

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, xxx
COM(2007)96 final

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

**Radio Frequency Identification (RFID) in Europe:
steps towards a policy framework**

{SEC(2007) 312}

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

**Radio Frequency Identification (RFID) in Europe:
steps towards a policy framework**

Table of contents

1.	Introduction	3
2.	Why RFID Matters	3
2.1.	The social contribution of RFID	3
2.2.	Industrial innovation and growth potential	4
3.	The need for legal certainty for both users and investors	4
3.1.	Public consultation	5
3.2.	Data protection, privacy and security	5
3.3.	Governance of resources in the future "Internet of Things"	7
3.4.	Radio spectrum	7
3.5.	Standards	8
3.6.	Environmental and health issues	8
4.	Actions at European Level	9
4.1.	RFID security and privacy	9
4.2.	Radio spectrum	10
4.3.	Research and innovation policy	10
4.4.	Standardisation	11
4.5.	Further actions on RFID technological and governance issues	11
5.	Conclusion	12

1. INTRODUCTION

Radio frequency identification (RFID) is a technology that allows automatic identification and data capture by using radio frequencies. The salient features of this technology are that they permit the attachment of a unique identifier and other information – using a micro-chip – to any object, animal or even a person, and to read this information through a wireless device. RFIDs are not just "electronic tags" or "electronic barcodes". When linked to databases and communications networks, such as the Internet, this technology provides a very powerful way of delivering new services and applications, in potentially any environment.

RFIDs are indeed seen as the gateway to a new phase of development of the Information Society, often referred to as the "internet of things" in which the internet does not only link computers and communications terminals, but potentially any of our daily surrounding objects – be they clothes, consumer goods, etc. It is this prospect that provoked the European Council of December 2006 to ask the European Commission to review the challenges of the next generation of Internet and networks at the 2008 Spring Council¹.

RFID is of policy concern because of its potential to become a new motor of growth and jobs, and thus a powerful contributor to the Lisbon Strategy, if the barriers to innovation can be overcome. The production price of RFID tags is now approaching a level that permits wide commercial and public sector deployment. With wider use, it becomes essential that the implementation of RFID takes place under a legal framework that affords citizens effective safeguards for fundamental values, health, data protection and privacy.

It is for these reasons that the Commission carried out a public consultation on RFID in 2006, which highlighted the expectations of the technology based on the results of early adopters but also the concerns of citizens about RFID applications that involve identification and/or tracking of persons.

The present Communication is based on the results of this consultation and proposes follow-up steps to overcome barriers to wide take-up to benefit society and the economy while incorporating appropriate privacy, health and environmental safeguards.

2. WHY RFID MATTERS

2.1. The social contribution of RFID

RFID has the potential to benefit Europeans in many ways: safety (e.g., food traceability, healthcare, anti-counterfeiting of drugs); convenience (e.g., shorter queues in supermarkets, more accurate and reliable handling of luggage at airports, automated payment); and accessibility (e.g., patients suffering from dementia and Alzheimer's disease). It is already used in different sectors with an impact on the lives of Europeans. In transport, RFID is expected to contribute to improved efficiency and security, and provide new quality services

¹ Point 30 of Presidency's Conclusions of the European Council, 14-15 December 2006.

for mobility of people and goods². In healthcare, RFID has the potential to increase the quality of care and patient safety, and to improve medication compliance and logistics. In retail, RFID could help to reduce supply shortages, inventory levels, and theft. In many industries, including pharmaceuticals, medical devices, entertainment, consumer electronics, luxury goods, car parts, or retail, where counterfeiting is a significant source of products of unacceptable quality, the use of RFID may allow products to be recalled more efficiently and to prevent illicit goods from entering the supply chain or spot where these actually entered it. RFID tagging is expected to improve sorting and recycling of product parts and materials. This may result in a better protection of the environment and an improvement in sustainable development.

2.2. Industrial innovation and growth potential

Further development and widespread RFID deployment could further strengthen the role of information and communication technologies (ICT) in driving innovation and promoting economic growth.

Already today, Europe is a leading region in RFID-related research and development, not least thanks to the support of the European research programmes. Main research areas concern innovative applications, smart sensors and RFID-enabled actuators, as well as intelligent networks. Substantial effort is also spent on nanoelectronics, which supplies the intelligence, memory, sensing, and Radio Frequency capability to RFID tags.

On the industrial side, several large European enterprises, including technology companies and service providers, are at the forefront of bringing RFID solutions to the market and many small- and medium-sized enterprises (SMEs) have successfully introduced this technology. However, although the market for RFID systems in the EU is growing at about 45 % a year, it lags behind the almost 60 % growth in the global market³. Such a "growth gap" will hold back the contribution of the Information Society to growth and jobs.

3. THE NEED FOR LEGAL CERTAINTY FOR BOTH USERS AND INVESTORS

RFID is technologically and commercially ready, but several factors are holding back its take-up. Not least, a clear and predictable legal and policy framework is needed to make this new technology acceptable to users. This framework should address: ethical implications, the need to protect privacy and security; governance of the RFID identity databases; availability of radio spectrum; the establishment of harmonised international standards; and concerns over the health and environmental implications. As RFID technology is inherently transborder, this framework should ensure consistency within the Internal Market.

² COM(2006) 314 final "Keep Europe moving – Sustainable mobility for our continent" (http://ec.europa.eu/transport/transport_policy_review/doc/com_2006_0314_transport_policy_review_en.pdf).

³ Source: "RFID chips: Future technology on everyone's lips", Deutsche Bank Research, February 20, 2006.

3.1. Public consultation

To meet these challenges the Commission launched a wide public consultation, which involved five thematic expert workshops and an online consultation that was open from July until September 2006 – to which 2190 participants contributed. The consultation phase was closed in October with an open seminar that presented the preliminary results of the consultation.

3.2. Data protection, privacy and security

In the public debate on RFID, there are serious concerns that this pervasive and enabling technology might endanger privacy: RFID technology may be used to collect information that is directly or indirectly linked to an identifiable or identified person and is therefore deemed to be personal data; RFID tags may store personal data such as on passports or medical records; RFID technology could be used to track/trace people's movements or to profile people's behaviour (e.g., in public places or at the workplace). Indeed, the Commission's public consultation underlined the concern of citizens about the potential of RFID to be an intrusive technology. Adequate privacy safeguards are called for as a condition for wide public acceptance of RFID. Respondents to the online consultation expect these safeguards to emerge from privacy enhancing technologies (70%) and awareness raising (67%); specific legislation on RFID was seen as the best solution by 55%. In addition, views are evenly balanced on whether societal applications are really positive, with about 40% of responses on each side. Stakeholders have raised concerns about potential infringements of fundamental values, privacy and greater surveillance, especially in the workplace resulting in discrimination, exclusion victimisation and possible job loss.

It is clear that the application of RFID must be socially and politically acceptable, ethically admissible and legally allowable. RFID will only be able to deliver its numerous economic and societal benefits if effective guarantees are in place on data protection, privacy and the associated ethical dimensions that lie at the heart of the debate on the public acceptance of RFID⁴.

The protection of personal data is an important principle in the EU. Article 6 of the Treaty on the European Union states that the Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms; Article 30 requires appropriate provisions on the protection of personal data for the collection, storage, processing, analysis and exchange of information in the field of police co-operation⁵. The protection of personal data is set as one of the freedoms in Article 8 of the Charter of Fundamental Rights.

The Community legislation framework on data protection and privacy in Europe was designed to be robust in the face of innovation. The protection of personal data is covered by

⁴ The ethical implications of data protection have been addressed in several Opinions of the European Group on Ethics in Science and New Technologies (EGE). See in particular the Opinion of the EGE on the ethical aspects of ICT implants in the human body http://ec.europa.eu/european_group_ethics/docs/avis20_en.pdf.

⁵ The Commission has submitted a proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM(2005) 0475 final) to the Council.

the general Data Protection Directive⁶ regardless of the means and procedures used for data processing. The Directive is applicable to all technologies, including RFID. It defines the principles of data protection and requires that a data controller implements these principles and ensure the security of the processing of personal data⁷. The general Data Protection Directive is complemented by the ePrivacy Directive⁸ which applies these principles to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. Due to this limitation, many RFID applications fall only under the general Data Protection Directive and are not directly covered by the ePrivacy Directive.

Pursuant to these Directives, public authorities in Member States are charged with the monitoring whether the provisions adopted by Member States are correctly applied. They will have to ensure that the introduction of RFID applications complies with privacy and data protection legislation. It may therefore be necessary to provide detailed guidance on practical implementation of new technologies, such as RFID. For these purposes both directives foresee the drawing up of specific codes of conduct. This process implies a review of these codes at national level by the competent data protection authority, and a review at European level through the "Article 29 Working Party"⁹.

Concerning security, a joint effort of industry, Member States and the Commission shall be made to deepen the understanding of the systemic issues and related security threats potentially associated with the massive deployment of RFID technologies and systems.

An important aspect of the response to the above challenges will be the specification and adoption of design criteria that avoid risks to privacy and security, not only at the technological but also at the organisational and business process levels. In this respect, ensuring security, by protecting against major disruptions of RFID-enabled business processes, would also improve privacy protection. In addition, good practices shall be developed to address new security threats and related countermeasures to support the widespread deployment of RFID systems.

However, RFID information systems, and related security and privacy risks are a moving target and hence require continuous monitoring, assessment, guidance, regulation, and R&D. The specific security and privacy risks largely depend on the nature of the RFID applications: a one-size-fits-all approach would not be able to address the full range of possible applications. Therefore, a close examination of the cost and benefits of specific security and privacy-related risks prior to the selection of RFID systems and the deployment of RFID applications is needed.

⁶ Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31.

⁷ Art. 17, Directive 95/46/EC.

⁸ Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

⁹ The Article 29 Working Party has adopted a "Working paper 105 on data protection issues related to the RFID technology" (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf).

Given that nearly two-thirds of the responses to the online questionnaire indicated that, thus far, the information available is insufficient to allow the public to come to an informed judgement on the balance of risks of RFID, it would appear that awareness and information campaigns need to be an essential part of the policy response.

3.3. Governance of resources in the future "Internet of Things"

The policy issues raised by RFID are generally seen as including standards, Intellectual Property Rights and associated licensing regimes, but there are also concerns about the openness and neutrality of the databases that will register the unique identifiers that lie at the heart of the RFID system, the storage and handling of the collected data, including its use by third parties. This is an important issue in view of the RFID's role as the carrier of a new wave of development of the Internet which will eventually interconnect billions of smart devices and sophisticated sensor technologies into a global networked communication infrastructure.

In the responses to the online questionnaire, 86% of respondents were concerned that the system for registering and naming of identities in the future "Internet of Things" should be interoperable, open and non-discriminatory. It should guard against breakdown or unintended use that could cause havoc. It should not fall into the hands of particular interests that could use these databases and naming systems for their own ends, whether they relate to commercial, security or political aspects of governance. In addition, security, ethics and privacy requirements should be safeguarded for all stakeholders from individuals to companies, whose sensitive commercial information is contained in the RFID-enabled business processes. Governance definitions and public policy principles developed in the context of the World Summit on the Information Society (WSIS)¹⁰ will be relevant to emerging policy debate on these issues.

3.4. Radio spectrum

Like all wireless devices, the availability of radio spectrum is essential for RFID applications. In particular, harmonisation of spectrum usage conditions is important to allow easy mobility and low costs. Currently, several frequency bands are available for RFID systems on an unlicensed basis¹¹, and have been so for many years in most EU Countries. Recently, to liberate more spectrum for the growing demand for RFID usage, the Commission has adopted a Decision¹² for RFID frequencies in the UHF band. This will establish a harmonised European base for RFID applications in the European single market. In the consultation most respondents (72%) found this allocation to be adequate on a time horizon of between three to ten years. However, there is a need to monitor demand as the use of RFID increases.

¹⁰ Towards a Global Partnership in the information Society: Follow-up to the Tunis Phase of the World Summit on the Information Society (WSIS) - COM(2006) 181 final.

¹¹ 'General Authorisation', according to Article 5(1) of the Authorisation Directive (2002/20/EC).

¹² Commission Decision 2006/804/EC of 23 November 2006 on harmonisation of the radio spectrum for radio frequency identification (RFID) devices operating in the ultra high frequency (UHF) band.

3.5. Standards

The rapid pace of RFID developments requires continual modification, and adaptation of technologies, products and services. Standards and their development process must keep pace with this fast-emerging market globally. Therefore, the streamlined adoption of international standards¹³ and the harmonisation of regional standards are essential for smooth take-up of services, as is interoperability in RFID-enabled information systems, not least to encourage an open Europe-wide e-services market. In the consultation, an active stance by the Commission was seen as important to ensure the development of a European approach to RFID standards.

3.6. Environmental and health issues

In the consultation concerns were raised about the environmental and health impacts of the widespread use of RFIDs.

Regarding the environment, RFID meet the definition of electrical and electronic equipment provided for in the Directives 2002/96/EC on waste electrical and electronic equipment (WEEE) and 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS). RFID can be considered to fall under Category 3 "IT and telecommunication equipment". Therefore, RFID components are covered by RoHS, which means that the use of the hazardous substances Cd, Hg, Pb, CrVI, polybrominated biphenyls (PBB) or polybrominated diphenyl ethers (PBDE) is restricted.

On health, the Commission has long been monitoring the possible human health effects of electromagnetic fields (EMF) with the support of its Scientific Committees¹⁴ and a legal framework for the protection of workers and citizens is in place. This framework recommends limits to the exposure to EMF of the general public (Council Recommendation 1999/519/EC¹⁵, currently under review) and imposes strict rules for the exposure of workers (Directive 2004/40/EC¹⁶). Moreover, restrictions on EMF emissions from products on the EU market have been established to ensure the safety of both users and non-users (Directive 1999/5/EC¹⁷). Electromagnetic fields related to RFID applications are generally low in power. In such cases, and under normal operating conditions, exposure of the general public and workers to RFID-related EMF is expected to be well below the current standard limits. However, RFID take up is expected to happen alongside a generalised increase in wireless applications (Mobile TV, Digital TV, Wireless broadband, etc). The Commission will therefore continue to monitor the respect of the legal framework at EU and/or Member State

¹³ In particular the ISO (International Organisation for Standardisation) RFID tag standard for item identification (ISO 18000) and the ISO regulation in preparation for active transponder.

¹⁴ http://ec.europa.eu/health/ph_risk/committees/committees_en.htm

¹⁵ <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999H0519:EN:HTML>

¹⁶ [http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004L0040R\(01\):EN:HTML](http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004L0040R(01):EN:HTML)

¹⁷ http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/l_091/l_09119990407en00100028.pdf

level, and to actively support research and review of scientific evidence, especially in relation to the cumulative effects of exposure to EMF from different sources¹⁸.

4. ACTIONS AT EUROPEAN LEVEL

Realising the potential of RFID technology requires addressing a number of interrelated issues pertaining to security and privacy, governance, radio spectrum and standards.

Over the next two years, the Commission will continue to analyse the options to respond to the concerns and to address the issues at stake, taking into account the discussions with the relevant stakeholders. In some areas, such as radio spectrum, research and innovation, and standardisation, the Commission will pursue on-going initiatives in co-operation and dialogue with relevant stakeholders. In other areas, in particular security, privacy, and the other policy issues posed by the shift from RFID to the "Internet of Things", while it is possible to map out some concrete steps from now to the end of 2007, further more detailed debate between concerned stakeholders is necessary to deepen the analysis of follow-up actions.

In this respect, the Commission will establish as soon as possible and for two years a RFID Stakeholder Group with a balanced representation of stakeholders. This group will provide an open platform allowing a dialogue between consumer organisations, market actors, and national and European authorities, including data protection authorities, to fully understand and take co-ordinated action on the concerns that have been raised in relation to the issues mentioned above. It will also support the Commission in its efforts to promote awareness campaigns at Member State and citizen level about the opportunities and challenges of RFID.

The Commission will also strengthen its international contacts with third country administrations, particularly in the United States and Asia, with the objective to strive for global interoperability on the basis of open, fair and transparent international standards.

4.1. RFID security and privacy

Privacy and security should be built into the RFID information systems before their widespread deployment ("security and privacy-by-design"), rather than having to deal with it afterwards. The requirements of both the parties actively involved in setting up the RFID information system (for example business organisations, public administrations, hospitals) and the end users that are subjected to the system (citizens, consumers, patients, employees) must be considered during the design of this system. As end users typically are not involved at the technology design stage, the Commission will support the development of a set of application-specific guidelines (code of conduct, good practices) by a core group of experts representing all parties. To this end, all security related activities and initiatives will be conducted in line with the strategy for a Secure Information Society set out in COM(2006) 251.

¹⁸ Such review will be carried out with the support of the Commission's Scientific Committees, in particular SCENIHR (http://ec.europa.eu/health/ph_risk/committees/04_scenihr/docs/scenihr_o_006.pdf).

By the end of 2007, the Commission will issue a Recommendation to set out the principles that public authorities and other stakeholders should apply in respect of RFID usage. The Commission will in addition also consider including appropriate provisions in the forthcoming proposal for the amendment of the ePrivacy Directive and will, in parallel, take into account input from the forthcoming RFID Stakeholder Group, the Article 29 Data Protection Working Party¹⁹ and other relevant initiatives such as the European Group on Ethics in Science and New Technologies. On this basis the Commission will assess the need for further legislative steps to safeguard data protection and privacy.

4.2. Radio spectrum

The results of the public consultation show that a majority of the respondents believe the Commission Decision for RFID frequencies is sufficient to provide a favourable environment for the initial deployment of RFID systems operating in the UHF Band.

Nevertheless, further long term requirements for additional spectrum are currently being studied by industry. If the need for additional spectrum should arise, the Commission may use its competences under the Radio Spectrum Decision²⁰ to identify additional harmonised spectrum for RFIDs throughout the Community.

4.3. Research and innovation policy

RFID technology is still an area of active research and development. Cost reductions of passive tags to less than 1 cent, needed for mass application, require two complementary avenues of research: further miniaturisation of silicon chips through innovations in design and assembly; research on non-silicon organic materials that hold the promise to produce printable RFID tags. More research is also needed on security (authentication, encryption) and larger rewritable memories. Future applications will need larger memories, more complex cryptographic engines, active networking capabilities, integrated sensors and power management techniques²¹.

The 2007-08 work programme of the ICT theme of the 7th Framework Programme (2007-2013) has identified four challenges which mention RFID in a number of situations (healthcare, intelligent vehicle and mobility systems, micro and nanosystems, organic electronics, and future networks) as well as the eMobility²² Platform. In the future, the Commission will stimulate research on security of RFID systems, including light-weight security protocols and advanced key distribution mechanisms, with a view to preventing direct attacks on the tag, the reader and the tag-reader communication. In response to the

¹⁹ The Article 29 Working Party has established a subgroup on RFID to analyse the concept of 'personal data' and how far RFIDs are covered by the Data Protection Directive. If deemed necessary, the Working Party can make proposals on which kind of legal amendments to the directive are required or which other measures could help to close data protection gaps.

²⁰ Decision 676/2002/EC on a regulatory framework for radio spectrum policy in the European Community.

²¹ This, complemented by more accurate location functionality offered by terrestrial, satellite and hybrid location technologies, could provide Europe a valuable opportunity to develop applications leading to state-of-the-art products and services.

²² eMobility European Technology Platform. www.emobility.eu.org

results of the European consultation, the Commission will also support further development of privacy-enhancing technologies as one means to mitigate privacy risks.

Since the dynamics of RFID deployment in the various application domains differ significantly and experiences are still scarce, awareness of the expected benefits and possible risks is low, and barriers to a given application domain are high. In Europe, most countries have only limited experience with the implementation of RFID. To improve this situation, there is a need to carry out in-depth overall evaluations of RFID implementation through large-scale pilots in specific application domains, taking into account technical, organisational, societal and legal issues, as a prerequisite for widespread take-up and adoption of this technology.

4.4. Standardisation

At European level, the relevant group of the European Committee for Standardisation (CEN) supports the development of international standards for automatic identification and data capture technologies, and has been a key player in the work of the relevant working group of the International Organisation for Standardization. The European Telecommunications Standards Institute (ETSI) has developed specific standards for RFID operating at UHF frequencies as well as generic short range devices (SRD) standards for LF, HF and microwave equipment which can be used for RFID.

The Commission calls upon the European standardisation bodies, in co-operation with relevant industry forums and consortia, to ensure that international and European standards meet European requirements (in particular as regards privacy, security, IPR, and licensing issues), to identify standardisation gaps and to provide the appropriate framework for the development of future RFID standards. In this respect, it is crucial that standard-setting initiatives establish rules which ensure fair and transparent procedures as well as early disclosure of relevant intellectual property.

The activities on standardisation will be complemented with an international dialogue between the Commission and counterparts in the US, China, Korea and Japan, with a view to ascertain the need for, and desirability of, co-operation on standards for certain application sectors (e.g., security of containers, counterfeiting, air transport, pharmaceutical goods).

4.5. Further actions on RFID technological and governance issues

The RFID Stakeholder Group will be invited to build visions and develop position papers that define user guidelines for RFID applications taking into account longer-term issues as well as economic and societal aspects of RFID technologies.

The Commission will continue to closely monitor the move towards the "Internet of Things", of which RFID is expected to be an important element. At the end of 2008, the Commission will publish a Communication analysing the nature and the effects of these developments, with particular attention to the issues of privacy, trust and governance. It will assess policy options, including whether it is necessary to propose further legislative steps to both safeguard data protection and privacy and address other public policy objectives.

5. CONCLUSION

The Commission calls upon the European Parliament and the Council, to actively endorse the programme of initial steps outlined in this Communication.