



# **Your voice on RFID**



**Background document for public consultation  
on Radio Frequency Identification (RFID) –**

**Summary of five workshops**

Open for discussion July-September 2006



## *Table of contents*

Introduction.....	4
RFID application domains and emerging trends .....	6
RFID security, data protection and privacy, health and safety issues.....	13
Interoperability, standardisation, governance and Intellectual Property Rights .	20
Frequency spectrum requirements and recommendations .....	23
From RFID to the Internet of Things .....	26
Your voice counts .....	30

### *What is RFID technology?*

The purpose of Radio Frequency Identification (RFID) systems is to enable data to be transmitted by a mobile device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application.

In a typical RFID system, individual objects are equipped with a small tag containing a transponder with a digital memory chip that is given a unique electronic code. The reader, an antenna packaged with a transceiver and decoder, emits a radio signal activating the RFID tag so it can read (and write) data to it. When an RFID tag passes through the electromagnetic zone, it detects the reader's activation signal. The reader decodes the data encoded in the tag's integrated circuit and the data is passed to the host computer for processing. The data transmitted by the tag may provide personal identification or location information, or specifics about a tagged product, such as price, colour, date of purchase, etc. As the technology is refined, more pervasive uses for RFID tags are in the works.

The transfer of data between the tag and reader is done over four different basic frequency ranges: 100-500 kHz (LF), 10-15 MHz (HF), 850-1000 MHz (UHF) and 2.4-5.8 GHz (microwave.) The choice of frequencies impacts data rates and signal ranges. Other ranges are also used, and there is discussion ongoing to try and create agreed international standards.

## Introduction

Radio Frequency IDentification (RFID) attracts attention from citizens, Non-Governmental Organisations (NGOs), businesses and policy makers throughout Europe, because of its potential for improving *inter alia* supply chain logistics, transport, asset tracking, theft prevention, counterfeit detection, and other possible functions such as paying with the mobile phone. At the same time, RFID is sometimes associated with tracking and tracing of persons, profiling of individuals, and radical changes in organisational processes.

As the development of RFID technology is still in full swing, it is difficult to say the final word about the opportunities and threats of RFID. Nevertheless, sides seem to have already formed before all stakeholders are truly informed. In order to further the debate, the European Commission sees its role as providing a balanced overview of the state-of-play and the possible actions needed. The European Commission organised an extensive public consultation process, which will result in a Communication to the Council and the European Parliament concerning RFID at the end of 2006.

As a first step in this consultation, the European Commission organised five workshops with experts and stakeholders from all over Europe. On 6 and 7 March 2006, the European Commission hosted a technology-oriented workshop that provided an overview of the technological state of RFID development. The workshop on *RFID application domains and emerging trends*, held on 15 and 16 May, focused on the economic and societal rationale for different RFID applications; it also set the stage for three subsequent 'horizontal' workshops: one on *RFID security, data protection and privacy, health and safety issues* (that was held on 16-17 May), one on *RFID interoperability, standardisation, governance and Intellectual Property Rights* (1 June), and one on *frequency spectrum requirements of RFID* (2 June).

The workshops on 15, 16 and 17 May featured 57 distinguished speakers and attracted a large attendance of 243 participants. Also, remote access to the conference with web-streaming of the presentation was available: on Monday 15 and Tuesday 16 May, nearly 500 server requests have been received. On Wednesday, 211 successful server requests have been received.

The more focused workshops on 1 and 2 June featured 35 distinguished speakers from a wide range of organisations and attracted, on average, 75 participants. Again, web-streaming services were provided and offered the opportunity for

remote interaction with panellists: on Thursday 1 and Friday 2 June, nearly 750 server requests have been received.

This document represents the outcome of these sessions. It is available on [‘Your Voice in Europe’](#) website, and is open for comments until mid-September.

This consultation asks you, the stakeholders, to provide input to the question: *What are the main opportunities and challenges for the implementation of RFID, and what role should the European Commission play in ensuring that the adoption of RFID technologies takes place in the best possible way to contribute to a more competitive and social Europe?*

In order to contribute to answering this question we invite you to respond to the questions posed on the ‘Your voice’ website of the European Commission, which touch upon the main issues raised during the workshops. Your answers will be presented and discussed during a final conference in October 2006.

The European Commission has planned its Communication to the Council and the European Parliament for December 2006.

## RFID application domains and emerging trends

*RFID fits within a wide range of wireless technologies that allow for the “Internet of Things”, but in itself it also harbours different solutions that differ with regard to reading range and frequency used. Specific applications determine what kind of data will be needed, at what range the tags should be scanned, how the data will be protected and whether there are any concerns like privacy, interoperability and spectrum interference.*

RFID is not limited to one specific application, nor is it defined by one specific technology. Although this may seem obvious, the failure to understand that there are different uses will blur any discussion concerning the deployment of RFID. **RFID technology is a tool, an enabler of functionalities; it is not a goal in itself.** In discussing RFID, there should be a distinction in functionality, field or sector of deployment, and the main user of the technology (business, consumer, government). For some sectors, low-tech solutions would possibly suffice (e.g., 2-dimensional (2D) barcodes on pharmaceutical goods).

Each application of RFID can be analysed regarding their level of “sensitivity” (sensitivity is determined by: (1) how big would the damage be in case of mistakes or abuse in the use of RFID data for the specific application; and (2) how easy is it for things to go wrong through abuse or system failures for the specific application). This is a starting point for an analysis of the need for specific policy action, based on a number of distinguishing factors. The European Commission may **engage in an analysis of vulnerabilities** of different applications, functionalities and fields. From a policy point of view, the main distinguishing factors that would determine the level of “sensitivity” are:

- **Closed versus open (networked) systems:** is RFID used within a confined environment or closed user group; does it stop at a locally un-networked PC? Or is it linked to a public network? Can and will an RFID tag be switched off after a certain step in the value chain?
- **Identifying a person versus identifying a good or service:** does the RFID signal the presence of an identifiable person? This can imply a tag fitted to a person or a person’s belongings (carried outside the confinement of the person’s home), but may also include the traceability of cars and other vehicles.

Thus a matrix emerges, in which one corner represents the less sensitive uses of closed-network identifiable goods, versus open-network identifiable people. Generally speaking, a closed system that does not use RFID tags linkable to a

single person may raise concerns. On the other hand, a system in which item-level tagging reaches the consumer, may require more attention. There is strong evidence that RFID-enabled processes can lead to time saving, efficiency, and support personalisation: advantages that can pass on to consumers. Following the logic of the workshop, a brief overview of advantages and issues for different application areas is given below:

- For **supply-chain management**, RFID has the potential to link the physical world closer to the digital world, which could greatly improve transparency, enhance control of supplies, reduce inefficient ordering, and avoid out-of-stocks situations and phantom inventory. Furthermore, it can be used in preventing losses through theft and counterfeiting luxury goods or pharmaceuticals. RFID's benefits can be reaped to their fullest when all organisations in the supply chain can use the same technology end-to-end, but also implementation along (closed) parts of the supply chain have shown to be successful. At the same time, the more open systems are the more issues of interoperability and non-harmonised frequency bands come into play. From an economic point of view, a fully digital supply chain could become feasible in the next decade if the cost of tagging would drop even further. Yet, one speaker made the statement that it may be difficult to show the added value of implementing RFID as many operations are already optimised and investments may outweigh benefits. However, other presenters made the observation that continued emphasis by large market players could provide a more compelling reason to support the technology and trigger mass adoption. Also, the question whether box- or item-level tagging would lead to privacy issues (identification) at the consumer side should be resolved; however, any solution should be balanced with the fact that consumers can also derive value from using RFID.
- In **transport**, RFID will enable dynamic monitoring and self-organised micro-devices. RFID allows automated scans at different points, allowing for continuous data collection, which leads to: 1) better information on the origins, location, and destination of goods, as well as 2) speed in handling. Also, RFID tags can be re-written and allow for decentralised storage of the most pertinent data on the item tagged. The technology can be introduced for purposes such as quality monitoring (sensing the temperature of perishable goods), asset management, fleet management, and tracking and tracing of containers (e.g., sealing containers with an RFID seal and in the future 'smart containers' that can co-ordinate their own transport). On roads, RFID can help identify cars (an electronic number plate), reduce car theft, enhance road

safety and automate the collection of road tax. Public transport is another area where RFID-enabled smart cards could allow for easy intermodal transfer and cashless payment. However, speakers mentioned that a precondition for a pervasive deployment of RFID is that chips become cheaper, which may be achieved by research in materials and printing techniques. Also in this field of application, standards and interoperability can be problematic, as multiple (public) transport providers need to cooperate and adhere to the same standards – it becomes even more difficult when international parties are involved. When looking for solutions in this field, it is crucial to involve all relevant stakeholders; e.g., in international trade, Customs Departments are an important player, as many of the delays at the border occur when the right information on the shipments is not available. The interception of counterfeit goods also often takes place at Customs.

- For **government** use, RFID would offer applications to the benefit of both government and citizens, including combating forgery of official documents (passports, declarations and banknotes) and enhanced services for citizens. One of the promising prospects of deploying RFID in the public sector (in a “closed” setting) is workflow optimisation (easier retrieval of official documents) and the collection of statistical information to increase the processes’ transparency. Deploying RFID in more open settings could make some jobs, such as the tracking of stolen goods by the police and customs control, easier and more reliable. In addition, RFID can be instrumental in monitoring and controlling administrative processes. Clearly an active role by governments is required in this field: the European Commission could stimulate national governments to act as a launching customer, also involving small- and medium-sized enterprises (SMEs) in their procurement efforts. Privacy-enhancing technologies (PETs) are mentioned as an important element in this application area to ensure privacy that is inherently connected to official (personal) documents.
- In **healthcare**, the use of RFID technology to enhance patient safety and assisted living should be further explored. One speaker made the remark that three times more patients die due to avoidable mistakes than in car accidents every year in Europe. So far, only rudimentary applications have been tested, since testing integrated applications is difficult. Performing pilots to assess the effectiveness and feasibility of RFID in hospitals could be perceived as an important option to reduce the number of avoidable mistakes. Potential areas of success are: tracking and tracing of patients; patient prescription compliance and reducing medication errors; reducing medical errors by

linking electronic patient dossiers to tags; retrieving surgical equipment; and blood (quality) tracking. Although the complexities of introducing RFID in the hospital setting itself are already large, involving extramural health carers increases complexity. It should be noted that RFID is not always perceived as the best solution: in the supply chain for pharmaceuticals, the 2-dimensional (2D) data matrix<sup>1</sup> seemed to be considered at the moment a more cost effective solution with less deployment barriers and a similar level of enhanced safety. Yet, as speakers highlighted, this solution also requires prior harmonisation of labelling standards throughout Europe. The ERP (enterprise resource planning) systems that are put in place to handle 2D matrix information could at a later stage be adapted to handle RFID as well.

- The use of RFID in modern **mobile life** (e.g., coupling a payment function to mobile phones and other personal assistive devices) is already common practice in Japan. Tracking mobile assets and people (e.g., automatically transferring your phone to the office or meeting room you are in, monitoring visitors, monitoring the location of documents, etc.) applications are no longer science fiction. RFID may be used to retrieve product details of tagged goods or street posters. Combining RFID, mobile and location technologies make many more innovative services feasible, such as tourist information on demand, location based promotional offers, and guidance of poor-sighted citizens. Connecting tags to people should be used only for those applications where the persons affected agree that the perceived advantages of using RFID tags outweigh the perceived disadvantages.

### *Policy challenges raised at the workshop*

In the workshop, developers and early adopters of RFID warned against regulation that may hamper further uptake, as many of these applications are still in the early stages of development. Many speakers argued that at this stage of RFID development, **self-regulatory programmes and guidance** should be encouraged. It was suggested that the European Commission should **monitor the deployment and range of uses of RFID**. The positions expressed can be summarised as follows:

#### *Regarding consumers*

One thing seems clear: when RFID reaches consumers, **consumers want the right to choose**. They want to know how RFID may affect their convenience and

---

<sup>1</sup> Essentially, a 2D matrix is like a barcode, but made out of dots on a grid – thus more information can be stored.

security but also privacy. For instance, consumers want to know whether RFID tags on certain goods will still be readable after they are handed over (e.g., at cash register). When a consumer leaves a store, tags could be either deactivated or in privacy mode; it was suggested that more solutions should be developed that leave the consumer in control (e.g., reducing the range of tags by breaking the antenna, or portals that allow the customer to switch off the RFID functions). Apart from this area of research and development, also other system parameters (reading distances, encryption, shielding) need to be investigated.

Consumer representatives stated that much unease stems from the fact that RFID tags are small and that the process of accessing the tags cannot be physically checked. In order to increase transparency, the technology should be explained, and made understandable to consumers. Workshop participants suggested to make use of pictograms, and not to focus on details. **Information would have to be easy, understandable, and targeted to the needs of consumers.**

Self-regulation and guidelines may be needed to implement and clarify the existing framework for privacy and security. Whether further legislative steps (i.e. beyond currently existing legislation) are necessary, would be a matter of further experience with RFID use and debate with stakeholders on their needs and concerns. The role of the European Commission should be explored. For instance, the European Commission could be instrumental in proposing guidelines for informing consumers.

#### *Regarding governments*

If RFID is to develop beyond its current use, a more active approach to building interoperable systems could be useful. The European Commission and the European Union (EU) Member States could support such an approach. As an example, the Australian government's recent announcement of a 1.1bn A\$ smart card plan to replace 17 applications is mentioned. Such examples would show that **Government can act as a stimulator and support the emergence of new applications**, while not discriminating in favour of specific technology solutions.

Participants indicated that the European Commission could usefully support further development in specific fields through the instruments available to the European Commission. Taking into consideration the focal points of the i2010 initiative (single European information space, innovation and investment in ICT, inclusive European Information Society), the first two could be addressed broadly, but specific solutions may be found in the area of inclusion (e.g.,

support for visually impaired) and in the area of quality of life/healthcare (e.g., medical error reduction, assisted living).

According to some, when connected to identity management, RFID technology should be closely linked to and may work as a catalyst of a **European electronic identity policy**, which is considered one of the enablers of the recent eGovernment Action Plan.

#### *Regarding SMEs and businesses*

According to participants, one of the instruments governments can deploy is the stimulation of **awareness** on opportunities and challenges related to RFID deployment, and **knowledge transfer**. Without a focal point for exchanging plans and experiences, chances are that the wheel will be reinvented in several Member States and that the different solutions developed would not be interoperable. Knowledge sharing could take place in a multi-stakeholder platform or partnership. The Dutch *RFID Platform* and the German *Informationsforum RFID*, as well as the German Chambers of Commerce, are possible examples of such arrangements: emergence of such platforms on trans-national level could be useful.

This would not diminish the joint responsibility of retailer and manufacturer to correctly inform audience about the presence of tags. It would be important that the public is well informed: just putting a label (that nobody recognises) on a product would not do. There would be a need for a uniform label indicating RFID presence.

#### *In summary*

RFID can lead to efficiency savings and other added value services in a range of application areas. There are also concerns, such as privacy, health, interoperability and standards. However, these cannot be generally addressed for RFID technology as a whole; they should be focused specifically at the application in which RFID technologies are used. A matrix in which open/networked systems versus closed systems are set out against personal identification versus goods identification may be a way of distinguishing 'sensitive' RFID uses from less sensitive ones.

Many of the participants in the workshop suggest that, as it is still early days of the wider deployment of RFID, the European Commission should take a regulatory light approach in which self-regulation, together with guidance where

appropriate, could be a possible way forward. Monitoring the development of RFID technology is important to recognise both challenges and opportunities in this early phase, and to act with specific policy measures when necessary. One thing seems clear from the workshop: consumers demand the right to know, and the right to choose. Clear and comprehensive information on products is important in this regard, as well as development of solutions that allow the consumer to be in control of the RFID.

Governments may consider playing a catalyst role as a leading buyer of RFID services. Knowledge transfer could be supported in order to have industry and SMEs benefit from new opportunities and recognise challenges that arise across the European Union.

## RFID security, data protection and privacy, health and safety issues

*Whereas RFID tagging could allow many advantages related to production, tracking and tracing of people, animals and products, it cannot be at the expense of health, security, or the fundamental rights to privacy and data protection.*

*It seems currently socially unacceptable that citizens would be tracked and traced wherever they go, all the time. If citizens buy and carry products, this could allow indirect tracking and tracing. Clear information, accurate data, protection against abusive access and use of data are a legitimate requirement. Thus it needs to be clear what happens with data that are transferred via RFID from a tag to a reader. How do we know for sure that the data reading is correct, that the data are not hampered with, that someone who is not entitled to read the data does not read it? A data protection framework is already in place in order to protect our privacy. Next to that it is important to understand which RFID technologies may, and which will not affect physical health and safety.*

Whereas a wide range of issues has been presented during this workshop, the discussion predominantly focused on privacy concerns and can be summarised as follows.

The debate about privacy and data protection is complex, also since the concept of privacy is not necessarily understood universally in the same way. Concepts are bound by cultural and temporal differences, and affected by trade-offs that occur over time. Although some people would not want to share personal data at request, others are willing to use loyalty cards that register their purchases at their name in return for some discounts or “air miles”. Notwithstanding shifting values, one should still regard technology developments in the light of existing value frameworks.

The trend towards ubiquitous computing and technology convergence leads to seamless integration of the physical world with cyberspace. Automatic participation in an “always on” Internet is not easy to reconcile with existing requirements, such as EU law, or the OECD privacy principles: What is the specific purpose of a given use of technology? What are the limitations to data collection? Is there transparency and control? This could all lead to loss of confidence and trust.

In such an environment, institutional privacy invaders are not the only issue: as both private and public environments become smart, there is a risk of a loss of accountability from all sides. At the same time privacy and data protection concerns are mainly foreseen when there is **item level tagging at the consumer side**; implementing RFID in a production environment (a closed system) raises fewer concerns.

Moreover, RFID is merely an input technology: a large part of the privacy and data protection issues arise at the application level and in particular at the back-end of it, where databases are amassing and analysing personal data.

Currently, the [Data Protection Directive](#) (1995/46/EC) and the [Privacy and Electronic Communications Directive](#) (2002/58/EC) address data protection, privacy and to a certain extent, security.

One of the important questions raised at the workshop is, *what data carried on RFID tags can be defined as "personal data"* (this is being researched by the Article 29 Working Party of Directive 1995/46/EC). As a person can be linked to a RFID serial number (e.g., through the tag in his/her clothes), the distinction between personal data and non-personal data could be blurred. Some speakers were concerned about the consequences following from the application of the aforementioned Directives to systems that use RFID. Participants suggested that the European Commission should clarify through guidance or indeed **review regulations that are in place today**.

Participants also indicated that the general principles included in existing legislation are general enough to cope with developments such as RFID. Regulation is only valid for a specific timeframe; due to advances in technology regulation can become obsolete and therefore one should be careful with too early or too detailed legislation. At the current early state of development of RFID, many speakers therefore suggested that **guidelines** and **self-regulatory codes of conduct are needed** to implement existing privacy framework and work out practical details. These guidelines would also involve consumers. However, participants were afraid of the **lack of enforcement options** and who should control appropriate use of RFID technology. There may be a role for a **consumer ombudsman**<sup>2</sup>.

---

<sup>2</sup> An ombudsman is an official, usually (but not always) appointed by the government or by parliament, who is charged with representing the interests of the public by investigating and addressing complaints reported by individual citizens.

Also, the notion of the “**privacy impact assessment**” (PIA), or privacy threat analysis was introduced by some participants. Some even asked that such an analysis be mandated at EU level. As many operators and users of data-processing systems are not aware of the threats and possible abuses that concern personal data, such a PIA could provide an overview of threats and possible mitigation measures. In Canada, there is reportedly positive experience with privacy impact assessments. Such an approach could also be considered in Europe, although care should be taken that such instruments are also available to SMEs, and not too costly or unduly burdensome. Some even indicated in this context the possible involvement of the European Network Information Security Agency (ENISA).

According to several participants, notwithstanding the organisational and legal safeguards that can be put into place, an important role should be given to the consumers themselves<sup>3</sup>. Research suggests that users do not have sufficient knowledge of privacy-invading possibilities – they believe that technology is generally benign. A **major information campaign** to inform citizens and SMEs about the full potential (positive and negative) of RFID was strongly voiced.

Citizens are said to want the **right to choose**, but to do so, they would require a balanced overview of the advantages and disadvantages of the technology so as to be able to make informed decisions. This right to choose would require transparency from the side of the RFID systems operators about what data is captured at what point in time and at what place, and for what purpose. Such transparency would be important to develop trust and cooperation. According to various participants, RFID should be deployed in such a way that the **consumer is in control** and can either choose to take advantage of the benefits of RFID usage or value the costs higher and prefer to avoid RFID functionality. At the same time, choices should be easy for consumers to exercise: information concerning RFID should be clear, conspicuous and accurate.

Privacy-enhancing technologies (PETs) could provide solutions to some of the issues that may arise in the realm of privacy. Several stakeholders emphasise that privacy can and should be part of the design of the RFID system. Furthermore, it was suggested to **build privacy into the design of an application-specific**

---

<sup>3</sup> For example, several consumer privacy and civil liberty organisations have issued a [position paper](#) in November 2003 stating their opposition to item level consumer product tagging at least until appropriate solutions are developed and agreed upon regarding the protection of consumers against the potential risks of RFID technology. One of the organisations endorsing this position paper, the UK [Notags](#) participated in one of the workshops organised by the European Commission in May 2006.

**context (both technology and service)**, as for some applications this enhanced range would not be a problem. Some even pleaded for a mandatory usage of PETs.

### *Security and Identification*

Although security and reliability are important from the RFID users' (businesses) point of view, the issues in this area were hardly mentioned in the discussions. At this point in time, 100% accurate RFID reading cannot be guaranteed within the operational process of a firm and back-end systems such as databases are always under security threat. More research and development is still required for certain applications. This may not be directly the realm of governmental intervention, but it should be emphasized that RFID is still a set of technologies that are under development.

Furthermore, the fact that RFID is only an enabler may force the European Commission to go beyond the technology *per se* and **focus on digital identity and identification**. Looking at the discussions throughout the workshops, many of the issues hinge around the question whether RFID enables identification of a specific person (or animal, or service, although these uses are less contended) and the collection of data. A valid question is if Europe has not a more specific need for security enhancing standards compatible with the cultural importance given to privacy.

### *Health*

At present, [Council Recommendation](#) 1999-519-EC concerning the limitation of exposure of the general public to electromagnetic fields (EMF) and [Directive](#) 2004-40-EC of the European Parliament and of the Council regarding minimum health and safety requirements for workers together with national regulations are part of the framework to protect human beings against the established adverse health effects that may result as a consequence of exposure to electromagnetic fields. Despite the fact that such health effects have not been demonstrated at this point in time as far as consumer products are concerned (by the numerous studies performed), the "principle of precaution" should continue to prevail in all circumstances and studies and testing must go on. The relatively low power of RFIDs compared to other typical wireless applications (mobile communications, broadcasting, radars, etc.) would imply that the risk profile of RFIDs is probably lower than for most wireless communications products. If RFIDs have specific characteristics (i.e. distinctively different from other wireless

applications), this would require to address their potential health effects in any dedicated manner.

Another issue is the impact of RFID on biological pharmaceuticals, and RFID-tagged samples of living tissue. Currently, the effect of RFID-tagged blood bags on the quality of blood is being researched. However, it is under discussion whether the proper scientific approach is used and the outcomes are not yet available. One could also question the impact of RFID on pharmaceuticals. However, in the latter case the question arises whether a public body should pay for such research.

An original presumption was that non-ionising radiation does not affect tissue. However, the research in this field is still at an early stage. It is important that the necessary research is scheduled and takes place, and that there is clear **communication on the current state-of-the-art knowledge** with regard to the topic to prevent that deployment of RFID and other wireless technologies are not hindered by false information.

#### *Environment and labour practices*

During the workshop the environmental impact of a much wider implementation of RFIDs was mentioned as a major concern. Currently, **little is known about waste generated by RFID tags**.

Furthermore, the workshop addressed the issue of the use of RFID in the workplace<sup>4</sup>. The European Commission said it could not tolerate that data collected by the employer are used in any other ways than formally made known beforehand to the employee. Any misuse of this data would constitute a practice against the current EU laws.

#### *Technology aspects*

One of the objectives of European policy is to make Europe a global leader in crucial technological areas. Europe managed to reach that position in the rollout of cellular telephony. Also in RFID use Europe has taken a front-line position. However, at this point in time leadership in technology development has shifted to other countries. In order to not fall further behind, participants called on the

---

<sup>4</sup> The [UNI-Europa](#) European trade union federation informed the European Commission in May 2006 that it was preparing a UNI Code of Good Practice for RFID in the workplace. Last year, the UK trade union [GMB](#) called on the European Commission to ban the use of RFID and GPS satellite linked wearable computers to tag and track workers in the workplace.

European Commission and the EU Member States to **support technology research and development**.

Although the developments in RFID technology are progressing, there are still issues that need to be further researched regarding hardware reliability, manufacturing, systems integration, sensor network integration, air-interface, and communication protocols.

The vision of an “Internet of Things” is compelling, but many of the foreseen uses are **not expected in the near future (according to some participants not in the next 10 years)**. Therefore, in the Community’s Seventh research Framework Programme (FP7) specific RFID applications could be targeted. For example, implementing RFID (in vehicles moving at higher speed) requires tradeoffs between speed and range, but also speed and reliability, and size, range and power needed. RFID applied at long range will make tags difficult to localise, especially if several items are in the same zone. Also in supply chain management speed versus accuracy is an issue that has not been resolved.

One of the workshop discussion points was that not all RFID issues should be linked to privacy. However, privacy-enhancing technologies, data synchronisation, data harmonisation, data encoding and security were flagged as important areas of research.

Furthermore, some of the participants contend that the **RFID technology can and should be improved to encompass privacy requirements**. Much advantage could be gained from co-ordination of research at a European level and this is certainly seen as an excellent role for the European Commission.

#### *In summary*

Privacy and data protection concerns arise when RFID tags relate to people. Not only when people use RFID tags for identification and access to services, but also when products with RFID tags are transferred to consumers. According to participants, this use can raise serious privacy concerns, but for other applications the issue seems less relevant.

Participants asked that current legislation be examined to see how specific threats to privacy and data protection from RFID applications are addressed while not unduly hindering RFID deployment. Guidelines and self-regulatory codes of conduct may be advisable at this stage.

Further measures may be also needed to protect consumers. There was a strong voice towards informing SMEs and citizens on specific aspects of RFID.

For the development of RFID applications it would be important to consider the privacy and data protection aspects already in the design phase and to consider using PETs. Support for collaborative research and development of RFID at European level can be useful.

## Interoperability, standardisation, governance and Intellectual Property Rights

*The interoperability of technologies allows for broader deployment of these technologies across organisational and sectoral boundaries. In order to ensure interoperability, and thus facilitate wider deployment, a certain level of standardisation is required. In the past, standards have emerged because of market forces, sometimes facilitated by government intervention, sometimes because of market domination of certain market players ... either because there is a dominant technology provider or because there are dominant technology users. As RFID is reaching new stages of maturity, the issue of standardisation and interoperability needs to be discussed, as well as the need for and the nature of intervention by the European Commission in order to be able to reach better the objectives of a more open and competitive Europe. Put more strongly: **standards cultivate the marketplace.***

Standardisation is addressed at different levels within different standardisation organisations. In deployment of new technologies a problem can arise that there may be too **many organisations that are each trying to set their own standards**. Yet, intervening in the process that leads to standardisation is tricky (if consensus in establishing standards is achieved at the wrong level, this may stifle innovation), and ideally should be left to the market. Although harmonised usage of RFID technology across Europe would lead to benefits, it is not expected of the European Commission to add another layer of standard setting to this difficult process. Moreover, several presenters highlighted that adopting existing standards to new application areas may be wiser than designing completely new ones. But this does not necessarily mean that the emergence of a new RFID standard should always be deplored.

It was seen as important that governmental bodies **investigate the landscape of existing standards** and scrutinise those standards on their compliance with European values. Furthermore, it should also be investigated whether these standards imply hidden costs – so-called “submarine” Intellectual Property Rights. Mass adoption of standards can only be achieved if they are royalty-free (or with marginal royalty costs involved). At the moment, Europe is leading on electronic signatures; it may still take such a role for RFID standards as well.

As suggested earlier in this document, one should look at the intended use, sector, and application when investigating RFID<sup>5</sup>. There are strong reasons for sector-specific standards, as technological and organisational restrictions make a one-size-fits-all solution unlikely and impractical. However, during the workshop large stakeholders in the retail sector expressed their preference for the development of one cross-sectoral standard. The question is, whether this is an either/or situation, or whether it would be more appropriate to follow a double strategy. Besides, the international component in standardisation should not be forgotten, as **international standards facilitate global trade**. To that effect, participants suggested that the European Commission should encourage Member States to liaise with the USA, Japan, Korea, and China, and to join international initiatives.

Some participants in the workshop urged, however, not to applaud initiatives that re-evaluate existing standards, but to **support an environment that is beneficial to further RFID deployment**.

#### *Alternative governance solutions*

Currently, [EPCglobal](#) is strongly supported by industry (not only in the USA, but worldwide), but their solutions are not the only ones available on the market, and there are certain criticisms towards some of the solutions emerging in this framework. The Object Naming Service (ONS), as proposed by EPCglobal, is said to strain the underlying network infrastructure when readers detecting millions of tags start making requests to a specific server. This issue was not further addressed in the workshop, but it requires more examination when applied on a large scale. Alternatives may involve decentralised solutions such as peer-to-peer networks.

In addition, the question was raised if Europe does not need a more 'open bridge' instead of the closed ONS to the Internet of Things. The open bridge, in the format of possibly a European information centre, would enable more services in the interest of European entrepreneurs and citizens. The services could become pivotal to support intermodal transport solutions and in combating counterfeiting of drugs and other goods.

---

<sup>5</sup> For the transport sector, for example, one of the main barriers in progressing RFID use in container transport is related to global standards. There are already specific standards being used in this area: ISO 18185 for electronic active seals and ISO 10374 for passive container tags. The practical use of these standards still needs to be tested in trials.

Equally, although EPCglobal has a specification for globally Unique Product Identifiers, there are competing and simplified solutions that could be more appropriate for specific purposes: a first comparison has been performed by the Helsinki University of Technology, in which their own ID@URI and the World Wide Article Information (WWAI) protocols were considered; comparisons with other solutions should be supported.

#### *RFID and the network*

RFID is a technology that can play an important enabling role in realising the vision of a network of things. Yet, for many applications there are alternative technologies that may offer the necessary solution: RFID is not unique in being able to transmit information on an object to a receiver – competing technologies may be deployed that each provides its own advantages. Highly connected devices that are small, lightweight, and mobile, allow users to communicate with other users and things via a multitude of network technologies, ranging from Bluetooth to mobile telephony, GPS and wireless networking technologies to RFID. Whereas RFID has a place in this spectrum of technologies, **a forward-looking approach should be technology neutral, flexible** and anticipate differing regulations and technological solutions to deploying these technologies in either open/public or private networks to identify a person, animal or good.

#### *In summary*

Standardisation issues arise when RFID reaches a next level of deployment, driven by the ability to benefit from interoperability. Like was said in earlier workshops, specific needs for standardisation depend on the application. So does the need for government intervention. It was felt that for many applications standardisation could be left to the market. However, it was also recognised that the European Commission could provide a useful role in facilitating the process by investigating the landscape of existing standards and specifications. In this, the role of IPR should be considered.

Furthermore, standards for RFID tags in international trade would be highly beneficial, but are subject to international collaboration. The European Commission should encourage Member States to remain in contact with countries such as the United States, Japan, South Korea, and China, and be active in standardisation initiatives within international standards organisations.

## Frequency spectrum requirements and recommendations

*The availability of radio spectrum is an essential requirement for RFID applications. Regulations concerning spectrum access have therefore a determining influence on the large-scale deployment of RFID devices. Currently the 3 MHz of spectrum earmarked in the UHF band seems adequate for the particular application of this technology in logistics and retail distribution. Industry has now to identify the longer term needs for spectrum since the institutional process of allocating new bands is traditionally one with a long cycle. The needs of various users (not only RFID users) of spectrum have to be assessed and merits compared before new spectrum could be made available.*

### *Frequency plans*

There are currently only about two-thirds of the EU Member States which have adapted their frequency plans to accommodate the UHF bands identified for RFIDs as recommended by the European Conference of Postal and Telecommunications Administrations (CEPT) update of [Recommendation 70-03](#) on Short Range Devices (in October 2004). Although Member States which have not yet done so have promised to adapt their national frequency plans in the near future, the European Commission has deemed appropriate to accompany the process and to provide Europe-wide legal certainty to investors by the adoption of a specific regulatory measure (technical implementation decision).

Some participants in the workshops complained that a lot of effort was made on product development for specific European frequency bands, whereas it would be wise to **harmonise at global scale**. If spectrum allocation were harmonised, the cost of development and the time to deployment would be reduced. Yet it is recognised that globally disparate frequency allocations are a fact which cannot be modified, and that full global harmonisation can probably not be achieved, at least in the foreseeable future.

RFID deployment is still in its infancy. The short term response to immediate needs should be complemented by a **longer term review of needs, costs and benefits through the existing mechanisms** and management structures.

### *Spectrum in the future*

The fragmented spectrum legacy in Europe is a reality that prohibits radical changes to reallocate spectrum. As other types of Short Range Devices are also

dependent on the UHF band, it is difficult to allocate dedicated bandwidth in this band to a single technology like RFID. Therefore, a broader view balancing technical efficiency, allocational efficiency, and incentives to further research is needed. Since in the future more applications may be deployed that require dedicated spectrum with minimal limitations, there is a need for a long-range plan. Such a plan should contain the expected needs in combination with expected technological developments for the next 10 to 15 years. A system reference document (by ETSI) could be part of this process.

Such a study should be an **Integrated Assessment** weighing different market requirements in the future and determining frequency opportunities. Differing needs arise from various RFID applications (such as the amount of spectrum, spectrum parameters, and global interoperability). There is a need for a roadmap of spectrum needs and spectrum availability – with milestones and priorities – so that a trade-off can be made between sophisticated (sharing) and easy (dedicated) spectrum usage conditions as well as between other applicants for spectrum.

Although the current standards were recently introduced, the technology has further developed. We also see that although current focus is on UHF RFID technology, other RFID technologies are still being researched and should be considered as viable complements and/or alternatives. The optimal deployment of specific RFID tags depends, once again, on the application. New opportunities may be found in different frequency ranges or could be the result of technological solutions. Therefore, research and development activities are called for.

#### *Research and development*

Technological solutions to overcome spectrum related challenges may include: 1) the use of narrow beam antennas and electromagnetic absorbent material; 2) the use of two interrogators at the same portal that operate on different frequencies; or 3) the use of tags that respond at a higher data rate. However, solutions with narrow beams and shielded portals increase system complexity and reduce flexibility. In surroundings where 100 readers are requested to operate simultaneously, Dense Reader Mode (DRM) may be an option.

#### *In summary*

Frequency use is an issue that can be addressed with new technology solutions and/or with new spectrum allocation. As spectrum re-allocation is a difficult

subject in national and international discussions, the pressure on technology solutions is high and in many cases sufficient today, but in particular with an eye on the future deployment of many more applications that make use of RFID it is important to consider future needs and potential solutions early on.

## From RFID to the Internet of Things

*Although the workshop of 6 and 7 March 2006 was the first in the series, it is mentioned here last, as research is the next step towards the “Internet of Things”. This network of billions of machines communicating with one another is a major theme for the evolution of information and communications over the next few decades. This development is not only the result of a technology push; technology push in this field is mirrored by market pull, with short-term objectives and tangible application prospects.*

From a generic point of view, it can be concluded that the trend towards an ever larger population of integrated smart systems is irreversible because the economic value of a system of objects and devices is directly related to the fact that they are “networked”<sup>6</sup>. From the technological perspective, the Internet of Things will enable computing to melt invisibly into the fabric of our business, personal and social environments, supporting our economic, health, community and private lives.

The potential applications of pervasive networking are wide-ranging. To make this technology worthwhile, there is a need to address large classes of potential applications in order to better understand the various requirements (e.g., real time, quality of service) that will eventually drive the needed generic technology developments. However, application drive alone will not deliver the wide variety of solutions that have to be brought together. The list of research that needs to be undertaken is a long one that ranges across industrial sectors, beyond the classical telecommunication technology providers.

Within the competitive business conditions that prevail today, industry and other players have contributed to an endemic climate of “hype”. Economic prospects related to networking of large number of simple devices like RFID are huge. Still, the economic prospects related to more sophisticated computing devices such as sensors need further research with industrial players.

The Internet of Things is not a revolutionary concept. It fits well with the evolution of today’s networking technologies (Internet, wireless, service platforms, etc.). Even if evolutionary, a great deal of genuinely creative, innovative research is required to realise the Internet of Things. It is not simply a matter of re-engineering existing technology. Billions of connected devices are pushing current communication technologies, networks and services approaches

---

<sup>6</sup> As we know from *Metcalf’s law*, the value of the network is proportional to the square of the number of nodes.

to their limits and require new technological investigations. These cannot happen quickly and need to be tackled within a long-term perspective.

### *Research*

In particular, research is required in the field of Internet architecture evolution, wireless system access architectures, protocols, device technologies, service-oriented architecture able to support dynamically changing environments, security and privacy. Research is required in the field of dedicated applications integrating these technologies within a complete end-to-end system.

It is important that researchers, when pursuing less constrained “blue sky” topics, should remain aware of industrial and real-world problems. Industry and academic institutions should be encouraged to keep close contact, especially where the academic research might not attract internal funding within an industrial organisation.

### *Research on devices*

Although many examples of RFID deployment are already given, the technology is by no means at the end of its development. Costs are an important aspect: the drive for wider application depends on much lower costs. RFID costs are in the region of €0.50 for retail product tags and supply chain tracking applications, but rise dramatically beyond €25 for the more sophisticated devices used, for example, in highway toll collection. Printed circuitry is a possible approach, and a major driver in practice will be manufacturing scale and volume.

The feasibility of many applications depends on powering and power economy. Devices must have long lifetimes without the need to change batteries, yet there are many challenges in this area.

Sensor technology itself needs to evolve; in many cases, miniaturised sensors require further Research and Development (R&D). In addition, sensors have to be fitted with communication capability and also with service features to cover the most extensive use cases. These issues are clearly in the R&D domain, as the impact of these communication and service features on the devices are expected to have non-negligible cost impact.

### *Research on the network*

On the side of the network, also a whole range of research challenges can be identified: existing data communication protocols may be inappropriate in the

Internet of Things, as they rely on the transfer of relatively much metadata. Lighter protocols and lighter implementations that reduce (compress) the explicit protocol layers into a single communications module are now required.

The Internet of Things requires self-organising and self-scaling networking to arrive at mobility, economy and flexibility as well as network resilience. Self-organising networks must cope with varying requirements for physical and virtual link topologies. Service discovery and reuse by different applications has very high priority.

Furthermore, the Internet of Things must have a naming and addressing strategy by which objects can identify themselves, and can locate other objects and the communication paths to them. Because the network is heterogeneous, supporting many different devices offering different service types, a declarative interface, like Internet Description Language (IDL) or Extensible Markup Language (XML), will be needed. This will allow a device or node to describe what it presents to others.

A consistent set of middleware offering application programming interfaces, communications and other services to applications will simplify the creation of services and applications. Service approaches need to move from a “static” programmable approach towards a configurable and dynamic composition capability.

The Internet of Things must incorporate traffic and congestion management. This will sense and manage information flows, detect overflow conditions and implement resource reservation for time-critical and life-critical data flows.

### *Regulation*

The Internet of Things is a pervasive federated network in which unregulated personal area networks and local area networks will interoperate with more traditionally regulated electronic communications services. Regulators need to carefully monitor the challenges posed by these networks, taking action as necessary to regulate for technical interoperability, consumer protection, support for competition and the appearance of opportunities for the exploitation of market power. Here, traditional infrastructure regulatory frameworks should be reviewed.

A foreseen area where there is risk of monopoly market power is that of the ownership of the data resources in name servers. These are the resources that

networks must use to determine the way to reach a given person, device or resource. The implications in terms of Object Name Server (ONS) management should be evaluated. Existing regulatory issues that have been and are being tackled in existing networks, for example access, roaming and billing, may raise their heads in different guises. Also the manner of allocation and regulation of radio spectrum is a key issue for the development of the Internet of Things. Spectrum scarcity will remain an issue and flexible approaches to spectrum management have to be researched, especially for devices that will primarily be deployed in unlicensed bands.

*In summary*

RFID can enable the realisation of an Internet of Things. However promising many existing applications are, a lot of research is still needed before the long-term perspective can take hold. In the section above, some of the most pertinent issues are addressed, but this listing is based on workshop outcomes; a roadmap for RFID research would be needed. “Blue sky” research will be essential, though it needs to be strongly backed with industrial perspectives: companies are invited to share their problem issues with the academic world. Finally, also the regulatory and spectrum consequences of RFID are a topic for research, as was also proposed in the other workshops.

## Your voice counts

Over the last months, the European Commission provided an open platform for different stakeholders in the workshops held on 5-6 March, 15-17 May and 1-2 June. The presentations and findings were collected and presented in a very condensed form in this paper. You will find more information on the consultation workshops' [website](#) - not only the introductory papers, agendas and presentations given by the participants, but also a range of reports and position papers written by RFID stakeholders from the private or the public sector.

**Please let your voice be heard on “[Your Voice in Europe](#)” .**

Your answers will be presented and discussed during a final conference in October 2006. All the outcomes of the workshops, the discussion papers and the inputs by stakeholders will provide input to a Communication to the European Parliament and Council that the European Commission has planned for December 2006.

