With the ability of directly reading the tags, the inventory of your belongings may be stored in you mobile phone making insurance claims easier and facilitating the private sales of goods since a centralised registry of *things* will no longer be needed.

Logistics

It is important to remember that innovation in logistics normally does not change the industry fundamentally but allows improving efficiency of processes or enables new value adding features. The first observation to be made from the preceding discussion is that the warehouses will become completely automatic with items being checked in and out and orders automatically passed to the suppliers. This will allow better asset management and proactive planning on behalf of the transporter. Goods may be transported without human intervention from producer to consumer and the manufacturers will have a direct feedback on the market's needs. In this way the production and transportation can be adapted dynamically thus saving time, energy, and the environment.

Executable code in the tags enable the *thing* in transit to make intelligent decisions on its routing based on information received either via readers or positioning systems. This will help optimising the forwarding of the item and delegate routing authority from the transporter to the manufacturer or the customer. The *thing* could check back with the sender if it should continue towards the intended recipient, or alternatively moving to another recipient paying better to have the thing quickly.

Present day logistics is based on established supply chains from manufacturer to consumer. Supply chains based on legal agreement and existing over time. It is possible to envision that the things in transit form a marketplace and that a consumer could place a request on the Internet of Things, receive and accept an offer from a thing fulfilling the request. Equivalent to service composition in the virtual software world where an application is assembled of multiple services available on the Internet, may an assembled thing be constructed from parts automatically identified on the Internet of Things. This will change the way business deals are made since a customer may not place an order for a large volume of things with a manufacturer, but buy them in a sequence of individual orders and possibly from competing manufacturers.

Pharmaceutical

Pharmaceutical applications are fundamentally nothing but production, logistics, and retail of drugs as already outlined in the above sections. An added benefit of an electronic tag is that it may carry information related to drug use making it easier for the customer to be acquainted with adverse effects and optimal dosage.

Today, RFID technology is already used in order to prevent counterfeiting of drugs, although not on large scale. In the near future, the widespread use of secure RFID tags could limit the number of people that looses their lives because of counterfeit medicines. In the far future, smart biodegradable dust embedded inside pills may interact with the intelligent tag on the box allowing the latter to monitor the use and abuse of medicine and inform the pharmacist when new supply is needed. The smart dust in pills could know incompatible drugs, and when one is detected closely enough the pill could refuse to activate or release the active substances. The same mechanism could of course be used to prevent overdoses. If there is an accident or when someone perishes from drug abuse or misuse it will be possible to quickly identify the taken drug by asking the smart dust, which may also inform about the right antidote and dosage to enable the emergency treatment to be given faster and more correct and thereby saving lives.

Food

Europe is traditionally spoiled with excellent food and wine where the quest for the perfect taste has been ongoing for centuries. French law pioneered the idea of protecting produce of a limited geographical origin, and similar laws have since been established in many European countries. Traceable identities will help the consumers to verify the origins of the products and help Europe to preserve agricultural diversity and rural lifestyles.

The unfortunate outbreaks of BSE[9] or "mad cow diseases" have drawn public attention to food safety. There have also been cases where infective agents have been detected in a certain lot of food. Often these agents can only be detected in laboratory assays on samples taken from the lot, and regrettably the results may become available only after the produce has reached the market making a recall difficult and one has to resort to imprecise public warnings. Knowing the origin of each food item is thus essential to ensure that it is not carrying unwanted diseases, and to enable selective recalls of infected items avoiding to waste good food as a safety precaution. It will help assuring the consumers that the food they buy is of controlled origin, and that the quality control of the shop and the public authorities extends from the farm to the table. Should a food related disease be detected the traceability of the eaten food will enable faster detection of the origin of the infection and thus curbing its impact better and faster.

Finally, traceability may provide market feedback to the producers in a sector where the production is often planned well in advance according to wholesale dealers' prediction of the market for certain produce and the producers' flexibility is limited by long term contracts and politically decided production subsidies. The recent global food crisis highlighted that the feedback mechanisms in food market do not work as well as in other commodity markets making the food availability oscillate between periods of overproduction and shortage. All the major food producers in the world could have augmented their production had they only seen the increasing demand earlier. Knowing what the market buys could stimulate the farmers to time their produce and offerings better to market demand fluctuations. The social impact of improved food supply stability can not be underestimated as hunger is a strong driving force for social unrest and uprising.

9 Bovine Spongiform Encephalopathy.

Ubiquitous intelligent devices

In the current vision, the IoT will bring an even more pervasive revolution than the Internet and mobile technologies and today's acclaimed Information Era. The future ubiquitous IoT will make possible for virtually any object around us to exchange information and work in synergy to increase dramatically the quality of our lives. There will be smart clothes, made of smart fabrics, which will interact with the Climate Control of the cars or homes, selecting the most suited temperature and humidity for the person concerned; smart books of the future will interact with the entertainment module, such as a multi-dimensional, multi-media hypertext making the TV show more information on the topic we are reading in real time; and so on.

Most of these devices will be intelligent and able to execute behaviours according to predetermined set of actions. They will also be able to collaborate and make decisions following dynamically changing user preferences. As examples, consider intelligent buildings and intelligent cars. In addition to user customisation of the environment, the future house may also automatically work to reduce energy consumption and maximise comfort. Sensors and actuators in the car will collaborate to provide a safer and more pleasant journey for the driver, while preserving the environment as much as possible.

This new generation of intelligent devices could also collaborate to convey messages to the owner. The cleaning robot may inform the car to tell the driver with a voice message that it is out of detergent, and the driver may choose to add detergent to the shopping list in the mobile phone with a voice command. Although the mobile phone has already transmitted the shopping list of today to the automatic warehouse, it knows from the global positioning sensor in the car and the speedometer that there is still time to add this new item with a command to the warehouse.

In order to achieve this in a consistent and global way *interoperability* of devices through novel protocols is necessary. As already explained in the previous sections, self-* properties such as self-configuration and self-management are necessary to ensure the integration of the intelligent devices with any operational environment. One may easily understand the difficulty of this task by thinking about the "Plug and Play" technology existing today. With a well defined platform, such as a computer, with a well defined operating system, adding a device without going through a long and painful installation and debugging process is already a great achievement. The problem will be much worse when a device will enter an environment populated by hundreds, if not thousands or millions of other devices, possibly not even existing when the original device was conceived. The smart houses that are demonstrated until now have been carefully designed for everything to work optimally together by an overall system architect, in stark contrast to all the objects found in a normal household assembled by the inhabitants over several years. Without sufficient standardisation of the involved protocols and configuration mechanisms, there will be no ubiquitous intelligence.

Another major issue is how to ensure *reliability* of the ubiquitous intelligence. When individual entities are supposed to make intelligent decisions in collaboration, the issue is how do they converge to a solution, and if and how a "global" solution might be preferred to a local one. Emergent intelligence

motivated by biological systems like ant colonies have been studied through simulation, but today there is no theoretical or practical framework to ensure that a solution is found in finite time even if a solution exists. A related issue is fault protection. How to assess that a faulty device is really faulty and how to prevent that this fault propagates to other devices and makes the system deadlock, not to talk about malicious devices that will deliberately send wrong signals? This area of Byzantine behaviour has already received significant scientific attention for many years, but its complexity will explode when ubiquitous intelligence will be in place.

Ambient and assisted living

Health

Sadly, society pays a very high toll on human lives because of medication errors. More than 7000 people loose their lives in US hospitals every year and similar figures are likely in Europe. Health logistics, the flow of drugs and patients, is not different from any other delivery systems discussed above with the same logistic benefits. The challenge is to design systems that can be supported by the health care workers and integrated from the supply chain to the bedside, and even before the patient is admitted to an hospital.

New efficient diagnostics combined with nanotechnology enabled lab-on-a-chip technologies open a complete range of novel opportunities for new treatments and prevention of serious diseases. In-vivo equipment will assist in drug dosage closer to the affected organs thus reducing the amount of reagents needed and diminish the risk of adverse effects. It is an established fact that several serious common illnesses like breast cancer, cardio-vascular diseases and Alzheimer's disease have genetic components. It is also known that successful treatment depends on early detection. Thus, in-vivo laboratories may test persons at risk providing a sufficiently frequent sampling to allow early detection and improved recovery possibilities.

Biodegradable materials will offer the possibility to place temporary sensors and lab-on-a-chip equipment on the patient, or in the patient. Temperature and humidity can be measured inside a cast to prevent skin problems. Antigens may be detected on transplanted organs to help prevent rejection. Intelligent micro-robots may be guided to bring drugs to the infected areas by ex-vivo remote guidance, and assist in the diagnosis providing located measurements of vital parameters.

Furthermore, this new sort of personal medical equipment will enable the patient to stay longer and safer at home since the equipment itself can alarm the hospital in case of critical situations, or the patient can be relieved from the hassle of routine checks when there is nothing wrong. Medical research will advance on data from patients living normal lives and not like guinea pigs in hospitals. Telemedicine may replace costly travel and reduce patient stress.

The demographic trends for Europe show an aging society with more people dependent on assistance. Ambient intelligence and the Internet of Things may open up new possibilities for elderly to live longer and safer at home, and reduce risks of errors in dosage of drugs. In-vivo drug delivery may provide

ways to administer treatment that would otherwise require the visit of a nurse. Intelligent objects in the house could call for assistance if a person stays unreasonably long in an unexpected location, like the bath or the toilet.

The challenge is to find ways to provide the benefits and gain in efficiency while preserving the essential human contact since solitude and isolation may be as dangerous as many medical conditions. A further challenge is that technological risk and public restraint to intelligent objects and sensors are accentuated with the possibly fatal consequences in the domain of automated health care and pharmaceutics. Assisted living will become a necessity owing to demographic trends, but how to ensure that the smart *things* really serve the patient and improves the quality of life? How to prevent that the intelligent house gives the wrong mix of medication when the patient has refilled one box of medicine with the content of another? How to ensure that the automated shower assistant robot mixes the right temperature when the temperature sensor in the hot water tap is broken? In this case statistical error probabilities might not be satisfactory for the patient, and the design of safe and robust smart systems will be mandatory.

Intelligent Home

There are already examples of smart houses being demonstrated and the future intelligent home will build on these experiences. The present experience is tailor made, and each *thing* in the house has been carefully selected and tuned to interoperate with all the other intelligent devices. This is too costly for most houses and the intelligent home remains a dream for most people. The big paradigm shift comes when every smart object knows the interoperable protocols removing the need for the dedicated systems developed independently today. For instance, there are several solutions for intelligently controlling every power socket in the house thus allowing simple tasks like switching on and off lights, and more complex ones such as fine-grained management of electrical heaters, in order to set the ambient temperature. However, the control systems in operation today are quite basic and apply only to the wall socket, and can not manage appliances connected through extension cords. In the future Internet of Things the lamps or even the light bulbs will be addressable and intelligent, and a global house management controller will be able to control every single smart device.

Maintaining a comfort temperature and heating of water are the most energy consuming tasks of the house with huge potentials for energy conservation, and as a consequence a significant positive impact on the environment. This is further discussed under environmental aspects and resource efficiency below.

There will be robots taking care of the house, performing routine works such as cleaning or maintenance. These will collaborate autonomously with the house sensors, and the house control. The intelligent appliances will collaborate to conserve energy, and to signal need for new supplies of food, detergents, maintenance, etc. Some of which may be satisfied automatically by the maintenance robot. This will take away some of today's tedious housekeeping activities.

The house will also jointly try to maximise the comfort of each of its inhabitants by learning the individual preference profiles. The coffee will be ready at the right time in the morning, surround sound system will broadcast

and adapt to the right media (television, phone, radio, CD[10], DVD[11], or computer), and record the stream if the user is unavailable, the bathtub will be filled with water at the right temperature. Similarly, mobile robots and wireless smart devices will be able to seamlessly interact and communicate with the environment, thereby contributing to the efficient, secure and inclusive nature of the European societies. Elderly people and people with disabilities will find the house capable of taking charge of activities that today may require excessive effort or manual assistance.

Transportation

In modern cars a stunning 30% of the total cost is electronic components. These systems are the base of the much increased safety for the drivers and the environment. Despite a sharp increase in road traffic since 1970 and an increase in the number of car accidents, there has been a constant decrease of injuries and deaths thanks to the new systems introduced in cars like anti-blocking breaks and traction control. However, all of this has been achieved considering the car as an independent system.

This trend will be further amplified when the cars will be able to communicate and autonomously start gathering ambient information. For instance when there is a queue, the first cars may tell the cars behind if there is an accident or just too much traffic, and this will eventually make intelligent navigation systems re-plan the route of cars programmed to go down already saturated roads. The cars may help the driver to keep safe distance to the car in front, and may refuse dangerous actions like speeding if the weather conditions are unsafe or overtaking if the oncoming car goes too fast. The cars can go by autopilot on highways reducing the risk of fatigue related accidents.

Cars will also be able to maintain themselves, calling for the appropriate service based on the self diagnosis of the problem and ensuring that the right replacement parts are in stock. The car will plan the time of service according to the diaries and preferences of the usual driver to minimise the petulance of their lives, and make sure that there is a substitute car available if there would be a need for it.

The cars will also be able to manage better the energy needed, by harvesting it in much higher quantities, by storing it with novel storage techniques, and by producing it more efficiently thanks to engines based fully or partly on new sources of energy. Optimal route planning will reduce the number of kilometres driven, and better control systems for the car will make the ride more energy efficient. All of these individual factors will contribute to reduced emissions and less pollution.

The public transport sector may be radically changed when smart devices and travellers are identifiable. Ticketing based on RFID is already widely available: for instance 10 million daily travellers of the public transport system in Paris have already access to an electronic ticket[12]. One may easily envision that this system not only permits user access to the stations, but also that readers in the doors of the trains and buses enable an accurate tracking of every connection and route of every traveller. This will provide the operating company with

10 Compact Disk.
11 Digital Video Disk.
12 The system is called *Navigo*, see https://www.navigo.fr/pages/accueil.html.

perfect traffic data to optimise the network and service level, and to decide on the establishment of new lines. In the case of an emergency, the rescue workers could know the number of travellers in a certain station, and the name of the subscribers of the rechargeable ticket. The incentive for the user could be notifications in the case of operational problems or closed stations, with alternative routes and connections proposed.

Society
People, security and privacy

The new information age has introduced exciting new capabilities, distributed decision and control processes including unprecedented awareness at the consumer level. There is a hunger for faster responses to needs, for greater security, for instantaneous access to information. The development of novel technologies will allow the widespread use of smart devices that will clearly bring many advantages to everyday life. Thanks to the traceability information on any product, everyone will be able to make more informed choices; networks of sensors and smart devices will orchestrate the environment surrounding us, relieving us from trivial but annoying and time-wasting regulations and information retrieval. Everyone and everything will be connected to the network. Eventually every person on the planet will be connected to the network. In the same way will virtually every "thing" with a electronic identification be connected to the "Internet of Things". The resulting network traffic will require highly scalable, reliable systems.

On the other hand, the trust issue is seen of highest importance in the social acceptance of the Internet of Things. Currently RFID technology is regarded as very intrusive for privacy and although general public seems accustomed to more and more "invasive" technological way of controlling, such as the overwhelming and almost ubiquitous presence of CCTV[13] cameras in the United Kingdom, the RFID technology is often seen as the last step towards a "big-brother" control of personal freedom. One reason can be found in the non-obvious advantages that this technology brings. Drawing a parallel with mobile phones technology, knowing where a mobile phone is located will with high probability tell where its owner is. On the other hand, as it was an extension of a known technology and brought significant and clear advantages to the state of the art, the acceptance of mobile phones has been wide and almost unconditional, although some questions remain open regarding, in particular, the long-time health safety. Thus, the community of stakeholders must develop security and privacy mechanisms and establish security guidelines for RFID developers and operators of RFID systems.

For what concerns electronic tags, though, issues about privacy and security are put in front of potential beneficial advantages. Only by developing solutions that are clearly respectful of people's privacy, and devoting an adequate level of resources for disseminating and explaining the technology to the mass public, from the appropriate sources, this major obstacle can be overcome.

For instance, there are many situations where an individual would like to share personal information. When a traveller arrives in a smart hotel room, it would be desirable if the room could check back with the smart house for preferences regarding temperature, lighting and configuring the television set with the right set of channels. When an accident occurs the victims would like their medical records to be available to the arriving ambulances to ensure that optimal treatment can be provided.

13 Closed Circuit TV.

It is therefore important that any citizen will trust that the information embedded in any device will be handled securely, and in a way that maintains the individual's privacy.

A central question to be clarified is who owns the data in networked systems? Any traveller would probably feel extremely uncomfortable if the hotel would sell any kind of information about his preferences, and later suffer from targeted marketing, and the victims of accidents would almost certainly disagree in divulging information about their medical conditions and treatments, and have them available to employers, colleagues, friends and insurance companies. Thus, even if someone might give his/her consent to share some personal data for a temporary need, there is the stringent need to have a way to ensure that data will never be misused. The only clear way to ensure it is to develop privacy by design, and not something to be considered only after introduction of innovative technologies.

Society and culture also play important roles in the general public's attitude towards new technology and the Internet of Things. In the US there is a wider public acceptance of surveillance and authority control to increase the personal and national security, while people in Europe are generally more concerned about privacy and will reject technology that could allow outside surveillance and control. It is therefore important that the Internet of Things is able to meet the expectations of the society and the citizens. Research is needed to understand what these expectations are and where the sensitivities and concern for personal privacy and information may block applications.

For humans, whenever we interact with other people we give them some form of information which may directly or indirectly identify us. This choice has to be implemented in the future IoT devices as well. For some applications and some devices there will be no anonymity at all, a state called "verinymity", and for other applications and devices there will be total anonymity or detachable anonymity. In between these two levels different degrees of anonymity such as persistent pseudonym and linkable anonymity could be defined by standards and regulation for specific applications and devices.

Europe's aging population may be more willing to accept to give up privacy for better assistance in their daily life. Thus, demographic changes may change attitude towards technology originally perceived as intrusive. It is imperative that companies and governments are able to capture these trends and time the introduction of new technologies like the Internet of Things to ensure that it is received as useful.

A policy for people in the Internet of Things

Education and Information

Education and Information are central aspects for the success of the upcoming IoT. As discussed in previous sections, privacy concerns about the misuse of information are high, and final users do not clearly see the advantages of the widespread adoption of this technology. Therefore, education about the potential use and clear benefits of the IoT must be carried out, together with significant advances in Privacy Enhancement Technologies. As well, information to the users about the presence of RFID tags, the reading range, the kind of data contained in the devices and in the back system, and the use of those, must be clear and easily available.

Legislation

When moving towards the Internet of Things it is mandatory that policy keeps up with technology so that citizens gain confidence in the new technology and will accept to live in the "Internet of Things". When bar codes were introduced they received public uprising and rejection. Attempts to introduce electronic health cards have been unsuccessful based on public fear for information misuse. RFID tags have seen a similar resistance leading to tags that can be erased when clients leave the supermarket, or temporarily disabled, or just be read by trusted readers.

In addition to research of current concerns, it is important to engage the wider public in a political debate and dialogue about the Internet of Things. People's momentarily context and roles can determine their attitudes towards new technology: as an example, an employee will resist his boss' access to his or her mailbox while the same person may demand the same insight into the mailboxes of subordinates.

Environmental aspects

Resource Efficiency

Energy conservation is a prerequisite for the Internet of Things. Therefore research producing new knowledge on how to develop more energy efficient electronics will influence the design of all electronics. Concept of energy harvesting will enable larger and larger portions of the consumed energy to be generated by ambient renewable sources available locally thus reducing the losses in long distance energy distribution.

Similar effects will be experienced by road transport and cars. Already today there are hybrid cars available harvesting the kinetic energy of the drive. This, in combination with better and more environmentally friendly energy storage in the future will make electrical vehicles achieve longer range and become more attractive alternatives.

Abundant sensory information will enable unprecedented energy optimised control. Climate control is the most energy consuming activity in modern buildings. The house could adjust the room temperatures according to the personal preferences of those in the room, and avoid heating or cooling rooms excessively without benefits to the inhabitants. Furthermore, it is a major problem for the electricity grid that heaters or air conditioning equipment start simultaneously at full speed creating peaks in power consumption. Dimensioning the grid to survey these peaks is extremely costly, and can be avoided if one could apply predictive control of the temperature in buildings. If the building knows the expected weather conditions in advance by exchanging sensory information with other buildings around it may adjust the interior climate with less energy and apply predictive control instead of reactive control. This will eventually reduce the need to invest in improved grids and new power plants.

Pollution and disaster avoidance

Combining sensory information will allow early warnings and prevention of catastrophies. An open gas valve on a stove may be detected by comparing the gas flow measurement with the lack of increased temperature in the room. Accidental emissions polluting water may be stopped by a sensor in the drain

detecting the emission and communicating with the next valve in the sewer to block the pollutant to progress. The advance over today's situation is that the control is *distributed* hence offering faster and more cost efficient responses than what is achievable with centralised monitoring and control.

The widespread use of future, to-be-developed IoT technologies and concepts will play a fundamental role in Life Cycle Management of goods, reducing the environmental impact of discarded products. Because of the human nature, the objective of 100% recycling can be attained only if technology will allow products to "dispose" themselves, each product identifying the best recycling path, which parts should be recycled, how and where.

Future mobile robots and micro robots and sensor networks using smart systems communication technology will also be used to develop efficient, robust and versatile hybrid and heterogeneous networked systems that can be deployed in inaccessible or remote locations like oil platforms, mines, forest, tunnels, and pipes. These may assist in preventing, detecting and correcting dangerous situations, and can be deployed either permanently or in cases of emergencies or hazardous situations like earthquakes, fire, floods, and in areas of high radiation.

Outlook to the future

When looking at today's state of the art technologies, they should give a clear indication on how the Internet of things will be implemented at a universal level in the years to come as well as indicate important aspects that need to be further studied and developed in the coming years. Firstly, the need exists for significant work in the area of governance. Without a standardised approach it is likely that a proliferation of architectures, identification schemes, protocols and frequencies will develop side by side, each one dedicated to a particular and separate use. This will inevitably lead to a fragmentation of the IoT, which could hamper its popularity and become a major obstacle in its roll out. Interoperability is a necessity, and inter-tag communication is a pre-condition in order for the adoption of IoT to be wide-spread.

In the coming years, technologies necessary to achieve the ubiquitous network society are expected to enter the stage of practical use. It is widely expected that RFID technology will become mainstream in the retail industry around 2010. As this scenario will evolve, a vast amount of objects will be addressable, and could be connected to IP-based networks, to constitute the very first wave of the "Internet of Things". There will be two major challenges in order to guarantee seamless network access: the first issue relates to the fact that today different networks[14] coexist; the other issue is related to the sheer size of the "IoT". The IT industry has no experience in developing a system in which hundreds of millions of objects are connected to IP networks. Other current issues, such as address restriction, automatic address setup, security functions such as authentication and encryption, and multicast functions to deliver voice and video signals efficiently will probably be overcome by ongoing technological developments.

Another very important aspect that needs to be addressed at this early stage is the one related to legislation. Various consumer groups have expressed strong concerns about the numerous possibilities for this technology to be misused. A clear legislative framework ensuring the right for privacy and security for all users must therefore be implemented by all member states. A sustained information campaign highlighting the benefits of this technology to society at large must also be organised, a campaign which emphasizes the benefits that this technology can bring to ordinary citizens in their every day lives be it improved food traceability, assisted living or more secure healthcare.

Traditionally, the retail and logistics industry require very low cost tags with limited features; such as an ID number and some extra user memory area, while other applications and industries will require tags that will contain a much higher quantity of data and more interactive and intelligent functions. "Data", in this context, can be seen as an "object" and under this vision a tag carries not only its own characteristics, but also the operations it can handle. The amount of intelligence that the objects in the IoT will need to have and if, how and in which cases this intelligence is distributed or centralised becomes a key factor of development in the future. As the "IQ" of "things" will grow, the pace of the development and study of behavioural requirements of these objects will also become more prevalent in order to ensure that these objects

[14] I.e. mobile phone networks, fixed telephone networks, broadcasting networks, and closed IP data networks for each carrier.

can co-exist in seamless and non-hostile environments. These developments should lead to interactive standards, followed eventually by behavioural ones.

These types of tags will contain features ranging from sensors and actuators and will interact with the environment in which they are placed. One such example could be an interactive device placed in the human body with the scope of delivering the right medicine at the right place at the right time. In this context of greater "wireless", "mobility", "portability" and "intelligence" two trends will influence the future development of smart systems: the increased use of "embedded intelligence" and the networking of embedded intelligence.

Intelligent nodes will be integrated in hybrid wireless networks and used in applications like ambient monitoring in buildings, environmental monitoring, home automation, personalization, localisation, positioning. Real Time Locating Systems using active tags can also be included in this category.

Other topics for research include not only the integration of electronic identifiers into materials, such as ceramics, metals, or paper, but also the creation of devices from non-silicon based materials, such as, for instance, eatable tags. This will allow, for instance, embedding tags into medicines, which can be seen as a giant step to putting receivers into packaging. Additionally, the future IoT will have to be built within recyclable materials and therefore have to be fully eco-friendly. Future smart objects must also be power independent, harvesting energy from the environment in which they operate. Finally, the things of the future will have to be resistant to very harsh and extreme conditions, including: temperature, vibrations, humidity, and hostile environments.

The technology trends foreseen for the next 20 years are outlined in the following tables. While the first table concentrates on developments that can be foreseen within current research priorities, and can be seen as an evolution of the current technological advancements, the second one focuses on more radical and ground breaking technology trends.

Extrapolation of technology trends and ongoing research

Vision society People	• Socially acceptable RFID	• Pervasive RFID	• Interacting objects	• Personalised objects
	• Realising benefits (food safety, anti counterfeiting, health care) • Consumer concerns (privacy) • Changing ways to work	• Changing business (processes, models, ways to work) • Smart appliances • Ubiquitous readers • Access rights • New retail and Logistics	• Integrated appliances • Smart transportation • Energy & Resource conservation	• Mastered ambient intelligence • Interaction of physical and virtual worlds • Search the physical world (google of things) • Virtual Worlds
Politics & Governance	• De-facto governance • Privacy legislation • Address cultural barriers • Future Internet governance	• EU governance • Frequency spectrum Governance • Sustainable Energy Consumption guidelines	• Authentication, trust and verification • Security, social well-being	• Authentication, trust and verification • Security, social well-being
Standards	• RFID security and Privacy • Radio frequency use	• Sector specific standards	• Interaction Standards	• Behavioural Standards
	Before 2010	**2010-2015**	**2015-2020**	**Beyond 2020**

	Before 2010	**2010-2015**	**2015-2020**	**Beyond 2020**
Vision technology Use	• Connecting objects	• Networked objects	• Executable objects /semi-intelligent objects	• Intelligent objects
	• RFID adoption in logistics, retail and pharmaceutics.	• Increased interoperability	• Decentralised code execution • Global applications	• Unified network that connects people, things and services • Integrated industries
Devices	• Smaller and cheaper tags, sensors and active systems	• Increasing memory and sensing capacities	• Ultra high speed	• Cheaper materials • New physical effects
Energy	• Low power chipsets • Reduced energy consumption	• Improved energy management • Better batteries	• Renewable energy • Multiple sources	• Elements of energy harvesting

Topics requiring new or intensified research

	Before 2010	2010-2015	2015-2020	Beyond 2020
Vision society	• Wide take up of RFID	• Integration of objects	• Internet of Things	• Unlocked full potential of the Internet of Things
People	• Socially acceptable RFID	• Ambient assisted living • Biometric IDs • Industrial ecosystems	• Smart living • In-vivo health • Security based living	• Mastered continuum of people, computers and things • Automated healthcare
Politics	• First global guidance • Standardisation	• First global governance • Unified open interoperability	• Authentication, trust and verification	• Inclusive Internet of Things
Standards	• Network security • Ad-hoc sensor networks • Protocols for distributed control and processing	• Interoperability protocols and frequencies • Power and fault resilient protocols	• Intelligent devices cooperation	• Health security

	Before 2010	2010-2015	2015-2020	Beyond 2020
Vision technology	• Low power and low cost	• Ubiquitous integration of tags and sensor networks	• Code in tags and objects	• Smart objects everywhere
Use	• Interoperability framework (protocols and frequencies)	• Distributed control and databases • Ad-hoc hybrid networks • Harsh environments	• Global applications • Self-adaptive systems • Distributed memory and processing	• Heterogeneous systems
Devices	• Smart multi-band antennas • Smaller and cheaper tags • Higher frequency tags • Miniaturised and embedded readers	• Extended range of tags and readers and higher frequencies • Transmission speed • On-chip antennas • Integration with other materials	• Executable tags • Intelligent tags • Autonomous tags • Collaborative tags • New materials	• Biodegradable devices • Nano-power processing units
Energy	• Low power chip sets • Thin batteries • Power optimised systems (energy management)	• Energy harvesting (energy conversion, photovoltaic) • Printed batteries • Ultra low power chip sets	• Energy harvesting (biology, chemistry, induction) • Power generation in harsh environments • Energy recycling	• Biodegradable batteries • Wireless power

Appendix 1: Acknowledgements

Workshop

This report is based on the outcome of a joint European Commission / EPoSS expert workshop on RFID / Internet-of-Things which took place on the 11 and 12th February 2008 in Brussels. The workshop was initiated by Director Dr. Joao Schwarz Da Silva, EC DG INFSO and EPoSS Chairman Dr. Klaus Schymanietz, CTO Defence & Security, EADS Deutschland and organised by the European Commission and the RFID working group of EPoSS with the support of the EPoSS Office.

Report

The workshop report was written by Alessandro Bassi, Hitachi Europe and Geir Horn, SINTEF. Overall coordination was done by Gérald Santucci, Dr. Peter Friess, Thomas Sommer and the assistant team from the European Commission, and by Dr. Sebastian Lange and Dr. Gereon Meyer from the EPoSS Office. Additional advice was provided by Dr. Ovidiu Vermesan, SINTEF and Jesper Holmberg, Hitachi Ltd.

Workshop participants

A particular recognition goes towards the workshop participants who dedicated their knowledge and time to this event. The following experts were invited to participate in this high level expert workshop.

First name	Surname	Affiliation	Country
Manfred	Aigner	Technical University of Graz	Austria
Stéphane	Amarger	Hitachi	France
Marylin	Arndt	France Telecom	France
Marie	Austenaa	Telenor	Norway
Henri	Barthel	GS1 International	Belgium
Alessandro	Bassi	Hitachi	France
Robby	Berloznik	Flemish Institute for Science and Technology Assessment	Belgium
Alfred	Binder	Carinthian Tech Research (CTR)	Austria
Neil C	Bird	Philips Research	Netherlands
Holger	Bock	Infineon technologies	Germany
Jean-Louis	Boucon	Turbomeca	France
Jean-François	Buggenhout	European Commission	Belgium
Véronique	Corduant	Deutsche Post World Net	Germany
Brian	Cute	Eastham Global Strategies, L.L.C.	USA
Jürgen	Ficker	PolyIC	Germany
Jocelyne	Fiorina	École Supérieure d'électricté	France
Fabio	Forno	Istituto Superiore Mario Boella (ISMB)	Italy
Florent	Frederix	European Commission	Belgium
Anthony	Furness	AIDC European Center of Excellence	UK

First name	Surname	Affiliation	Country
Birgit	Gampl	METRO Group Information Technology	Germany
Volker	Gehrmann	Fraunhofer IIS	Germany
Wolfgang	Gessner	EPoSS Office	Germany
Inge	Gronbaek	Telenor	Norway
Patrick	Guillemin	ETSI	France
Christine	Hafskjold	Norwegian Board of Technology	Norway
Stephan	Haller	SAP Research	Switzerland
Mark	Harrison	University of Cambridge Auto-ID Lab	UK
Jesper	Holmberg	Hitachi	Japan
Geir	Horn	SINTEF	Norway
Niko	Hossain	Fraunhofer IML	Germany
Marc	Houben	VDEB	Germany
Ryo	Imura	Hitachi	Japan
Simon	Japs	Informationsforum RFID	Germany
Marisa	Jimenez	EPCglobal	Belgium
Uwe	Jockel-Kordes	Sun Microsystems	Germany
Werner	John	Fraunhofer IZM	Germany
Ivan	Kocis	ARDACO / SMARTRENDS	Slovakia
Stephan	Kolnsberg	Fraunhofer IMS	Germany
Pawel	Korczak	PPU COMEX Sp. z o.o.,	Poland
Jerzy	Korczak	Wroclaw University of Economics, Institute of Informatics	Poland
Eleni	Kosta	Katholieke Universiteit Leuven	Belgium
Sebastian	Lange	VDI/VDE-IT, EPoSS Office	Germany
Jean-François	Legendre	AFNOR	France
Andrej	Litwin	European Commission	Belgium
Octávio	Lopes	Centro IBERLog	Portugal
Indra	Macrì	CNIPA	Italy
Elena	Mayer	University of Freiburg, IMTEK	Germany
Carlo Maria	Medaglia	CNIPA	Italy
Christian	Meiss	Fraunhofer Institut Materialfluss und Logistik	Germany
Georg	Menges	NXP Semiconductors	Germany
Gereon	Meyer	VDI/VDE-IT, EPoSS Office	Germany
Noel	Middleton	TRICON Consulting	Austria
Jarkko	Miettinen	Confidex	Finland
Gilles	Mohn	CARI	France
Yiannis	Mourtos	Athens University of Economics & Business	Greece
Kaj	Nummila	VTT	Finland

First name	Surname	Affiliation	Country
Britta	Oertel	Institute for Future Studies and Technology Assessment (IZT)	Germany
Thomas	Ostertag	RSSI GmbH	Germany
Hana	Pechackova	European Commission	Belgium
Jorge	Pereira	European Commission	Belgium
Alexander	Pflaum	Fraunhofer ATL	Germany
Viktor	Plessky	GVR Trade SA	Switzerland
Josef	Preishuber-Pflügl	CISC Semiconductors	Austria
Ken	Sakamura	University of Tokyo, Director YRP Ubiquitous Networking Lab	Japan
Gérald	Santucci	European Commission	Belgium
Mikhail Victorovich	Simonov	Istituto Superiore Mario Boella	Italy
Thomas	Sommer	European Commission	Belgium
Marco	Sorgetti	CLECAT - European Association for Forwarding, Transport, Logistic and Customs Services	Belgium
Sarah	Spiekermann	Humboldt Universität Berlin	Germany
Lara	Srivastava	ITU New Initiatives	Switzerland
Jens	Strueker	University of Freiburg	Germany
Harald	Sundmaeker	ATB	Germany
Ko	Takahashi	Hitachi	Belgium
Bora	Turan	Alvin Systems	Turkey
Ovidiu	Vermesan	SINTEF	Norway
András	Vilmos	Safepay	Hungary
Gerd	von Bögel	Fraunhofer IMS	Germany
Martin	Vossiek	Clausthal University of Technology Institute for Electrical Information Technology	Germany
Jean-Marie	Willegens	Deutsche Lufthansa	Germany
Harald	Witschnig	NXP Semiconductors	Germany
Jun	Yamada	YRP Ubiquitous Networking Lab	Japan
Cristina	Zabalaga	Fédération Internationale de l'Automobile	Belgium
Lin-Rong	Zheng	Royal Institute of Technology (KTH)	Sweden
Eric	Zinovieff	France Telecom	France