EUROPEAN COMMISSION
ENTERPRISE AND INDUSTRY DIRECTORATE-GENERAL

Innovation policy
ICT for Competitiveness and Innovation

Brussels, 8 December 2008
DG ENTR/D4

M 436 – EN

STANDARDISATION MANDATE
TO THE EUROPEAN STANDARDISATION ORGANISATIONS CEN, CENELEC AND ETSI IN THE FIELD OF INFORMATION AND COMMUNICATION TECHNOLOGIES APPLIED TO RADIO FREQUENCY IDENTIFICATION (RFID) AND SYSTEMS

1. RATIONALE

1.1 Introduction

Radio frequency identification (RFID) is a technology that uses radio waves to do automatic identification and data capture.. The salient features of this technology are that they permit the attachment of an 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 food, clothes, consumer goods, etc.

In order to respond to the challenges created by the extensive implementation of RFID, the Commission published, on 15 March 2007, the Communication COM(2007) 96. This proposes follow-up steps that overcome barriers to wide take-up of RFID which will benefit society and the economy while incorporating appropriate privacy, health and environmental safeguards.

As envisaged in this Communication, the Commission is planning to issue a Recommendation on the implementation of privacy, data protection and information security principles in applications supported by radio-frequency identification technologies. Draft text of this Recommendation was submitted to a public online

consultation which ran until the April 25th, 2008. The Recommendation should be published in early 2009.

1.2 The policy environment

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 including a lack of interoperability to innovation can be overcome. The production price of RFID tags is now approaching a level that permits wide private 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, environment, data protection, privacy and security.

The "OECD Policy Guidance on Radio Frequency Identification" was published on the occasion of the OECD Ministerial Meeting on the Future of the Internet Economy that took place in Seoul on 17-18 June 2008[1]. This report contains policy and practical guidance principles to enhance business and consumer benefits from the use of RFID while proactively taking into account information security and privacy issues. It is supported by a report on economic aspects of RFID that reviews major fields of applications, economic impacts and country initiatives, as well as a report that analyses information security and privacy challenges and possible measures and safeguards to address them.

1.3 The legal environment

RFID is technologically and commercially ready, but several factors are impeding 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; concerns over the health and environmental implications. As RFID technology is inherently cross-border, this framework should ensure consistency within the Internal Market.

A public consultation launched by the Commission in mid-2006 showed that 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). Adequate privacy safeguards are called for as a condition for wide public acceptance of RFID. Stakeholders 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.

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

---

[1] The report is published at http://www.oecd.org/dataoecd/19/42/40892347.pdf .

societal benefits if effective mechanisms 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 RFID[2].

1.3.1. Privacy and data protection

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-operation[3]. It is also set as one of the freedoms in Article 8 of the Charter of Fundamental Rights.

The protection of personal data is covered by the general Data Protection Directive[4] regardless of the means and procedures used for data processing. The Directive is applicable to all technologies and for all who operate a system in Europe, including RFID. It defines the principles of data protection and requires that a data controller implements these principles and ensures the security of the processing of personal data[5]. The general Data Protection Directive is complemented by the ePrivacy Directive[6] 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. However, RFID readers and writers and passive and active tags are included in the scope of the Directive 1999/5/EC (the "R&TTE Directive"), in particular in its Article 3[7]. According to this Directive, privacy requirements can include mechanisms to control data read processes, to provide disablement or kill functionalities and a notification of the reading process.

---

[2] 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).

[3] 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.

[4] 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.

[5] Art. 17, Directive 95/46/EC.

[6] 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.

[7] Directive 1999/5/EC on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Pursuant to these Directives, public authorities in Member States are charged with monitoring whether the provisions adopted by Member States are correctly applied. The 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"[8].

At a more aggregate and fundamental level, and related to the issue of data protection, is the recent Communication COM(2007) 228 on Privacy Enhancing Technologies (PETs), which aims at promoting the development of PETs, supporting the use of available PETs by data controllers, and encouraging consumers to use PETs.

The European Data Protection Supervisor expressed an official opinion on 23 April 2008 that there is a need for privacy-by-design in case of RFID. It was recommended to make use of the existing mechanism of Article 3(3)c of Directive 1999/5/EC, in consultation with the RFID Experts Group.

1.3.2. Information security

Many organisations have a tendency to look at RFID security in the rear view mirror, i.e. rushing to find a solution to a security problem after it has happened. Such behaviour can no longer be contemplated as emerging security threats, combined with the increased use of and dependence on RFID, leave organisations in both the private and the public sectors with an obligation to plan, design and implement clear strategies.

Security risks can be structured according to the traditional dimensions of information security – **availability** (i.e. assurance of timely and reliable access to data services for authorised users), **integrity** (i.e. assurance that data has not been altered during transmission, from the point of origin to reception), and **confidentiality** (i.e. assurance that information is accessible only to those who are authorised to have access). Attacks can concern the tag (falsification of contents or tag identity, deactivation, detaching the tag from the tagged item) via radio-communications outside of control of the user (or the person carrying the tagged object), the reader (falsification of identity), and the air interface (eavesdropping, blocking, jamming). The purposes of such attacks include spying, deception, Denial of Service, or privacy violations. It is indeed essential to note that many security risks become privacy risks when information related to identified or identifiable individuals is involved.

Most security threats to, and vulnerabilities of, RFID systems are common to all information systems. There is one component in RFID systems, which distinguishes them from others, namely the transmission of information between tags and readers. In reply to this specificity, typical security mechanisms which are in the scope of the R&TTE Directive could be mutual authentication between tag and reader/writer, encryption procedures and check of data integrity. Beyond tags and readers, other components of RFID systems may present security risks, in particular databases, such as the global distributed database of tag identifiers known as the Object Naming Service (ONS) designed by EPCglobal, containing information associated to tags, which is transmitted over the Internet.

---

[8]   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).

To combat the new threats and vulnerabilities to RFID systems and to cater to the evolving demands of their end-users, ICT professionals should convince their organisations to treat security as a core business function that should anticipate user demand, predict future risks and design solutions to potential security events. 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 technical level (e.g. password authentication, digital signatures, encryption of data, electromagnetic shielding, temporary deactivation of tags, kill feature, tamper resistance) but also at the management level (e.g. RFID usage policy, security policies, agreements with external organisations, data stored on tags minimised) and the operational process level (e.g. physical access control, appropriate placement of tags and readers, secure disposal of tags, information signs, separation of duties). In this respect, ensuring security, by protecting against major disruptions of RFID-enabled business processes, would also improve privacy protection. In addition, good practices will 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 measures against risks prior to the selection of RFID systems and the deployment of RFID applications is needed.

1.4 The standardisation environment

At European level, TC 225 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 CEN Workshop on Data Protection and Privacy (WS/DPP) is the interface with the Article 29 Working Party, and is currently addressing in its work programme a work item concerning the "Voluntary Technology Dialogue System".

TC ERM of 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. In addition, ETSI has recently created a new work item for the development of RFID security and privacy by design specifications for the protection of RFID users and RFID operators.

ISO published several standards addressing RFID, e.g. ISO 18000 "RFID for Item Management: Air Interface".

Attention will also be paid to the European norms, developed under CENELEC TC 106X, covering the exposure of populations and workers to magnetic fields; examples of these standards are EN 50357 and EN 50364.

2. SCOPE AND DESCRIPTION OF THE MANDATE

The Mandate addresses data protection, privacy and information security aspects of RFID. It complements the existing legal framework but does not substitute it. The Mandate shall be executed in two phases.

1) Phase 1.

The objective of the first phase is to prepare a complete framework for the development of future RFID standards. This framework will include a detailed standardisation work programme in response to the identified gaps. The standards will refer to all elements of the RFID value chain, from the tags themselves – power levels, reading distances, encryption tradeoffs, to the architectures, infrastructures and services relevant for the networking of tags – security frameworks, object naming, tracking, addressing, data processing etc. Appropriate use of intermediate results from relevant EU-funded projects (including GRIFS, CASAGRAS) shall be made. Intersections with other standards should be avoided.

Particular attention would need to be given to the likely technological evolutions to be expected in this domain especially in the perspective of the future Internet of Things, and the requirements (including openness and interoperability) to cope with environments where networked tags (i.e. a network of uniquely identified tangible and intangible items capable of interacting with organisations and the relevant stakeholders) offer significant functional capabilities beyond what is state-of-art today.

Furthermore, the work programme should fulfil the following requirements:

- Draw up an inventory of all the actors involved, and of their work and deliverables, and assess to which extent this state-of-the-art addresses the issues raised.

- Reflect the technical requirements, the required levels of privacy, security, data protection and interoperability as defined by the policy context described in section 1.2 to ensure the deployment of RFID applications with the appropriate technical features ("privacy-by-design").

- Identify standards ensuring that privacy and security requirements, especially safeguards for the physical system components as well as the policies that guide the implementation of a RFID system, can be incorporated into the system from the very outset of the design process ("privacy and security by design"). RFID systems should be designed with consistent, robust interfaces allowing individuals to learn to trust them and distinguish them from fraudulent ones.

- Elaborate the concept of user control over deactivation and re-activation of RFID tags at point of sale by developing a standard which can transfer control to the consumer and liability to the developer of the tag.

- Identify standards that can complement the requirements set by the Recommendation on RFID applications[9] and the Communication on Privacy Enhancing Technologies [COM(2007) 228], especially as regards the development of good practice frameworks to be established at Community level to support privacy impact assessments.

- Assess the requirements to apply different levels of security to different data objects in high capacity and/or functionality tags It will be necessary to group the variety of RFID applications in different security levels to ensure their adequate treatment according to the risks involved and avoidance of over-specifying requirements for many applications.

- Identify a classification of applications in different security and risk levels to ensure that risks are handled but over specification avoided.

- Identify to which extent different sectoral applications have a need for specific RFID standards.

- Assess the developments on various standards and procedures for object identification in the world and their implications for Europe, taking into full account the broad range of identification schemes.

- Assess, and follow-up as appropriate, the opportunity to develop standards implementing Article 3.3 of Directive 1999/5/EC, subject to the adoption of a Commission Decision on additional essential requirements over R&TTE.

- Identify the needs and the requirements for cooperation to reach global interoperable solutions where appropriate.

- Define clear objectives, task assignments and timetables for the delivery of the required standards (e.g. EN, ES, TS, CWA) or guidelines.

- Assessment of the important interoperability needs in a broader Internet of Things perspective covering sensor and geographic location data standards.

- Assess if a standard on the recycling characteristics of a RFID tag is needed and feasible.

The resulting standardisation work programme will be submitted to the Commission services which will consult the Committee 98/34. At the completion of the first phase a reporting to member states will be done.

2) Phase 2.

The objective for the second phase is to implement the standardisation work programme agreed upon in the first phase. The execution of the specific standardisation tasks shall be carried out in close co-operation with all relevant stakeholders.

---

[9] Planned for the autumn of 2008.

European standardisation bodies are invited to ensure that European standards meet European legislative and other requirements (in particular as regards privacy, security, IPR).

CEN, CENELEC and ETSI are also invited to develop sector specific RFID implementation guidelines, as complementary documents of general nature. The guidelines are intended to assist the user in the choice of appropriate technology for particular applications, and should provide technical advice on how to implement RFID systems in a functional, secure and economic way in a given sector.

3. EXECUTION OF THE MANDATE

3.1. Modus operandi and co-ordination aspects

CEN, CENELEC and ETSI are invited to establish adequate and efficient co-operation mechanisms in view of achieving the widest possible consensus amongst all parties concerned. In addition, arrangements shall be made to establish relevant international co-operation. In this respect, the following principles shall be followed:

- Close co-operation with relevant industry fora and consortia as well as open consultation of the relevant consumer organisations and civil society groups shall be established, as appropriate.

- International co-operation shall be ensured, in particular with IEC, ISO, ITU, as appropriate.

- The development efforts should in the first instance be targeted at the international level.

- Results of relevant EU research projects and national guidelines for RFID application shall be taken into account.

- Particular attention shall be given to the involvement of national organisations and authorities concerned with the implementation of the Directive 95/46/EC and Directive 2002/58/EC, including the European Data Protection Supervisor and the Article 29 Working Party.

3.2. Arrangements for the execution of the mandate

Within two months of the date of acceptance of this Mandate by all of them, CEN, CENELEC and ETSI shall present a joint report to the Commission setting out the arrangements they have made for the execution of this mandate. Particular attention shall be given to the involvement of all relevant parties and to the working arrangements with relevant industry fora and consortia.

3.3. Work programme

Within six months of the date of acceptance of this mandate, CEN, CENELEC and ETSI shall complete Phase 1 of the work and shall present the proposed work programme (with the definition of the objectives, target dates, and performance criteria). Subject to the

acceptance of the proposed work programme by the Commission, CEN, CENELEC and ETSI are invited to execute Phase 2 of the work.

3.4. Standstill

With acceptance by CEN, CENELEC and ETSI of the Mandate the appropriate standstill period in accordance with Article 7.1 of the Directive 98/34/EC as amended will start only if the work item(s) to be created result in ENs.

3.5. Progress reports

Adequate monitoring mechanisms for the work will be put in place as soon as possible. CEN, CENELEC and ETSI shall present annual progress reports to the Commission services.

3.6. Evaluation

Two years after the commencement of the work in Phase 2, an evaluation report shall be presented by CEN, CENELEC and ETSI to the Commission on the results achieved in terms of market impact. The terms of reference of the report shall be agreed between the three European standardisation bodies and the Commission services.

3.7. Results

CEN, CENELEC and ETSI will present the standards listed in the programme in accordance with the Mandate to the Commission services.